2017 TAG CYBER SECURITY ANNUAL
VOLUME 1

Practical Handbook and Reference Guide for the Working Cyber Security Professional

Expert Advisory Research

Dr. Edward G. Amoroso
Chief Executive Officer, The Amoroso Group (TAG Cyber)

Version 1.0 – September 2016

Designer – Vision Creative
Finance – M&T Bank
Administration – navitend
Promotion – Braithwaite Communications
Research – TAG Cyber LLC
Lead Author – Dr. Edward G. Amoroso

TAG Cyber LLC
P.O. Box 260, Sparta, New Jersey 07871

Security experts and practitioners must recognize that best practices, technologies, and information about the cyber security industry and its participants will always be changing. Such experts and practitioners must therefore rely on their experience, expertise, and knowledge with respect to interpretation and application of the opinions, information, advice, and recommendations contained and described herein.

Neither the author of this document nor TAG Cyber LLC assume any liability for any injury and/or damage to persons or organizations as a matter of products liability, negligence or otherwise, or from any use or operation of any products, vendors, methods, instructions, recommendations, or ideas contained in any aspect of the 2017 TAG Cyber Security Annual volumes. The opinions, information, advice, and recommendations expressed in this publication are not representations of fact, and are subject to change without notice. TAG Cyber LLC reserves the right to change its policies or explanations of its policies at any time without notice.

September 1, 2016

To the Reader:

I wrote every word of this *2017 TAG Cyber Security Annual* based on my experience, opinion, and research – and I wrote it for one purpose: To serve as a useful guide for Chief Information Security Officer (CISO) teams. My desire was to make all three volumes of the *2017 TAG Cyber Security Annual* free to practitioners, and any other persons or groups who might find the content useful. To that end, roughly fifty cyber security vendors served as sponsors, agreeing to distribute this Annual with no pre-arranged agreements about the nature of the analysis included. They kindly offered their advice, expertise, and knowledge in the development of this report – and to that end, they are referenced here as *distinguished vendors*. Without their assistance, this report would not exist.

As with any researcher, I must admit to my biases. With the publication of this report, I am only several months removed from three decades of proud service to the customers and people of AT&T. During that time, I poured my heart and soul into the development and operation of the vast assortment of cyber security services that the company continues to market. To that end, it is impossible for me to remain unbiased in my conviction that these services are world class, and that the underlying promise of AT&T's software defined network, led by John Donovan, to support on-demand virtualized cyber security will prove to be exactly the right technical and infrastructure approach to stopping advanced malicious actors.

Furthermore, I have served proudly over the years on a variety of informal advisory boards for cyber security vendors, such as Koolspan, over the past decade. I also serve as an independent director on M&T Bank's Board of Directors, as a Senior Advisor to the Applied Physics Lab at Johns Hopkins University, and as an Adjunct Professor in the Computer Science Departments at the Stevens Institute of Technology and New York University. While none of these affiliations should introduce any untoward bias, all inevitably have some bearing on the advisory material included here. Discussions with students and faculty at Stevens and NYU, in particular, have had considerable influence on my opinions regarding cyber security technology.

You will notice that the research presented here differs significantly from the advisory work of firms such as Gartner and Forrester. Where such firms rank vendors based on in-depth feature analysis, my approach is to try to educate readers in the fundamentals. The emphasis is therefore on broad themes that are likely to remain constant, rather than detailed feature-by-feature comparisons that can change in an instant. Also, the decision to avoid rankings is made in the observation that all vendors provide some value to their customers – or they would not be in business. And the familiar process of "asking around" to see what "customers are saying" is both unscientific and misleading – not to mention fraught with the conflicts that arise when advisory firms sell consulting services to the same vendors they are ranking.

One major caveat regarding this *2017 TAG Cyber Security Annual* is that the reader must expect a plethora of errors and inaccuracies, especially in Volume 3, where facts about company names, product offerings, and executive positions change so quickly that it is impossible to keep up. But this should not detract from the usefulness of the report. Readers should use the volumes as an Alpha Guide to their own understanding, and should take the initiative to augment this guide with their own research, which hopefully will be shorter and easier based on the material provided here.

I hope that this guide is useful to you. Expect updates – and a completely revised edition next year.

Dr. Edward G. Amoroso, Chief Executive Officer, TAG Cyber LLC

Purpose and Overview of
2017 TAG Cyber Security Annual

The purpose of this *2017 TAG Cyber Security Annual* is to assist the women and men who are tasked with protecting their organizations from the potentially damaging effects of cyber attacks. Throughout the report, these dedicated cyber defenders are referred to as members of Chief Information Security Officer (CISO) teams. The report provides CISO team members with detailed technical and architectural guidance based on *fifty specific controls* that support the reduction of cyber risk.

Offering cyber security guidance based on a control methodology is hardly a new idea. Literally dozens of cyber security frameworks are available to working professionals. What is unconventional here, however, is an underlying security framework that uniquely embraces cloud, virtualization, and mobility as *solutions* rather than problems. It is a cyber framework that seeks to support proactive avoidance, rather than just passive acceptance, of malicious attacks.

The underlying architectural framework of this report consists of a three-step infrastructure improvement process that every CISO team should embrace: In Step 1, they must *explode* their perimeter-based infrastructure into smaller, distributed micro-segments. In Step 2, they must *offload* these segments onto virtualized, cloud-based systems with advanced security protections. And in Step 3, they must *reload* their cyber security technology with superior technologies from the myriad of expert commercial vendors available.

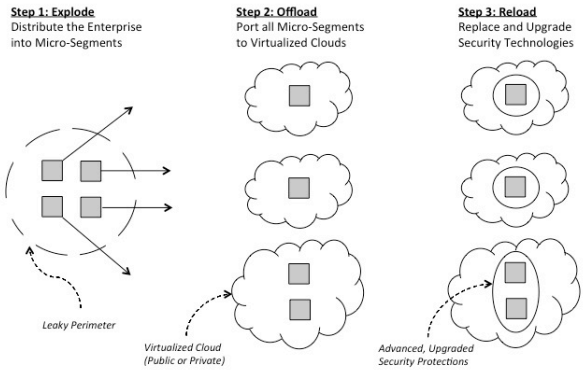

Figure 1. Three-Step Methodology for Enterprise Security Teams

It is argued throughout this report that these three steps – *exploding, offloading, and reloading* – are absolutely required to stop the advanced cyber attacks being aimed at commercial and government systems. The case is made in these pages that these three steps cannot be ignored by CISO teams if they wish to regain control of their infrastructure from malicious intruders and re-establish dependability and trust in the computing and networking systems that support our world. The argument is

made repeatedly here that the consequences of following the familiar perimeter-dependent path are simply unthinkable.

The report does, however, recognize the practical and budgetary realities of the modern enterprise, and that no CISO team can simply wave a magic wand and move their applications and systems to some micro-segmented cloud with advanced machine-learning analytics. To that end, the report includes specific guidance on the most likely existing types of systems and infrastructure that will exist in companies and agencies – including, for example, mainframe systems. This approach is taken so that readers can translate the underlying three-step process and associated framework into a feasible plan.

This *2017 TAG Cyber Security Annual* is organized around a comprehensive set of resources, technical information, and guidance designed to assist the CISO team with the recommended distribution, virtualization, and improvement tasks. It does so in the context of *fifty specific cyber security controls* that must be present in the CISO team's arsenal as they upgrade their infrastructure. Some of these controls are familiar, such as firewall platforms and anti-malware tools. But others might be new including security analytics, network monitoring, and deception. All of the controls, however, are relevant and essential to the success of the modern CISO team.

One final point on purpose and overview: This report is *not* written for C-suite managers or board-level executives, and it is *not* written to raise awareness amongst industry observers or politicians with casual technical backgrounds. It is written instead for the hard core, working CISO team member professional. The report targets those individuals and groups with the requisite experience, expertise, and ability to make decisions and to take positive steps to improve our global cyber security infrastructure.

So if you don't know the difference between an IP packet and a USPS envelope, or if you don't know the difference between a virtual and physical machine, or if you have no idea why signature-based processing makes variant writing so easy – then please toss this book aside. It's not for you.

Introduction to the
2017 TAG Cyber Security Annual

To be successful at protecting infrastructure from cyber attacks, modern Chief Information Security Officer (CISO) teams must attend properly to the following four focus areas in their organizational cyber protection scheme:

1. *Compliance* – Frameworks such as PCI DSS, NIST SP 800-53, and ISO 27000, serve as the underlying basis for regulatory and audit controls.
2. *Technology* – Thousands of global cyber security technology vendors offer a plethora of product and service options for different security environments.
3. *Architecture* – Evolving from the traditional perimeter, new security architectures must now focus on virtualization, mobility, and cloud.
4. *Innovation* – Clever innovative strategies and techniques to protect assets are becoming more commonly found in defensive controls.

The traditional security metaphor that emerges in this context involves the use of a *fence* to prevent attacks. Where any one of the four focus areas might have been sufficient in the past as the basis for *fence height*, the emergence of nation-state actors has raised the bar literally, on what is needed to stop the most advanced cyber attacks.

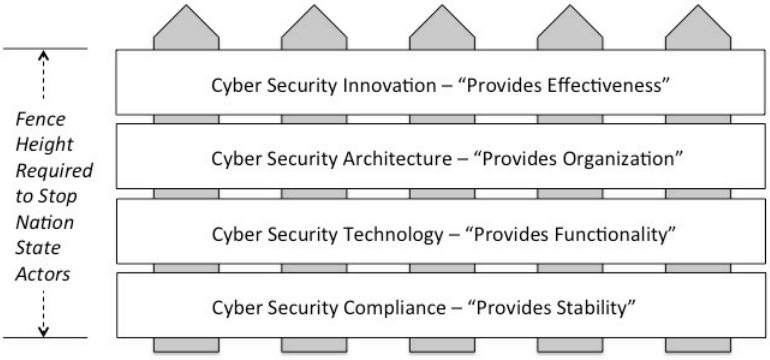

Figure 2. Cyber Security Focus Areas – "Fence Height"

Of these four focus areas, *cyber security compliance* has received the most attention in the security community over the past few years. When a company is hacked, for example, the recommended solution from managers, auditors, and regulatory groups is based invariably on improved compliance controls. Such emphasis stems from the ease with which compliance control requirements can be prescribed, tested, and managed. As a result, most organizations find themselves dealing with multiple compliance frameworks simultaneously, and the result is a relatively mature compliance discipline (albeit one with continued policy violations).

In contrast, the proper selection of *cyber security technology* products and services is performed in a largely ad hoc manner from one organization to the next. CISO teams will get information on specific vendors from security conference booths, industry magazine articles, peer word-of-mouth, carry-over vendor inertia, and previous experiences by local team members. Perhaps worse, many CISO teams will obtain their guidance from analyst reports ranking vendors into categories, often based on criteria that might be irrelevant to the buyer. The result is usually a hodge-podge of selected product and service solutions, rarely optimized to the specific needs and budget of the organization and based largely on a lack of information about alternate vendor options.

The *cyber security architecture* that dictates how products and services are deployed is often more structured. Specifically, enterprise architectures have evolved from the firewalls of the mid-Nineties to the complex perimeters found today. The perimeter is so ubiquitous that if an observer randomly picks a group of companies, their perimeters will have roughly the same design, construction, and functions. This would be true regardless of the size or sector of the company. Sadly, however, these perimeters are now ineffective at stopping cyber attacks. As a result, a deliberate shift to a virtual, mobility-supporting security solution across a software defined network (SDN) will be required for most current and new security architectural initiatives.

The one security imperative receiving the least attention today is *cyber security innovation*. Unlike cyber hackers, nation-state cyber warriors, and even drug dealers on the Dark Web who continue to shift and reinvent their novel tactics, CISO teams have been boxed into pre-scripted defensive solutions dictated by regulators and auditors. Such stiff, non-inventive approaches, sometimes derisively referred to as "clipboard solutions," are another reason cyber attacks to businesses have been so successful. Clever innovation in cyber security solutions is therefore going to be increasingly required in future state architectures.

Purpose of the 2017 TAG Cyber Security Annual

This *2017 TAG Cyber Security Annual* is intended as a practical handbook and reference guide for Chief Information Security Officer (CISO) team members. The report offers CISO teams with guidance on fifty cyber security control areas, insights into cyber security industry market trends, and detailed vendor information to support local architecture improvements using modern cyber security technologies. This report is written under the firm assumption that the CISO team is willing to *distribute* their infrastructure into segments, *virtualize* these segments into cloud-based systems, and *upgrade* the associated cyber security technology using modern, advanced protection methods.

Great effort has been made to avoid turning this report into a marketing contest between vendors over who has the most extensive features. To that end, *this*

report specifically avoids vendor rankings, recommendations, and comparisons, since such efforts are generally meaningless in the context of the CISO's day-to-day work activities. Smaller vendors, for example, with fewer features tend to rank poorly in popular advisory rankings, even though they might provide world-class support to their customers. Similarly, larger vendors with massive global offerings will tend to shine in most advisory rankings, even though their products might be too complex or expensive for customers with only modest needs.

Since so much material is included in this report, it had to be organized into the following three separate volumes:

- *Volume 1: TAG Cyber Security Fifty Controls* – Volume 1 introduces the fifty primary control areas required for CISO teams to be more effective. These areas include traditional controls such as firewall platforms and two-factor authentication along with somewhat non-traditional controls such as security recruiting and security R&D. For each control area, an extensive list of vendors is included to support distribution, virtualization, and upgrade.
- *Volume 2: Interviews with Distinguished Vendor Principals* – Volume 2 attempts to faithfully reproduce the extensive technical and market discussions held with select distinguished cyber security vendor principals in the production of this report. It offers a brief digest of the expert guidance and amazing cyber security insights offered by these principals during the research stages of this report.
- *Volume 3: TAG Cyber Security Vendor Listings* – Volume 3 serves as a sort of "Barron's Guide" to the cyber security industry – albeit with listings for only those vendors which time permitted to cover. While this 2017 version includes 1337 vendors, an additional separate list of 500 more vendors will be incorporated into next year's report. The volume also does its best to help sort out the on-going mergers and acquisitions in this industry.

The material offered here is designed specifically to address the needs of both large and small enterprise CISO teams – although the bias might lean *ever so slightly* toward larger companies with more options. Companies and government agencies in critical infrastructure industries with large, complex enterprise systems will find the treatment here especially useful. Smaller companies who outsource (or ignore) many of their security obligations might find some aspects of the report to be beyond their basic size and scope.

Finally, the treatment here is designed to have global applicability. While a majority of the companies listed and analyzed are domestic to the United States, a healthy percentage of the vendors included have wide, international footprints, serving customers in countries located around the word. Many new cyber security start-ups have recently emerged in Israel, for example, and CISO teams should take the time to determine whether any of these vendors offer value to their mission. Information about companies in China and Russia tended to be more difficult to

obtain, with most collected data coming from Internet and Web-based research, as well as cyber security community word-of-mouth.

TAG Cyber "Enterprise 50" Security Controls

The cyber security guidance offered in this report attempts to cover the *full range* of solution areas that must be included to support improved enterprise cyber security. Different frameworks such as the NIST Framework or PCI DSS might address these solutions using alternate names and under different groupings, but the treatment here was derived from practical experience across various industries. Readers should have little trouble mapping the categories included here to ones that might have been adopted locally with different names or meanings.

The treatment in this report is unique in the sense that it weaves technical recommendations on common and familiar areas such as identity and access management with areas that typically receive less attention such as security recruiting and cyber insurance. The unifying theme, however, is their practical relevance to any CISO teams trying to improve defensive posture. The fifty specific categories included in the security solution guidance in this section are as follows:

Perimeter Controls

1. *Intrusion Detection/Prevention* – Traditional signature-based intrusion detection and prevention products have improved their accuracy and false positive rates recently through the use of improved algorithmic techniques such as behavioral profiling and contextual adjustment.
2. *Data Leakage Prevention* – Enterprise data leakage prevention (also known as data loss prevention) has evolved from simple egress traffic sniffing and file download blocking into more comprehensive data management systems coordinated with file and record markings based on sensitivity.
3. *Firewall Platform* – Five-tuple firewall products have been enhanced to now incorporate next-generation, application-aware security policy enforcement across distributed perimeters virtualized over enterprise network, mobile carrier, and public/hybrid cloud infrastructure.
4. *Network Access Control* – Local area network admission and access controls based on PC and hardware credentials are expanding their perimeter-based enterprise focus to support more heterogeneous arrangements of mobile, cloud, and virtual computing.
5. *Unified Threat Management* – Small and medium sized businesses continue to demand highly economical, integrated product solutions for managing multiple security appliances such as firewalls and data leakage prevention systems through simple, common interfaces.
6. *Web Application Firewall* – Web application firewalls are evolving from appliance-based gateway products that block the familiar cross-site scripting and SQL injection attacks to much more dynamic, virtualized filters that

mitigate advanced, zero-day attacks in HTTP conversations across distributed cloud systems.

7. *Web Fraud Prevention* – Tools to detect on-line misuse of e-commerce are extending their original focus on user account origination and takeover to include more advanced fraud detection algorithms such as navigational analysis and transaction monitoring.
8. *Web Security Gateway* – The use of forward and reverse proxies combined with dynamic filtering of URLs based on live threat intelligence continues to offer essential enforcement of organizational security and acceptable use policies for Web traffic.

Network Controls

9. *CA/PKI Solutions* – Certification authority (CA)-supported public key infrastructure (PKI) solutions remain essential for secure e-commerce, mobile authentication, network encryption, and many other enterprise and infrastructure applications such as Internet of Things (IoT) and Industrial Control Systems (ICS).
10. *Cloud Security* – Security solutions for public, hybrid, and private clouds include cloud access security brokers, cloud-resident data encryption schemes, and virtual perimeters for modern data centers and software-defined networks.
11. *DDOS Security* – DDOS security protection platforms have evolved from support for simple detection and scrubbing of volume-based Layer 3 botnet attacks to now include the detection and prevention of advanced Web-based attacks at the application-level.
12. *Email Security* – Current email security product solutions include traditional malware and Spam filtering, end-to-end encryption and digital signatures, and public key infrastructure controls designed to reduce the risk associated with fraudulent senders.
13. *Infrastructure Security* – Modern enterprise cyber security solutions rely heavily on the centralized protections embedded in Internet infrastructure components such as the familiar Domain Name System (DNS) and Border Gateway Protocol (BGP).
14. *Network Monitoring* – Network monitoring product solutions consist of platforms and tools that are designed to collect and process network meta-data and content at line speed across network gateways to support real time security analysis.
15. *Secure File Sharing* – Enterprise users require secure means for internal and external file sharing, information transfer, and project collaboration usually with encrypted repository support.
16. *VPN/Secure Access* – Simple employee VPN tools have evolved to more comprehensive product platforms that support the complex needs of

enterprise users with distributed partners and suppliers requiring secure access to sensitive data and systems from locations around the world.

Endpoint Controls

17. *Anti-Malware Tools* – Early signature-based anti-virus and Internet security tools for protecting PCs from viruses now incorporate more advanced static and run-time heuristic algorithms to detect the presence of malware.
18. *Endpoint Security* – Modern endpoint security controls for PCs and servers include a plethora of options including the use of virtual on-device containers as well as virtualized, cloud-based isolation techniques to prevent malware infections through browsers.
19. *Hardware/Embedded Security* – Solutions focused on enhancing the underlying platform through embedded controls in hardware build on the earliest security industry requirements for trusted execution environments.
20. *Industrial Control System/Internet of Things Security* – Threats to Industrial Control System (ICS) and Internet of Things (IoT) infrastructure and endpoints demand new cyber security protections integrated into relevant support systems such as Supervisory Control and Data Acquisition (SCADA).
21. *Mainframe Security* – Because so many larger enterprise teams continue to rely on older mainframes in the data center, tools for data governance, authentication, and access controls on legacy mainframes continue to be essential in these environments.
22. *Mobile Security* – The protection of mobile devices, mobile apps, and supporting mobility infrastructure from cyber attacks has emerged as one of the most significant product growth areas in the cyber security industry along with cloud and virtualization.
23. *Password/Privilege Management* – Proper handling of passwords and privileged account credentials is an effective deterrent against advanced attacks. Many expert offensive attackers regard weak privilege management as a prime means for gaining entry to a target enterprise.
24. *Two-Factor Authentication* – Every enterprise now recognizes the security advantages of transitioning from simple password authentication to the validation of user and machine identities using multiple factors that leverage biometrics, smart phones, and software tokens.
25. *Voice Security* – Over-the-top products that encrypt voice communications are essential wherever the underlying telecommunications infrastructure and services cannot be fully trusted, especially in countries with less modern infrastructure protection and support from the local government.

Governance Controls

26. *Brand Protection* – Enterprise brand and reputation protection schemes include Web-based solutions that identify fraudulent use of Internet

domains, corporate trademarks, company logos, and proprietary information.

27. *Bug Bounty Support* – Controlled, negotiated reimbursement to security researchers who find vulnerabilities in externally visible systems is an essential means for reducing the risk of zero-day weaknesses in enterprise systems.
28. *Cyber Insurance* – The insurance industry is beginning to aggressively underwrite policies that transfer security risk away from corporations and their directors based on formulas that estimate the probability of a consequential cyber attacks.
29. *Governance, Risk, and Compliance* – Automated platform support for coordinating management governance, enterprise cyber risk, and regulatory compliance has become one of the most essential underlying components of every enterprise security program.
30. *Incident Response* – Incident response products and services include platform support for managing and automating the post-breach incident response task including team workflow.
31. *Penetration Testing* – Penetration testing engagements involve deliberate white hat attacks performed under controlled conditions by sanctioned parties in order to demonstrate the presence of security weaknesses in a target system.
32. *Security Analytics* – Virtually every modern cyber security technique integrates some form of security analytics using platforms and associated tools that support deep, holistic, correlative assessment using advanced algorithms.
33. *Security Information Event Management* – The enterprise security information event management (SIEM) system serves as a collection repository for security analysis of log output, metadata, and security alarm information.
34. *Threat Intelligence* – Threat intelligence services provide a range of value including the detection of enterprise assets for sale on the Dark Web as well as real time information about externally reported security vulnerabilities.

Data Controls

35. *Application Security* – Application security products now include static and dynamic methods to prevent security issues in software applications for enterprise, Web, cloud, and mobile.
36. *Content Protection* – Protecting content using digital rights management (DRM) is not only useful for enterprise data, but also for a range of content industries including entertainment, gaming, music, and publishing.
37. *Data Destruction* – Tools for ensuring that information is properly destroyed from retired physical systems are essential to enforce any enterprise records management policies.

38. *Data Encryption* – Data encryption tools, including the associated key management utilities, remain perhaps the most fundamental underlying technologies for protecting data in transit and at rest.
39. *Digital Forensics* – Enterprise data analysts, corporate investigators, and law enforcers rely heavily on digital forensic tools for extracting information from physical media or systems to support security, restoration, or legal requirements.
40. *Identity and Access Management* – Enterprise identity and access management systems support a range of complex lifecycle requirements including user provisioning, account maintenance, role-based access control, administrative privilege management, and many other enterprise features.
41. *PCI DSS Compliance* – While every enterprise team must support a large number of different security compliance frameworks, the recent crisis in retail point-of-sale attacks has elevated PCI DSS requirements to heightened status in the cyber security industry.
42. *Vulnerability Management* – Modern vulnerability management products support scanning, detection, and assessment of weaknesses in enterprise systems through automated tools that are increasingly being positioned in public or private clouds.

Industry Controls

43. *Industry Analysis* – Enterprise security teams can improve their product and service source selection process through use of industry analysis, subjective opinions, and framework rankings of cyber security vendors and solutions from experts.
44. *Information Assurance* – Information assurance refers to the set of advanced products and services that are focused on reducing the cyber security risks associated with government or military organizations.
45. *Managed Security Services* – Managed security services have evolved from simple third-party monitoring of firewalls to comprehensive sets of outsourced and managed services including emerging on-demand virtual security from SDN providers.
46. *Security Consulting* – Security consulting can range from executive-level engagements providing high-level views of enterprise risk areas with recommended actions, to more detailed, project-based professional services from subject matter experts offering working-level support.
47. *Security Recruiting* – CISO teams must maintain relationships with security recruiting teams in order to ensure continuity of support in an industry where cyber security talent is being obtained at a premium.
48. *Security R&D* – Enterprise security teams should either directly perform forward-looking security research and development (R&D) or make use of reported results from security research groups, perhaps obtained through academic partnership.

49. *Security Training* – Security training programs are required for developers and administrators to maintain currency with evolving threats, while security awareness is essential for every employee and support staff to avoid introducing unnecessary cyber risk.
50. *VAR Security Solutions* – Value added reseller (VAR) groups provide customized resale, integration, and consulting on security technology products and services with the ability to simplify the procurement details for buyers across large portions of the vendor community.

The cyber security solution areas listed above in these fifty categories correspond to the most commonly found day-to-day work activities in modern CISO teams of all sizes. CISO teams who wish to map these categories to their favorite compliance frameworks should have little trouble doing so. The graphic below offers a more visual representation of the controls. Several vendors dubbed this graphic as the *TAG Cyber Periodic Table*, a moniker that just seemed to stick around through the research process – hence, its reference below.

Perimeter Controls		Network Controls		Endpoint Controls		Governance Controls		Data Controls		Industry Controls	
1	Intrusion Detect/Prevent	9	CA/PKI Solutions	17	Anti-Malware Tools	26	Brand Protection	35	Application Security	43	Industry Analysis
2	Data Leakage Prevention	10	Cloud Security	18	Endpoint Security	27	Bug Bounty Support	36	Content Protection	44	Information Assurance
3	Firewall Platform	11	DDOS Security	19	HW/Embedded Security	28	Cyber Insurance	37	Data Destruction	45	Managed Security Svcs
4	Network Access Control	12	Email Security	20	ICS/IoT Security	29	GRC Platform	38	Data Encryption	46	Security Consulting
5	Unified Threat Management	13	Infrastructure Security	21	Mainframe Security	30	Incident Response	39	Digital Forensics	47	Security Recruiting
6	Web Application Firewall	14	Network Monitoring	22	Mobile Security	31	Penetration Testing	40	Identity and Access Mgmt	48	Security R&D
7	Web Fraud Prevention	15	Secure File Sharing	23	Password/ Privilege Mgmt	32	Security Analytics	41	PCI-DSS/ Compliance	49	Training/ Awareness
8	Web Security Gateway	16	VPN/ Secure Access	24	Two-Factor Authentication	33	SIEM Platform	42	Vulnerability Management	50	VAR Security Solns
				25	Voice Security	34	Threat Intelligence				

Figure 3. TAG Cyber Periodic Table of Fifty Enterprise Controls

While this 2017 TAG Cyber Security Annual can serve collectively as a bookshelf reference guide for the working CISO professional, a specific *usage roadmap* served as a backdrop during its development. This roadmap involved presumption that CISO teams would follow these steps:

- *Download* – Since all three volumes of this report are made available to CISO teams in PDF format free of any licensing restrictions or fees, the material should be downloaded to a common file share or server that is accessible to the entire CISO team. Some teams may also opt to download the report (for a

small purchase fee) for tablet or smart phone usage from one of the popular eBook stores on the Internet.

- *Mapping* – The security solution areas in the TAG Cyber Periodic Table of Fifty Enterprise Controls should be mapped to the local CISO program to help identify gaps. This mapping can be done manually or with the assistance of an automated GRC tool. Major gaps should not be expected (hopefully), but some areas included in the TAG Cyber taxonomy such as data destruction tend to be poorly covered in most enterprise security contexts.
- *Analysis* – Each of the individuals or sub-teams responsible for given aspects of the CISO team program – such as identity and access management or firewall management – should review the respective section for ideas, trends, or gaps. Product and service architecture design in each area will benefit directly from the analysis and vendor listings.
- *Vendor Contact* – During enterprise security design and integration, the extensive list of vendors included in Volume 3 should provide a means for extending or validating local understanding. It can also serve as an alpha guide for CISO teams just getting started in the process.

As the first of a planned on-going annual series of cyber security industry reports, this release will serve as a basis for identifying where and how the report is most useful to CISO teams. Subsequent reports in 2018 and beyond will emphasize those areas deemed most useful by working CISO professionals during this initial phase.

1. Intrusion Detection/Prevention Systems

⇒ *Signature* – Traditional intrusion detection/prevention systems based on signature processing have been largely ineffective in detecting APTs.
⇒ *Behavioral* – Next-generation intrusion detection/prevention methods based on behavioral heuristics with virtualization have been more effective.
⇒ *Deception* – Creative new security features such as support for deception enhance the overall value of intrusion detection/prevention tools.

Intrusion detection/prevention systems reduce the risk of cyber attacks through real time data collection, on-the-fly security analysis, and automatic response and mitigation. If data is collected as an early indicator, perhaps during the initial stages of the attack lifecycle, then the associated security mitigation can be viewed as preventive. While at-rest data can be collected and processed on a server host, the majority of systems collect data in motion from logical network chokepoints, usually adjacent to the firewall.

The earliest intrusion detection system (IDS) tools relied on static signatures, similar to the black list functionality found in early anti-virus systems. Intrusion detection products from companies such as the WheelGroup and Internet Security Systems (ISS) came bundled in the late Nineties with signature descriptions of the

attacks popular at the time. This signature detection technique soon became ineffective, however, as intruders created variants to sidestep signatures. As an illustration, virtually every prominent nation-state attack targeting credit cards and personal data in the past two years passed through signature-based IDS at the corporate gateway.

In spite of this ineffectiveness, CISO teams know that every compliance, regulatory, and corporate security auditor will nevertheless demand that IDS be deployed at every untrusted network gateway. Furthermore, auditors will rarely differentiate good IDS deployments from bad ones, so it is up to the CISO team to make good vendor and architectural decisions. Luckily, IDS products have improved considerably, both as stand-alone solutions and as integrated components of other products such as next-generation firewalls (NGW) and unified threat management (UTM) systems.

The first improvement occurred a decade ago with the introduction of automatic source IP address mitigation. Usually such action, referred to generically as intrusion prevention, involves the automatic shunning of those source IP addresses initiating a suspected attack. In addition, on the detection of attacks, IDS tools improved their ability to notify CISO teams through more extensive integration with the local protection environment. Such automatic mitigation steps became common enough that IDS, IDPS, and IPS soon just became referenced collectively and generically as IPS (which we will follow here).

A second improvement occurred as intrusion detection systems soon split into tools focused on the host operating system and ones focused on network traffic. The resulting network intrusion prevention systems (NIPS) and host intrusion prevention systems (HIPS) could thus optimize their detection capabilities to the types of attacks expected. CISO teams must obviously take into consideration the relative differences in NIPS and HIPS in source selection.

But perhaps the most significant improvement came as IPS functionality shifted from pure signature-based processing to a more adaptive set of detection capabilities based on profiles, behaviors, and analytics. Thus, while signatures remain in place for most IPS deployments, CISO teams can now expect their IPS vendor to offer a more rigorous set of detection and mitigation solutions that incorporate more extensive security methods. This includes clever techniques based on honey pots, traps, and other forms of deception.

Most IPS deployments are done at the perimeter next to the firewall perhaps attached to some SPAN (switched port analyzer) port on a LAN switch. The IPS will typically include a signature database, as well as advanced detection technology for identifying anomalies in collected traffic. Such technology is usually proprietary, and vendors will be coy about revealing to their customers (or to analysts) the real secrets of how they employ analytics to detect indicators of an attack.

Since all analytics can be viewed at the highest level as involving *some* sort of signature (yes, analytics is still a form of signature), CISO teams are advised to model the most basic underlying behavior of an IPS as including three simple steps: First, an intruder who wants to compromise some target asset initiates a series of

attack steps. Second, the IPS will detect these attack steps based on its signature database – which can and will certainly include advanced analytics, behavioral profiling, advanced deception, and mathematical modeling methods. And third, the IPS might place shun rules on the offending source, or it can take other types of mitigation steps including the creation of alarms or the generation of a report.

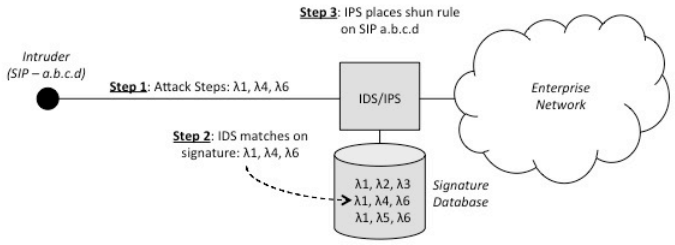

Figure 1-1. Most Basic Underlying IPS Functionality

When signature information is obtained from authoritative sources, the IPS should be more accurate in locating *known* attack indicators. In the United States, the Federal Government uses classified signatures as part of a service called Enhanced Cyber Security (ECS), which attempts to increase the accuracy of detecting advanced attacks. The ECS service is still somewhat new and evolving, so the true efficacy of using classified signature information to detect cyber attacks remains to be fully determined in practice.

By populating signatures rapidly, the possibility arises that an attack gaining momentum across the Internet might be sufficiently throttled by IPS infrastructure before it can cause extensive damage. This advantage has led to the almost universal adoption of real-time threat feeds into the IPS functionality located at Internet-facing gateways or major choke point between networks. Even PCs and systems tend to have real time threat feeds into the IPS functionality embedded.

Unfortunately, however, as suggested above, in spite of all the wonderful progress in this area, IPS products truly have experienced considerable operational challenges over the years in the accurate detection of live threats. The major technical issues are as follows:

- *Signature Deficiencies* – As mentioned above, the relative ease with which an attacker can slightly modify an attack, resulting in a so-called variant, continues to make it almost impossible for any system to have fully up-to-date signature databases. Cyber security experts have done their best, trying to design signatures that are as general as possible, without losing visibility into the target attack. CISO teams should ask their vendors for information about how signatures are developed and what sort of live threat feeds are supported.
- *Source IP Spoofing* – The simplicity of pointing attack traffic at an IPS with packets spoofed to be some third-party dupe makes source IP-shunning a

potentially troublesome attack tool. For example, if Eve attacks Bob, dishonestly claiming to be Alice, then an auto-shunning IPS protecting Bob would quickly take mitigation steps against Alice.

- *Content Encryption* – With more content being encrypted both at rest and in transit, the ability of IPS systems to perform deep inspection to identify indicators is restricted. If you want to deploy an IPS on an encrypted network, then you must either stick to visible telemetry such as five-tuple header information, broad traffic profiles such as volume metrics, or someone must be given the keys to decrypt, analyze, and then re-encrypt. This restricts the option of using a managed security service (MSS) provider for IPS in highly regulated industries such as banking where such key sharing would not be permitted by regulators.

An additional issue for IPS systems is the gradual dissolution of the enterprise perimeter. This is not necessarily bad news for IPS vendors, since the functionality will gravitate to a virtual perimeter or into the protections inherent in a cloud workload micro-segment. Even endpoint IPS functionality will follow the progression to cloud workload or mobile endpoint processing. But the fact remains that the obvious positioning of an IPS at the perimeter chokepoint is likely to go away.

Since compliance auditors and information security regulators will not waver from their demands that IPS remain at enterprise perimeters, CISO teams are advised to do their best to optimize the use of these tools. This can be done first by demanding the best available threat intelligence feeds for the best available, up-to-date IPS signatures. Additionally, by sending all IPS alarms and indicators to the enterprise SIEM, they become useful contextual input to the overall threat fusion process.

One of the most creative new solutions in the IPS landscape involves collecting data, inspecting it, and then using virtualization to find indicators of malware. This real-time cyber security technique, pioneered by FireEye and others, involves collecting the suspicious code or data, usually in the form of a payload, and detonating it in a safe virtual environment. The result is a highly effective means for attack detection – and if the indicator is found early, an effective means for attack prevention.

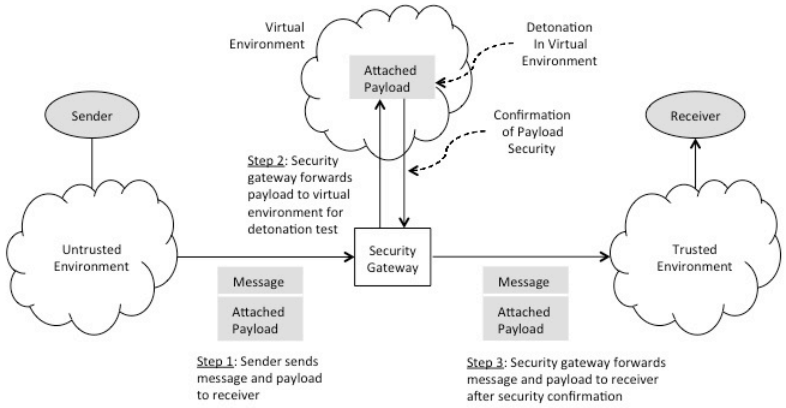

Figure 1-2. Virtual Detonation of Suspicious Code and Data

In virtual detonation, what happens first is that a malicious sender initiates traffic, usually email, through a security gateway. That gateway, presumably running special IPS functionality with virtual detonation, plucks off suspicious code or data such as a payload and sends it off to be tested virtually. If everything looks fine, then the traffic proceeds; otherwise it is stopped and notifications would be provided in the form of alerts for the security team. This novel technique, which has come to be viewed as *essential* in the modern enterprise for advanced persistent threat (APT) detection, serves as the basis for the success and growth of virtual attack detection tools over the past few years.

Another useful trend in the modern intrusion detection/prevention marketplace involves the use of deception and honey pots to trap hackers. Once an attack has been detected, and this is increasingly based on behavioral analysis, an in-line function routes the attacker to bogus systems set up with realistic honey pot content. In the best case, the attacker will expose its techniques in this deceptive environment allowing the enterprise CISO team to take immediate forensic and response actions. Obviously, the design challenge is to be subtle in the deception, and many vendors such as Attivo Networks have begun creating tools that are ready for live deployment.

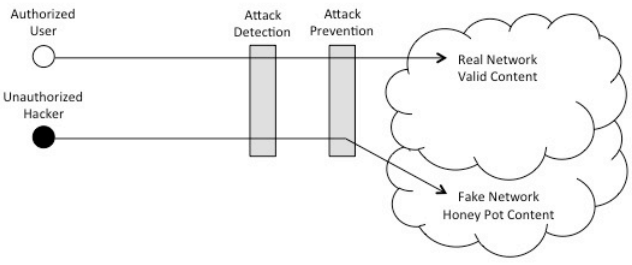

Figure 1-3. Using Deception and Honey Pots to Detect and Prevent Attacks

Marketplace trending in the *existing* perimeter deployment of IPS tools is likely to be flat to slightly negative in the coming years. Forces driving the existing market down will be the clear challenges associated with signature processing as well as the substitution of network behavioral analytic tools in compliance and regulatory frameworks. Furthermore, the popularity of next-generation firewall (NGFW) solutions in the mid-larger markets and unified threat management (UTM) in the mid-smaller markets has introduced embedded IPS into these environments. Thus, even with improved next-generation IPS functionality as described above, there is often competition with similar embedded functionality.

These forces are significant enough that virtually all signature-based IPS products, as designed over the past twenty years, have reached maturity, with no new star-up entrants focused in this traditional area. All new IPS entrants focus instead on advanced persistent threat (APT) defenses in network or enterprise security analytic contexts, or on the use of deception to detect and prevent attacks. The market is likely to see a convergence of these new capabilities with existing IPS products, which will create renewed growth for vendors and value for CISO teams.

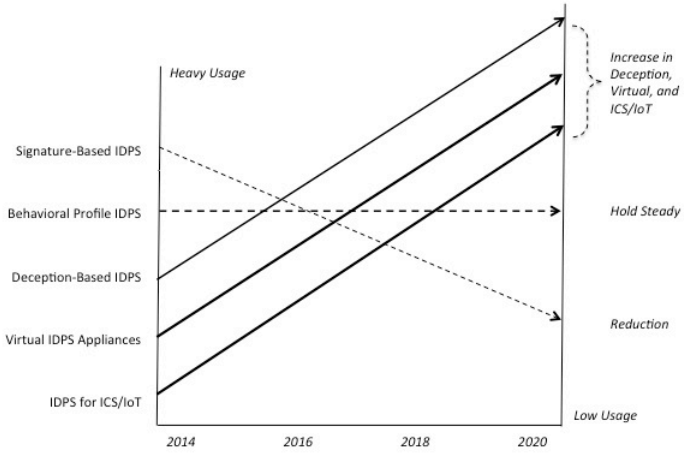

Figure 1-4. Marketplace Trending for Intrusion Detection/Prevention

An additional force that is good news for intrusion detection/prevention product vendors will be the desire amongst many participants to embed IPS into the fledging industrial control system (ICS) and Internet of things (IoT) markets. The idea that IPS functionality might become a desired component in billions of mobile devices will keep vendors busy for the years to come. This will not be an easy integration, however, since the protocols in ICS and IoT include legacy, proprietary, and even analog control handshakes that must be reverse engineered before any meaningful intrusion detection or prevention functions can proceed.

Additionally, virtual cloud workload protection will require IPS, and this is a welcome trend for vendors, even though hardware platform differentiation will obviously become less important. Instead, buyers will be more interested in the

detection algorithms and the degree to which the IPS can be integrated with the virtual SIEM. CISO teams moving to micro-segmented cloud workloads will still have to demonstrate IPS protection in the virtual ring, so IPS vendors are advised to begin optimizing for such new architectures.

Intrusion Detection/Prevention System Providers

Many IDS/IPS vendors explicitly avoid reference to the terms "intrusion detection" or "intrusion prevention" in their marketing materials, given the somewhat pejorative views associated with signatures. Nevertheless, the product vendors listed below provide IDS, IPS, or related product functionality such as deceptive computing to trap attackers in honey pot networks.

Product vendors offering network monitoring, security analytics, DDOS security, and other functions will also often make the reasonable claim that their solution provides IPS support. IPS also comes available embedded in a variety of next-generation firewalls and unified threat managements solutions, as well as through managed security service contracts.

CISO teams should therefore be open to a variety of different possibilities, beyond direct product purchase, to gain the benefits of signatures, behavioral analytics, virtual detonation, deception, and automatic response in their networks and hosts.

2017 TAG Cyber Security Annual
Distinguished Intrusion Detection/Prevention Providers

Attivo Networks – Tushar Kothari and his fine team from Attivo Networks were kind enough to share deep insights on numerous occasions about the growing cyber deception marketplace. The team continually stressed to me how deception can pervade so many aspects of the cyber security equation, and this perspective influenced my thinking considerably. Having breakfast in New York City with Tushar is always a delight, and his extensive knowledge of the cyber security industry and market is a great asset to the entire community.

CyberFlow Analytics – The capable team at CyberFlow Analytics includes my good friend, former boss, and AT&T Labs mentor Hossein Eslambolchi, who has helped me over the years to understand how innovation drives technology. His business partnership with Steve Nye and Tom Caldwell has resulted in a powerful cyber security platform that includes some of the most advanced attack detection heuristics and algorithms that I found during my extensive research for this report.

IronNet Cybersecurity – My longtime friend General Keith Alexander and his experienced team at IronNet were kind enough to host a wonderful day long visit for me in Maryland, offering technical insights into their heuristic algorithms and showing demos of their advanced user management interface. The cyber operations team at IronNet includes many former military staff and civil servants who learned their craft under the toughest of circumstances. We all appreciate their service.

SS8 – My good friend Faizel Lakhani from SS8 helped me to recognize the value of *time* in the detection and analysis of attacks. He and I worked together on a short paper and corresponding technical conference presentation on the use of time-based analysis in virtual systems including software defined networks. I am so impressed with how his team has managed to create cyber security tools that integrate this advanced concept with the more traditional collection and processing techniques they helped pioneer in their many years of support for law enforcement.

2017 TAG Cyber Security Annual
Intrusion Detection/Prevention Providers

AlienVault – AlienVault is a successful SIEM vendor with a huge following in the middle and smaller markets that includes a range of IPS security functions in its crowd-sourced cyber security capabilities. Larger companies are beginning to discover the benefits of the AlienVault products with their unique crowd-sourced intelligence.
Attivo Networks – Attivo Networks is a cyber security product vendor led by veteran Tushar Kothari that provides deception-based attack detection and prevention capabilities. This type of security control is being used more often in modern enterprise networks, and is likely to see increased deployment as the advanced algorithms for maintaining stealth operation continue to improve.
Bricata – Bricata offers high performance IPS product solutions that are designed to operate at line speed with a large network.
BluVector – BluVector provides advanced threat detection including a capability based on artificial intelligence.
Check Point Software – Traditional cyber security pioneering company Check Point Software offers a range of solutions with IPS capabilities available as integrated features or stand-alone capabilities.
Cisco – Cisco is one of the earliest vendors to offer intrusion detection products in the mid 1990's. With their purchase of NetRanger in that period, Cisco helped to establish the enterprise IPS market.
CyberFlow Analytics – The network monitoring and cyber security analytics company located in California offers an advanced breach detection product for enterprise customers. Tom Caldwell and the CFA team placed great emphasis during product development on including algorithms that cleverly detect subtle cyber attack conditions as early indicators.
Cymmetria – Cymmetria offers deception-based computing for the purpose of detecting advanced cyber security threats. The company uses virtual machines to decoy and detect hackers.
Damballa – Damballa provides a platform for real time network data collection and security analytics.
DB Networks – DB Networks provides continuous monitoring and attack detection for database infrastructure. The company uses advanced behavioral analysis to identify database attacks.

Deep Instinct – Deep Instinct provides advanced real time APT protection for endpoints, servers, and mobiles. Deep learning techniques are used to enhance the accuracy and efficacy of the solution.
Endian – Endian provides a range of UTM, firewall, VPN, and related solutions, many with integrated IPS capability.
enSilo – enSilo provides data exfiltration detection solutions for enterprise customers experiencing a breach.
Extreme Networks – Extreme Networks offers an intrusion prevention system based on its Enterasys acquisition many years ago.
FireEye – The FireEye product provides advanced persistent threat (APT) detection and prevention through data collection and virtual detonation of suspicious payloads in network traffic. The company can reasonably be credited with having invented this type of protection.
Fortinet – Fortinet offers the Fortinet Intrusion Prevention System with ability to customize signatures. CISO teams looking for a highly integrated cyber security solution with the IPS built-into the overall experience should take a close look at Fortinet.
HPE – The Tipping Point product, acquired by HPE, was one of the earliest intrusion prevention systems.
Huawei – Huawei is a major Chinese technology and network provider that includes IPS solutions for enterprise. Many US domestic firms have tended to shy away from Chinese firms as part of a supply chain integrity program. Increasingly, this practice is being questioned, and no one should consider a program of just avoiding certain countries as a reasonable means for assuring integrity.
IBM – Global technology solution powerhouse IBM offers its Security Network Intrusion Prevention system appliances powered by X-Force R&D.
Idappcon – Idappcon offers in-line network intrusion detection solutions with the ability to write Snort-based security rules.
Illusive – Illusive provides intrusion detection solutions utilizing deception techniques based on the experience of the principals working in Israel's elite Unit 8200.
Intel Security (McAfee) – Intel, previously McAfee, offers intrusion prevention system products with signature and signature-less inspection.
Intrusion – Intrusion has been offering IDS and IPS solutions since 2000. The company provides a range of different IPS solutions today.
IronNet Cybersecurity – IronNet is a network monitoring and security analytics firm started by General Keith Alexander in 2015 for the purposes of advancing the state-of-the-art in attack detection at line speed. The IronNet product is an example of the type of platform focused on a broad set of cyber security behavioral and profile-based indicators, rather than traditional signature IPS.
LightCyber – LightCyber supports behavioral attack detection through its Magna platform.
MetaFlows – MetaFlows has developed intrusion prevention technology based on in-line Snort operation.

Niara – Niara provides a security analytics platform that supports forensics and basic real time attack detection capabilities.
NIKSUN – NIKSUN is a mature network collection and security monitoring company that has the ability in their product to maintain packet capture and analysis at extremely high network capacity rates.
NSFOCUS – NSFOCUS includes a range of IPS capabilities in its anti-DDOS product and service suite.
Onapsis – Onapsis provides automated security assessment services for SAP, which are essentially application-specific intrusion detection systems. CISO teams with deep deployments of SAP cloud applications should look for vendors such as Onapsis to offer highly tailored protection.
Palo Alto Networks – One of the industry's leading NGFW vendors, Palo Alto Networks provides embedded, integrated support for IPS in its products. Few CISO teams go wrong buying Palo Alto Networks products, which are well designed and highly effective.
PrivacyWare – PrivacyWare offers intrusion prevention and Web application security software for Microsoft IIS.
Radware – The DefensePro Network Intrusion Prevention is integrated with DDOS and SSL-based attack protection.
Reversing Labs – ReversingLabs provides automated support for detecting malware in files and across enterprise Web, email, and file transfer traffic.
Seculert – Seculert provides a virtual, cloud-based platform that is accessible to the enterprise via APIs. Their service for customers offers a range of security protections including detection and mitigation of advanced persistent threats.
Securonix – Securonix provides a platform for collecting and analyzing cyber security intelligence for threat detection.
Shadow Networks – Originally known as Zanttz, Shadow Networks creates virtual networks where programmers can simulate cyber attacks. The technology is not traditional IDS or IPS, but the simulated environment allows for exercise of this technology.
Snort – Snort consists of free intrusion detection software used extensively in academic, research, and innovative environments. Many practical IDS deployments in live settings today are based on Snort.
SS8 – The emergence into IPS of product vendors such as SS8 with legacy expertise in law enforcement data collection and processing was inevitable. Support for functions such as lawful collection and response is so adjacent to the type of support required for modern IPS that companies like SS8 could easily adjust their collection platform to support the ability for deep inspection for cyber attacks in communication systems.
Symantec – Symantec offers mature network-based IPS protection solutions as part of its wide range of security offerings.
TrapX – TrapX provide attack detection through the use of camouflaged malware traps and deceptive computing.

TrustedMetrics – TrustedMetrics offers an intrusion detection system with advanced threat and malware detection.
TrustWave – The well-known solution provider includes IPS capabilities in its range of IT security offerings for enterprise.
Vectra Networks – Vectra provides real time continuous monitoring of networks for evidence of cyber attack.
Veedog – Veedog offers a malware prevention solution that sandboxes suspicious files and screens them for problems.

2. Data Leakage Prevention

⇒ *Keywords* – Traditional data leakage prevention (DLP) methods based on keyword search can detect benign, inadvertent leakage of known data types.
⇒ *Improvements* – Next-generation DLP methods reduce false positives through improved data inventory, type categorization, and breach remediation.
⇒ *Cloud* – DLP for the enterprise is shifting from on-premise, hosted DLP at the gateway to more virtual, cloud-based, on-demand DLP capability.

Data Leakage Prevention (DLP) product solutions, also sometimes referred to data loss prevention, reduce the risk of information leaks such as proprietary data to unauthorized individuals. Because traditional DLP tools depend on clearly identifiable signature patterns such as document markings, they are more effective at detecting inadvertent leakage than advanced malicious exfiltration. If, for example, an employee mistakenly sends sensitive corporate data across a gateway, the DLP system will usually detect such action. It will also help expose the corporate processes that were causing this data to be sent out in this inappropriate manner.

Traditional DLP solutions do not prevent determined adversaries from exfiltrating data, because the algorithms are typically not developed with this threat in mind. In fact, even in the presence of more advanced, next-generation DLP systems, the more determined adversary still has a range of exfiltration options that sidestep the DLP. This includes snapping pictures of sensitive data with a phone camera or making print copies of proprietary materials.

Newer DLP systems from companies such as Digital Guardian *do* incorporate better algorithms with advanced discovery, categorization, and analytics to combat exfiltration. The goal of such systems is to be less predictable to the adversary and to learn to identify the indicators present when data is being exfiltrated. Many current DLP implementations include improved tagging of sensitive document to ensure better coverage. The goal is to detect more leakage indicators with fewer false positives.

While these improvements are admirable and newer DLP systems are definitely improving, the reality is that most *current* DLP implementations still rely on pretty obvious phrases, markings, and expressions, often just sniffing traffic at an egress gateway. The typical DLP architecture *today* for an enterprise will include

email and Web DLP services at gateways, potentially augmented with endpoint leakage detection software to prevent use of memory sticks.

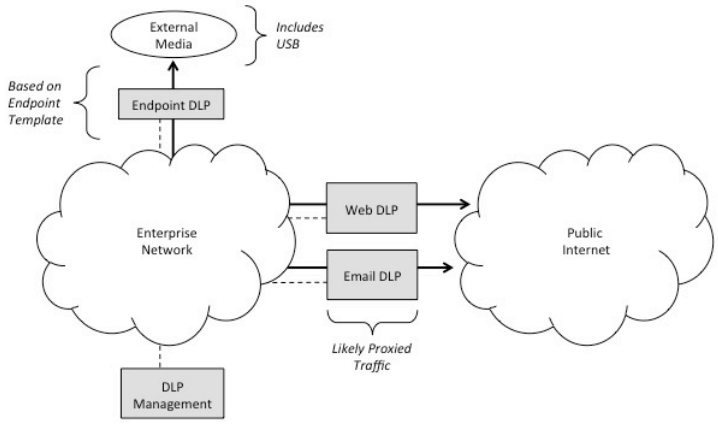

Figure 2-1. Typical Enterprise DLP Architecture

The extension of DLP to endpoints PCs and mobiles is intended to greatly reduce exfiltration risk. The idea is that by having a software control on the PC or mobile device, the employee will be less likely to try to copy sensitive data to a personal thumb drive or other storage device. Furthermore, as IoT devices continue to multiply, DLP vendors will begin to create similar endpoint leakage prevention extensions into industrial and consumer devices. DLP software libraries will be developed, for example, that IoT endpoint manufacturers and developers can embed into their endpoint devices.

The current signature-based algorithmic approaches for detecting leakages do not vary widely for different target use cases. All are excellent at detecting inadvertent leaks – hence they are essential in the corporate environment, but less effective against attacks such as advanced persistent threat (APT) exfiltration. They also struggle with enterprise encryption that might create gateway bypass.

The good news for vendors and CISO teams is that the marketplace for DLP has grown steadily in recent years based on three specific factors:

- *Inadvertent Leak Detection* – Most CISO teams run DLP at their gateways and potentially on endpoints or specific applications to deal with non-malicious cases. This approach, which uses phrase marking and keyword search, has been successful and will continue to grow. Just the detection of bad corporate processes, such as requesting social security numbers from customers over plaintext email, is worth the price of the DLP system and its deployment. No CISO team should consider operating their enterprise without the prudent use of a good DLP system.
- *APT Risk Reduction* – Some CISO teams have purchased and deployed DLP systems in the hopes that they will help reduce APT risk. While it would be a

stretch to conclude that DLP is effective in addressing military attacks, it is reasonable to conclude that DLP does provide some risk reduction, especially if it encourages better inventory and management of corporate information. Furthermore, next-generation DLP systems include much more advanced processing including behavioral analytics to determine whether data is being leaked. This technique, often referred to as user behavioral analytics (UBA), must be used carefully as it can drive employees to shadow IT if the perception of monitoring is too intrusive.

- *Expansion to Endpoints* – The expansion of DLP onto endpoints and applications has been quite useful in preventing employees from spilling data onto memory sticks or other external media. Also suppression of memory stick usage makes it less likely that employees will *actually insert* an infected stick in their PC. By the way, CISO teams need to recognize that the best malware will infect a PC when inserted on a memory stick, even if endpoint DLP is running.

Future trending in the DLP marketplace will be directly affected by a variety of positive and negative forces. Certainly, the three growth factors cited above have led to a successful vendor marketplace for DLP with thriving product offerings and very few unsuccessful or canceled offerings. The thrill of detecting leakages and closing the associated offending business process can be among the most rewarding experiences a CISO team ever experiences. So DLP will continue to be essential. As a complement to this, the existing enterprise-hosted market will shift slightly based on the following factors:

- *Embedded Cloud DLP Services* – As more consumer-based and enterprise computing moves to the cloud, the need for perimeter egress DLP will shift toward embedded virtual capabilities in the cloud. Mobility and IoT, in particular, will change the architecture of DLP systems. This is good news for next-generation DLP vendors.
- *Lighter Virtual DLP for Cloud Workloads* – The shift to workload protection in the cloud eases the complexity of DLP for individual virtual machines and applications, simply because the DLP processing does not need to account for every possible case at the perimeter. Buyers will thus need more lightweight DLP capabilities with virtual, on-demand deployment options in the cloud.
- *Continued DLP Algorithmic Improvements* – Continued advances in DLP heuristics and algorithms should be expected – always with the goal of improving accuracy, which in turn reduces the number of false positives that must be handled. Behavioral analytics is a useful technique for observing the conditions under which an individual might be leaking data. This can include profiles of usage such as social media postings, Webmail, and other factors.

These three business forces on the DLP market are depicted through 2020 in the diagram below.

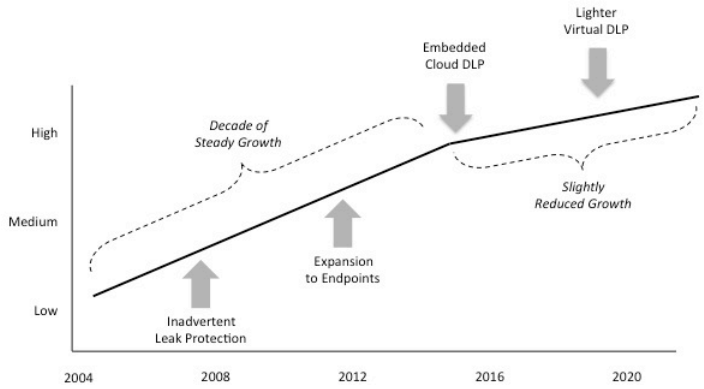

Figure 2-2. DLP Market Trends and Forces

To summarize: In spite of the minor drawbacks of DLP for advanced attacks, and the transition of enterprise networking and processing to embedded cloud systems, the market for DLP products and services will remain strong for the foreseeable future. This includes obvious growth in the need to embed DLP into all access paths to data resident in public and hybrid clouds.

To that end, the most successful next-generation DLP vendor solutions in the coming years will include a transition plan for handling the virtualization of enterprise computing and networking into public, private, and hybrid cloud systems. At minimum, DLP products should include a virtual appliance for the cloud service that CISO teams expect to utilize. At maximum, they should include means for providing DLP services in the northbound interface for SDN controllers in data centers and WANs. This will allow on-demand provisioning of DLP functions for any customer of virtualized wide area networking via SDN or data center support using SDN controllers to manage East-West traffic between different enterprise cloud workloads.

Data Leakage Prevention Providers

The product vendors listed below focus specifically on detecting and preventing data leakage from enterprise networks and endpoints. Included also are several cyber security companies who include some measure of data leakage detection or prevention in complementary products such as unified threat management (UTM) systems. Managed security service providers who include DLP in their offering are addressed in a separate section.

Quite a few DLP systems have been developed by vendors outside the United States, perhaps reflecting the relatively high interest in maintaining privacy in countries across the globe. Also, as mentioned above, many products are as designated as “data loss prevention,” and it was surprising how many marketing teams reinforced their desire to be designated as such. I must admit to perhaps

being less diligent than I'd promised in trying to make this distinction in terminology throughout this report.

2017 TAG Cyber Security Annual
Distinguished Data Leakage Prevention Providers

Digital Guardian – My friend Ed Durkin from Digital Guardian provided me with an introduction to the company's fine cyber security and DLP technology. This was followed by numerous deep technical discussions with the team, where I learned so much about how advances in cyber security technology can be used to improve not only DLP, but also many other aspects of the enterprise protection equation. I am in debt to the Digital Guardian team for their assistance throughout my research.
Skyhigh Networks – I certainly found a kindred spirit in Rajiv Gupta, CEO of Skyhigh Networks. His team and I spent considerable time discussing not only their specific technology, which extends far beyond just DLP, but also their approach to securing enterprise use of public cloud systems. I frequently draw on the image Rajiv shared with me of a "virtual cloud edge," which I think captures the essence of virtual security in a highly visual and easy to understand manner.

2017 TAG Cyber Security Annual
Data Leakage Prevention Providers

Absolute Software – Through its acquisition of Palisade Systems, the company offers enterprise DLP solutions.
Axway – Axway provides secure file transfer and email security solutions with support for DLP.
BHC Laboratory – BHC is a cyber security consulting and training firm in Estonia that includes DLP products.
Blue Coat – Blue Coat, now part of Symantec, includes advanced DLP functionality in its Web security gateway product. Egress proxy solutions provide DLP protection by ensuring that embedded malware cannot exfiltrate data to uncategorized Websites.
Boole Server – Boole Server is an Italian encryption software firm includes DLP solution for data protection.
CA – The large software company located on Long Island has expanded its cyber security offerings beyond its original mainframe focus to include a range of enterprise capabilities including DLP.
CenterTools – The German company offers IT security and data protection tools including DriveLock software for DLP.
Check Point Software – Check Point Software is a major security vendor that offers a range of DLP solutions embedded in its product line and available for on-premise or virtual deployment.
ClearSwift – ClearSwift provides an advanced data leakage prevention capability for the enterprise that is referred to as Adaptive Data Loss Prevention.

CipherCloud – CipherCloud supports DLP-based compliance solutions for public, hybrid, and private clouds.
Cisco – The famous network product company offers the Cisco IronPort product for high performance protection of email and Web data.
Comodo – Comodo acquired and now offers the MyDLP data loss prevention software product.
CoSoSys – CoSoSys includes data loss prevention functionality as part of its endpoint security offering.
DataLocker – Kansas-based DataLocker includes a USB-based DLP protection solution with digital rights management.
Deep-Secure – Deep-Secure provides a range of next-generation content inspection solutions for its firewall and related enterprise products.
DeviceLock – DeviceLock offers the DeviceLock DLP solution for protecting personal and business data.
Digital Guardian – Originally known as Armor5, Digital Guardian offers advanced next-generation DLP products for enterprise that control data, enforce egress policies, support advanced classifications, and provide for granular controls. The company acquired Code Green Networks, which provided enhanced data loss avoidance capabilities via its TrueDLP product.
Fidelis CyberSecurity – Spun off from General Dynamics in 2015, Fidelis has established itself as a leader in providing high quality cyber security solutions including support for enterprise DLP.
Forcepoint – Forcepoint was created via a series of business acquisitions and spin-offs involving Raytheon and Websense. The Forcepoint product solution provides integrated cyber security protection for the enterprise. The company includes a DLP Module in its TRITON APX product as a means for detecting consequential data and endpoint breaches from the premise or cloud.
Fortinet – Data leakage prevention functionality can be configured using the FortiGate product. Fortinet is one of the world's leaders in offering an integrated set of cyber security solutions in convenient products such as UTM and NGFW.
GajShield – The GajShield next-generation firewall appliances include DLP functionality.
GroundLabs – The Enterprise Recon solution from the Singapore-based vendor includes sensitive data discovery and management.
GFI Software – GFI Software provides data leakage protection and data awareness for portable devices.
GTB Technologies – The California-based firm offers increasingly popular enterprise data loss prevention and cyber security solutions.
HPE – The HP Enterprise Atalla information protection and control solution includes DLP functionality.
IBM – Global technology firm IBM offers data loss prevention products as part of its Data Security suite of solutions.
InfoWatch – Russian firm, InfoWatch, offers the Traffic Monitor Enterprise integrated data loss prevention system.

Intel Security (McAfee) – With its acquisition of McAfee, Intel quickly became a leader in many areas of enterprise cyber security including DLP.
Intellinx – Intellinx offers a data leakage prevention solution as part of its overall set of products.
JIRANSOFT – JIRANSOFT provides a range of SaaS-based data leakage prevention solutions for enterprise.
Microsoft – Microsoft includes data loss prevention as part of its suite of solutions including Office 365. Microsoft is increasingly integrating native data security protections into its offerings and cloud-based services. Originally the recipient of great criticism in the 1990's and 2000's for having buggy software, Microsoft has made amazing strides in cyber security in the past decade with great contributions to the field.
Mimecast – UK-based firm Mimecast provides data loss prevention functionality for email to support governance, risk, and compliance.
Minereye – This Israeli start-up company applies machine-learning controls to protect companies from data loss.
Pentura – Formerly InteliSecure, Pentura is a UK-based cyber security company that provides a managed DLP service.
Proofpoint – Proofpoint includes DLP functionality in its advanced Email security filtering technology. The technology offered by Proofpoint has emerged as one of the industry leaders in malware detection and prevention.
RSA – The famous cyber security pioneering company includes data loss prevention in its overall cyber security suite of enterprise solutions.
Secure Islands – Secure Islands focuses on data loss prevention in its suite of endpoint and mobile protection solutions.
SilverSky – Now part of BAE Systems, SilverSky offers range of email DLP solutions for enterprise customers.
Skyhigh – Skyhigh offers a cloud-based security solution, including advanced data leakage prevention products with support for enterprise. The solution provides a unique virtual leakage edge for enterprise customers using a variety of public cloud services. Skyhigh refers to its overall cloud security solution as providing a "last mile" implementation of a virtual edge.
Sophos – Sophos includes data loss prevention in its suite of cyber security protection solutions.
Somansa – The company, which has presence in the US and Mexico, offers DLP for network, email, and other enterprise systems.
Spambrella – Spambrella offers cloud-based data loss prevention as part of its email filtering service.
Symantec– The large cyber security firm includes a popular data loss prevention product in its overall cyber security suite of enterprise solutions.
TrendMicro– TrendMicro includes integrated data loss prevention solution in its security suite.
Trustwave – Trustwave offers data loss prevention solutions through its acquisition of Vericept in 2009.

Zecurion – Zecurion provides a mobile data loss prevention solution that addresses BYOD.
ZixCorp – ZixCorp integrates its email encryption product with data loss prevention features.

3. Firewall Platform

⇒ *Five-Tuple* – The use of five-tuple firewalls at corporate perimeters with packet filtering and application gateway functions will gradually decline.
⇒ *Next-Generation* – The use of next-generation, application-aware firewalls will continue to grow in modern data centers and enterprise networks.
⇒ *Virtual* – The deployment of virtual firewalls as a component of distributed perimeters around public, private, and hybrid cloud workloads will increase.

Traditional *firewalls* were invented in the 1990's to separate networks at defined chokepoints. This approach resulted in what is now commonly known as an *enterprise perimeter*. To this day, the enterprise perimeter remains a primary control for most security audits, and CISO teams rely on its components, especially the firewall, as the collective backbone for the cyber security architecture. Reports of the demise of the firewall perimeter are thus greatly exaggerated – although architectural change is clearly coming.

In addition to the firewall, the enterprise perimeter has evolved to include additional security devices such as intrusion prevention systems, anti-malware filtering, and data leakage prevention tools. These tools complement weaknesses inherent in firewalls to improve security at chokepoints and gateways. Most companies have also expanded their enterprise perimeter to cover many different connections from their business edge to external untrusted networks such as the Internet or a business partner.

Unfortunately, however, with this expansion in enterprise networking, has come a corresponding expansion of scope and complexity. In particular, CISO teams have had to contend with unimaginable growth in the types of traffic, services, endpoints, applications, third parties, and other entities that are affected by enterprise perimeter policy – usually enforced by firewalls. Specifically, firewalls in modern enterprise networks have evolved from simple chokepoint elements to cover many different purposes including the following:

- *Internet Gateway Firewall* – This type of firewall provides protection of the organization from ingress traffic originating on the Internet, as well as egress exfiltration to sites on the Internet. A large business might have hundreds of rules at the Internet gateway, and this is the place where ingress DDOS attacks might be directed from botnets on the Internet.
- *Third Party Gateway Firewall* – This type of firewall provides protection of the organization from business partners, suppliers, outsourcing vendors,

consultants, and any other group requiring access to sensitive or critical infrastructure. A typical business will have multiple third party gateways and the management of these gateways might include hundreds, thousands, or even *millions* of firewall rules. Keeping track of this is not easy.

- *Endpoint Firewall* – This type of firewall provide protection for PCs, mobile devices, and other endpoints from certain types of malicious attacks. The idea here is to control ingress and egress traffic on an endpoint using policy rules. Many users hate this type of protection because it can cause certain applications to behave badly or just break.
- *Cloud Firewall* – This type of firewall provides virtualized protection to cloud workloads as part of an orchestrated micro-segment around an application. Cloud firewalls are virtual and usually operate via a service chain in a software defined network (SDN) environment, or as part of a dynamic micro-segment as in VMware NSX or OpenStack Security Groups.

CISO teams are advised to take inventory of these different firewall options for the purpose of *simplification*. Such simplification can focus on reducing rule set size, removing or reducing the number of firewalls required in a network, or replacing cumbersome hardware with more manageable virtual appliances. This advice is provided with the caveat that network segmentation designs might lead to *more*, rather then fewer firewalls in an enterprise.

One of the more popular advances in modern firewall architecture design involves companies using *network-based security* to provide complementary mitigation for heterogeneous networking entry and exit points. The idea is that if traffic is destined for some ingress gateway, the possibility arises to provide mitigation and policy enforcement upstream on the network to ease congestion at the corporate gateway and keep malware as far from the enterprise as possible. This transition from simple choke point perimeter firewalls to network-based security for complex enterprise networks is shown below.

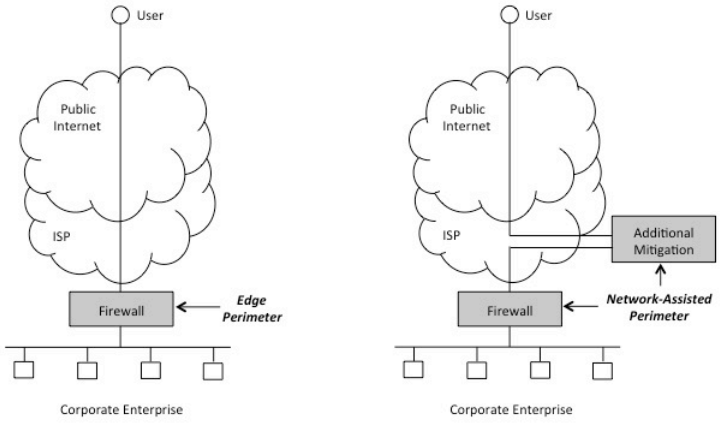

Figure 3-1. Transition from Pure Edge Perimeter to Network-Based Security

Network-based security solutions usually focus on services that integrate naturally with man-in-the-middle processing. Removing viruses and Spam from email is a good example, because email is a store-and-forward protocol that is easily diverted to a network-based filtering location without the sender or receiver even noticing. DDOS defenses are another good example, because the collective packet volumes from a botnet are better scrubbed in the network, where the sizes are more modest, than at a perimeter where energy gathers into something potentially overwhelming.

Examples where network-based security solutions might be more challenging include environments that rely on end-to-end encrypted sessions, or ones where the local services are especially sensitive to latency. In these cases, extraordinary means might exist to deal with the challenge – as in the ISP offering to manage cryptographic keys or the network-assisted perimeter solution having a sufficiently economical design to minimize latency. CISO teams need to have (or hire) the expertise necessary to make these determinations in advance of any network-assisted perimeter security solution deployment.

For enterprise networks that utilize global virtual private networks (VPNs), perhaps based on the multi-protocol label switching (MPLS) protocol, perimeter gateway chokepoints don't always integrate naturally. In the worst case, nodes on the MPLS/VPN ring all have their own Internet connections, and drawings of the enterprise network begin to look like some weird porcupine. As a result, many ISPs have begun offering creative network-based firewall solutions that share multi-user firewall processing nodes to enforce policy among different customers.

An additional evolution in firewall platform design is increased awareness in the application logic, protocol handshake, and operational environment in which the firewall is to operate. Such improved devices include Web application firewalls and intrusion prevention systems that are designed specifically to understand the Web capabilities of an application being protected, as well as next-generation firewalls that offer the ability for firewall administrators to more closely fine-tune the rules in a given environment to specific local needs, rather than generic five-tuple situations. Application-aware firewall functionality is depicted below.

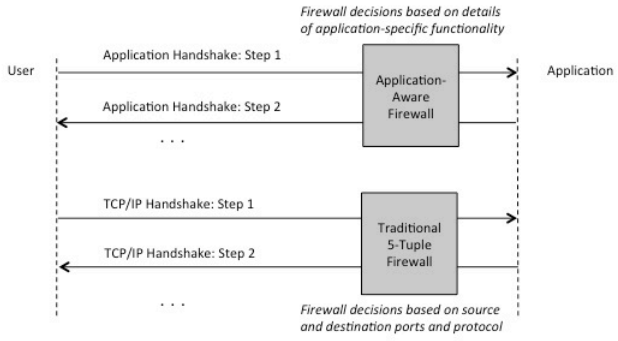

Figure 3-2. Application Aware Firewalls

As new virtualized firewall capabilities begin to emerge in the coming years, including as native functions in OpenStack software, a new type of firewall capability will become more popular that can be dynamically provisioned with virtual machines or applications in the cloud. Users accessing virtual machines or applications would thus have to deal with mediation from a virtual firewall from companies such as vArmour and Fortinet, rather than a generic firewall positioned in front of the cloud infrastructure serving all hosted applications and virtual machines. This virtual machine or application-specific firewall concept is shown below.

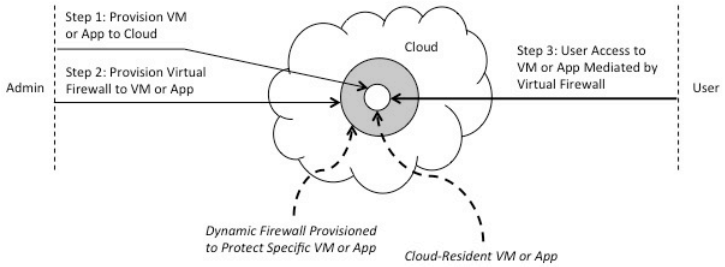

Figure 3-3. Dynamic, Cloud-Resident Virtual Firewall

CISO teams are strongly advised to make sure someone on the team understands the concept of dynamic, cloud-resident virtual firewalls. These will be closely integrated with the emerging notion of a micro-perimeter or micro-segment in the cloud-based enterprise, which involves shrink-wrapping security to smaller workloads than is done today with massive enterprise perimeters.

Many CISO teams have allowed their strategic firewall knowledge and capabilities to atrophy in recent years, particularly in environments where a group outside the CISO team operates the firewall on a day-to-day basis. The time has come to re-invigorate technical and architectural discussions on firewalls and their role in modern, virtual enterprise architecture. Specific firewall-related trends that should be managed carefully by CISO teams in the coming years include the following:

- *Endpoint Firewalls* – Just as server computing has moved in the direction of virtual operating systems, endpoint computing is likely to move in the same direction. This will allow for more flexible implementation of new functionality. The most likely result will be endpoint-containerized access to cloud resident applications with firewall protection of the underlying endpoint operating system. The result is that endpoint firewalls will hold steady as a market offering.
- *Traditional Firewalls* – On-going needs will remain for traditional firewalls for many years to come, particularly as companies feel pressure to better protect their legacy systems. But the practical situation is clear that

companies are moving away from traditional architectures requiring a five-tuple, choke-point filter. As such, this market will see gradual degradation.

- *Network-Based Firewalls* – Like traditional firewalls, network-based firewalls offering mediation assistance in advance of an existing or virtual perimeter will remain relatively stable. Transition of support, such as email Spam filtering or DDOS protection, from physical to virtual will help maintain stability, but will not be sufficient to support hyper growth.
- *Threat Information* – The use of crowd-sourced, real time threat information for firewalls will become ubiquitous, and will no longer differentiate next-generation firewalls from other vendors. This requirement will remain important, but will wane as a separate revenue generator or product selection differentiator. Every buyer will expect this capability to be a native component of firewall platforms.
- *Virtual Operation* – Every indicator suggests firewalls becoming more virtual and more dynamically generated for specific purposes. Binding firewalls to virtual machines and cloud applications seems the optimal choice for most IT environments. This will replace traditional perimeter networks and will see significant growth in the coming years.
- *Distributed Perimeter* – The use of virtual firewalls to create a distributed perimeter around legacy wired local areas networks, emerging public, hybrid and private clouds, and mobile/wireless networks will emerge as the highest growth market. Distribution and virtualization, as a combined entity in firewall platform design, will be powerful differentiators in the market. CISO teams should ask for a roadmap accordingly from their preferred vendor.

These firewall industry trends are visually represented in the diagram below.

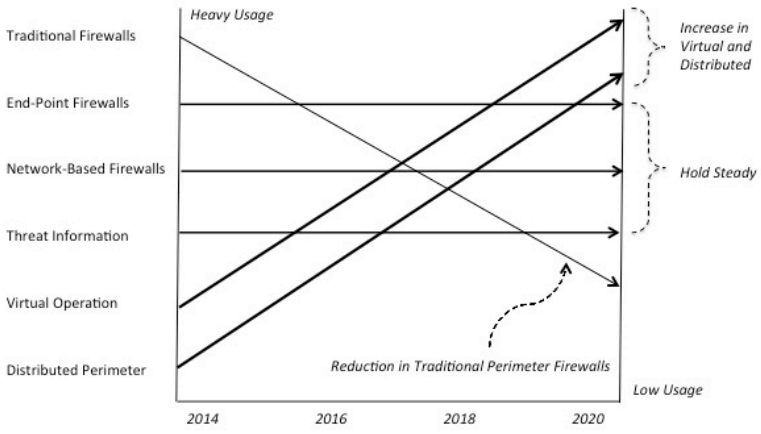

Figure 3-4. Firewall Industry Trends

The trends shown in the diagram above are likely to be relatively consistent across global enterprises. Differing privacy concerns in certain countries such as in

Western Europe should not have much influence on firewall evolution. Dramatic reductions in hardware appliances and associated control systems will truly drive the firewall marketplace toward virtual operation using software-defined controls over cloud infrastructure.

Additionally, the direction of application-aware firewalls is likely to move toward increased support for industrial control and IoT applications. By embedding such functionality into the cloud, new virtual gateways supporting machine-to-machine mediation with firewalls that understand legacy and new IoT protocols will be a significant growth market, especially for industrial control applications. The challenge will be finding vendors capable of embedding next-generation features into firewalls that are based on the unique, proprietary, and sometimes just-plain-weird nature of ICS and IoT devices in the field. This will require reverse engineering, customized analysis, and perhaps higher prices for applications that are especially hard to understand.

Firewall Platform Providers

The firewall platform providers listed below consist mostly of vendors offering either a conventional or next-generation firewall product bundled with many other features. Several vendors provide policy management and orchestration for firewalls, which has become an increasingly difficult task for organizations with large numbers of firewall gateways.

Several of the vendors included below are moving in the direction of virtualizing their product into a software appliance for cloud and virtual systems, most likely positioned in the architectural context of a cloud workload micro-segment. Many CISO teams gain access to the firewall platforms listed below by working with a managed security service (MSS) provider, covered in a separate section of this report.

2017 TAG Cyber Security Annual
Distinguished Firewall Platform Providers

Fortinet – I've counted Fortinet CEO Ken Xie as a good friend for many years. He was kind enough to write a jacket blurb for my textbook on critical infrastructure protection in 2013. His wonderful company has grown so much in recent years, driven largely by the deep technical competence of the team, along with Ken's steady leadership. His team was kind enough to help me immeasurably during this research in my understanding of the future direction of firewall platforms. I still have the impressive Manhattan skyline picture on my iPhone taken from the top floor of Fortinet's new innovation center in New York City.

Palo Alto Networks – Both Mark McLaughlin and Nir Zuk from Palo Alto Networks have been sources of great inspiration to me over the years with their visionary cyber security products and services. Most industry participants, including me, first learned the concept of a next-generation firewall from Nir, and the company

continues to provide world-class innovation in all that they do. I am so grateful to the Palo Alto Networks team for their support of the research leading to this report.
vArmour – Tim Eades from vArmour has been as generous in his time with me as any CEO in the cyber security business. I think I've lost count of our breakfasts, lunches, and drinks together discussing cyber security technology and industry trends. His team has also been so wonderful in helping me to explain and describe virtual perimeters and how distributed security can work in an enterprise using private, hybrid, and public cloud systems. CISO teams are advised to spend time reviewing and learning from the highly innovative vArmour approach.

2017 TAG Cyber Security Annual
Firewall Platform Providers

AlgoSec – AlgoSec provides a set of tools for supporting firewall policy management and operations.
Barracuda– Barracuda provides tools for supporting firewall policy management and operations.
Calyptix – Calyptix offers the AccessEnforcer firewall as part of its unified threat management solution.
Check Point Software – Check Point Software was arguably the first major firewall vendor in the 1990's and is still a major force in the firewall marketplace. CISO teams will rarely go wrong working with Check Point on security solutions, especially in this area.
Cisco – Cisco complements their router and switch offerings with a mature firewall product for premise and network as well as Sourcefire NGFW.
Clavister – Clavister provides software and appliance format firewall and VPN solutions for business.
Comodo – Comodo includes a free firewall for download, which focuses on PC security protections.
Deep-Secure – Deep-Secure is a UK-based company providing security solutions ranging from DLP to firewalls.
Dell – Dell offers the SonicWall firewall solution, which integrates hardware, software, and services into a common platform.
Endian – Endian provides a unified threat management (UTM) solution that includes firewall capabilities.
F5 – F5 is a successful network solutions provider with extensive security capabilities including firewall solutions. CISO teams are advised to take a close look at the F5 suite, which is generally high quality and effective.
Forcepoint – In 2015, Raytheon acquired and then spun off the former McAfee suite of next-generation firewalls, along with Websense, as part of Forcepoint.
Fortinet – Fortinet offers a comprehensive security fabric of premise and network-based firewall and related enterprise security products. The company has been aggressive in terms of expanding its platform to support protection and

virtualization from the endpoint to the cloud. Fortinet is also extending its solutions to IoT.
GajShield – GajShield provides next-generation firewall capability with DLP and cloud security support.
gateprotect – gateprotect is a German company offering next-generation firewall and UTM products.
Hillstone Networks – Hillstone Networks provides next generation firewall capabilities with behavioral analytics.
Huawei – Huawei is a major Chinese company that provides a range of high quality firewall appliances including high performance options.
Juniper – Juniper provides traditional and next-generation firewall solutions for the enterprise.
Kerio – Kerio offers a personal firewall, as well as firewall functionality in its UTM solution.
ManageEngine – ManageEngine offers a suite of network security products including firewalls.
NetAgent – NetAgent is a Japanese firm providing firewall solutions for the enterprise.
Palo Alto Networks – Palo Alto Networks essentially created the market for next-generation firewall solutions for advanced enterprise protection. They offer a suite of solutions that supports the need to fine-tune application-aware firewall and endpoint security to the local environment.
Sangfor – Sangfor offers a next generation firewall solution with support for SSL/VPN.
SmoothWall – SmoothWall consists of a free firewall product for software download and use.
Sophos – Sophos provides network security solutions, some based on the Astaro and Cyberoam acquisitions.
Tufin – Tufin provides a unique security policy orchestration solution that helps firewall administrators ensure an optimal firewall rule set.
vArmour – vArmour offers a virtualized firewall solution in support of a distributed perimeter for data centers and enterprise networks with emphasis on proper orchestration and management of the resulting architecture.
VenusTech – VenusTech is a Chinese firm offering network security solutions including firewalls.
WatchGuard – WatchGuard provides a unified threat management (UTM) platform with firewall capability.

Additional Firewall Platform Providers

Arkoon – Arkoon provides Stormshield network security solutions as the merger of Arkoon and Netasq.
Draytek – Draytek is a Taiwanese company offering routers, firewall, and other network products.

Global Technology Associates – Global Technology Associates develops UTM, firewall, VPN remote access, and other products.
NetASQ – NetASQ is a European manufacturer of firewall and VPN devices using proprietary technology called Active Security Quantification.
Netgear – Netgear is a provider of firewalls, routers, UTM, VPN, and related networking products.

4. Network Access Control

⇒ *Enterprise NAC* – Use of traditional network access control (NAC) will decline with cloud, mobile, and public WiFi enhancements to the enterprise LAN.
⇒ *Near-Term Enhancements* – The growing intensity of the enterprise threat helps justify continued investment in NAC enhancements in the near term.
⇒ *Long-Term NAC* – In 2020 and beyond, NAC functionality will be integrated with cloud and mobile to support the transition to a virtualized enterprise.

Network Access Control (NAC) is used to enforce security policy controls on endpoint devices such as laptops, PCs, servers, network elements, and mobile devices that are attempting to access a network, usually an enterprise local area network (LAN). The presence of guests on a corporate local area network is an important driver in the desire to use NAC to protect enterprise assets. The security concern is that guests might bring malware into the local environment by connecting a machine not properly patched or scrubbed.

NAC solutions are local, in the sense that they involve devices being connected to networks in a dedicated manner. Therefore, servers and endpoints with permanent connections are in-scope to NAC, as well as endpoints connecting temporarily to physical LAN or WiFi ports in an enterprise. Guests with their own PC, laptops, and mobiles requesting access to a private LAN using physical or WiFi connections are also in-scope to NAC. Remote entry across a network through a dedicated VPN or secure access gateway is considered a separate, albeit related technology. CISO teams going through NAC source selection should include VPN/Secure Access providers as part of the assessment.

Common NAC policy controls include running anti-virus software, scanning endpoints for vulnerabilities, performing authentication, or checking software patch levels. A slightly different policy control involves the enterprise security team recognizing a newly connected endpoint via unique identifiers such as the media access control (MAC) address. The IEEE 802.1X standard defines a typical set of functional properties for NAC implemented in several vendor solutions. CISO teams tend to talk frequently about this IEEE NAC standard, but very few have ever properly implemented it across a non-trivial environment.

Most enterprise NAC methods fall into one of two categories: *Pre-admission NAC*, which enforces policy in advance of a device being granted access to a network, and *post-admission NAC*, which involves attempts to ensure that devices already

admitted to a network comply with desired security policies. A huge advantage of post-admission NAC is that it introduces only negligible delays for endpoint access to networks, which is not true for pre-admission controls such as scanning that could take some time on a typical PC.

This is an important point, because the time it takes to scan and validate security and patch properties on a PC is far too long for users to wait for a NAC solution to complete before LAN entry is granted. Even several minutes wait time is not considered an acceptable duration for someone trying to gain access to the enterprise. For this reason, the seemingly obvious idea of doing a complete and thorough check and scrub of any device requesting entry is not going to be feasible in the vast majority of current environments.

CISO teams desiring this functionality should check with their NAC vendor for ideas on how to at least approximate the requirement. Furthermore, NAC tends to be an area where advance testing is difficult to perform, given all of the various infrastructure components that must come together for the solution to work. So at minimum, careful paper analysis of performance and flow should be done before a NAC solution is obtained and deployed.

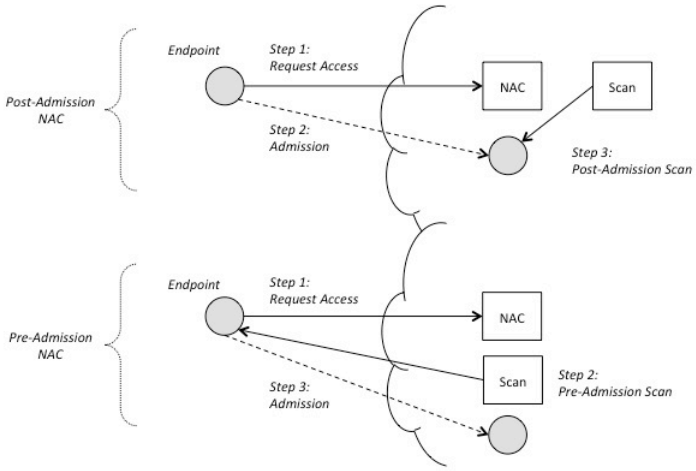

Figure 4-1. Post versus Pre-Admission Network Access Control

A common technique used in some NAC implementations involves the use of an intermediary virtual LAN (VLAN) often referred to as a *quarantine.* The idea is that when an endpoint requests admission to a LAN, if it does not appear to comply with local security policy, then it can be directed to a special VLAN that will only provide access to resources supporting proper remediation of policy violations (e.g., patch updates, security updates). Similarly, from such a VLAN, Web requests are redirected to sites that only provide support for policy remediation. These redirections are easy to describe, but introduce quite a bit of routing complexity for most enterprise networks, especially if multiple LAN switch vendors are deployed.

Many NAC solutions make use of a software agent on the endpoints in order to provide better information about the integrity and policy compliance aspects of the endpoint system. These agents communicate with a NAC server on the network to coordinate and interpret collected information. An alternate approach relies more on network scanning of agentless endpoints to try to discern policy compliance levels. Agentless solutions reduce endpoint complexity and are consistent with environments allowing guests to snap into wireless networks and open jacks. The use of endpoint agents, however, provides more penetrating information about the relevant characteristics of endpoint operating systems and applications.

In spite of these many desirable features and functions, traditional NAC deployments have been only partially successful in certain enterprise environments over the past decade. Reasons include the following:

- *Routing Complexity* – A variety of networking and computing decision paths are required to properly route guests with non-policy compliant endpoints, guests with policy-compliant endpoints, authorized users with non-policy compliant endpoints, and authorized users with policy-compliant endpoints. These decision paths require integration with complex identity management systems, endpoint MAC address inventory systems, and role-based access (RBAC) management. Spotty 802.1X compliance amongst switch vendors also complicates interconnection of LAN switches.
- *Transition to Mobile* – More employees utilize mobile devices to access corporate resources, and with BYOD initiatives, any agent-based NAC solution will require some adjustment. Mobile access to cloud apps reduces the need for enterprise LAN NAC. This is a clear trend in modern enterprise networks.
- *Guest Use of Open WiFi* – On-site guests to an enterprise who require network admission for Internet accessibility (perhaps for a marketing demo) would have previously requested access to the corporate LAN gateway. Today, however, the ubiquity of open WiFi access in most environments provides support for these scenarios without the need for NAC. This is also a clear trend in enterprise networks, and it is difficult to underscore its importance. Consultants and visitors were always the scourge of security teams, because they required LAN access to do their work. Now, with open WiFi, they can access their home network, or use approved remote access methods with two-factor authentication to enter the local LAN.
- *Reduced Perimeter Emphasis* – NAC is inherently based on the idea of gaining entrance to a perimeter-protected enterprise network. With common transition to public and hybrid clouds operating on the Internet, the need for NAC is supplanted by authentication over VPN to cloud-hosted applications. Stated more simply, as enterprise networks move to cloud-based virtual systems, guests can more conveniently and securely access these resources.

Each of the factors listed above will eventually *reduce* the need for traditional network access and admission controls to enterprise perimeter defined LANs. On the surface, this would seem like bad news in the moderate to long term for NAC vendors; however, with the increased intensity of malicious threats to existing enterprise networks, NAC companies will have the opportunity to expand in the near term, especially as companies receive failed internal and external audits on their access and admission controls.

The best NAC vendors will use the near-term growth to invest in more cloud-based, virtual solutions consistent with mobile. In fact, this growing need for mobile access to virtual, cloud-based infrastructure provides an attractive growth area for companies currently specializing in NAC, because the technology, processes, and skills are transferable. Some of the NAC vendor features and functions that are most compatible with the emerging architecture of the modern enterprise, and that can contribute to renewed growth in the NAC market include the following:

- *Agentless Operation* – As suggested above, agentless NAC is much easier to deploy in an enterprise than endpoint agent NAC support, and emerging solutions are doing a better job at collecting useful profile and guest information. Agentless operation increases the assortment of device types that can be supported for enterprise NAC and will ease the transition to virtual environments.
- *BYOD Provisioning* – Current NAC vendors are providing better tools for provisioning and onboarding BYOD devices in the enterprise. This is a required feature in most enterprise networks since the use of mobiles and tablets by guests is common. Free WiFi in the local environment eases the need here somewhat.
- *Guest Provisioning* – Improved quarantines and temporary access to limited resources allows CISO teams to be more flexible with the management of guests on an enterprise LAN. This type of protection is required wherever public WiFi is simply not sufficient for the needs of guests in the local environment.
- *Compliance Integration* – Modern NAC solutions are doing a better job collecting compliance information and linking with other security solutions in the enterprise such as the SIEM and next-generation firewall. This idea of NAC as an integrated enterprise security component makes good sense.

The simple relationship demonstrated in the figure below shows the expected growth of NAC solutions with the corresponding positive forces, resulting in a slightly growing traditional market in the near term with faster growth in mobile access and admission control. The overall market for access and admission controls to networks can thus be viewed as growing at a comfortable, albeit linear rate. Granted, the overall cyber security product marketplace is experiencing such hyper-growth in so many areas that these NAC trends appear to compare less favorably to other areas of the industry.

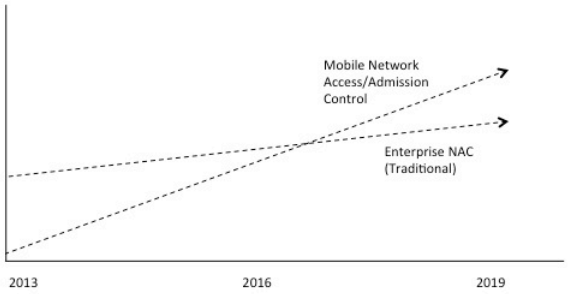

Figure 4-2. Factors Influencing the NAC Market

As for longer-term trends, perhaps 2020 and beyond, the likely integration of NAC functionality into future virtualized environments such as software defined networks (SDNs) and network function virtualization (NFV) will introduce the idea of access and admission to cloud workloads, rather than to enterprise networks. This new form of cloud virtualized NAC will require dynamic, adaptive access and admission decisions based on the attributes of requesting entities such as administrators operating on cloud software through portals, or cloud workloads accessing other cloud workloads through APIs.

A challenge that must be addressed in such environments is the explosion of MAC addresses that has occurred, and will continue to occur in virtualization of the data center and network. Where NAC solutions previously dealt with somewhat manageable numbers of MAC addresses in physical networks, the rise of virtual servers stretched geographically across Layer 2 Ethernet wide area networks creates the need for more scalable cloud and virtual NAC solutions. With the shift to mobile, virtualization, and cloud, however, this issue might eventually become moot.

Network Access Control Providers

The NAC product vendors listed below offer network access and admission control to the enterprise network based on hardware and media access control credentials. Most vendors are moving in the direction of supporting NAC functionality for mobile and bring-your-own-device (BYOD) initiatives. Many NAC vendors also sell network products, so the functionality usually integrates well with their entire product line.

2017 TAG Cyber Security Annual
Distinguished Network Access Control Providers

Juniper Networks – I was happy to see that my colleague Bob Dix had taken a senior executive position with Juniper Networks recently. He was instrumental in helping me connect with the extended Juniper team, and especially their experienced CISO Sherry Ryan. Juniper's fine portfolio of cyber security products including NAC is driven by their deep experience and expertise in networking. Juniper is a great

example of a technology company that understands the importance and relevance of software defined networking and virtualization for the cyber security industry. To that end, they helped me understand the proper balance required for a great cyber security vendor to support deployed legacy products while also making investment in new innovative methods such as SDN.

2017 TAG Cyber Security Annual
Network Access Control Providers

Bradford Networks – Bradford Networks provides a network access control solution for the enterprise called Network Sentry/NAC.
Cisco – Cisco has traditionally embedded NAC functionality into its LAN solutions for enterprise. The company offers the Cisco NAC Appliance (formerly Cisco Clean Access). If any CISO team wants to learn more about NAC products, services, and future directions, Cisco sales representatives tend to be well versed in this area and can provide assistance.
Endian – The Italian firewall and IPS vendor includes NAC solutions are part of its enterprise offering.
Extreme Networks – Extreme Networks offers NAC as part of its networking and security product portfolio and integrates with PAN firewalls for notification.
ForeScout – ForeScout provides a network access control solution called ForeScout CounterACT for the enterprise. The company is headquartered in California and is run by Michael DeCesare, the former President of McAfee.
Great Bay Software – Great Bay Software provides a range of network access control solutions for enterprise.
Impulse Point – Impulse Point provides the SafeConnect network access control solution for the enterprise.
InfoExpress – InfoExpress provides a unique peer-to-peer network access control solution for mobile devices and laptops.
Juniper – Juniper is a traditional network products vendor offering a unified network access control solution for the enterprise. Juniper embeds NAC into its EX Series Ethernet Switch product. Juniper sales teams and product representatives are also well versed in enterprise NAC design issues.
Macmon – The small company, headquartered in Berlin, provides full IEEE 802.1x NAC solutions.
Portnox – The Israeli company, with presence in New Jersey, provides its Portnox NAC network access control solution for the enterprise.
Pulse Secure – Pulse Secure is a spin-ff of Juniper and provides a mobility and BYOD-supporting network access control solution for the enterprise.
SnoopWall – SnoopWall acquired the NetBeat network access control solution for the enterprise from Hexis in 2014.
StillSecure – StillSecure provides the Safe Access network access control solution for the enterprise.

TrustWave – TrustWave provides a managed network access control solution for the enterprise.
United Security Providers –The Swiss company offers a variety of network access control solutions.
ViaScope – Located in South Korea, ViaScope offers integrated IP address management, DHCP, and NAC solutions.

Additional Network Access Control Providers

Adamant Solutions – Adamant Solutions provides the SWAT network access control solution for the enterprise.
Aruba Networks – Aruba Networks provides the ClearPass Policy Manager NAC solution for enterprise.
Auconet – Auconet provides a network access control solution for enterprise customers.
Avaya – Avaya provides a range of network access control solutions for the enterprise.
PacketFence – PacketFence provides a network access control solution for the enterprise.

5. Unified Threat Management

⇒ *Combined Functions* – Unified Threat Management (UTM) platforms combine functions such as firewall, IDPS, and DLP into a common interface.
⇒ *Near-Term Success* – UTM hardware solutions will remain popular with small and medium sized business for existing perimeter LAN usage.
⇒ *Cloud UTM* – As businesses shift to virtual perimeters with cloud services, UTM vendors will have an opportunity to invent distributed UTM for cloud.

Unified Threat Management (UTM) systems integrate the management and monitoring of a variety of different security appliances into a common interface. Typical functions covered in a UTM system include firewalls, IPS, DLP, and gateway anti-virus, all of which either connect to an embedded or external SIEM. UTM systems are built around customized software to control each of these security functions in a highly convenient manner.

Such commonality in management is a natural evolution for perimeters that began with the simple firewall and then grew into a cluster of different security appliances located at an enterprise network edge. UTMs save customers the trouble of having to do the source selection, procurement, integration, and technology evolution for each of the embedded functions.

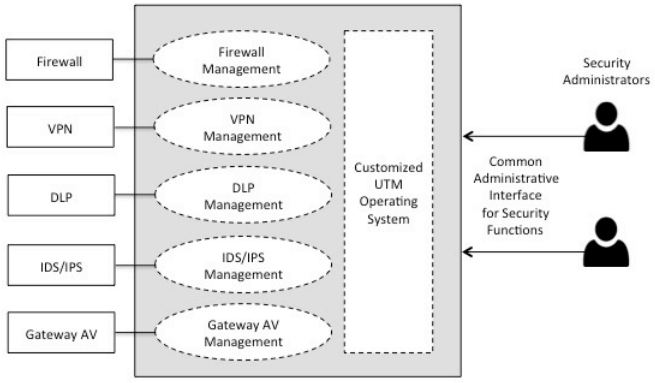

Figure 5-1. Typical UTM Arrangement

Small and medium sized businesses, in particular, have been attracted to UTM systems simply because they reduce the required surface knowledge for managing enterprise security. In an era where it is difficult to attract and retain capable security administrators – especially in small and medium sized businesses, this reduced surface is attractive. Features commonly found in UTM systems include the following:

- *Firewall* – UTM products usually include the packet filtering and proxy capabilities one would expect in a typical five-tuple firewall. Next-generation, application aware functions are beginning to emerge in some UTM products. Next-generation firewalls share many common elements with UTM, especially in their focus on integrating multiple security functions into a common management system.
- *Virtual Private Networking (VPN)* – UTM typically includes VPN support for encrypting connections to branch offices and mobile users – both of which are important technical considerations in many growing businesses.
- *Intrusion Prevention Systems* – UTM almost always involve traditional IDS and IPS functionality combined with the ability to try to block attacks based on network, application, and protocol information.
- *Web Security* – UTM includes URL filtering based on specified criteria and active threat feeds from the vendor. All good UTM products come with the ability to ingest threat feeds to maintain current views.
- *Application Security* – UTM usually includes the ability to monitor application usage and provide granular controls for applications such as Facebook and Twitter.
- *Anti-virus and Anti-Spam*– UTM products include gateway management of anti-virus and Spam blocking functionality for ingress traffic. This is best coordinated with the desktop anti-virus and Spam blocking solution, but this is not always possible.

Most current UTM products are created as hardware appliances. Marketing claims from UTM vendors usually tout the protection coverage that comes with embedding so many functions into a singly managed appliance, along with the performance benefits that come from hardware implementation. This hardware orientation is both a blessing and a curse for the UTM vendor community. It is a blessing since so many current enterprise customers desire these functions in their existing operation – and hardware appliances are easily deployed and managed to the perimeter; but it is also a curse with so many functions being virtualized to public clouds, where the natural integration of a UTM hardware component into the architecture is less obvious.

Typical UTM functional requirements used in source selection will focus on the performance of the solution. Most vendors will describe their throughput capability in terms of capacity loads for both firewalls and VPNs, as well as the number of users that can be supported. CISO teams tend to make a very big deal about these ratings during source selection, perhaps because it is so easy to compare numbers. If Check Point's NG Threat Protection Appliance, for example, looks to handle twice the capacity of a corresponding Cisco solution, then the presumption might be made that the Check Point solution is twice as good.

CISO teams are advised to be very careful in making such determinations. The example above withstanding (since Check Point and Cisco both make excellent products), teams can be easily led astray using numbers to rate UTM solutions. Google searches showing numeric charts comparing and assessing throughput can be very misleading. All it takes is for one unusual application in the enterprise to work poorly through the selected UTM, and all that numeric analysis begins to look silly. The only solution here is to install and test – and this is not always an easy process.

The outlook for UTM products and related professional services remains strong in the near future since the enormous benefit that comes from the security and performance of an integrated appliance is so obvious. This is especially true for smaller businesses, which will continue to benefit from UTM appliances as long as they operate perimeter-protected enterprise networks. Furthermore, with small and medium sized business becoming an increasingly attractive target for hackers, criminals, and advanced actors, it's hard to imagine UTM vendors not seeing substantial growth in this customer segment – at least in the near and moderate terms.

Over the long run, as small, medium, and large organizations continue to virtualize their IT and network operations, the coordination function and common interface provided in a UTM will begin to emerge as features in cloud security orchestration tools; and in fact, this may be the correct future for UTM products in the enterprise architecture. UTM vendors with experience serving the needs of security administrators will be well positioned to carry this knowledge into the creation of similarly integrated management tools for complex arrangements of public, hybrid, and private clouds.

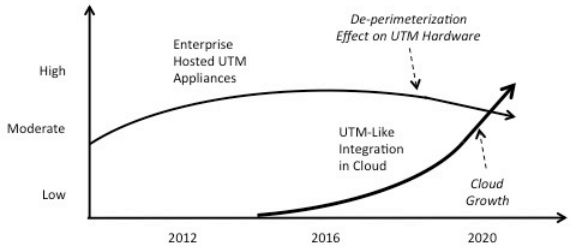

Figure 5-2. Likely Market Trending for UTM

Surprisingly, few existing UTM providers currently tout their public cloud and virtualization strategy. This lack of attention suggests a market opportunity for any vendor choosing to take the leap to virtual. It also suggests good acquisition opportunities for larger cloud security vendors to take on a UTM product – or vice versa. CISO teams should keep a close watch on the evolution of the UTM market. If a UTM solution is in place today, then the motivation for such attentiveness is obvious. But even if UTM solutions are not deployed in a given CISO team's enterprise security environment, with the convergence of cloud, UTM, and the desire for common security management, UTM-like solutions might become more attractive.

Unified Threat Management Providers

Unified Threat Management (UTM) providers listed below include traditional vendors focused on simplifying security gateway management for small and medium-sized business, as well as newer entrants who are factoring in the complexity of managing multiple, disparate cloud systems. UTM products are sometimes grouped as entry-level versus mid-range solutions, but this distinction can be confusing as the ability to handle high throughput continues to increase. Arguably, with the progression to cloud, a more relevant grouping would be UTM solutions with a design strategy for cloud, but this has not yet materialized.

2017 TAG Cyber Security Annual
Unified Threat Management Providers

Barracuda – Barracuda provides its X-series UTM solution as part of its firewall and related product portfolio.
Calyptix – Calyptix offers a unified threat management solution focused on small and medium sized business.
Check Point Software – Check Point is a familiar security technology product and service vendor that includes a mature and capable UTM product offering.
Cisco – Cisco is a traditional cyber security vendor with range of network security solutions including UTM. Their all-in-one UTM security solution has been an

excellent choice for small businesses desiring simple management with accurate threat intelligence.
Dell – Dell includes a unified threat management offering under the SonicWall brand.
Endian – Endian offers a unified threat management solution with firewall and IoT security.
Fortinet – Fortinet includes an extensive range of firewall and gateway security solutions in their UTM offering. Their solutions are well known for being able to handle high capacity throughput, as well as many different types of functional requirements.
gateprotect – gateprotect is a German company that offers unified threat management and next-generation firewall solutions.
Guard Site – Guard Site provides UTM, SSL-VPN, and firewall solutions under the WatchGuard brand.
Juniper – Juniper's SRX series is among the highest rated UTM solutions for capacity and throughput. Networking vendors have been able to apply their experience and expertise integrating multiple functional capabilities to the development of UTM solutions.
Kerio – The company offers its Kerio Control NG Series unified threat management solution for enterprise.
NetPilot – NetPilot is a UK-based company offering a Unified Threat Management solution with content filtering and secure cloud connectivity.
MyDigitalShield – MDS is a security-as-a-service provider with a unified threat management offering.
SecPoint – Located in Denmark, SecPoint offers a cloud protector UTM solution for enterprise.
Sophos – Sophos markets a unified threat management solution for small and medium sized business based on Cyberoam acquisition.
Topsec Science – Topsec Science is a Chinese company offering a range of information security solutions including UTM.
TrustWave – TrustWave includes unified threat management in its comprehensive solution offerings.
VenusTech – VenusTech is located in Beijing and offers network security solutions including UTM.
WatchGuard – WatchGuard provides a unified threat management appliance including anti-Spam, malware detection, and intrusion prevention.

6. Web Application Firewalls

⇒ *WAF Appliance* – The use of Web Application Firewall (WAF) appliances has grown with more intense application security compliance requirements.
⇒ *WAF Integration* – CISO teams have learned to integrate their WAF appliance with LAN IPS and perimeter gateway firewalls in the enterprise.

⇒ *Cloud WAF* – The logical progression for WAF functionality is toward more dynamic provisioning and use in cloud-based, virtual environments.

Unlike conventional five-tuple firewalls that operate using source and destination IP addresses, source and destination ports, individual packet bits/flags, selected protocol, and other packet characteristics such as direction, a *Web Application Firewall* (WAF) is an appliance, server plugin, or filter that uses more in-depth knowledge of HTTP applications to enforce policy rule mediation.

The operation of a WAF involves inspection of all packets into and out of a given application. The presumption is that these packets will correspond to the usual sort of protocols used by Web applications including HTTP, HTTPS, SOAP, and XML-RPC. If something appears unusual in the packet streams, then an alarm or mediation will occur. Similarly, if the now-familiar signature emerges for a common Web attack such as cross-site scripting, SQL injection, buffer overflow, or session hijacks, then the WAF would take appropriate rule-based action to stop the attack.

Unlike the typical enterprise placement of a gateway firewall or a LAN-based intrusion prevention system (IPS), a WAF is generally deployed as a proxy in front of a Web application in order to focus only on the packets coming into and out of that specific application. Firewall devices and IPS devices, in contrast, try to analyze all gateway and LAN traffic, respectively.

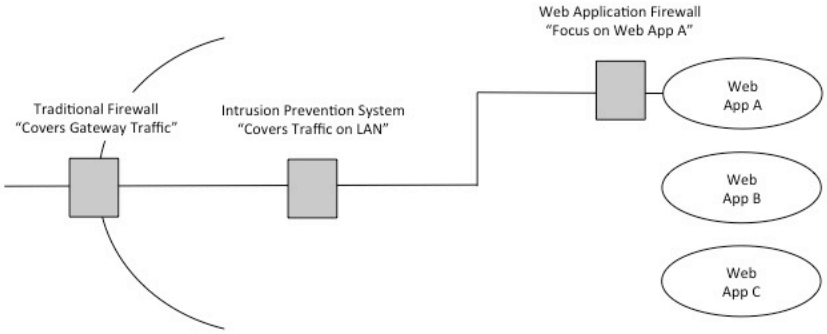

Figure 6-1. Typical Architecture using Traditional Firewall, IPS, and WAF

WAFs became popular in recent years as compliance managers began to recognize their usefulness in stopping nagging Web attacks (e.g., cross-site scripting) that seemed to occur over-and-over. The PCI DSS standard, for example, incorporated the use of WAFs as a recommendation for strengthening Web application in retail environments. The market for enterprise WAFs from companies such as Imperva has therefore been in growth mode for several years now.

Where the application environment is carefully studied and well-understood by both IT and security teams – as one would find, for example, in retail point of sale (POS) infrastructure, the use of a WAF is usually an excellent decision. In POS applications, for instance, WAFs can sit between card processing and other

functions to ensure that exfiltration to some unexpected server is not possible. Where the application environment is poorly understood, however, as in many complex Intranets, the use of WAFs can be frustrating and replete with outages. This is not the fault of the WAF, but rather of the poorly understood application environment.

A key trending issue with respect to WAF functionality is that as applications increasingly gravitate to cloud infrastructure and virtualized data centers, the associated application security controls will have to be adjusted accordingly. Many CISO teams have assumed that traditional WAF products, mostly implemented as physical appliances, will continue to be situated in the access path of future applications, virtual or otherwise. This is possible for fixed virtualized data center architectures, but in more flexible, ubiquitous, on-demand cloud environments, hardware appliances scale poorly. As a result, virtualization of the WAF protections might be a more suitable approach.

CISO teams considering a WAF solution should make sure to coordinate network-level IPS protection with application-level protection. The typical CISO team will utilize IPS in conjunction with a SIEM on the enterprise LAN to detect signature-based attacks or evidence of infected systems. WAF protections are much more application specific, so their protection method should be coordinated with the IPS to ensure optimal efficiency. Also, before making a commitment to WAF technology, it pays to discuss migration plans with your WAF provider to virtual and cloud. As applications move to private, hybrid, and cloud hosting, having the ability to integrate existing WAF might ease transition planning.

Trending in WAF usage and the WAF marketplace are likely to follow these basic points over the next few years:

- *Virtualization*: CISO teams will continue to experience increased need for virtualized WAF capabilities in the enterprise. Today, this involves hosted WAF functionality in the cloud, separate from the application execution environment. In the future, virtualization will enable more flexible WAF usage such as peak-time, on-demand WAF rule augmentation.
- *Cloud Integrated*: CISO teams will increasingly expect their cloud providers – public, hybrid, or private – to offer WAF as a managed, on-demand option. This will allow for integrated, run-time protections to be embedded in the same execution environment as the application being protected. SDN service chaining seems a natural architectural method for inserting WAF protections into a Web application access stream, but this is not common today.
- *App Integration*: Since WAFs are closely aligned with specific applications, seamless integration with these applications using virtualization is feasible. This makes sense because virtualization allows for WAF and application functions to be maintained separately, but aligned closely in the cloud.

These trends, which point to increased virtualization in the immediate term, and seamless app integration in the coming years, are shown in the figure below.

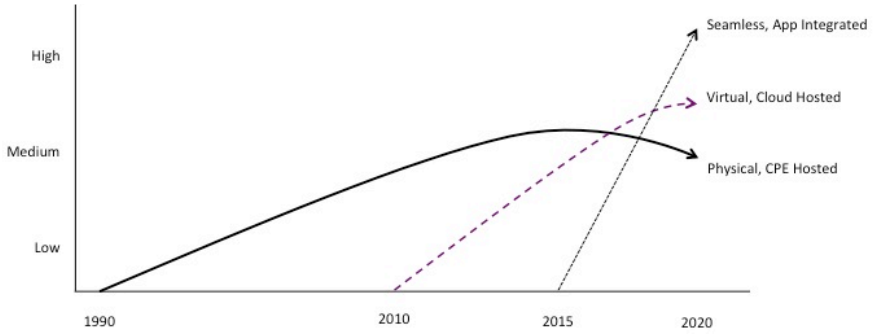

Figure 6-2. Trends in WAF Usage

The drop off in physical, CPE-hosted WAF follows the progression from the current enterprise perimeter-based architecture to more cloud-based arrangements. The dramatic growth in seamless, app-integrated WAF is also made possible by the ease with which virtualization enables new capabilities.

A balancing concern, however, is that deep understanding of an application continues to be required for proper tuning of WAF rules. For popular off-the-shelf applications, this may not be an issue; but for custom designed and developed applications as one would find in a large organization, the ability to code rules in a WAF is directly related to the available detailed knowledge of the application logic and protocol.

Furthermore, as WAF rules track more closely to the specific nature of a Web application – as in the detection of zero-day attacks based on anything that looks unusual for a given application – security managers should expect to see an increase in false positive WAF alarms whenever software changes are made. This is not a new problem, but it will require innovation such as machine learning or tighter integration with the code update process to dampen noisy alarm streams and outages based on improper WAF rule firing.

Luckily, with virtualization, tighter WAF integration with application code is more feasible, and one should thus expect to see more managed security service (MSS) providers begin to include virtualized, SDN-chained WAF functions as options for their managed solution customers. WAF vendors would be wise to begin looking for ways to create more multi-tenant hoteling options for MSS as well as better enablement and billing hooks to support MSS provision of their solutions in virtual, cloud based environments.

Web Application Firewall Providers

Web Application Firewall product vendors offer functionality that is closely related to intrusion detection/prevention, firewall platforms, Web security gateways, and Web fraud prevention systems. CISO teams are therefore strongly advised to perform source selection taking these types of vendors into full account. Next-

generation firewalls, in particular, are often difficult to differentiate with WAFs, and the marketing literature sometimes uses the terms interchangeably. CISO teams are cautioned to keep this in mind.

2017 TAG Cyber Security Annual
Distinguished Web Application Firewall Providers

Imperva – Anthony Bettencourt and his capable team at Imperva have demonstrated the ability to expertly integrate their products, including Web application firewall security, with accurate and meaningful threat intelligence. The importance of seamless WAF integration with the local environment came up over and over in my research. The fine technical team at Imperva spent considerable time helping me understand the proper balance in providing world-class Web application security with related protections against cloud and DDOS attacks. I truly appreciate their assistance and support during this research.

2017 TAG Cyber Security Annual
Web Application Firewall Providers

Ad Novum – Ad Novum is located in Switzerland and provides nevisProxy reverse proxy and WAF solution.
Akamai – Akamai has increasingly focused on security as part of its core offerings to complement the content distribution network (CDN) services it pioneered. Akamai offers its customers the Kona Web Application Firewall, which provides always on, scalable protection.
Alert Logic – Alert Logic offers customers a managed Security-as-a-Service Web application firewall.
Applicure – Applicure offers the dotDefender enterprise-class Web application firewall solution.
A10 Networks – A10 Networks provides its Thunder TPD Web application security product line.
Barracuda – Barracuda is an industry-leading provider of Web application firewall product solutions. Many CISO teams have reported excellent, cost-effective deployment of Barracuda WAFs for a variety of small, medium, and large-scale applications.
Bee Ware – Bee Ware makes Web application security solutions available as an offering for its customers on Amazon Web Services.
BinarySEC – BinarySEC offers the EasyWAF Web Application Firewall solution for protection, acceleration, and statistics.
Blue Coat – The global Web security firm includes Web Application Firewall capability as an integrated component of its suite of offerings. Existing Blue Coat customers, perhaps using its proxy offering, would be wise to considering integration of an on-premise or cloud based Blue Coat WAF.

Citrix – The well-known cloud virtualization company offers its Citrix NetScaler AppFirewall solution for customers. Companies like Citrix have deep knowledge of virtualization and will thus have an advantage moving into SDN, cloud, and virtualized implementation of enterprise security.
CloudFlare – CloudFlare's Web Application Firewall includes features such as strong default rules sets and customized Layer 7 defenses.
ControlScan – ControlScan includes a WAF solution as part of its MSS and DDOS security services for SMBs.
DBAPP Security – The Web application security firm offers customers its DAS-WAF solution.
Dell – Dell provides customers with an advanced Web application firewall called SonicWall.
DenyAll – DenyAll is a French security vendor offering a WAF appliance as part of its next-generation Web security solutions.
F5 – F5 provides its BIG-IP family of solutions including a Web Application Firewall product. The product is designed to support so-called positive and negative security models (e.g., white and black listing) to improve accuracy and reduce false positive rates in WAF policy mediation.
5nine – The small company offers the 5nine Web Application Firewall with Microsoft server integration and support for Hyper-V.
Fortinet – As part of its product line, Fortinet offers enterprise customers the FortiWeb WAF solution. Fortinet has always offered solutions that are well integrated across its entire product line. CISO teams using other Fortinet products, and that also desire a WAF, would be wise to strongly consider the FortiWeb WAF.
Forum Systems – Forum Systems provides an API gateway for secure integration across Web applications, services, and infrastructure. API gateway solutions are well positioned to support transition to virtualization where cloud workloads sharing Web traffic would benefit from WAF arbitration.
Imperva – Imperva offers customers a range of advanced Web application firewall solutions including SecureSphere. The solution is enhanced by a real time threat stream service from Imperva that feeds the WAF with live updates.
NSFOCUS – NSFOCUS offers a Web application firewall solution with coordinated blacklist and whitelist capabilities as part of DDOS and network security offering.
Penta Security – Penta Security offers a Web application firewall product called WAPPLES.
Port80 Software – Port80 Software includes the ServerDefender VP host-based Web application security solution.
PrivacyWare – PrivacyWare offers Web application firewall and intrusion prevention software for Microsoft IIS.
Qrator Labs – Qrator Labs is a Russian firm that provides the Wallarm WAF solutions over the Qrator network working in coordination with DDOS protection solutions.
Qualys – The well-known cyber security company Qualys includes a next-generation cloud-based Web application firewall solution. Qualys has such good technology

support for its security offerings that CISO teams will rarely go wrong selecting its products. Qualys has also understood and implemented cloud-based security solutions as long as any vendor in the industry. Qualys also manages the IronBee open source Web application firewall software solution.
Radware – Radware offers enterprise customers the AppWall Web application firewall.
Shaka Technologies – Shaka Technologies includes the Ishlangu Web Application Firewall product.
SilverSky – SilverSky provides Web application firewall solution as part of its cloud security services.
SiteLock – SiteLock offers enterprise customers the TrueShield Web Application Firewall.
Sophos – Sophos includes enterprise WAF solutions as part of the Cyberoam and Astaro acquisitions.
Sucuri – The small company located in Delaware offers the CloudProxy Web Application Firewall.
TrustWave – TrustWave provides Web Application Firewall appliance for real time continuous security protection. Existing TrustWave platform or MSS customers would be wise to consider use of this WAF offering to ease integration.
United Security Providers – United Security Providers is a Swiss firm that includes the USP Secure Entry Server for Web security access management.
Wallarm – Located in Russia, Wallarm offers a Web application solution for defending Web front-ends and APIs.
Zscaler – The Web security firm, which pioneered cloud-based security filtering in the network, includes cloud-based next-generation firewall capability including WAF.
Zenedge – Zenedge markets a Web application firewall capability embedded in the ZenEdge DDOS protection solution.

Additional Web Application Firewall Providers

Armorlogic – Armorlogic provides the Profense Web Application Firewall and load balancer.
Brocade – The technology company from San Jose offers enterprise customers the Brocade Virtual Web Application Firewall solution.
Ergon – The Swiss company provides an enterprise security solution called Airlock WAF.
Kemp Technologies – Kemp integrates Web application firewall functions with load balancing offers.
NinjaFirewall – Embedded in WordPress and applicable to PHP, the Ninja Firewall is essentially a Web application firewall.
Positive Technologies – Positive Technologies focuses on retail point-of-sale and includes security and WAF capabilities for its customers.

Riverbed – Riverbed provides tools for Web caching and optimization of traffic with WAF capability embedded.
Sungard – Sungard includes managed WAF as part of its availability services for business.

7. Web Fraud Prevention

⇒ *Web Fraud* –The traditional confidentiality, integrity, and availability (CIA) model for cyber security is deficient in its omission of fraud as a threat.
⇒ *Integrated Solutions* – CISO teams have different options for preventing fraud in Web services ranging from endpoint security to transaction profiling.
⇒ *Advanced Analytics* – The algorithms for mitigating Web fraud will continue to require improved analytics to keep up with clever fraudster tactics.

The most commonly cited taxonomy of cyber threats is the so-called CIA model, which includes confidentiality, integrity, and availability as the primary security concerns. This taxonomy is repeated in textbooks frequently, and is memorized by students working toward their Certified Information Systems Security Professional (CISSP) certification. Surprisingly, however, an additional threat use case exists – in fact, it has *always* existed – and it simply does not match any of these CIA categories. The use case corresponds to the familiar occurrence of *fraud*.

The two salient aspects of fraud are the *deliberate use of deception* and the *motivation to achieve monetary or personal gain*. In essence, fraudsters deceive in order to steal. While fraud has existed for centuries, it fits poorly into the CIA model, since "deception to steal" constitutes neither loss of secrets, degradation of assets, nor blocking of resources. Fraud is thus a fourth type of threat to the enterprise, and any organization handling money, such as any financial services firm, retail organization, or e-commerce site, will be particularly susceptible.

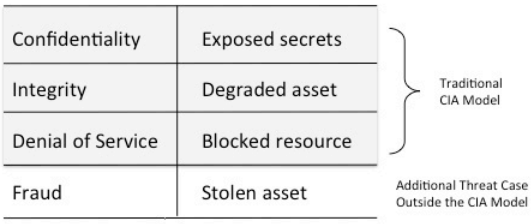

Figure 7-1. New CIAF Model of Cyber Security

The occurrence of fraud in the context of Web services is referred to as *Web Fraud*, and a plethora of different anti-fraud solutions exists across the Web services industry to deal with the growing problem. Perhaps more than any other type of threat, security solutions to Web fraud tend to be all over the map. In fact, virtually every security solution vendor, from firewall platforms to log management tools will

list Web fraud prevention as one of their benefits. This is certainly true in a holistic sense, since good security will help stop all types of threats; but specific approaches *do exist* to reduce the risk of fraud in Web services – and CISO teams should understand how these work.

The first type of anti-fraud solution for Web services involves dealing directly with *endpoints*. The collection of data about a user endpoint for the purpose of establishing normal patterns of user access has become one of the most common techniques for dealing with fraud. Consumers and business users are familiar with this approach, and are rarely surprised when a service provider makes contact with a user after a browsing or other user session is initiated from a device that has not been previously seen. This type of approach is definitely useful and recommended for dealing with straightforward types of user spoofing, but it is generally not considered a *strong* anti-fraud measure.

The second type of anti-fraud solution involves Web session *navigation analysis* on the target site. The Web fraud security system analyzes Website traversal statistics, links passed, and time spent on certain parts of a Website to detect possible fraud. Specifically, user behavioral profiles help determine whether a given session has been initiated by someone who has stolen the credentials of an authorized user. This is not an easy task, and vendors are using proprietary analytic methods to develop competitive advantages. As one might expect, high false positive rates abound in navigational analysis. The innocent act of skipping over several steps in a software wizard, for example, is often mistaken for fraudulent activity.

A third type of anti-fraud solution for Web services involves the examination of *transactions* for the purpose of detecting anomalies. The algorithmic method here involves comparison of an observed transaction with what are believed to be normal profiles of transactions. The financial services industry has the most mature notion of transaction behavior, and has been more aggressive in deploying solutions in this regard. This is a tough area to master, because fraudulent transactional behavior can be subtle, easily masquerading normal activity. As an early example, the "salami" attacks in the 1980's and 1990's involving transactional theft of miniscule percentages of financial activity proved particularly tough to stop.

All of these anti-fraud solutions for Web services will generally work together in a defense-in-depth architecture. Threat intelligence feeds, for example, provide a dimension of effectiveness in anti-fraud solutions that ensures up-to-date information for any behavioral or profile-based methods. Similarly, email solutions that address phishing are often complementary to anti-fraud systems, to the point where some vendors such as Easy Solutions actually integrate the approaches into a common, end-to-end solution. CISO teams should therefore start the Web anti-fraud conversation with recognition that multiple techniques will be required.

Strong authentication for example, is certainly complementary to any type of anti-fraud solution, but is obviously less effective in cases of account theft or takeover. This is a particular challenge in environments where fraudulent activity occurs in the presence of authorized access to data. When a contact center, for example, is given access to personal data in order to assist customers, the potential

exists that they will misuse this access for personal gain – as in, for example, selling identity information to criminal groups. Adding authentication will do little to stop the problem, since the access is already authorized. Techniques such as data masking, least privilege controls, and stricter auditing are about the best one can do with current technology.

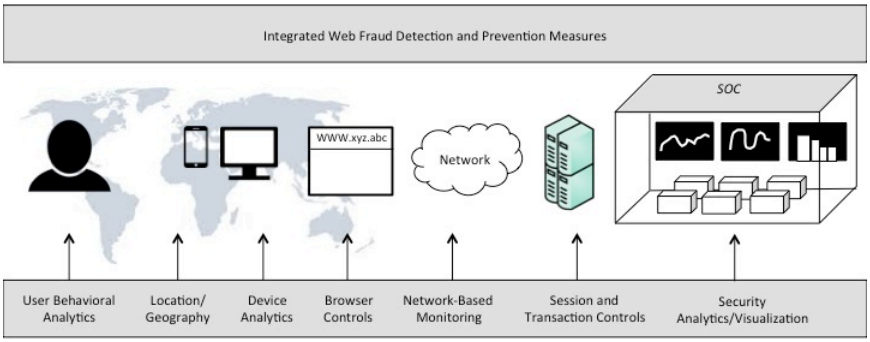

Figure 7-2. Combining Web Fraud Measures into a Common Approach

Some cyber security vendors are innovating in the detection and prevention of Web fraud. Advanced machine learning techniques in security analytic processing to reduce false positives is one example. Systems with feedback loops that flag and learn from false positives can potentially become accurate predicators of errant behavior. Another area of innovation is the visualization of a user transaction or Web session so that analysts can visually replay the activity to determine levels of security risk.

The desired mitigation, whenever Web fraud is suspected, is obviously to stop whatever transaction is occurring and to initiate appropriate measures to takedown the stolen accounts. Since evidence is rarely associated with a clearly drawn delineation, most Web anti-fraud solutions make use of risk measures to identify high-risk users. The entire process becomes probabilistic in nature, which suggests that risk will always exist that Web fraud prevention solutions will produce some level of occasional business interruption. Anyone who has ever had a credit card declined because the issuing company detected fraud will understand this point.

A typical enterprise and network architectural arrangement for many popular gateway Web fraud security solutions involves either local platforms in the form of on-premise appliances or software that reside between users and Web server content, or cloud-based fraud detection solutions that require data collection from the user-to-Web session path. In either case, the mitigation path will vary, depending on the specifics of the Web services being offered. The harshest mitigation, obviously, involves termination of the session and the user account based on observed behavior.

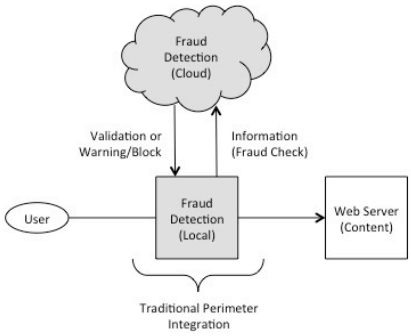

Figure 7-3. Local and Network-Based Gateway Web Fraud Detection

With such a hodge-podge of methods for dealing with Web fraud, and with the view here that holistic treatment across the cyber security spectrum will be the best way to minimize the risk of Web fraud, predicting market trends is tricky. Nevertheless, the following observations are made with respect to the anti-fraud marketplace for Web services:

- *Migration to Mobile* – Business and personal applications will increasingly migrate from Web apps that *happen* to be available for mobile to the reverse: Mobile apps that *happen* to be available on the Web. This will shift the focus in fraud detection and prevention to mobile broadband.
- *Improved Application Profiling* – Rather than rely solely on man-in-the-middle fraud detection within user sessions, increased emphasis will be placed on profiling the holistic behavior of an application to detect misuse. In some environments, this technique is referred to as watermarking, which is unfortunate, since it produces confusion with the cryptographic method of the same name.
- *Improved Authentication* – Newer forms of identity validation based on roles, privileges, and need-to-know will become more complementary to existing Web fraud prevention technology.

CISO teams should recognize that as long as money or valued assets are available to be stolen, individuals and groups will always attempt to commit theft. As such, the risk of fraud in the presence of valued assets will always be present; and the corresponding goal of anti-fraud technology and programs will be to minimize this business risk. C-suite executives and corporate directors should understand this situation, since board risk committees have had to make the point for years that risk reduction is different than risk removal.

For all of these reasons, business trends for vendors and usage trends for CISO teams in the Web fraud prevention market will be *strongly positive* for the foreseeable future. This positive trend will be sustainable for as long as the value of assets on the Internet continues to grow, and the skillset on the part of offensive actors continues to improve.

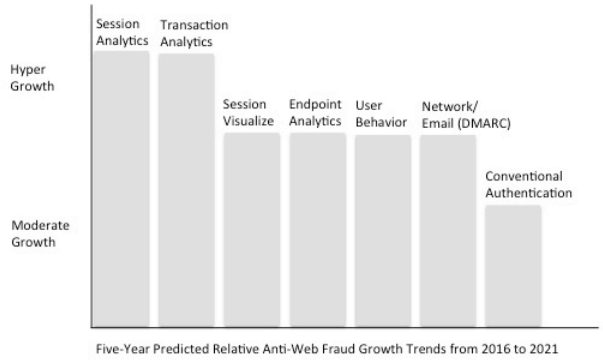

Figure 7-4. Trends in Web Fraud Prevention

Some anti-fraud techniques, such as advanced session analytics based on behavioral profiling, will see more aggressive growth than other techniques such as the use of conventional user authentication to reduce fraud. But all areas in this marketplace should see healthy growth for a long period of time. Venture capital is also likely to continue flowing in this direction for some time.

Since the use of advanced analytics is clearly an important part of the anti-fraud ecosystem for Web services, CISO teams addressing Web fraud should perform their source-selection in concert with evaluation of security analytic vendors. This holistic approach is consistent with the view that Web fraud, like most other cyber risks, is best addressed through multiple layers of complementary cyber defense.

Web Fraud Prevention Providers

Virtually all of the Web Fraud product vendors listed below provide a range of heuristic, behavioral, and account-related techniques for detecting potential fraud or misuse of Web resources such as e-commerce systems. Some e-commerce chargeback risk vendors are listed as well, even though they sometimes work in areas somewhat divorced from the CISO team role. If a CISO team works in an industry where payment fraud and chargeback are issues, then the tiny sampling of vendors included might be a useful starting point, although nowhere near a comprehensive listing.

2017 TAG Cyber Security Annual
Distinguished Web Fraud Prevention Providers

Easy Solutions – Ricardo Villadiego and his capable team at Easy Solutions were kind enough to spend time with me on multiple occasions explaining the need for an integrated, end-to-end solution for Web fraud prevention. During my own career, I was well aware of many different point solutions that looked for things like odd

browser behavior, but the Easy Solutions team explained how a fraudster might slip through any singular defense that does not include end-to-end seamless controls from the user to the Web application. I am grateful to Ricardo's team for helping me understand this important aspect of the modern cyber security equation.

2017 TAG Cyber Security Annual
Web Fraud Prevention Providers

Agari – Agari's DMARC protections are an important component of any enterprise approach to reducing fraud across email and domain usage.
Agilence – Agilence provides exception-based reporting for retail payment fraud prevention.
Attachmate – Attachmate offers a range of enterprise security products including fraud and misuse management.
Caveon – Caveon offers digital forensics and security audit services to prevent test fraud in schools. This is a growing type of solution for academic environments.
Easy Solutions – Easy Solutions offers a comprehensive end-to-end total solution for dealing with Web fraud. Perhaps more than any other company, Easy Solutions focuses on offering the various pieces of the puzzle to provide a true defense-in-depth architecture from a common vendor.
F5 – The F5 Web Fraud Protection solution detects potential fraudulent activity and secures transactions.
Forter – Forter provides so-called frictionless fraud prevention for online retail systems.
41st Parameter – The company, now part of Experian, offers global fraud management solutions for financial institutions
First Cyber Security – The company offers independent verification of Website authenticity to reduce fraud risk.
FraudCracker – FraudCracker provides a platform for reducing fraud risk through anonymous employee reporting.
Guardian Analytics – Guardian Analytics provides behavior-based fraud detection software and services.
IBM – IBM offers the IBM Security Trusteer fraud prevention solution for advanced malware and on-line fraud detection.
Iovation – Offers device-based solutions for authentication and fraud prevention by detecting payment fraud, account takeover, and other misuse.
Imperva – The company offers threat intelligence and fraud prevention as part of its Web application security solution.
Intellinx – Intellinx supports enterprise fraud management through data collection and analysis to detect account and transaction anomalies.
Kaspersky – Kaspersky Fraud Prevention for Endpoint (KES) is designed to prevent security incidents and fraudulent activity.
Kount – Kount is an Idaho-based firm that provides anti-fraud solutions for e-commerce merchants.

Network Kinetix – Network Kinetix offers business assurance and anti-fraud solutions for carriers to improve revenue assurance.
NuData – NuData offers a behavioral analytics platform for reducing the risk of on-line fraud.
Pindrop Security – Pindrop Security provides solutions for detecting ad preventing phone scams and fraud in call centers.
RSA – The well know security firm offers industry-leading Web fraud prevention through its SilverTail product, obtained through acquisition. Silver Tail offers an appliance solution that integrates seamlessly with Web servers to detect fraud.
ThreatMetrix – ThreatMetrix refers to itself as a Digital Identity Company, which emphasizes the important role identity plays in helping businesses prevent fraud.
Trustev – The company, part of TransUnion, offers on-line fraud prevention based on contextual pattern matching.
VU Security – VU Security focuses on intelligent transaction analysis for behavior-based fraud detection.
Webroot – Webroot provides advanced online fraud prevention for PCs and mobile devices.
Whiteops – Whiteops provides a solution for preventing botnet fraud in on-line advertising. Increasingly, advertising has become a base for fraudulent activity.

Additional Web Fraud Prevention Providers

Accertify – Accertify is a provider of fraud prevention, chargeback management, and payment gateway products and services.
CyberSource – CyberSource offers online payment fraud management across multiple channels and devices.
Feedzai – The machine learning platform from Feedzai focuses on fraud and risk from a cloud-hosted or on-site deployment.
Hybrid Security – Hybrid Security offers third generation heuristic Web fraud prevention.
MaxMind – MaxMind offers IP intelligence and online fraud prevention tools that leverage Geolocation.
NoFraud – NoFraud provides e-commerce risk management through transaction analysis to determine pass and fail decisions.
Signifyd – The company focuses on e-commerce fraud prevention and chargeback risk by approving orders via certified fraud experts and technology.

8. Web Security

⇒ *Web Security* – Tactics for securing Websites, applications, and services include administration, scanning, filtering, policy mediation, and encryption.
⇒ *Web Security Gateway* – The dominant current implementation for enterprise Web security support is the Web Security Gateway (WSG).

⇒ *WSG Evolution* – WSG security functionality is evolving toward software-based, virtualized support for enterprise cloud workload Web access.

The original purpose of *Web Security* was to stop site defacement by vandals. While this remains an important task, the general control area has evolved toward the more critical task of protecting the enterprise from the effects of malicious inbound or outbound Web-based activity. The dominant tool for performing such protection is called a *Web Security Gateway (WSG)*. In particular, the WSG provides threat intelligence-powered URL filtering of enterprise Web egress and ingress traffic either from a cloud or perimeter gateway vantage point. The WSG is one of the most important aspects of any modern protection architecture against APT attacks.

CISO teams often describe the outbound filtering aspect of their WSG as a safety net in case malware happens to find its way into the enterprise and attempts to exfiltrate data. By forcing outbound proxy interrogation at the WSG, perhaps with man-in-the-middle interruption and user interrogation of the browser session, CISO teams can make sure external connections to Websites are only established with vetted or categorized sites. This method also helps with the enforcement of acceptable use policies for Website access in the enterprise.

WSG solutions thus offer needed protection between the enterprise and the Internet via URL filtering, data leakage prevention (DLP), malware detection, and Web application controls. When an enterprise requires flexible access controls for users connecting to external servers, *forward proxy* functionality in the WSG enforces policy, keeps track of requests, and provides an intermediary between users and external services. In contrast, when an enterprise wants to make its servers available to external users, *reverse proxy* functionality in the WSG works in much the same manner, except supporting inbound requests.

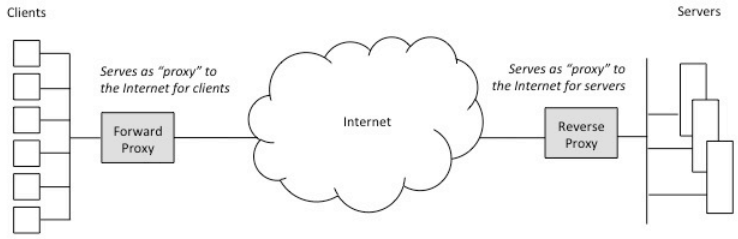

Figure 8-1. Forward and Reverse Proxy

As suggested above, a popular feature in many WSG solutions involves so-called outbound browser "speed bumps" that interrogate or block outbound connections to sites that are uncategorized by the WSG threat management system, usually supported by a real-time feed of URL-related intelligence. Speed bumps provide effective APT data exfiltration protection since most advanced infections involve use of uncategorized infected sites for storing stolen information. It is hard to imagine any exceptional business requirement in any enterprise that would sufficiently

warrant not running speed bumps at the WSG outbound gateway. Stated more simply: CISO teams need to implement speed bumps for outbound connections – *period*. A typical WSG use case for uncategorized site access is depicted below.

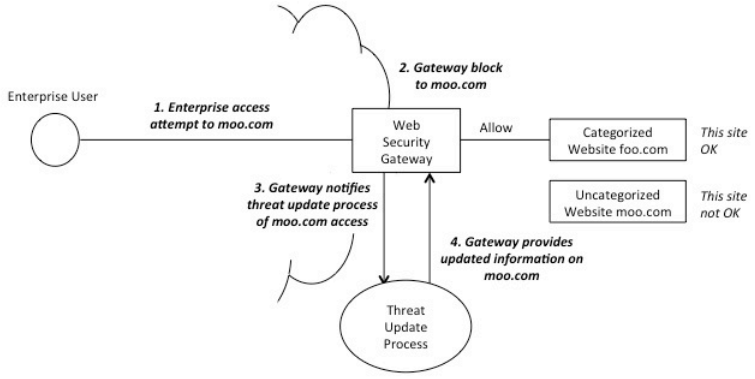

Figure 8-2. Web Security Gateway Uncategorized Site Use Case

The assumption in the use case shown above is that the WSG is positioned at the edge of the enterprise perimeter. A more flexible, albeit less controlled version of this architecture involves the gateway being positioned in the wide are network or on the public Internet. Such a network-based approach is consistent with cloud computing architectures and useful for companies that are evolving away from a traditional enterprise network. The following diagram depicts a typical network-based WSG arrangement for an enterprise user.

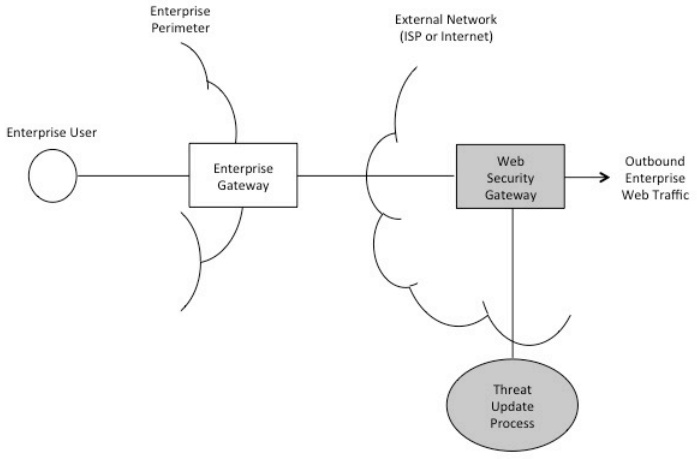

Figure 8-3. Network-Based Web Security Gateway

The near-term market trends for WSG solutions will continue to be impressive. As companies continue to experience significant APT problems, and as enterprise architectures shift to more complex, virtual arrangements, the need to have a

dependable safety net through outbound proxy-based speed bumps or blocks on uncategorized Web access will become ever more important. Companies in this category will thus continue to see dramatic growth in revenue and market capitalization. One would also expect a vibrant marketplace here for public offerings and acquisitions.

As enterprise infrastructure shifts toward more virtual operation, however, the manner in which WSG functionality is provided will shift dramatically. In particular, virtualized protection for cloud workloads in a more dynamically arranged architecture (including micro-segmentation) will be the natural way in which Web traffic is protected from attack. Orchestration of threat intelligence to distributed WSG functions located within multiple micro-segments will emerge as the new challenge. Luckily, not all cloud workloads will require filtering and interrogation of Web traffic, which is why the East-West APT risk drops so dramatically in micro-segmented virtual enterprise arrangements.

Given all of these different WSG industry shifts and pressures, the expected market trending for WSG solutions involves leveling off of enterprise-hosted WSG at the perimeter, with commensurate linear growth in network-based WSG solutions in the cloud. The most dramatic growth will occur for WSG functions embedded in on-demand virtualized provisioning as one finds in the SDN solutions being implemented by ISPs for wide area traffic and by data center managers to reduce costs.

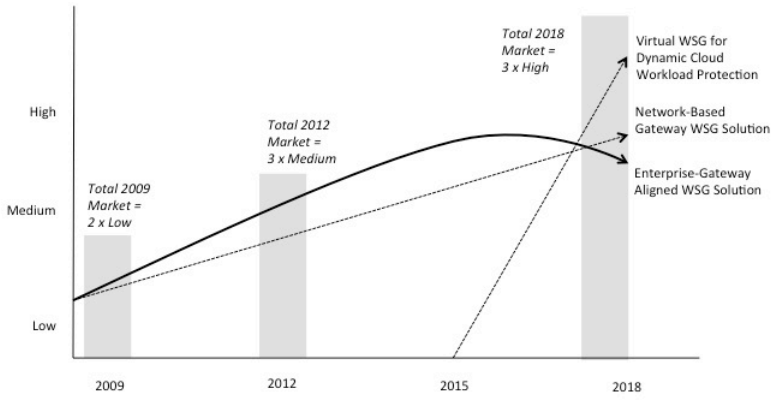

Figure 8-4. Web Security Gateway Market Trends

An additional market force is that as Web traffic continues to shift toward mobile apps, WSG products will have to incorporate better support in this area. One could see "Mobile App Security Gateway" becoming an important complementary area. In addition, the usual challenges for encrypted traffic across security gateways is also true for WSG solutions. As such, the importance of integration with encryption architectures for decryption of the browsing session will become important for WSG deployments.

Furthermore, as applications move toward the use of mobile ecosystem arrangements, the likelihood that malware will target cloud hosted applications increases. If the app is hosted in a private cloud, then the enterprise WSG solution can deter Web exfiltration. But if the app is hosted in a public cloud, then some public cloud-hosted WSG, probably hosted in cloud access security broker (CASB) real estate, will be needed to integrate with the enterprise policy enforcement. With the introduction of software defined network (SDN) infrastructure from Internet service providers (ISPs), integration of Web security solutions with service chaining in SDN will become a more common practice in the future.

Web Security Product Providers

The majority of the *Web Security* product vendors listed below provides WSG gateway solutions with URL filtering via forward and reverse proxy platform solutions. Many of these vendors also offer Web acceleration solutions for the enterprise as well. Some vendors offer Website scanning and related Website security administration and encryption protections that are also included in this category.

Increasingly, Web security solutions from vendors will become embedded in virtualized access to cloud via mobile devices. Managed security service (MSS) providers are extremely well positioned to take advantage of this trend. This software-defined initiative is covered in the managed security service provider section of this report.

2017 TAG Cyber Security Annual
Distinguished Web Security Providers

Blue Coat Systems – My friendship with the principals of Blue Coat Systems goes back many years. It includes a partnership with Hugh Thompson started a decade ago, when we collaborated on a series of cyber security talk shows filmed in front of live studio audiences. When I began this project, the Blue Coat team was an enthusiastic supporter, offering invaluable advice and technical guidance on the direction of the Web security marketplace, and related areas such as cloud security and CASB. And for this help, I am so grateful. During the very final stages of this project in 2016, the Symantec acquisition of Blue Coat was announced, with my good friend Greg Clark assuming the role of CEO. Since the integration was just underway as this writing was largely complete, the two companies are covered in this report separately.

Forcepoint – I was so happy when my colleague and friend David Barton assumed the role of CISO for the newly commissioned Forcepoint. I was further impressed when industry veteran Matt Moynahan took over as CEO. Through numerous technical and market discussions with David during my research, I came to better understand the power of the Raytheon and Websense legacies in creating an innovative new means for establishing Web security and related cyber protections

for the enterprise. My thanks are offered to the Forcepoint teams for their valuable assistance with this project and initiative.

2017 TAG Cyber Security Annual
Web Security Providers

Banff Cyber – The Singapore-based company focuses on prevention of Web defacement.
Barracuda – The well-known security company offers the Barracuda Web Filter, which is a comprehensive Web Security Gateway.
BeyondTrust – BeyondTrust includes the Retina Web Security Scanner for protection of Web applications.
BinarySEC – The French company provides a managed security solution for reducing the risk of Website attacks.
Bloxx – The Bloxx Secure Web Gateway, now part of Akamai, focuses on so-called *zero-second* protection for users.
Blue Coat – Blue Coat, now part of Symantec, provides industry-leading Web security gateway services based on forward and reverse proxy technology. The company has been successful in growing its base considerably in recent years through both acquisition and native sales growth, often through partnerships with international VAR solution providers.
CA – CA offers the Web Services Security platform (formerly CA SiteMinder Web Services Security).
Celestix – The CelestixEdge platform includes a range of Web Application Proxy capabilities.
Check Point Software – The famous security company founded by Gil Schwed includes Web security in its extension portfolio of cyber security products and services for the enterprise.
Cisco – Cisco's Web Security Appliance, Cloud Web Security, and Cloud Access Security offer a range of Web security protections.
Clearswift – The UK-based Clearswift SECURE Web Gateway focuses on incoming and outgoing Internet communications.
CloudFlare – CloudFlare, based in San Francisco, provides acceleration, domain, and security services for Websites.
ContentKeeper – ContentKeeper, headquartered in Australia, provides Web threat protection and Web filtering on their next-generation platform.
DeepNines – The Dallas-based company provides a unified security gateway solution for enterprise.
Distil – Located in Arlington, the company protects Websites from botnet attacks and data mining.
EdgeWave – EdgeWave provides cloud-based remote Web filtering services via an appliance solution.
FireEye – FireEye offers an industry-leading Web and network security solution for detecting and preventing APT attacks.

First Cyber Security – The UK firm includes Web security in its portfolio of anti-fraud and cyber security solutions.
Forcepoint – The acquisition of Websense moved Raytheon into the commercial Web security solution business. Forcepoint offers an integrated portfolio of solutions with the discipline and advanced strategic and tactical information assurance expertise of Raytheon.
Fortinet – Fortinet includes Web security gateway functionality in its extensive security product line.
GFI Software – Located in Luxembourg, GFI's WebMonitor product helps control Web activity and avoid Web-based threats.
iBoss – The iboss Cloud Secure Web Gateway Platform offers a range of Web security capabilities.
Imperium – Now part of Google, the group provides automated tools for removing malware from Websites.
Imperva – Imperva includes a range of advanced Web security protections in its fine set of WAF and DDOS offerings for enterprise customers.
Intel Security (McAfee) – Intel continues to offer the McAfee Web Gateway solution for analyzing Web traffic.
Litous – Located in Iceland, Litous provides a range of Web security products including the Malware Spider.
Menlo Security – The start-up led by Amir Ben-Efraim includes Web security in its unique isolation technology.
Netsparker – Netsparker, located in the UK, offers a Web application and vulnerability scanning solution.
Panda Security – Headquartered in Spain, Panda Security offers the GateDefender solution for business that includes filtering for Web browsing.
Penta Security – Located in Seoul, Penta offers its customers Web security capabilities in its offerings.
Port80 Software – The San Diego-based company provides Web security in its range of WAF and application security solutions.
PortSwigger – PortSwigger markets testing tools and solutions for Web application security.
SafeNet (Ingenico) – Ingenico offers an XML-based cryptographic hardware security module for integrating security services into Web applications.
Sangfor – Sangfor provides its Internet Access Management gateway for securing Web traffic.
Sentrix – Sentrix offers Web security through its Infinite security solutions for enterprise.
Shaka Technologies – The UK firm includes Web security capabilities with its load balancing, acceleration, and related network security functions.
Shape Security – Shape Security provides protection of Web content from automated attacks such as botnets.
SiteLock – Located in Florida, SiteLock provides WAF and Web security capabilities for customers.

Smoothwall – Originating in the UK, Smoothwall provides content-aware Web security filtering and gateway functions.
Sophos – The Sophos Cloud Web Gateway offers secure Web gateway functionality for enterprise.
Spikes Security – The Los Gatos firm includes Web security features in its isolation technology.
Sucuri – Sucuri offers Web security capabilities to completely its WAF and DDOS protections.
Symantec – The Symantec Web gateway offers content filtering and related data loss protections. Integration with Blue Coat will enhance Symantec offerings in this area.
Tinfoil Security – Tinfoil Security provides both Web security and vulnerability management solutions.
TrendMicro – The TrendMicro InterScan Web Security Virtual Appliance provides Web security functionality.
TrustWave – TrustWave includes Web security gateway functionality in its product line tracing back to its M86 Security acquisition in 2012.
Webroot – The California-based company includes Web security in its portfolio of endpoint and Internet security solutions.
WhiteHat – The Santa Clara-based firm provides the WhiteHat Sentinel product, which offers continuous security assessment for Websites.
Zscaler – Zscaler offers cloud-based Web security gateways across its global infrastructure. Zscaler pioneered Web security proxy solutions in the cloud, focusing on network-based security, before most companies knew it was an option.

Additional Web Security Providers

Acunetix – The vulnerability management company includes solutions for Website security.
CronLab – CronLab provides an Integrated Web Filter solution for business customers.
Optenet – Optenet is a Spanish company providing multi-tenant Secure Web Gateway product.
Total Defense – The company merged with Untangle to provide security solutions for Internet browsing and application protection.
WebTitan – The company offers the WebTitan Gateway, which includes content filtering and related security controls.

9. CA/PKI Solutions

⇒ *CA/PKI* – Requirements for secrecy and digital signatures led to the development of certification authorities and their support infrastructure.
⇒ *CA/PKI Support* – The majority of enterprise CA support today consists of signing services for e-commerce sites.

⇒ *Evolving CA/PKI Need for Mobile/IoT* – With the progression to mobility and IoT, the need for certificates as a strong authentication factor will increase.

The primary purpose of a *Certification Authority* (CA) is to issue digital certificates, usually to support protocols such as the Secure Sockets Layer (SSL) or security processes such as software code signing. Digital certificates offer a trusted means for binding public keys to identities. The resultant certificate can be distributed to entities to support secure interactions and connections, such as e-commerce sites accepting credit cards.

The security features supported by certificates usually include secrecy and digital signatures. CA services are usually considered a fundamental component of a larger framework known as *Public Key Infrastructure* (PKI). Many companies also provide broader PKI services, including integration and consulting services. PKI services have traditionally been viewed as complex and difficult to scale, although infrastructure support has improved in the past decade.

The deployment of certificates into Web browsers was one of the fundamental contributions from Marc Andreessen at Netscape in the 1990's. By hardcoding public key certificates for CAs directly into the browser, end users could decrypt certificates from merchant Websites signed by any CA that has prearranged a deal with the browser vendor. This revolutionary idea and the associated ecosystem shown below created a small industry for CAs, and a massive industry for on-line sellers such as Amazon.com.

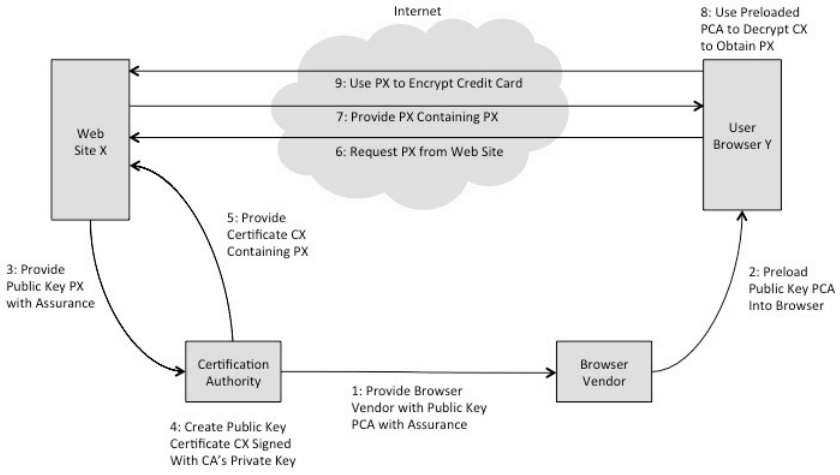

Figure 9-1. Certificates in Browsers for e-commerce Support

The certificate marketplace includes many different options for buyers and sellers. Enterprise CISO teams must be careful, however, to properly vet the background and reputation of any selected CA vendor. Since a CA essentially sells trust, this reputation is especially critical to the selection process. Some of the more common certificate types from CAs that arise in practice include the following:

- *Domain Validated Certificates (DV)* – These are typically lower priced certificates, popular with smaller businesses, issued based on low assurance verification that the certificate is being delivered to the correct owner of the requesting domain.
- *Organization Validated Certificates (OV)* – These certificates take into account the requesting company name and address, resulting in slightly higher assurance identity validation.
- *Extended Validation Certificate (EV)* – These are higher assurance certificates that require company review by the Certification Authority/Browser (CAB) Forum. Browsers designate a Website with an EV certificate by turning the address bar green.
- *Wildcard Certificates* – These are essentially parent certificates that are issued to secure a single domain, as well as any sub-domains that might exist or be added in the future.

Regardless of the certificate type or assurance level associated with the certificate issuance, a clear trend in the certificate marketplace involves the increasing demand for encryption of virtually all traffic on the Internet. This extends beyond basic browser sessions to merchant Websites, to now include Internet of Things (IoT) traffic, as well as the emerging Industrial Control System (ICS) support required across the Internet.

Mobility usage in the enterprise also drives the need for certificates as an additional strong authentication factor. Users with mobiles can use thumbprint biometrics to unlock devices, followed by certificate management from device to server handled by mobile device management (MDM) systems. This can also include a third authentication factor in the form of a password or PIN. This is a powerful strong authentication approach, and the certificates are desirable because they are invisible to the user.

One area of potential hyper-growth in the PKI area is the need for proper protection of keys and certificates during their lifecycle application. This is a newer concern for more CISO teams, since so few compliance auditors and regulators understand this critical concern. Vendors such as Venafi have done a good job creating the products and services for protecting keys and certificates that will become the base for a new sub-industry in the area of CA/PKI solutions for enterprise.

Given all of this, three specific business trends will occur in the CA/PKI marketplace. First, the need for certificates will grow steadily, along with the need mentioned above for proper protection of keys and certificates. However, with such a low barrier to entry for new certificate issuers, the unit cost for certificates will continue to drop. The end result is a somewhat flat view of the overall CA/PKI marketplace, albeit with some participants benefiting directly from the increased usage and protection needs for certificates, especially in IoT.

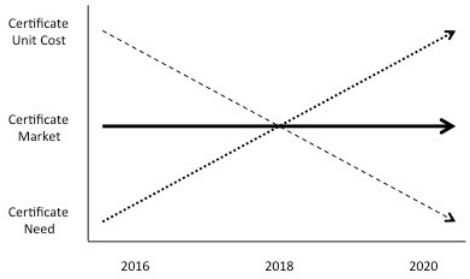

Figure 9-2. Certificate Market Trends

In spite of the relatively flat expectation for certificates, the professional service marketplace for PKI, especially in larger enterprise, will flourish. The high level of complexity required to integrate PKI and certificates into evolving enterprise, browser, cloud, application, mobility, and virtual computing environments will keep expert PKI security consulting groups busy for many years. Companies such as Google and Microsoft who embed this technology into their products will also be busy finding ways to make the cryptography and support invisible to users, but also meaningful in terms of security.

In addition, digital certificates and public key infrastructure capabilities also enable new types of services such as Bitcoin/block chain and security-enhanced versions of infrastructure protocols such as the Domain Name Service (DNS) and the Border Gateway Protocol (BGP). Furthermore, with the expansion of IoT, it is entirely possible that embedded security solutions will require PKI-based support, which could lead to significant growth. So these new areas might help CA/PKI solution providers identify meaningful growth opportunities.

In this evolving market, CISO teams should be especially certain to match their assurance needs and budget to the selected certification authority. For high traffic Websites with large revenue, the time, effort, and cost associated with higher assurance certificates with CAB certification are recommended. For smaller businesses, more options are available at lower assurance levels, albeit with some risk. CA/PKI providers such as DigiNotar have been hacked in the past and others such as TurkTrust have issued faulty certificates. The lower assurance firms have the highest risk of either being hacked or making a mistake in the future.

In the selection of CA/PKI solutions, CISO teams should also make sure to read and understand any certification authority's public documentation on their assurance processes and data handling. A major issue with any PKI-related product or service is that the trust associated with issuance and operations is basically invisible. The only way to truly understand the level of assurance that should be associated with a certificate is to carefully inspect the CA certification practices. It's been my observation that CISO teams rarely, if ever, bother to really go through Certificate Practice Statements, and this is roughly as neglectful as not bothering to read the rule sets in your gateway firewall.

CA/PKI Providers

Identifying a comprehensive list of global CA/PKI solution providers is a particular challenge for several reasons. First, the number of companies offering CA services with low cost SSL certificates is large and changes frequently. Determining the viability of CAs is therefore not an easy task and generates unreliable results. In addition, many cyber security products and services come with embedded PKI capabilities, but do not qualify as standalone CA/PKI solutions for the enterprise.

2017 TAG Cyber Security Annual
Distinguished CA/PKI Providers

Venafi – I've known Jeff Hudson and his fine team at Venafi for some time. Through this association, I've learned how valuable the protection of certificates and keys can be for enterprise security. During a recent dinner with Jeff in New York City, it became clear to me that CISO teams continue to neglect this important step for their SSL, eCommerce, secure email, and related higher assurance tasks, as evidenced by the many international hacks that have occurred in these areas. Part of my current research involves trying to understand why auditors have not been more aggressive in their demands related to key and certificate protection. Jeff and the Venafi team have been indispensable in supporting this work with their time and expertise.

2017 TAG Cyber Security Annual
CA/PKI Providers

Certicom – Now part of Blackberry, Certicom is a Canadian group that owns the embedded, core Elliptic Curve cryptographic technologies used across the world.
Certified Security Solutions – The professional services firm in Ohio supports projects involving identity, access, and PKI.
CertiPath – CertiPath is located in Virginia and offers a PKI-based trust framework and set of identity services.
Comodo – Comodo provides a full range of SSL certification solutions for small, medium, and large customers.
Cryptomathic – The French firm specializes in data encryption and CA/PKI technologies and services.
CV Cryptovision – CV Cryptovision is a German company focusing on data encryption and CA/PKI solutions.
Deutsche Telekom – The German telecommunications company offers certification authority and PKI services.
DigiCert – DigiCert provides high assurance, low-priced SSL certificates along with code signing and other PKI services. The company acquired Verizon's PKI/SSL business in 2015.
Entrust – Entrust provides a full range of CA and PKI services supporting ten million identity and payment credentials issues daily.

Gemalto – Gemalto has expanded its range of cyber security offerings to include authentication and related support in areas closely connected to PKI.
GlobalSign – GlobalSign offers its customers a full range of personal, SSL, and code signing certificates.
PrimeKey – PrimeKey is a Swedish company that offers open source PKI-based products and services.
Qualys – Although not technically a CA/PKI provider, Qualys provides an SSL server test function for public Web servers to increase assurance.
QuoVadis – QuoVadis provides managed PKI services to assist with deployment of digital certificates.
SafeCipher – SafeCipher offers a range of security consulting services including PKI solutions, PCI services, and encryption.
Symantec – The large cyber security provider offers industry-leading certificates and CA/PKI services including managed PKI.
Thales e-Security – The Thales Group is a French multinational aerospace, defense, and space contractor that offers a range of cyber and data security solutions including CA/PKI capabilities from Thales e-Security.
Thawte – Thawte serves as global certification authority with SSL certificates, code signing, and related PKI services.
TrustWave – TrustWave offers certificate lifecycle management solutions for enterprise customers.
Venafi – Venafi provides enterprise cryptographic key and certificate security solutions.
WISeKey – WISeKey supports communications and data security with personal, corporate, and server SSL digital certificates.
WolfSSL – Located in Washington State, WolfSSL offers an embedded SSL library for devices and IoT.

Additional CA/PKI Providers

ACCV – Agencia de Tecnologia y Certificacion Electronica is a Spanish public entity providing CA/PKI services.
Buypass – Buypass is a European firm that offers enterprise certificates to secure electronic communications and other applications.
Camerfirma – Camerfirma provides electronic security services including PKI and authentication across Spain.
certSIGN – certSIGN is a UTI company providing a range of certification services in Romania.
Chunghwa Telecom – The Taiwanese company provides public certification authority services for SSL and other applications.
CNNIC – CNNIC is a Chinese certification authority group that had some bumpy interactions with Google and other browser vendors in 2015.
Disig – Disig is a Slovakian certification authority and PKI services provider located in Bratislava.

E-Guven – E-Guven is located in Turkey and provides certification authority and PKI services.
E-Tugra – E-Tugra is a Turkish CA/PKI solution provider supporting SSL and related services.
GeoTrust – GeoTrust provides online customer security with SSL and code signing certificates.
GoDaddy Group – The major domain services and hosting provider issues certificates as part of its service.
Hongkong Post – Hongkong Post issues e-Cert certificates signed with a digital signature supported by a Hongkong Post CA root certificate.
IdenTrust SSL – IdenTrust SSL, now part of HID Global, provides a range of standard and multi-domain SSL certificates.
Izenpe – Izenpe is a Spanish X.509 certificate authority owned by the Basque government.
Japanese GPKI – This Japanese Government PKI group provides various CA/PKI services.
Logius – Logius is a digital government service of the Netherlands Ministry of the Interior and Kingdom Relations offers CA/PKI support.
Microsec – Microsec is the largest Hungarian certification authority and PKI supplier of electronic signatures.
NetLock – NetLock is a Hungarian solutions provider offering digital signature, SSL, and related PKI services.
Network Solutions – Network Solutions is a Web hosting provider offers certificates as part of its services.
OpenTrust – OpenTrust supports enterprise and citizen trusted identities with CA/PKI-based solutions.
QualitySSL – QualitySSL offers a full range of high assurance 256-bit encrypted SSL certificates.
Secom Trust – Secom Trust is a Japanese security company offering various CA/PKI services.
Sertifitseerimiskeskus – The Estonian PKI/CA services company provides Certification Centre services.
SwissSign – SwissSign is a Swiss company providing certificates and related PKI services.
StartCom – StartCom is an Israeli firm supporting SSL and related PKI services for the enterprise.
Turktrust – Turktrust is a Turkish firm in Mozilla's root program supporting e-signature, PKI-related R&D, and SSL applications.
TWCA – TWCA is a Taiwanese firm offering certificate services, SSL, PKI software, and certificate hardware.
Unizeto Technologies – Unizeto technologies is a Polish firm providing PKI/CA solutions.

10. Cloud Security

⇒ *Virtualization and Cloud* – Advances in virtual computing have driven growth in virtual data centers, software defined networks, and cloud services.
⇒ *Cloud Compliance* – The regulatory and compliance challenges associated with public clouds will ease across all industries in the coming years.
⇒ *Cloud Security Solutions* – Effective techniques do exist for securing cloud services, including cloud access security brokers and micro-segmentation.

Virtualization in computing has enabled a new class of products and services based on the separation of hardware and software. That is, a new layer of software is created called a *virtual machine* that looks exactly like a real computer and associated operating system. The reality is that applications running on this virtual machine are truly separated from the underlying hardware.

By focusing computing resources on the virtual creation, provisioning, and use of software objects that are decoupled from hardware, great operational flexibility emerges. Obviously, with the ability to create multiple virtual machines on one physical machine, usually orchestrated with software called a *hypervisor*, great hardware savings can be obtained. But several less obvious, but nonetheless consequential opportunities emerge with virtualization, including the following:

- *Data Center Virtualization* – Racked hardware appliances with a physical top-of-rack switch are being replaced with virtual machines running over a hypervisor-based operating system decoupled from the underlying hardware. The primary goals here are simplification of East-West traffic, most of which is between servers in a data center, and cost reduction through hardware procurement savings. This has massive implications for cyber security because East-West enterprise traffic will be controlled within the virtual data center, rather than across the enterprise IP-based LAN.
- *Software Defined Networking (SDN)* – Traditional hardware/software infrastructure in wide area networks is being replaced with a software defined network (SDN) that is managed by an SDN controller reminiscent of the old signaling system found in circuit-switched networks. The SDN controller provides many different advantages from a cyber security perspective for data center and WAN managers. It is also becoming the new point of aggregation for performing enterprise security functions such as IPS.
- *Public, Hybrid, and Private Cloud Usage* – Automated communication between programs over application programming interfaces (APIs) is the underlying technology driving the adoption of ubiquitous cloud services. A useful comparison of virtual data centers and the cloud is that the former involves humans and portal, whereas the latter involves workloads and APIs.

Each of these initiatives comes with unique security requirements. Virtualization of data centers, for example, requires making the perimeter security located around data centers more tightly bound to virtual workloads, which could easily be shifted around on underlying infrastructure. SDN infrastructure in data centers and across large area networks must also integrate proper levels of security. Carriers, for example, must create SDN applications on the northbound SDN controller interface to ensure holistic threat coverage for the entire network.

Virtualization and SDN initiatives certainly have generated some interest in the cyber security product and service community. Vendors have begun to offer solutions that are driven by each of these initiatives. Infrastructure security products that understand SDN standard interfaces, or operating system security products that protect hypervisors, represent an important area of growth, and venture capital is clearly flowing in this direction.

Nevertheless, the vast majority of cyber security investment in the area of virtualization is being directed at *cloud security*. The specific purpose of *cloud security* products and services is to provide data security for enterprise or consumer use of public cloud services. For companies with the ability to create their own private or hybrid cloud infrastructure, cloud security solutions must extend to this use case as well. As a result, general references to "cloud" in this section include virtualized data centers (public and private), XaaS ("as a service") offerings, and public/private/hybrid cloud services. Cloud security products can be grouped as follows:

- *Cloud Security Brokers* – These components reside between users and cloud systems to offer man-in-the-middle security services such as authentication and logging. Usually a broker is designed as a centralized architectural component, but security designers are increasingly trying to build virtual edges that look more like a flexible perimeter than a man-in-the-middle mediation point.
- *Cloud Data Security Solutions* – This includes encryption support to protect sensitive data in cloud services, especially ones with public Internet visibility. Overlaying encryption onto XaaS offerings is easier said than done, because once the data is obfuscated by the cryptography, basic functions such as search are often broken. CISO teams must exercise great care in the selection of a cloud data security solution, focusing on assurance that critical tasks such as forensics, eDiscovery, and search can be performed in the presence of overlay security such as encryption or data masking.
- *Cloud Workload Protection* – These solutions offer perimeter and enterprise-type protections for the cloud workload, either as a micro-segmented perimeter or as an embedded root agent to detect integrity issues. As illustrations, micro-segments are supported through NSX in VMware environments and Security Groups in OpenStack implementations.
- *Application-Specific Cloud Protection* – These solutions target specific SaaS applications such as Salesforce. Increasingly, applications are being

virtualized into the cloud with open interfaces in order to encourage the cyber security community to write protections that can be integrated with the open application.

In addition to the components listed above, a fully end-to-end cloud security solution also requires endpoint security protections including containers and anti-malware software, as well as virtual private network (VPN) connections that are encrypted and authenticated. The generic cloud security architecture driving our analysis here is shown below.

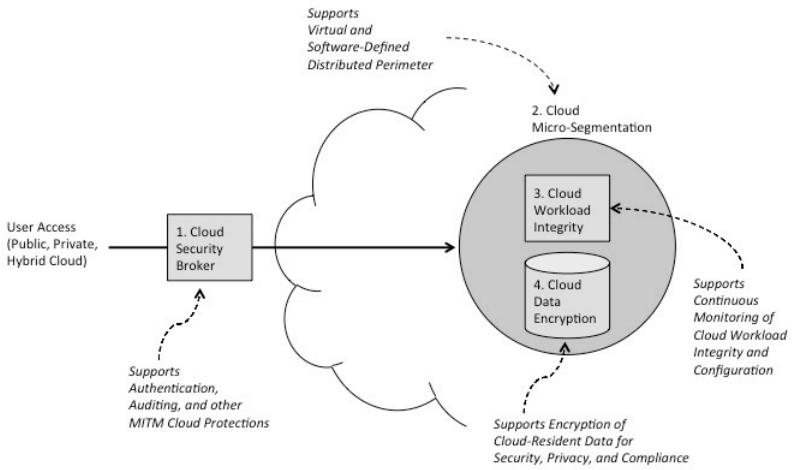

Figure 10-1. Cloud Security Architecture Components

The instantiation of the above capabilities for specific public cloud services such as Salesforce or ServiceNow follows the same schema as shown, but also provides tailored protection for the specific protocols, commands, and utilities in the supported cloud service. CISO teams should consider the pros and cons of this sort of tailored arrangement. For example, embedded security will always work more smoothly and provide more seamless protection than a defensive scheme that sits outside the native application environment. However, a protection solution designed outside the application environment might remain comfortably in place through major changes to the underlying applications.

One of the major challenges for businesses and government agencies desiring public cloud capabilities is that regulators and compliance auditors remain skeptical of the control posture in many popular cloud offerings. While this is a very real issue in the near term for CISOs, especially in financial services, the chances are high that this constraint will ease in the coming years. One reason is that with the exiting perimeter being so porous, changing to external cloud support is at least *different*. The argument that placing data "out there" in the cloud is less safe than keeping it "in here" with perimeter protection, is thin in the presence of rampant APT attacks.

The general marketplace for cloud security protections involves *hyper growth* in virtually every architectural area. This does not guarantee success for all vendors doing virtual solutions, because the competition will be enormous in this area. In addition, the currently fragmented target enterprise market will consolidate toward more common cloud service infrastructure, and public cloud services will begin to offer these capabilities natively. Furthermore, with open APIs in ISP-delivered SDN services, a new market will emerge for on-demand, service-chained security embedded in the wide area network.

The primary need for cloud security will be driven by significant reduction in dependence on corporate perimeters, increased demand for use of mobile devices in business, and increased confidence in the auditable operation of public cloud companies. The diagram below depicts the forces on cloud security growth in the coming years.

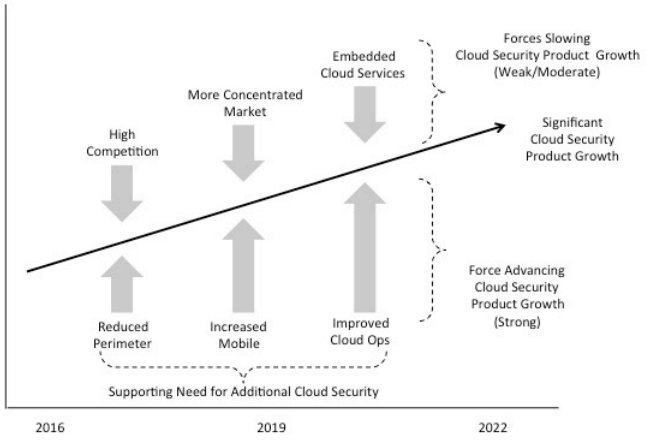

Figure 10-2. Cloud Security Growth Trends

A note on security product virtualization is worth mentioning. As enterprise business moves more and more toward virtualized data centers for their internal applications and systems – driven mostly by cost reduction – the marketplace for virtualized security appliances has grown. This implies that if your data center includes physical firewalls, intrusion detection systems, and log management systems from companies such as Palo Alto Networks, Fortinet, and LogRhythm, then the need arises for virtualized versions that run on cloud operating systems such as VMware or OpenStack. This virtualization trend is supportive of cloud security growth.

What this means for CISO teams is straightforward: Any enterprise cyber security capability being considered for deployment should be required to come with a commensurate migration plan to support future virtualization. This does not mean just demonstrating that hardware capabilities can be simply ported to a cloud operating system, but rather that the overall solution has been redesigned for optimal use in a cloud virtualized environment.

Any security product performance advantages that rely on fast hardware, for example, should be shown to be covered through distribution, replication, or some other virtualized orchestration means to deliver the required performance in a cloud environment. This may not always be possible, but CISO teams should at least demand that the technical and architectural discussions occur.

Cloud Security Product Providers

The vendors listed below under Cloud Security reduce the risk of using public and hybrid clouds. So many vendors reference "cloud" in their product marketing literature, that it can be confusing for CISO teams to determine whether a given product or service was designed for cloud. Providers of SDN and virtualization security product solutions are also included below. ISP SDN service providers are not included in this section, but rather are covered under managed security.

2017 TAG Cyber Security Annual
Distinguished Cloud Security Providers

Catbird – David Keasey and his fine team have become one of my go-to groups when I want to better understand technical issues related to cloud architecture, security, and visibility. I've met with David many times to discuss advanced cloud and virtualization technologies, and my understanding and insights have improved so much as a result. I am truly in debt to Catbird for all of their consistent and willing technical assistance during the production and research associated with this report.
CloudPassage – Carson Sweet from CloudPassage has been an inspiration to me in the area of cloud security and compliance. He first explained to me how he was going about protecting cloud-based technology and systems over sushi in Hoboken. Since then, I've really dug into his innovative solution and it exemplifies the type of protection that is fast becoming the new primary control for any virtualized workload in both industry and government. My thanks are offered to Carson and the CloudPassage team for their world-class assistance.
Netskope – I've known Sanjay Beri from Netskope since his earlier days at Juniper. He has always had such a broad understanding and perspective of cyber security, and his growing team at Netskope helped me understanding the intricacies of cloud access security broker capabilities. Sitting down with Sanjay over coffee in Washington recently, I came to fully realize just how vibrant the CASB market has become. For enterprise teams integrating public cloud and SaaS offerings into their architecture, CASB solutions provide obvious security and compliance benefits. I offer my thanks to the Netskope team for their fine friendship and assistance during my research.
VMware – My good friend Alex Tosheff from VMware has helped me countless times to better understand the cloud operating system ecosystem and the vital role it plays in virtualization, SDN, and cloud security. I also had the great opportunity to spend a day recently with the VMware executive team in New York, listening to their

strategy for driving virtualization across the enterprise. Perhaps my greatest insight from Alex and the VMware team, hopefully reflected in this report, is the vital role cloud platforms will play as a base for an emergent cyber security product marketplace, provisioned on-demand, and adjusted in real-time based on threat posture.

2017 TAG Cyber Security Annual
Cloud Security Providers

Afore – Previously CloudLink, the Canadian company offers encryption for cloud applications and systems.
Alert Logic – The Houston-based firm offers security services such as IPS and log management from the cloud via SaaS delivery.
Amazon Web Services – AWS is one of the premier platforms on which to integrate virtualized cloud capability with embedded or overlay virtual security services.
Armor – Rebranded from its original name as FireHost, the company offers secure cloud hosting.
Avanon – Avanon provides cloud access security with DLP, scanning, sanitization, and other features.
Big Switch Networks – Big Switch is an SDN solution provider with support for in-line security services.
Bitglass – Bitglass provides cloud access security broker services to support mobile access to cloud applications.
Blue Coat – Blue Coat offers cloud access security and cloud data security through its Perspecsys and Elastica acquisitions.
Blue Data – The small stealth start-up provides secure, Big Data cloud solutions for enterprise.
Boxcryptor – Boxcryptor, located in Germany, offers encryption software products to secure files stored in public clouds.
Bracket Computing – Backed by several well-known venture capital firms, Bracket focuses on secure information for multiple clouds with embedded security.
Buddha Labs – Buddha Labs is a consulting firm that makes available a pre-hardened secure Amazon Machine Image.
Catbird Networks – Catbird is a cloud security developer with VMware and OpenStack appliance solutions for virtual applications. The company was one of the first to focus on software virtualization for protecting cloud workloads.
Cato Networks – The Israeli firm provides cloud-based secure networking solutions for enterprise.
CipherCloud – CipherCloud, which includes funding support from major investors such as Andreessen Horowitz, supports enterprise cloud security solutions for monitoring and encryption.
CipherGraph – Cipher Graph, located in California, provides secure, cloud-based VPN access.

Citrix – Citrix is a pioneer in virtual computing, and offers a range platform services including security support for its customers.
Cisco – The well-known company recently acquired Neohapsis, which offers a range of cloud security and compliance professional services. Cisco's product line includes extensive support for SDN, cloud, and virtualized networking.
CloudLock – CloudLock is a Massachusetts-based company offering cloud access security broker and cyber security-as-a service.
CloudPassage – The CloudPassage Halo product provides innovative cloud compliance, security visibility, and vulnerability management solutions for virtual workloads.
Digital Guardian – The company provides cloud security solutions via its acquisition of Armor 5.
Dome9 – Located in Israel, Dome9 offers a security and compliance solution for public and private cloud services.
Evident.io – Evident.io provides a continuous cyber security platform for AWS customers.
F5 – F5 includes cloud security solutions in its extensive range of network and security products and services.
Forum Systems – Forum Systems provides API security management in support of cloud and enterprise systems.
FireLayers – FireLayers offers a secure means for extending the perimeter to allow access to cloud-resident apps.
5nine – The Illinois-based company provides a range of cloud and virtualization management solutions and security applications.
FlawCheck – Located in San Francisco, FlawCheck offers malware protection for virtual Linux containers.
Fortinet – The well-known cyber security company has an extensive range of network security products and services including solutions for cloud security.
Forum Systems – Forum Systems provides proxy solutions for cloud storage in its suite of API and cloud gateway products.
GajShield – The Indian firm includes cloud security support with its firewall and DLP offerings.
GuardiCore – The Israeli start-up offers real time threat detection and mitigation via SDN.
HyTrust – HyTrust offers a range of cloud and virtual security solutions for the enterprise.
IBM – IBM supports a range of cloud security requirements through intelligence, access management, and other product features.
Illumio – Illumio, located in Sunnyvale, offers a range of dynamic virtual and cloud workload security protections.
Imperva – Imperva offers cloud broker solutions, and makes SecureSphere available for AWS customers.
IronSDN – The small company offers a unique security functional protection solution for integration with SDN infrastructure.

Juniper – The networking company has an extensive portfolio of network and security products supporting SDN, cloud, and virtual networking.
Managed Methods – The Boulder-based company offers a range of cloud monitoring and cloud access security solutions.
Microsoft – Microsoft integrates cloud access security brokers services through its Adallom acquisition.
nCrypted Cloud – Located in Massachusetts, nCrypted Cloud supports secure cloud collaboration and secure file sharing solutions.
Nakina Systems – The Canadian firm provides a suite of network integrity and security solutions for SDN.
Netskope – Netskope provides cloud access security broker services via the Netskope Active Platform, which is deployed as a cloud service. The solution is particularly effective in helping the enterprise to gain visibility into public cloud usage.
Netwrix – Located in Irvine, Netwrix offers solutions for auditing hybrid cloud environments.
Palerra – Palerra enables cloud security automation with threat detection and incident response support.
PerfectCloud – PerfectCloud is a Canadian firm supporting a range of security protections for cloud computing including identity and access management.
Porticor – The small company, headquartered in Israel, provides cloud security and data encryption.
PrivateCore – PrivateCore, which was acquired by Facebook, offers virtual solutions for trusted execution of software in the cloud.
Protectwise – The Denver firm offers cloud security through network capture, forensics, and analysis.
Protegrity – Protegrity provides a range of Big Data and cloud security solutions including encryption.
Rackspace – Rackspace integrates security protections into its suite of cloud computing solutions.
SAP – The large German firm includes a range of security and data protection solutions for customers using its products in the cloud.
Seculert – Located in Menlo Park, Seculert provides a virtual, cloud-based platform accessible to enterprise APIs for security protection.
SilverSky – Now part of BAE Systems, SilverSky offers a range of cloud security capabilities.
Skyhigh Networks – The Cupertino-based firm offers a solution for security management of cloud access by the enterprise. The focus at Skyhigh is on providing a virtual cloud perimeter, including data leakage prevention and exfiltration.
Symantec – The well-known cyber security firm includes cloud security solutions in its extensive range of products and services for the enterprise.
Threat Stack – The Boston-based company provides continuous security monitoring for elastic infrastructure protecting cloud assets.

Trend Micro – Trend Micro offers Secure Cloud to protect data in virtualized cloud environments.
Twistlock – Located in San Francisco, Twistlock offers vulnerability detection and related protections for virtual containers.
vArmour – vArmour's distributed perimeter solution provides an effective means for virtualizing the enterprise edge.
Vaultive – Vaultive provides cloud and SaaS application data encryption solutions via network-level proxy.
Vidder – Vidder provides software defined perimeter security, which can be integrated with cloud architectures.
VMware – VMware offers an industry-leading cloud platform on which to integrate security solutions. It offers security embedded in its NSX virtual protection suite.
Zscaler – Zscaler's Web security solutions are well positioned to support security protections of cloud-based computing.
Zentera – The San Jose-based firm offers an overlay virtual network to connect the enterprise to cloud services securely.

11. DDOS Security

- ⇒ *Layer 3 DDOS* – First generation DDOS attacks involved botnets directing huge volumes of packets at an Internet gateway in order to disrupt.
- ⇒ *Layer 7 DDOS* – Second generation DDOS attacks involved malicious actors manipulating application logic to create volume bottlenecks.
- ⇒ *Cloud Gateway Attacks* – Future generation DDOS attacks will involve attempts to overwhelm cloud provisioning portals and cloud workload APIs.

Practical DDOS attacks aimed at business networks have intensified since the late 1990's. Most attacks come from botnets that use endpoint PCs or servers to direct disruptive attack traffic toward either a target gateway or a selected application. The trend since 2012 has been toward use of servers in order to increase the amount of bandwidth available for attack traffic generation, even though this increases the confidence security teams have in the source address origination.

To deal with this threat, the first thing a CISO team must ask itself is whether the DDOS threat is *truly consequential* to the operation being protected. For example, while no business ever wants its Website to be down for any period of time, the consequences of an outage for an e-commerce site is obviously much greater than for a small construction firm. So this critical step of categorizing the true risk of DDOS to the business is essential – and many CISO teams will come to the conclusion that DDOS risk is somewhat overblown in their local context. Other teams, however, will find the potential threat to be quite frightening.

The three most likely DDOS attack use cases that are being seen by all enterprise network owners are shown below.

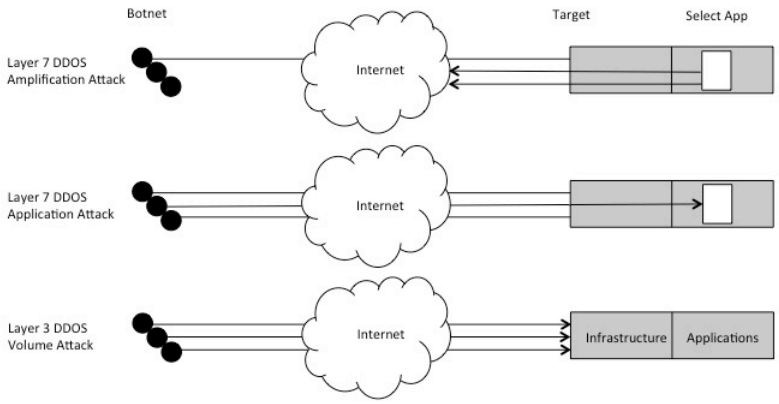

Figure 11-1. DDOS Attack Cases

Layer 3 attacks involve pure volume generation intended to clog or fill network gateway processing capacity. Layer 7 attacks use specific, select application logic to cause DDOS conditions, either by utilizing application logic to evade layer 3 filters, or to amplify attack traffic outbound, thus clogging outbound network links at the target. As suggested above, most of these attacks involve botnets, and most also involve amplification using protocols such as the Domain Name System (DNS) or Network Time Protocol (NTP) that are particularly vulnerable to such activity.

The general manner in which service providers and special DDOS security vendors deal with the attack involves upstream, in-the-network filters that try to divert, filter, or block the attack traffic in order to sort good from bad packets, sessions, and payloads. Because target gateways can be overwhelmed by attack traffic, the location of DDOS security cannot be situated adjacent to that gateway, but must rather be done upstream.

This architectural issue is often not recognized by CISO teams who become inundated with DDOS vendor marketing pitches that position the filter at the enterprise DMZ. Such an arrangement does not prevent the inbound routing infrastructure from becoming *itself* overwhelmed. It also does not account for the difficulty DDOS tools will have in dealing with huge volumes of data at an enterprise gateway with no simple means for load balancing or sharing of processing volume. As such, the use of DDOS filters upstream by providers allows for more manageable sharing of workload and for preventing DDOS volumes from coalescing into larger target streams.

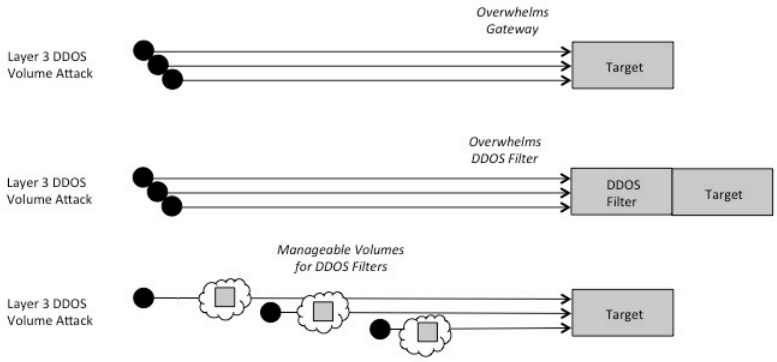

Figure 11-2. DDOS Security Locations

Analysis of the DDOS landscape and market requires tracking and predicting of three attack and protection-related issues:

- *Attack Size* – The size of DDOS attacks increased substantially from 2000 to 2016, a trend that is likely to level off in the coming years. Volume sizes will hit ceilings with total peering capacity amongst providers, and malicious groups will find other ways to cause outages in target sites. When DDOS vendors flippantly reference terabyte-sized attacks, they ignore the infrastructure plumbing problems that arise with moving that amount of data. Such plumbing will offer natural throttling, albeit with likely interruptions for weaker carriers.
- *Attack Design* – The general approach to DDOS attacks has used botnets of either PCs or servers to generate attack volume. PCs are useful simply because they are so plentiful and poorly managed, but they are limited to the outbound broadband capacity of the PC owner. Servers are useful because they generally have larger outbound network connections.
- *IoT/Mobile DDOS* – Significant increases in IoT and mobile botnet-originated DDOS attacks should be expected to grow from 2016 onward. The size of these attacks in the worse case could approach the total peering capacity of carrier networks by 2018. Alternatively, such attacks could be more focused on a specific radio access network (RAN) geography.
- *Protection Approach* – DDOS protection approaches are usually categorized into Layer 3 protections that dynamically divert and redirect volumes to so-called scrubbing complexes of equipment that strip the good traffic from the bad, and Layer 7 protections that try to address application-level probes made to target Websites. Both types of protections will be important in the future, but carrier blocking of traffic at the peering edge will serve as a useful tool when server attacks are used, thus increasing confidence in the source IP. This common DDOS attack detection and redirection approach is shown below.

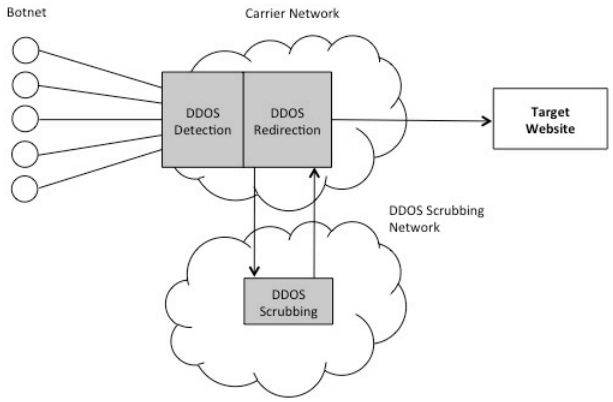

Figure 11-3. Common DDOS Security Protection

The primary trends one should expect in the DDOS area include the following: First, conventional DDOS attacks will level off around the 500 Gbps range by 2018, which is still well below the total peering capacity of many providers. As this occurs, however, dramatic increases in IoT/Mobile botnet-originating attacks might drive the total volumes to nearly 1 terabyte of attack traffic. Service providers will adjust, but target Websites could experience bumpy times.

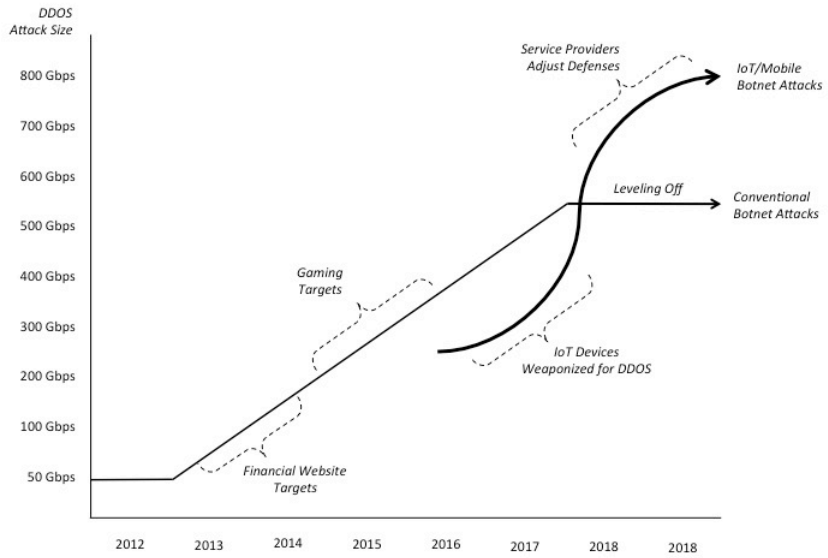

Figure 11-4. DDOS Attack and Mitigation Trends

Enterprise CISO teams should prepare themselves for DDOS increases, especially from IoT/mobile botnets by working only with experienced and capable DDOS solution providers. This obviously includes the conventional IP service providers, but will also include all mobile providers in the near future. Existing DDOS product

platforms rarely offer support for mobile protections so CISO teams should exert influence to drive the market in this direction quickly. ISPs have a clear advantage here since their backbone handles all forms of traffic, and with SDN integration, the flexibility of handling and moving traffic will increase dramatically.

An additional practical consideration involves so-called agnostic DDOS services. Internet service providers will have the ability to natively block DDOS attacks on their own network. If the associated backbone is MPLS-enabled, as with carriers such as AT&T, then diversion from the scrubbing complex of the ISP will not require additional tunneling support. Nevertheless, if multiple carriers are providing Internet services to your Website, then you might need to consider the possibility of a carrier agnostic scrubbing service if your carrier does not already offer such capability to handle your architecture. This will likely require additional encryption tunneling, but will reduce the need to coordinate traffic management between carriers during an attack.

A trend that the global enterprise and Internet communities should expect in the near future involves DDOS attacks focused on clogging entry points to cloud. This can include rogue cloud workloads taking advantage of open APIs, or it can involve malicious individuals or bots clogging cloud provisioning in open portals. Both of these attacks will require a different approach to DDOS security than is found today. Specifically, it will require advances in the throttling of service requests from software processes in cloud operating systems.

From a practical perspective, CISO teams have two options for dealing with all of the threat, trends, and issues related to DDOS attacks, whether layer 3, layer 7, or API. The first option is to buy a service from a provider who will analyze the network infrastructure and recommend suitable detection and mitigation points upstream in the network. The second is to buy technology from a vendor such as Arbor and to design a solution that can be perfectly suited to the local network environment.

Broadly speaking, most smaller and mid-sized companies can only do the former, whereas larger businesses might have the luxury of the second option. In all cases, as the DDOS threat moves to API-based clogging of virtual software gateways, all organizations of all sizes will have the ability to construct their own solution either in a virtual data center, a service-chained SDN, or directly into the code execution environment.

DDOS Security Solution Providers

As recent as perhaps three years ago, the total list of DDOS security product and service providers would be quite short. Since the well-documented large financial DDOS attacks targeting American banks in the summer of 2012, however, a plethora of good vendor options have emerged and the DDOS security product and service marketplace has developed a more reasonable level of platform and service diversity. The DDOS landscape now includes a wide range of service providers and platform developers who can focus on attacks at both layers 3 and 7.

2017 TAG Cyber Security Annual
Distinguished DDOS Security Providers

Arbor – The fine technical team at Arbor has created an aggressive plan to extend their DDOS platform support into the next generation. Over too many drinks of Bourbon in New York, the Arbor team helped me understand the direction his team is taking to deal with the growing threat of more advanced application layer attacks. Arbor has been at the forefront of this area of cyber security for several years. When the primary market leader Cisco discontinued support for the Cisco Guard about half a decade ago, Arbor picked up most of the infrastructure load – just in time for the 2012 attacks on the banks. No measure of testing or product design can battle-harden a team more than dealing with live attacks, and Arbor proved that they could adjust and improve with the never-ending shifts in that series of attacks.
AT&T – It's been over a decade and a half since my colleagues Tim Battles and Rick Huber from AT&T Labs handed me a BGP spec and showed me a public document being developed with several other carriers including MCI to try to divert traffic to a so-called scrubber (then provided by Riverhead Networks, soon to be the Cisco Guard). Since that time, I've learned so much from the AT&T team, as have so many others in the industry, about how network traffic can be moved around during an attack, and how it can be filtered and carefully sifted to keep customers up and running, while also keeping the bad guys scratching their heads as attacks seem to fizzle. I am in debt to the entire AT&T security team under Bill O'Hern for their continued fine work in this area.

2017 TAG Cyber Security Annual
DDOS Security Providers

Akamai (Prolexic) – Akamai provides a carrier-independent DDOS filtering service for enterprise. Their acquisition of agnostic-DDOS solution provider Prolexic led them into this market, which they address through tight coordination with their content distribution network (CDN) services.
Arbor Networks – Arbor Networks, acquired by NetScout, created an advanced DDOS detection and mitigation platform as Cisco exited marketplace in early 2000's. During the 2012 DDOS attacks on American banks, the Arbor platform was the primary workhorse providing detection and mitigation across the entire landscape. Any organization looking to build a DDOS protection platform will benefit from Arbor's deep level of experience and expertise in this area.
A10 Networks – San Jose-based A10 Networks is an application delivery network provider, which includes DDOS services.
AT&T – AT&T provides world-class DDOS mitigation services for managed Internet enterprise customers. Their native MPLS backbone greatly simplifies the transfer of traffic from gateways to scrubbing stations located around the world. Without native MPLS, GRE tunnels are required in order to prevent the "bounce" effect of

trying to trick traffic into moving to the scrubber versus its truly intended destination. Increasingly, the mobile ISP will play a role addressing DDOS solutions native to the SDN infrastructure.
Bell Canada – Bell Canada provides DDOS mitigation services for managed Internet enterprise customers.
BT – BT provides DDOS mitigation services for managed Internet enterprise customers.
Black Lotus – Newly acquired by Level 3, Black Lotus offers enterprise customers DDOS security capabilities.
CloudFlare – CloudFlare is an application and content delivery network provider including DDOS services.
Corero – Corero, located in the UK, is a network security services company that includes a line of DDOS defense solutions.
Crypteia – Crypteia is a threat intelligence and managed security service provider located in Greece that includes DDOS prevention services.
DOSarrest – The Canadian firm offers a cloud-based Website defense for DDOS attacks.
F5 – F5 offers the Silverline DDOS defensive product based on its acquisition of defense.net.
Fortinet– Fortinet provides a distributed denial of service (DDOS) technology solution for carriers and large enterprise.
Huawei– Huawei provides a distributed denial of service (DDOS) platform for carriers and large enterprise.
Imperva – The Web security, cyber security, and database security company includes DDOS solutions.
Link11 – German CDN and hosting firm, Link11, offers DDOS protection services for customers.
Neustar – The Virginia-based company offers infrastructure security solutions including DDOS protection.
NexusGuard – San Francisco-based NexusGuard provides a range of DDOS detection and mitigation services for enterprise.
NSFOCUS – Chinese company, NSFOCUS, offers DDOS mitigation solutions in conjunction with its WAF and IPS solutions.
Qrator Labs – The Russian firm provides network-based solutions for DDOS attacks to the enterprise.
Radware – Radware provides an advanced distributed denial of service (DDOS) platform for carriers and large enterprise including layer seven capabilities.
RioRey – RioRey provides a high performance distributed denial of service (DDOS) platform for carriers and large enterprise. For a relatively small company, RioRey has extensive experience in DDOS security as an early entrant to the field.
SecurityDAM – SecurityDAM, headquartered in Tel Aviv, focuses on DDOS solutions for use by MSSP and Communication Service Providers.
Sentrix – Located in Massachusetts, Sentrix offers cloud-based Web application security and DDOS protection.

Shape Security – Shape Security offers detection of automated attacks such as botnets aimed a Websites.
Sharktech – Las Vegas-based Sharktech offers a gateway solution for protecting enterprise networks from DDOS.
Staminus – Located in Newport Beach, Staminus offers hybrid DDOS protection and mitigation services.
Sucuri – Sucuri provides Website protection from malware and denial of service attacks.
Verisign – Verisign provides a carrier-independent DDOS filtering service for enterprise. The company provides integrated infrastructure security including support for threat intelligence and DNS.
Verizon – Verizon provides advanced DDOS detection and mitigation services for its managed Internet enterprise customers.
Zenedge – Zenedge offers a DDOS protection solution embedded in its Web application firewall.

12. Email Security

⇒ *Malware Filtering* – The most common technique for enterprise email security involves identifying and filtering malware in attachments.
⇒ *Infrastructure Security* – Standards-based solutions for improving email sender validation are becoming more important to CISO teams objectives.
⇒ *Emerging OTT Services* – Emerging OTT communications will eventually shift email usage patterns and thus shift the threat and corresponding solutions.

Modern commercial *email security* solutions focus on a wide range of different cyber security threats. Such threats include ensuring the confidentiality of email content between senders and receivers; validating the identity of email senders; demonstrating the integrity of received email content; reducing the risk of email phishing attacks to individuals and enterprise; and reducing the risk of fraudulent email creation. This broad set of security goals can be addressed using the following types of security methods:

- *Malware Filtering* – This method involves the use of collection and processing technology, which is usually implemented in an enterprise or service provider security gateway. The gateway filters email attachments for evidence of malware, with emphasis on identifying phishing schemes targeting users in an enterprise. Increasingly, these filtering solutions utilize behavioral analytics to address accuracy and false positive issues with signature pattern matching.
- *Infrastructure Protection* – This approach involves protections at the underlying infrastructure level including DomainKeys Identified Mail (DKIM), which allows email recipients to validate senders. Individuals and

most businesses must rely on infrastructure providers to ensure such advanced cyber protections. A surprising number of CISO teams are ignorant to how these email infrastructure security solutions work – and this must change.

- *Content Protection* – This method involves the use of advanced encryption algorithms and various types of related signing and authentication protocols that provide content protection and validation of sent and received email. Incredibly, the vast majority of sensitive business email today is sent fully unencrypted and unsigned – and this includes critically important sectors such as financial services and nuclear power. CISO teams in all sectors are strongly advised to think through the risk associated with poor content protection in business communications. Quite a few companies, for example, have had embarrassing financial transfers of money made at the request of a low-end phishing attack.

CISO teams must recognize that email security is multi-dimensional, and is best achieved through a layered defense. No single point solution can or ever will provide email security across the wide spectrum of malicious threat. Instead, CISO teams must work with a variety of vendors and solution providers (or even open source software) to create a proper email security defense. This can and should be coordinated with training and awareness programs to help users know when it is considered acceptable to click on links in received email. The diagram below depicts the potential interplay of the various email security mechanisms in an enterprise.

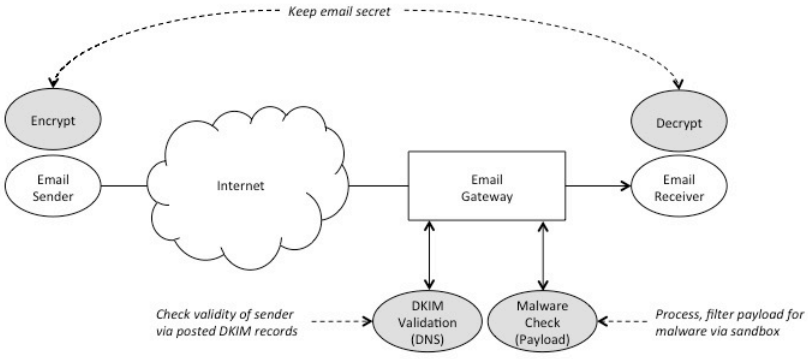

Figure 12-1. Interplay of Email Security Mechanisms

While the interplay between email security mechanisms would seem an obvious goal for any organization, most enterprise groups do not plan for such integration. Filtering might be done in various places using different tools and techniques; encryption might be spotty across different business units; and the use of underlying anti-fraud and anti-phishing infrastructure solutions might also be pretty ad hoc and unplanned. Furthermore, significant security and operational challenges have tended to exist in each of these three areas that have caused email

security to be one of the less successful and most often complained about aspects of enterprise security. The most prominent of these challenges are listed below:

- *Key Management Issues Across Different Enterprises* – Amazingly, it is still unlikely today that any two different enterprise organizations can easily share secure email (authenticated and encrypted) without a special administrative process to synchronize handoff and exchange keys. One explanation is that no entrepreneur or vendor has ever figured out a good monetization plan for such communication, as with SSL and e-commerce. Another explanation might be the motivation to keep email unencrypted to advance Big Data marketing objectives. Open source initiatives such as OpenPGP have tried to ease this key management issue, but most companies today find the use of open source email security tools on Windows, Android, and other operating systems to be uneven in their compatibility with external business partners.
- *Uneven Deployment of DKIM and SPF* – Uneven deployment continues to exist across the Internet for DomainKeys Identified Mail (DKIM), which embeds validation information in the body of the email, and for Sender Policy Framework (SPF), which creates files or records to help validate sender identities. All CISO teams must begin to write explicit policy that requires comprehensive coverage across the enterprise for these important standards-based techniques from companies such as Agari advancing approaches based on Domain Message Authentication Reporting and Compliance (DMARC).
- *Difficulty Identifying Payload Malware and Spear Phishing* – The process of identifying and removing malware from email payloads has proven to be especially challenging. Attackers find the use of Spam for malicious or monetary gain to be cheap and easy to implement, and they have demonstrated great dexterity in adjusting phishing attacks to get around ever-changing defensive algorithms by email security companies. Most companies deal with the problem by trying to train their employees not to click on anything that looks suspicious. This is a laudable goal, but will never produce comprehensive results.

In selecting email security vendors for a defense in depth solution, CISO teams should not only address the concerns mentioned above, but should also make sure to check user visible interfaces and tools. This is especially important for email filtering solutions that have temporary email quarantines for captured messages that match some signature or rule. These interfaces can sometimes be clumsy and difficult for users to navigate easily.

CISO teams should also make sure to understand the cross-organizational support offered for any email security solution. The biggest challenge for email encryption has involved scalable key management between different organizations. Within a single corporate domain under a common user directory, key management

support for enterprise email encryption has improved in the past decade. But encrypting email between different groups, companies, agencies, and individuals has continued to be a nagging problem. The majority of cross-domain encryption solutions tend to use man-in-the-middle, Web-based solutions that require encrypted retrieval from target recipients for stored, sent messages.

While no serious businessperson would ever *presently* consider trying to be productive without the heavy use of email, the longer-term prospects for email usage, in general, are unknown. Even with advances in popular email services such as Gmail, as well as continued investment in enterprise email systems usually based on Microsoft Exchange, email is increasingly being replaced in personal and business settings with text messaging, mobile communication apps, video chatting, and social networking services such as Twitter, Instagram, Snapchat, and even Twitch (for gamers).

The marketplace for email security solutions will nevertheless experience continued steady growth in the near and medium terms driven by increased spear phishing threats, greater volumes of Spam to be filtered, and more intense email payload malware threats. In the longer term, however, the marketplace for any value added email security services will have to adjust to email usage pattern shifts. Young people entering the workforce in the coming years will drive more diverse means of communication, and considerably less dependency on email.

In spite of these expected shifting email usage patterns, the good news for email security vendors is that as long as there are means for communication, there will be security issues, and existing secure email solution providers can and should evolve their long-term focus accordingly. Algorithms for detecting malicious content in email, for example, should be easily reused in settings where that malicious content is attached to some other communication approach.

The market for email security experienced low usage for encryption in 2009, but that has grown to medium/high usage today. Infrastructure protections such as DKIM and SPF across email systems were also low/medium in intensity in 2009, with growth to medium/high usage today. Email filtering for malware has grown from medium/high usage in 2009 to high usage across personal and enterprise systems today. All three of these areas for email will eventually level off at high usage, and will remain important at that level.

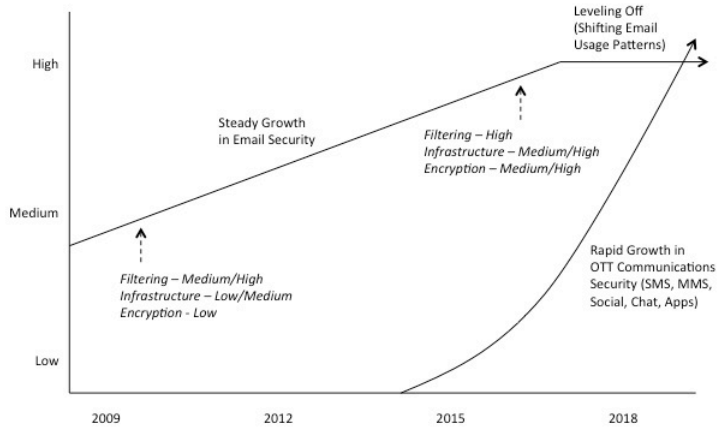

Figure 12-2. Marketplace for Email Security

The over-the-top (OTT) secure communications marketplace, including tools for secure texting, secure messaging, and secure social media usage will grow more quickly than email security solutions in the next decade. This should not be a near-term concern for vendors in either market, but strategic acquisitions will occur, such as email security solution providers buying smaller OTT solution providers. Also, the most successful email security vendors will have little trouble adjusting their security technologies to support OTT.

Email Security Providers

The Email security providers listed below offer product solutions that range from network-based filtering to payload encryption. CISO teams considering an email security solution should include application security and infrastructure security in the source selection analysis. CISO team should also note that the products listed below offer the security filtering and processing component of an end-to-end solution. The actual application of this technology can be provided in-house, via a managed security solution (MSS), which is covered in a separate section, or through a value added reseller, which is also covered in a separate section.

2017 TAG Cyber Security Annual
Distinguished Email Security Providers

Agari – Pat Peterson from Agari has been a good friend of mine for several years now, and I think his knowledge of DMARC and related technologies is unequaled. He and his team were kind enough to spend face-to-face time with me over drinks recently before one of my lectures at the Stevens Institute of Technology in Hoboken. I continue to be impressed with their collective drive to improve cyber security protections in the global email infrastructure. Pat has posted a couple of

YouTube videos that explain DMARC in the clearest of terms. They certainly helped me understand how it all works.
Proofpoint – I spent a wonderful day with the Proofpoint team in New York recently and have learned so much about email security from my association with these fine security technologists. Gary Steele has assembled such a capable team, and the Proofpoint solution includes precisely the types of algorithms that are now required to stop advanced cyber attacks from entering the premise through email. Getting this email filtering, malware detection, payload analysis, and live mediation correct is one of the most critical elements of any enterprise defense. I offer my thanks to Gary and his team for all their help through this research project.

2017 TAG Cyber Security Annual
Email Security Providers

Agari – Agari provides a range of email security infrastructure monitoring including DKIM and SPF-based misuse and fraud analysis. The challenge for any solution based on the DMARC standard is that it requires considerable maturity on the part of the CISO team buying the service. This is a challenge for newer or smaller security teams.
AppRiver – AppRiver is a cloud-based secure email hosting with Spam and virus protection capability.
AT&T – AT&T offers an advanced network-based email security filtering and policy enforcement service through technology partnership. ISPs such as AT&T are well positioned in their emerging SDN infrastructure to provide service chained product integration in areas such as email security.
Barracuda – Barracuda provides products and services for email Spam and virus filtering.
Blue Coat – Blue Coat offers in-line email threat defense solution, which is designed to prevent email-borne malware in link and attachments.
Cisco – Cisco provides a solution, based on its IronPort acquisition, which includes standard email security platform and service features.
Clearswift – The Clearswift Secure Email Gateway includes content-aware security protections for secure email.
Comodo – Comodo includes a free Email security solution, an anti-Spam gateway, and encryption/authentication support.
Dell – The Dell SonicWALL solution includes anti-Spam and additional features to secure email.
EdgeWave – EdgeWave offers cloud-based secure email hosting with Spam and virus protection capability.
FireEye – FireEye provides a solution integrated with its APT-detection platform for addressing email Spam and filtering malware.
Forcepoint – The TRITON AP-EMAIL provides the standard set of secure email gateway features for this Raytheon Websense combination.

Fortinet – Fortinet provides an integrated platform solution for addressing email Spam and filtering malware.
GFI – GFI offers cloud-based secure email hosting with Spam and virus protection capability.
Google – The popular Gmail provider includes a range of security features including OpenPGP for encryption.
HPE – The Voltage solution from HPE offers a range of email encryption capabilities for enterprise. Voltage was one of the first solution providers to address the shortcomings in PKI-based email security by providing a common arbitrated solution using an Internet-hosted server.
Intel Security (McAfee) – Intel is a previous market leader with its McAfee email security solution still supporting legacy customers. He company discontinued support in 2015.
Microsoft – Microsoft supports a range of security options for email with Outlook and Exchange offering.
Mimecast – Mimecast offers cloud-based secure email hosting with Spam and virus protection capability.
OPSWAT – OPSWAT includes email security features with the Metascan mail agent, which helps detect malware and email-borne threats.
Proofpoint – Proofpoint's email security product platform provides advanced malware detection and removal for email with quarantine. The company integrates the best available algorithms, techniques, and heuristics to advance detection rates and minimize false positives.
ReturnPath– ReturnPath provides an advanced and highly effective set of email security infrastructure services including DKIM and SPF-based misuse and fraud monitoring.
SilverSky (BAE) – SilverSky offers a portfolio of secure email communication, collaboration, and infrastructure services.
Sophos – Recently acquiring Cyberoam, Sophos offers secure email gateway with DLP, threat detection, and anti-Spam.
Symantec – Symantec includes range of secure email features including end-to-end encryption.
TargetProof – The TargetProof solution focuses on fraud prevention for email, Web, and user authentication.
ThreatTrack – ThreatTrack includes advanced threat detection for email in its anti-malware solution.
TrendMicro – TrendMicro offers policy-based encryption capability for enterprise and consumer email.
TrustWave – The TrustWave Secure Email Gateway includes the standard set of secure email features for the enterprise.
Verizon – Verizon offers a network-based email security filtering and policy enforcement service.
WatchGuard Technologies – WatchGuard provides a secure email and Web gateway as part of its UTM and firewall offerings.

ZixCorp – ZixCorp offers secure email solutions including encryption for companies and individuals.

13. Infrastructure Security

⇒ *DNS and BGP* – The Domain Name System (DNS) and Border Gateway Protocol (BGP) infrastructure systems are vulnerable to cyber attacks.
⇒ *Infrastructure Security* – CISO teams are dependent on service providers to ensure proper underlying infrastructure security protection.
⇒ *Next-Generation* – Infrastructure security protections will increasingly shift toward centralized providers offering virtual, cloud-based services.

CISO teams have long recognized that the range of exploitable cyber security architectural vulnerabilities in their enterprise can originate from one of three possible network locations:

- *Internal Networks* – Vulnerabilities can be embedded in the local enterprise network, which is often the result of a weak enterprise security compliance program or just bad software. Insider or malware-based access to these private vulnerabilities over an internal local area network is possible and security experts refer to this as an East-West exploitation, especially if it involves lateral movement across an enterprise.
- *External Networks* – Vulnerabilities can be embedded in the external systems and networks operated by partners, suppliers, customers, and other ecosystem participants. Similarly, external malicious actors can locate and exploit private vulnerabilities by simply compromising the organizational perimeter, with its inevitable series of intentional and unintentional holes.
- *Network Infrastructure* – Vulnerabilities can be embedded in the underlying infrastructure fabric supporting communication and interaction across the Internet. This problem exists outside the purview of the typical CISO, and is thus especially troublesome since no action plan can be easily taken by the enterprise CISO to reduce this risk. Instead, the CISO must work with infrastructure providers to manage risk according to a reasonable plan.

Most cyber security experts have known for some time that many of the truly frightening vulnerabilities that exist across the global cyberspace ecosystem originate in this underlying, external, wide area network infrastructure. It is where all DDOS attacks gain momentum; it is where nation-state wide area routing attacks originate; and it is where naming services can be tampered with to affect companies that rely on the Internet for their business.

The Border Gateway Protocol (BGP), for example, stitches together the autonomous systems (AS) supporting Internet and private IP networking. The potential is thus high for anyone with administrative control over an AS to pollute

routes, either accidentally or purposefully. Furthermore, the ability for AS owners to accurately monitor the correctness of distributed route advertisements is unfortunately quite low. The result is that BGP infrastructure is often cited as a significant cyber security enterprise risk – and one that does not lend well to manageable risk reduction by any given enterprise.

Even with such frightening risks posed by BGP, perhaps the most security consequential component of cyberspace infrastructure is the domain name system (DNS). Every cyber security expert agrees that well conceived DNS attacks can easily bring down infrastructure through the combined use of source spoofing, protocol reflection, target distribution, and response amplification. In fact, other protocols such as the network time protocol (NTP) that support distribution and amplification are vulnerable to targeted infrastructure attack.

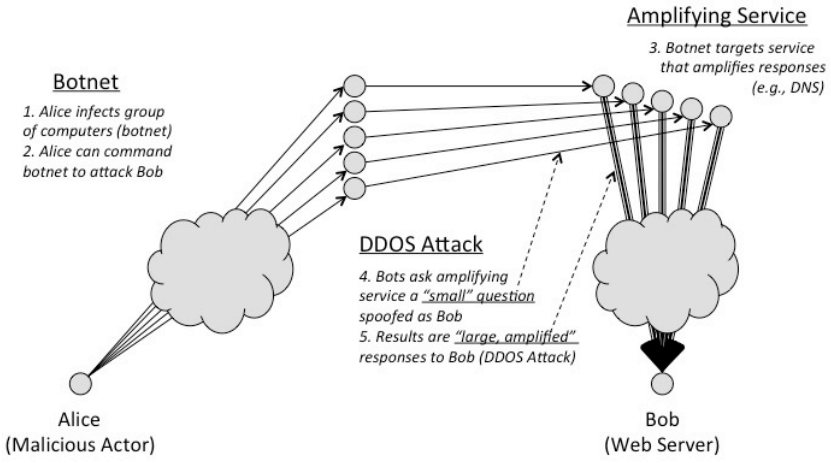

Figure 13-1. Infrastructure Attacks Using Distribution and Amplification

A major challenge for enterprise teams involves differentiating between those cyber security risks that are under direct, local control by the CISO team, and those cyber security risks that require coverage from an infrastructure provider or partner. Clearly, the cyber security risks associated with BGP routing and DNS/NTP amplification require coordinated protections from Internet Service Providers (ISPs) and Global Domain Providers. To this end, CISO teams are advised to ensure that their ecosystem is properly covered by all supporting entities – and this includes cloud and mobile application services.

Furthermore, any organization offering shared infrastructure services that support multiple enterprise users has a special obligation to properly attend to cyber security. A wonderful range of vendors is available with risk reduction measures for DNS and other protocols that have wide ranging implication if attacked. Compliance managers are also urged to include these types of risks, previously viewed as almost existential, as part of the review packages for regulatory and certification projects.

Future trends in infrastructure security can be analyzed and depicted in the context of two categories of technical and operational support: private, enterprise-managed infrastructure for large organizations, and shared, centrally managed infrastructure supporting everyone.

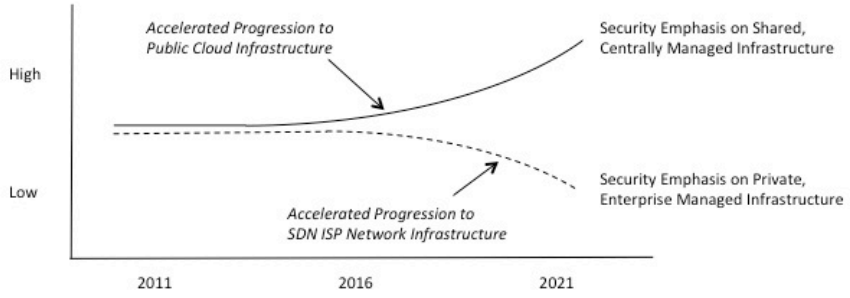

Figure 13-2. Trends in Infrastructure Security

With the clear progression toward greater use of shared public cloud systems, along with the increasing use of virtualized SDN services from providers using security service chains for managed security, the importance of shared, centrally managed infrastructure security grows accordingly. Furthermore, with increased use of mobility-enabled applications for enterprise, the corresponding shared mobile broadband infrastructure becomes more important.

CISO teams should therefore expect, and security vendors should plan for, an accelerated shift from privately to centrally managed infrastructure. This includes shared hosting services, domain naming, virtual routing, and data center support. In each of these cases, the centrally managed infrastructure will include cloud-like capabilities such as common, underlying computing support as one finds with hypervisors in public clouds.

The challenge of achieving global routing security and providing effective BGP monitoring is a near-term opportunity for vendors. This has been a challenging business environment for vendors to make money to date, with one particularly well-known company, Norse, apparently experiencing some temporary business problems. Nevertheless, the function is so important – one that perhaps should be included in every SOC – that expanded functional coverage from security monitoring companies into this area would be an excellent idea.

Infrastructure Security Providers

Creating a list of infrastructure security providers is challenging because many companies provide forms of network infrastructure support without a primary emphasis on cyber security. Similarly, many companies focus on providing products and services in support of local infrastructure such as would be found in an enterprise data center. As a result, the list below is a hodge-podge of different ISPs and other larger companies trying to stitch together some sort of infrastructure

protection. This area of infrastructure security is perhaps the least developed of all vendor support areas in cyber security, which is ironic, because the associated risks for DNS and BGP might be the amongst the highest found anywhere.

2017 TAG Cyber Security Annual
Infrastructure Security Providers

Agari – Agari supports email security at the infrastructure level through DKIM and SFP monitoring and controls.
Akamai – Akamai offers CDN-based controls and DDOS protection at the infrastructure and global network level.
AlphaGuardian – AlphaGuardian supports data center infrastructure protections for servers and telecommunications.
Amazon Web Services – Cloud services providers have an obligation to ensure proper infrastructure controls into and out of their services as well as for virtual services.
AT&T – Global Tier 1 ISPs like AT&T play a key role in protecting infrastructure for enterprise networks for both wireline and wireless services.
BT – Global Tier 1 ISPs such as BT play a key role in protecting infrastructure for enterprise networks.
CloudFlare – CloudFlare offers CDN, optimization, DDOS, and DNS infrastructure security solutions.
Deutsche Telekom – Global Tier 1 ISPs such as Deutsche Telekom play a key role in protecting infrastructure for enterprise networks.
DomainTools – DomainTools provides a range of domain, network, and monitoring tools for look-up, research, investigation, and threat intelligence.
Farsight Security – Farsight Security provides threat intelligence feeds from real time passive DNS solutions.
Google – Google ensures proper infrastructure controls into and out of the Google cloud. The company is working on productizing its BeyondCorp approach for perimeter-less security. It also offers a set of Google Identity controls for individuals and enterprise.
IBM – IBM focuses on ensuring proper infrastructure controls into and out of the IBM cloud as well as for virtual services.
Infoblox – Infoblox offers a range of secure DNS, network services, and network automation services.
Microsoft – Microsoft provides infrastructure controls into and out of the Azure cloud as well as for virtual services.
Neustar – Telephony provider Neustar offers a range of infrastructure security solutions including focus on DDOS and DNS.
NCC – NCC includes domain support through the high assurance ".trust" solution for reduced network risk.
Nominum – Nominum supports DNS network infrastructure and cyber security analytics.

Norse – Norse provides active monitoring of network and BGP-related telemetry and security metrics. The company is undergoing significant management changes as of this writing.
NTT – Global Tier 1 ISPs play a key role in protecting infrastructure for enterprise networks.
OpenDNS – The San Francisco-based firm offers cloud delivered network security through enhanced DNS protection.
ReturnPath – ReturnPath offers a range of infrastructure-level email and related security services.
Tufin – The Israeli company offers firewall policy orchestration, which is an example of the type of configuration and management solution required in the enterprise infrastructure.
Verisign – Verisign provides a range of infrastructure services including domain services, DDOS, and related controls.
Verizon – Global Tier 1 ISPs such as Verizon play a key role in protecting infrastructure for enterprise networks.

Additional Infrastructure Security Providers

APC (Schneider Electric) – The company provides solutions for data center and infrastructure management.
Box – Box includes a range of services to ensure proper infrastructure controls into and out of their services as well as for virtual services.
Dropbox – Dropbox includes infrastructure security controls into and out of their services.
ThousandEyes – ThousandEyes monitors BGP routing, paths, and VOIP for improved trouble-shooting and protection.

14. Network Monitoring

- ⇒ *Network Monitoring* – Network monitoring consists of collection, processing, and analysis of real time network information to identify security indicators.
- ⇒ *Advanced Correlation* – The specific techniques used to derive intelligence from network data is the prime differentiator in this market.
- ⇒ *Next-Generation* – Network monitoring will shift from focus on handling large capacity to handling virtual distribution over SDN.

Network monitoring product and service solutions collect large amounts of data in real time and at network line speed to identify security indicators. Usually, the most difficult aspect of network monitoring involves collecting and capturing the right data, which is a challenge for vendors, because they often cannot control all aspects of this process. If a CISO team has its hands tied on gaining access to the proper

networks for collection, for example, then any network monitoring initiatives will likely fail – regardless of how capable the selected vendor solution might be.

An additional consideration in network monitoring solutions involves the back-end analysis capabilities inherent in a vendor product or service for deriving intelligence from captured data. Since network monitoring for cyber security is so heavily dependent on this type of analysis, the products and services in this category are also referred to by the term *network security analytics*. Usually, the analytics component of a network monitoring solution is high-end and designed to handle large capacities at high speed and in real-time.

Most network monitoring tools will be used in close conjunction with related tools in use by CISO teams, such as the enterprise SIEM, intrusion prevention systems, server log management tools, and more modern security analytics tools deriving intelligence from data collected in repositories from software applications and systems. A common differentiation from these related tools is that network monitoring involves real time, line speed collection with automated response, versus security analytics, which involves non-real time investigation by human beings from all-source repositories.

One can also view network security analytic products as direct descendants of traditional intrusion detection and intrusion prevention products. In fact, major overlap exists between network security analytics tools and intrusion prevention to the point where the categories are tough to distinguish. Many network monitoring tools are also direct descendants of network management tools, less focused on security as on performance, capacity, and other engineering attributes. Network security analytics products are assumed here to include at least the following capabilities:

- *Network Access* – Network access includes the capability to capture relevant data in motion (e.g., metadata, packet content) from network media using physical taps, virtual connectors, or other means. As networks change toward more virtual, SDN-based methods, network access issues will shift from the challenge of greater capacity to the challenge of greater distribution. Nevertheless, network monitoring tools are often differentiated from IPS in their ability to handle larger networks.
- *Metadata and Content Collection* – Collection includes the ability to combine and aggregate data captured from a network into a suitable storage medium (e.g., Hadoop) for caching, analysis, and archive. Speed requirements drive most engineers toward hardware-based solutions, but virtualization is a natural balance to this approach. Most network monitoring tools have the ability to provide full packet capture, which will be superior to sampled collection for certain types of meta-data analysis.
- *Network Analytics* – Network analytics includes the tools and technology, increasingly non-signature based, for performing advanced correlation, search, and other heuristic processing on collected data for the purpose of creating actionable intelligence. Improved analytic methods are the primary

means by which network monitoring solutions have been able to keep up with modern attack trends.

Network monitoring products differentiate themselves from traditional enterprise security analytic tools by including the ability to handle high volume network transmission data (i.e., data in motion) at line speed or near-line speed rates. As suggested earlier, virtual SDN infrastructure changes this by introducing greater network distribution. The good news is that SDN architectures can be designed to include network monitoring applications on the northbound SDN controller interface. One can therefore expect to see distributed algorithms emerge for real time threat sharing and correlation between network monitoring applications running on different controllers across a network.

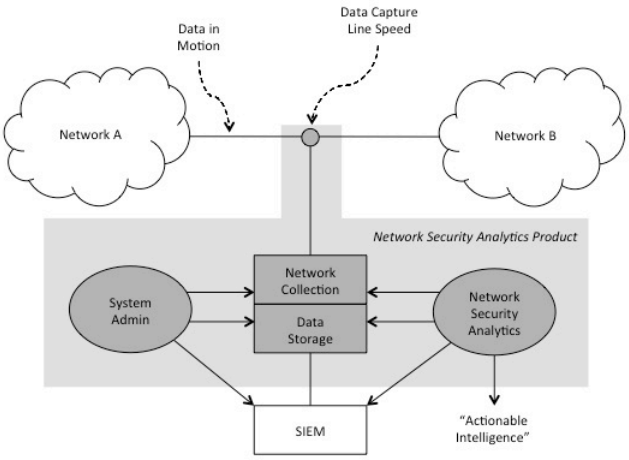

Figure 14-1. Network Monitoring Products

Not all network monitoring tools will have exactly the same set of capabilities, but virtually all exhibit some sort of data capture, network collection, data storage, network security analytics, and system administration. The deployment of network security analytic solutions generally targets familiar chokepoints on an enterprise network. That is, any location where firewalls and intrusion detection systems would be deployed would be considered desirable for network monitors.

CISO teams are advised to drive down into the specifics of how a given network monitoring vendor provides for security analytics in their tool. The words "aggregation" and "correlation" tend to be over-used by marketing teams, so it is advised that more detail be demanded. From a foundational perspective, all security analysis involves looking for subtle relationships between disparate data for the purpose of deriving useful threat intelligence. To the degree that such analysis learns dynamically, or includes connectors for unstructured data, or does something similar that assists the analyst, this should be considered in source selection.

A typical use case example one might examine in assessing the degree to which a network monitoring product can be embedded in an enterprise security environment involves time correlation. The most common after-the-fact learning that security analysts report after an incident is the often methodical, step-by-step planning and execution involved in a cyber attack. This process usually involves malicious attacks to disparate and unrelated systems and networks, so that the relationship is not easily evident to the observer. But in the optimal security analytic environment, the analyst has advanced tools that can collect this disparate data in real time to bring the step-by-step attack process to light.

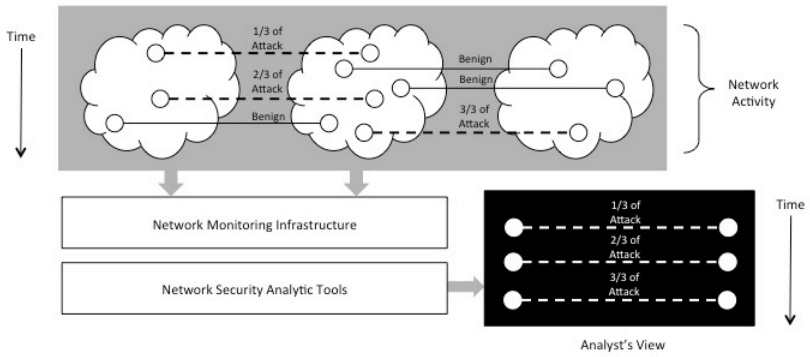

Figure 14-2. Time Correlation of Attack Using Network Security Analytics

Managed security service providers (MSSPs) and Internet security providers (ISPs) deploy network monitoring products in a manner consistent with other managed security solutions. Multi-tenant solutions with the ability to optimize MSSP management have not been an important feature in this product marketplace to date, suggesting the relative immaturity of this technology in the security community. This is likely to evolve.

CISO teams also need to work with their network monitoring provider to ensure that their roadmap is consistent with enterprise network architecture plans. Most enterprise teams are involved in network evolution toward more cloud-based and virtual environments. Regardless of the actual plan, teams should make certain that their network monitoring vendor is working on product enhancements that are meaningful in the context of their proposed architecture.

CISO teams must also ensure minimal overlap between any network monitoring and security analytics tools being used in the enterprise. Many enterprise teams will have some sort of analytic tool being used in conjunction with their SIEM or log management systems. This should be factored into any plans to obtain and use a network security analytic tool. At minimum, the two tools should not collide in their use of stored data.

A key additional factor in network monitoring involves the dimension of time in the detection of attacks. On one end of the spectrum, tools and technology exist (e.g., IronNet) that attempt analytics at very large line speeds (e.g. approaching

100Gbps) to prevent attacks from occurring. On the other end of the spectrum, tools and technology exist (e.g., LightCyber) that take advantage of the long lifecycle time associated with the typical APT, and that try to detect breaches that are presumed to have already occurred.

The prognosis for the network monitoring marketplace is mostly positive, but mixed. Clearly, in the near term, these products are likely to experience great success and growth, especially for large enterprise and MSSP buyers. Increased budgets at large banks, for example, are likely to include provision for these types of tools on their networks. With the gradual reduction in perimeter dependence at all enterprise networks, however, the use of network monitoring and their associated security analytic products should level off, and perhaps even drop somewhat.

Replacing this use will be a dramatic increase in the use of network monitoring tools that are designed to collect and process cloud and virtual traffic across APIs. This will be especially powerful as software defined network (SDN) infrastructure provides the ability to virtualize enterprise traffic across mobile infrastructure.

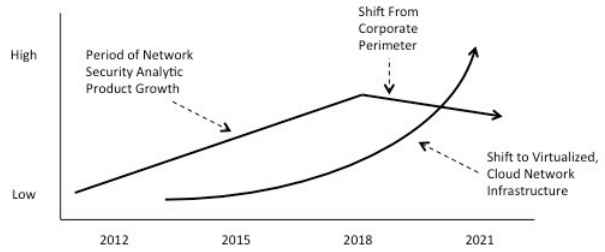

Figure 14-3. Trends in Network Monitoring

The shift to virtualized, cloud-based network monitoring also has the benefit of *potentially* extending this capability to smaller companies, albeit with the requirement that these companies have sufficient staff to interpret results. Furthermore, even with virtualization, the real potential for a small company to employ network security analytics remains bounded by the control they have over their network and the types of managed services available from their service providers.

As every company deploys their infrastructure to virtual cloud-based networks, however, the potential to realistically deploy advanced security analytics in an on-demand, user-controlled manner should become much more feasible for everyone. This will open new markets for network monitoring and analytics vendors.

Network Monitoring Providers

The following companies provide network monitoring product solutions for enterprise customers. The distinction between network monitoring and security

analytics is therefore not significant, so CISO teams should include both focus areas in any source selection for enterprise network security analytics and monitoring. Furthermore, the distinction between Web gateway solutions, intrusion prevention systems, and network monitoring is also not significant, so these areas must be considered as well during source selection.

Companies that offer network management utilities without a clearly designated focus on cyber security tended to not be included in this section. Several service providers are included here, since their native management and monitoring capabilities can be useful in a holistic network monitoring methodology. To the degree that their network monitoring solutions are part of managed security services, these are covered in a separate section.

2017 TAG Cyber Security Annual
Distinguished Network Monitoring Providers

NIKSUN – Parag Pruthi and his team from NIKSUN were generous with their time and assistance to me on numerous occasions during this project. The entire NIKSUN team spent the better part of a day back in April in their Princeton conference room helping me understand the deep technical and operational issues associated with enterprise and backbone network monitoring at extremely high network capacities. The team also helped me better understand how collected and analyzed data can be best presented to users through visual interfaces. I am so grateful to the team for their kind assistance and insights.

2017 TAG Cyber Security Annual
Network Monitoring Providers

Allot Communications – Allot Communications provides network monitoring optimization, monetization, and security solutions.
APCON – Oregon-based APCON offers network monitoring and optimization solutions for data centers.
Arbor – Arbor offers an industry-leading platform that supports monitoring network traffic for volume and other anomalous conditions related to DDOS. CISO teams concerned with detection of anomalies in Layer 3 traffic will benefit from Arbor's network monitoring experience.
AT&T – As AT&T virtualizes its network infrastructure, unique opportunities arise for SDN-based network monitoring solutions for security.
Attivo Networks – Attivo Networks provides deception-based attack detection and prevention capabilities that can be used for network monitoring.
Blue Coat – Blue Coat offers a Web security gateway solution that provides proxy, network security analysis, and related functions that monitor network traffic.
BluVector – The McLean-based firm offers an advanced threat detection and network monitoring platform.

Bradford Networks – Bradford Networks integrates NAC and live network connections view into a correlated network security monitoring and management approach.
Cisco – The acquisition of Lancope introduces the StealthWatch network security analytics tool into the Cisco suite.
CyberFlow Analytics – CyberFlow Analytics provides a suite of security analytics tools that collect and process network data for security anomalies. With advances in the underlying analytic algorithms, the accuracy of detecting anomalies in monitored traffic using tools such as from CFA is increasingly dramatically. Hossein Eslambolchi, one of the principals of CFA, spent years as the head of infrastructure at AT&T.
Fidelis – The Fidelis XPS system analyzes network traffic to detect tools and tactics of advanced attackers using so-called Deep Session Inspection.
FireEye – FireEye provides industry-leading Network Security (NX) solutions for detection of advanced attacks using the signature-less MVX engine.
Flowmon – Located in the Czech Republic, Flowmon offers network monitoring and security solutions.
FlowTraq – FlowTraq provides network flow analysis, monitoring, and anomaly detection to support network forensics.
Gigamon – The Gigamon platform supports complete views of network infrastructure for forensics, visibility into encryption, and threat detection.
GreeNet Information Services – Headquartered in China, GreeNet offers advanced traffic inspection for network monitoring and security.
Intel Security (McAfee) – The McAfee Advanced Threat Defense solution detects stealthy attacks and generates intelligence.
IronNet Cybersecurity – Retired General Keith Alexander, former Director of NSA, leads IronNet. IronNet has assembled a group of talented scientists and operation staff offering advanced network security analytics embedded in a network capture that can monitor packets at very high line speeds.
Juniper – The Juniper Security Intelligence Center is integrated into the SRX Series Gateways to support network security. Juniper has the advantage of a long history in the provision of network product solutions across many sectors and customer missions.
ManageEngine – ManageEngine supports network behavior anomaly detection through flow-based network security management.
Napatech – Napatech, located in Denmark, offers solutions for capturing, processing, and monitoring network traffic for real time visibility.
NIKSUN – NIKSUN is a mature network collection and security company that has the ability in their product to maintain capture at very high network capacity rates. While this is less important for host-based protections or IPS on smaller networks, some CISO teams do have to contend with high data rates approaching 100GBps.
Novetta – Novetta provides an advanced network security analytics platform that delivers actionable insights.

PacketSled – PacketSled offers a next-generation network security tool for providing continuous monitoring.
Plixer – Located in Maine, Plixer provides solutions for NetFlow capture, deep packet inspection, and log data replication.
Qosmos – The French firm, Qosmos, offers a platform for collecting network traffic for management and security.
RSA – RSA Security Analytics supports enterprise and network security monitoring and attack detection.
Savvius – California-based Savvius offers network monitoring and security solution software.
SolarWinds – In addition to network performance, application, and database monitoring, SolarWinds offers IT security and compliance solutions.
Verizon – Verizon's network infrastructure virtualization offers opportunities for the ISP to support SDN-based network monitoring for security.
Zscaler – Zscaler provides a Web security solution based on an extensive network of gateway functionality offering network monitoring, proxy, and other capabilities.

Additional Network Monitoring Providers

RISC Networks – The Cloudscape solution from RISC Networks offers IT and network security analytics.
Trisul Networks – Trisul offers a range of multi-layer streaming network analytics tools.

15. Secure File Sharing

- ⇒ *File Sharing Risk* – Most of the major cyber attacks to enterprise have involved weaknesses in file sharing within and across the perimeter.
- ⇒ *Security Methods* – Encryption, DRM, and man-in-the-middle sharing services are among the methods used to secure the file sharing process.
- ⇒ *Shift to Public Cloud Sharing* – Most organizations will increasingly adopt public cloud-based secure file sharing in the coming years.

Secure file sharing solutions support protected exchange of sensitive data between internal enterprise groups, as well as secure collaboration and sharing between untrusted entities such as companies and their third-party suppliers. This type of security solution is important for CISO teams since the majority of enterprise cyber attacks that have occurred in recent years have involved exploitation of either East-West file sharing inside a perimeter-protected LAN, or north-south file sharing across a remote access gateway for business partners. For this reason, *secure file sharing may be one of the most neglected components* in the CISO team toolkit.

To date, file sharing in the enterprise has typically been synonymous with the combined use of email attachments and file share software, usually from

Microsoft. While email attachments and Microsoft file sharing using SharePoint are certainly convenient and familiar, the likelihood is high for sloppy administration of file shares or incorrect selection of security settings from end users. For example, accidental transfer of sensitive data as an email attachment on a 'respond-to-all' operation is common. This introduces a huge data leakage risk for most organizations.

As a result, newer techniques are emerging for more secure file sharing and these new (or renewed) techniques fall into the following three categories:

- *Client-Server Security* – This method involves the renewed use of familiar protocols such as secure file transfer protocol (SFTP), secure shell (SSH), or virtual private network (VPN) solutions. These utilities provide secure encrypted channels for different entities, including machines, to access and transfer files. A distinct lack of agreed upon business standards make this type of solution applied in an uneven manner across most business-to-business environments. It is also unreasonable to expect executives or other non-technical staff to agree to any process that would require a special protocol or secure shell. They need simple, invisible controls.
- *File Security* – This involves the use of data encryption and digital rights management (DRM) to assign and manage privileges to files that are transferred or downloaded by end users. This area is also lacking in generally accepted standards, so most business-to-business environments with have ad hoc arrangements for file sharing security using encryption or DRM. It is also *extremely difficult* to administer enterprise DRM, especially across organizational boundaries.
- *Intermediary Security* – This approach involves trusted, man-in-the-middle intermediary systems that actively participate in the secure transfer of files between entities. This is a massively growing solution area with public clouds serving as the obvious intermediary, even in private enterprise environments. Most CISO teams will move in this direction, using public cloud services as the basis for sharing, along with a selected cyber security solution that offers the required compliance and security.

The diagram below shows the operation and typical application of these three newer secure file sharing methods for the enterprise.

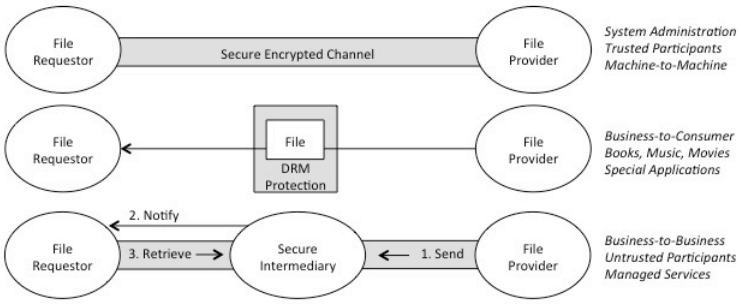

Figure 15-1. Secure File Sharing Methods

The majority of secure file sharing solutions for business-to-business applications – that is, between different organizational entities – now utilize secure intermediaries between participants. This approach is often provided as a monthly service, and billed based on the number of users with accounts on the secure file sharing system. The advantages of a man-in-the-middle solution include reduced dependency on complex public key infrastructure (PKI) handshakes and protocols, increased potential for exchanges between participants with zero pre-interaction, and utilization of familiar recipient notification approaches such as email and texting.

Additional secure file transfer solutions include the use of secure file vault capabilities, which are special cases of secure intermediary approaches. Such approaches are useful for clean room environments, such as projects involving many participants from different organizations, projects that involve advance planning for corporate mergers, and specially controlled legal environments. In all cases, a secure channel is established between participants and the centralized file store. The files to be shared are usually handled in a highly secure manner by the secure intermediary with encryption, monitoring, and other capabilities.

In the selection of a secure file sharing solution, CISO teams should investigate how the vendor integrates its solution with public, private, or hybrid clouds. Even if a given solution is not designed for use in a public cloud, CISO teams should understand how it would interoperate with other utilities hosted in the cloud. Obviously, if the vendor provides secure intermediary services through its own private cloud, then there might be an easier roadmap to integration with selected public cloud vendors. CISO teams should also ask vendors how they support data-at-rest protection, perhaps via DRM.

The market trend for secure file sharing is growing and also involves a shift toward the use of public clouds. Hesitation does remain with some CISO teams for using public clouds to securely exchange and distribute sensitive data. But as public cloud security, operations, and compliance become more accepted in all business sectors, it is hard to imagine any secure file sharing method competing effectively with the obvious cost, efficiency, and data ubiquity advantages of pubic cloud for such use.

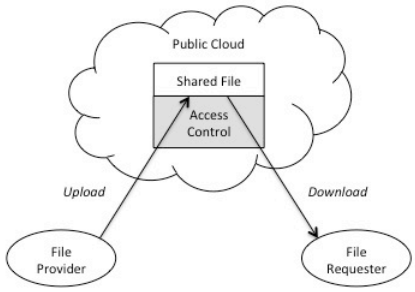

Figure 15-2. Using Public Cloud for Secure File Sharing

The advice for CISO teams here is to spend time investigating how public cloud file sharing works, including how mobile device access can be controlled, and to then create plans to move in this direction with a suitable overlay or embedded cyber security solution. Avoiding public clouds for secure file sharing in 2017 will be like avoiding browsers for information retrieval in 1994.

As a result, in the near and longer terms, secure file sharing methods for the enterprise will shift toward cloud-based tools, often with the associated concept of creating trusted sharing groups, or even a trusted sharing community. This is not only true for conventional sharing between business users with PCs and mobile devices, but also in newly emerging machine-to-machine environments where the concept of mutual cooperation between machines will increasingly rely on sharing. Enterprise-hosted tools for sharing will continue to see diminishing use and growth.

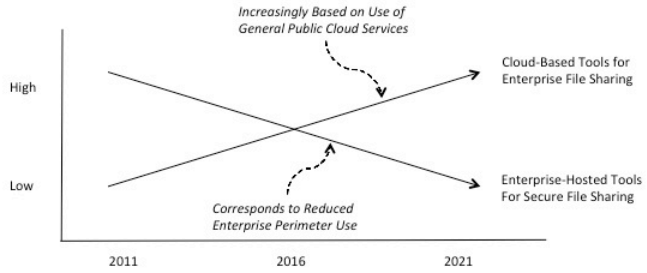

Figure 15-3. Trends in Secure File Sharing

Many companies still use plain text email to distribute sensitive files, so the need will certainly remain for improved methods of sharing. Similarly, many system administrators still access sensitive files such as configuration controls using untrustworthy protocols such as telnet. This practice is becoming increasingly unacceptable to auditors and regulators. The need will therefore remain, and likely increase, for more secure protocols such as SSH.

Advice for secure file sharing vendors here is straightforward: Every vendor offering secure file sharing must have a strong and clear roadmap for integrating their capabilities into public clouds or obtaining such capability through partnership

with, merger with, or acquisition of public cloud capabilities. Every secure file sharing vendor should also have the ability to create and support trusted sharing groups or communities, perhaps even with high assurance vetting.

The existential threat of native security in public cloud services, including ones that operate intimately with mobile device such as Apple's iCloud must be considered a serious business issue, however. The barrier to entry for existing cloud providers to extend more secure means for sharing is low – and could have a dramatic impact in this area. One might expect to see mergers and acquisitions between cloud operators and secure file sharing vendors in the coming years.

Secure File Sharing Providers

CISO teams should obviously include their legacy secure file-sharing providers in any source selection consideration, even if the deployment is currently enterprise-based and protected by the shrinking perimeter. Furthermore, just about any company offering cloud storage, collaboration, or sharing will likely include a set of security controls. So the source selection and consideration for secure file sharing for most CISO teams will often include a lot of companies and cloud providers who might not normally be viewed as cyber security companies. Companies such as Apple that provide mobile app ecosystem distribution and also sharing are considered outside the scope below.

2017 TAG Cyber Security Annual
Distinguished Secure File Sharing Providers

Securitinet – I had the recent good fortune to run into Dan Geer, one of cyber security's great luminaries at a computer science workshop held at MIT. I found out soon after that Dan was involved with Mark Morley in a small start-up called Securitinet that was focused on secure file sharing through trusted, vetted communities using cryptographic protocols. Mark was kind enough to explain the concept to me in person during two separate breakfasts in New York, and I learned quite a bit, especially with respect to the serious sharing challenges that exist in industries such as medical and insurance. My thanks are offered to Mark and Dan for their help in explaining this vital control area to me.

2017 TAG Cyber Security Annual
Secure File Sharing Providers

Accellion – Accellion provides range of secure file sharing capabilities for enterprise customers.
Amazon Web Services (AWS) – AWS offers impressive support for enterprise and individual file sharing and collaboration capabilities. The power and reach of AWS cannot be underestimated, and any CISO team choosing to ride the AWS technology curve will likely not go wrong.

ANX – Southfield-based ANX offers managed compliance and collaboration solutions for the enterprise.
AvePoint – AvePoint, located in Jersey City, specializes in security and compliance of Microsoft enterprise solutions including SharePoint.
Averail – Averail is a mobile security firm offering security solutions for accessing, managing, and sharing content on mobile devices.
Axway – Axway provides range of secure file sharing capabilities for enterprise customers including support for cloud APIs.
Biscom – Biscom provides support for secure file transfer of large and confidential files.
Blackberry (Watchdox) – The acquisition of Watchdox provides Blackberry with an excellent secure file sharing solution. CISO teams should keep an eye on Blackberry in this regard because they have such a fine legacy in the secure mobile area.
Boldon James – Boldon James offers data encryption and classification in support of file protection via sharing.
Brainloop – Brainloop, located in Germany, provides secure collaboration and control with external partners.
Citrix – The virtualization company offers sharing via its workspace-as-a-service solutions.
Cloak Labs – Cloak Labs provides end-to-end encryption of application data from the enterprise to partners.
Comilion – Comilion provides decentralized solutions for secure collaboration and sharing.
Content Raven – Content Raven provides cloud-based solutions for protecting the distribution of files to internal and external groups for enterprise customers.
Covata – Australian firm Covata offers encryption-based secure file sharing solutions.
Covertix – Covertix provides a range of encryption rights managed file security protection solutions.
Deep-Secure – Deep-Secure provides a cyber security guard solution for organizations to securely share information across their network boundary.
docTrackr – Part of Intralinks, docTrackr offers solutions for controlling and managing document sharing.
EMC (Syncplicity) – EMC provides a means for securely sharing and syncing files for business.
Exostar – Herndon-based Exostar includes secure collaboration along with identity and secure chain management products.
FinalCode – San Jose-based FinalCode offers a solution for secure file sharing in the enterprise.
Globalscape – San Antonio-based Globalscape offers managed, secure file transfer solutions.
Google – Cloud and computing services from Google include support for enterprise and individual file sharing and collaboration. With its identity and related security

solutions for enterprise, Google will be a powerful and strong partner for companies desiring enterprise file sharing solutions.
HoGo – New Hampshire-based HoGo offers DRM-based protection for sharing enterprise documents.
HPE/Voltage – The acquisition of Voltage by HPE provided the company with a world-class encryption capability with advanced secure file sharing support.
IBM – Cloud services from IBM include support for enterprise and individual file sharing and collaboration. IBM understands the enterprise and the cloud, so CISO teams will benefit from IBM as a partner in solving the secure file-sharing puzzle in the near and long term.
Ipswitch – Massachusetts-based Ipswitch includes secure, automated, managed file transfer and secure FTP solutions.
IRM Secure – IRM Secure provides security solutions for information usage control, information rights management (IRM), and secure outsourcing.
JIRANSOFT – The los Altos-based firm provides a SaaS platform for secure storage and control.
Kerio – San Jose-based Kerio offers UTM and secure collaboration solutions for the enterprise.
Linoma Software – Linoma offers a range of cyber security solutions including secure file transfer.
Microsoft – Microsoft is the undisputed leader in enterprise hosted file collaboration today with its fine SharePoint solution. Every CISO team likely has a SharePoint footprint today, and Microsoft will remain an excellent partner as these services are virtualized. Cloud services from Microsoft in their Azure infrastructure include excellent support for enterprise and individual file sharing and collaboration.
Mimecast – Mimecast, located in the UK, provides email cloud services support security, archiving, and collaboration.
nCrypted Cloud – nCrypted Cloud offers encryption-based data security solutions for sharing files in the cloud.
NEXOR – UK-based NEXOR offers security solutions for information exchange and information assurance.
Owl Computing Technologies – Owl offers a data diode for cross-domain secure data transfer.
Pawaa – Now part of Cisco, the Indian firm offers secure on-premise, encrypted file sharing capabilities.
SecSign – SecSign Technologies provides two-factor authentication, encryption, and related file sharing capabilities.
Securitinet – The small firm provides a range of cloud-based cyber security solutions for businesses with critical data. The design includes input from well-known Dan Geer, and includes support for medical applications. Securitinet is a good example of the type of vendor now focused on using the cloud to provide secure sharing capabilities for designated business applications.
SendSafely – New York firm, SendSafely, offers secure file transfer across a zero knowledge enterprise platform with encryption.

SendThisFile – SendThisFile, located in Kansas, offers products for secure file transfer with the capability to send files too big for email.
Soltra – Soltra supports open, automated intelligence with Soltra Edge, consistent with STIX and TAXII specifications.
Soonr – San Jose-based Soonr provides a cloud-based secure file sharing solution for enterprise and mobility.
STEALTH Software – Located in Luxembourg, STEALTH Software offers security protections for SharePoint and .NET applications.
Surevine – The UK-based Surevine provides a secure collaboration solution for the enterprise.
TeraDact – The Minnesota-based company offers secure information management and sharing solutions.
Terbium Labs – The small company offers fingerprinting solution that can detect stolen intellectual property.
TITUS – TITUS, located in Canada, offers secure file sharing and leakage protection solutions.
Tresys – The Tresys secure transfer product offers deep content inspection and related security features.
TruSTAR – TruSTAR provides an anonymous means for sharing of threat and vulnerability information with a community.
Varonis – The New York-based Varonis offers solutions for data governance via file sync and share.
Vera – Vera, located in Palo Alto, offers a solution for securing data and files with enterprise protections.
Votiro – The Israel-based company offers data security solutions including sanitization tools.
Workshare – The UK-based Workshare offers secure file sharing and document collaboration tools.

Additional Secure File Sharing Providers

Apple (iTunes) – Apple device and content services on iTunes includes support for file sharing and collaboration. The company has been slow to adopt strong enterprise support, and continues to struggle with offering compliance information for audits. But Apple is so omnipresent that every CISO must fold Apple sharing solutions for PCs and mobile devices into its strategy.
Authentica – Authentica supports data management solutions for a common data store across educational districts.
Box – Box cloud storage services include support for file sharing and collaboration. Box is a strong and growing company that will likely play an important role in many enterprise file sharing and collaboration plans in the future.
Connected Data – Connected Data offers a solution called Transporter that enables business and government to own and control information.

Egress Software Technologies – Egress offers managed file transfer with encryption and other security features.
Globalscape – Globalscape offers a range of secure file transfer and secure information exchange solutions.
Hightail – Formerly YouSendIt, Hightail provides secure file sharing services for small business and consumer applications.
Huddle – Huddle provides an offering that supports secure team collaboration services in the cloud.
JSCAPE – JSCAPE provides a Web-based solution for monitoring file transfer applications.
LeapFILE – LeapFILE offers business secure file transfer services via Web application or desktop client.
Safe-T – Israeli firm Safe-T offers solutions for managing secure data exchange between business, people, and applications.
Seclore – Seclore is an Indian firm that provides customers with secure file sharing services.
Senditonthenet – Senditonthenet is a free and secure file transfer and sharing services with client-side encryption.
ShareVault – ShareVault provides range of secure file sharing capabilities with emphasis on Microsoft SharePoint.
SmartFile – SmartFile offers secure file sharing service and FTP hosting for business customers.
SmartVault – SmartVault is an on-line document storage and secure file sharing capability for business.
Softlock – Softlock offers a Secure Data Exchange solution for secure document and file exchange.
Thru Inc. – Thru Inc. offers an enterprise file sync and sharing service with cloud storage and secure managed transfer.
Vaultize – Vaultize supports enterprise secure file sharing through a range of DRM support capabilities.

16. VPN/Secure Access

- ⇒ *Access Risk* – Lateral East-West traversal has been the primary means for cyber attack once north-south remote access is achieved into an enterprise.
- ⇒ *Two VPN Methods* – Clientless Secure Sockets Layer (SSL) and client-requiring IPSec access solutions are two currently popular VPN approaches.
- ⇒ *Shift to "Per-App" VPN*– Most organizations will begin accessing public cloud-resident application from mobile devices over dedicated "per app" VPNs.

Most of the prominent enterprise cyber attacks in the past few years have involved third-party break-in through poorly conceived *remote access*. For many years, companies ran partner and external gateways that would check source IP address

information to validate the network origination of the request, followed by simple password authentication to validate the user. Such methods have become child's play for hackers, and provide barely a speed bump for advanced threat actors.

In parallel with this increasing threat, a sector of the cyber security industry had been emerging that focuses on more secure point-to-point access between entities over untrusted networks. The result was a *virtual private network* (VPN), so-named because the privacy comes not from the underlying physical plant (as in old-fashioned circuit switching), but rather from logical controls, often cryptographic, that segregate communication and access from other public traffic. From a practical perspective, VPNs have been differentiated using a variety of factors, the most important of which is the type of client employed by end users.

Since the general concept of VPN is so broad, many additional network and computing offers use the same heading. For example, service providers offer large-scale "VPN" solutions to their enterprise customers, where the virtual separation in creating a local enterprise is done using protocol labels as in multi-protocol label switching (MPLS). Labels certainly do offer traffic separation in multi-user environments such as with an ISP, but they were never designed as strong security controls, and certainly do not include cryptographic controls to stop cyber attacks across traffic streams. For example, no enterprise would rely on MPLS labels as their security perimeter.

VPN offerings that allow for secure remote access, on the other hand, generally do include provision for stronger security separation and segregation. These offerings usually come bundled with front-end strong authentication, and support for securely administering the corresponding remote access server, if enterprise hosting and local support are the desired methods. When an enterprise outsources work to a remote third party, for example, the security aspects of a selected remote access VPN solution are often the primary security control.

Two basic types of underlying secure access-related technologies have become popular with VPN solutions in recent years: Secure Sockets Layer (SSL) and IPSec. The main differentiation between the two utilities is listed below:

- *Secure Sockets Layers (SSL)* – SSL provides secure access and encrypted VPN support where the initiating endpoint is the user's browser. When users buy items on the Internet securely from their browser, SSL is the presumptive method being used.
- *IPSec* – IPSec provides secure access and encrypted VPN support, but also requires the installation of a special client for end users. IPSec was smoothly designed into the IP protocol suite.

The main advantage of SSL obviously is its clientless operation, which reduces cost and administration. Open-source versions of SSL are available – albeit somewhat reputation-tarnished with the OpenSSL/Heartbleed security issues that occurred in 2014. Open/SSL is a viable solution for organizations with some technical talent, but a limited budget. Even with clientless operation, however, the configuration of a

VPN has generally been between external entities and the corporate perimeter, with VPN gateways positioned at the enterprise edge for access. As suggested above, ISPs offer such service to create an enterprise LAN, albeit with separation labeling as in MPLS, used for traffic management rather than strong security protection. Perimeter VPNs with encryption certainly improve the source IP address usage for network origination, and every small or medium sized business using password-based remote access should move to a more secure VPN usage immediately.

Even with such secure access improvement, businesses – especially large ones – remain vulnerable to East-West attacks by intruders once VPN access has been obtained. In cases where the VPN client is authenticated with nothing more than a password, this is clearly a greater risk. The risk can be mitigated somewhat with a second authentication factor, but unfettered enterprise traversal once access has been established is still highly concerning.

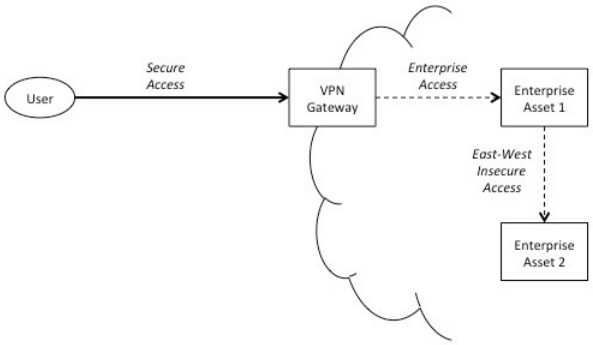

Figure 16-1. External VPN Access to Perimeter – East-West Risk

To deal with this East-West risk and to ensure consistency with the clear migration to mobility accessible cloud services, companies have begun to utilize a "per-app" VPN solution embedded in the client-server handshake from mobile to cloud-hosted application. This is a truly welcome transition because it combines so many different advantages from a security perspective.

First, it ensures encrypted communications between mobile and cloud app, which is essential over WiFi and other public communications. Second, it encourages a reduced emphasis on the corporate perimeter since the connection between client and app is point-to-point, without the open East-West traversal found in current enterprise. Finally, it enables a three-factor solution where users can biometrically authenticate to their device, a mobile device management solution can supply a cryptographic certificate to the application, and then the user can be interrogated to supply a password.

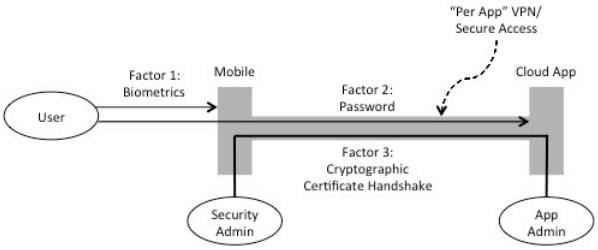

Figure 16-2. Three-Factor "Per-App" Security Between Mobile and Cloud App

A related capability generally viewed as part of the VPN/Secure Access marketplace involves hiding IP addresses from prying eyes during browsing sessions and other Internet activity by consumers, citizens, and individuals. This type of VPN-related capability has less implication on enterprise security, but utilizes similar technology and underlying infrastructure between end users and servers that act as intermediaries for online service access.

The market for VPN/Secure Access is healthy and growing, but will shift from gateways at the enterprise perimeter to "per app" VPNs that are embedded invisibly into mobile access to cloud workloads. CISO teams should look for creative vendor implementations of this concept, such as the Cryptzone approach of a so-called "segment of one," which is essentially a virtual private session between a client and an application.

This secure access shift is also true for the IoT market, where VPNs between industrial devices and control systems will require secure connectivity using VPN technology. Unfortunately, with so many legacy IoT devices having uneven operating system environments, the transition to more secure access for purposes of management and telemetry will be less smooth. Nevertheless, the VPN/Secure Access and enterprise mobility industries will begin converging on common, secure access methods for mobile and IoT devices to cloud infrastructure.

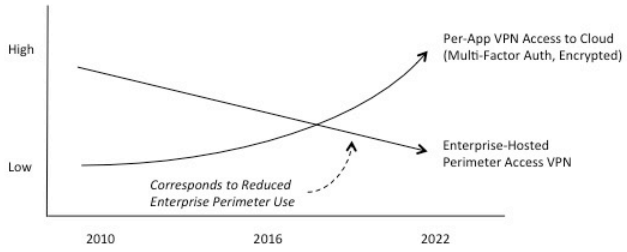

Figure 16-3. Enterprise VPN/Secure Access Market Trends

One final note worth reinforcing: Enterprise CISO teams should immediately review their perimeter-based remote access gateways to ensure that any VPN or secure access tools in place for external parties employ at least two-factors for authentication. Over time, this architecture will shift to cloud, but in the meantime,

weak authentication using passwords just asks for trouble. No modern CISO should be comfortable with password-authenticated remote access into the enterprise.

VPN/Secure Access Providers

The vendors listed below include companies focused on enterprise secure remote access needs, as well as the surprisingly large number of vendors trying to help consumers hide on the Internet from surveillance. These two purposes are fundamentally different, but the technology base involves similar functionality and infrastructure. CISO teams will certainly have much less use for these consumer-based VPN anonymity and privacy tools, but they are included below for completeness.

CISO teams should also recognize that their Internet Service Provider (ISP) and Mobile Service Provider (MSP) solution provider will invariably offer a range of secure remote access capabilities, as will any value added reseller. In many cases, especially with mobility solutions, this is done in the context of a larger network support arrangement to the enterprise, rather than as a stand-alone security solution.

2017 TAG Cyber Security Annual
Distinguished VPN/Secure Access Providers

Cryptzone – Barry Field and the team at *Cryptzone* sat down with me in San Francisco and gave me an extensive technical overview of their concept of a "segment of one." Embedded in their AppGate platform, the concept seemed to embody all of the different security requirements I've seen around modern remote access architectures. My friend Manny Medina from Medina Capital also provided useful guidance on the market to me on several occasions in New York City. I am grateful to Barry, Manny, and the entire Cryptzone team for their help at nearly every stage of my research.

2017 TAG Cyber Security Annual
VPN/Secure Access Providers

AnchorFree – Mountain View-based AnchorFree provides VPN solutions for secure Web browsing.
Anonymizer – San Diego-based Anonymizer provides a personal VPN service for private Internet access.
AT&T – The large US domestic carrier can design effective remote access service solutions for business customers with support for two-factor authentication. Carriers have an advantage supporting these solutions since the work is so adjacent to the types of provisioning and maintenance required for business VPN solutions. VPN-like capabilities will also begin to emerge between cloud workload and IoT endpoints from carriers like AT&T who are embedding SDN into their core. Support

for such VPN/Secure Access will likely be designed into the SDN controller (e.g., an ICS device needing access to a cloud-based database to drop telemetry will do so through secure access over a virtual SDN connection).
Barracuda – Barracuda offers an SSL VPN client-less solution for secure access via a Web browser.
Bomgar – Headquartered in Mississippi, Bomgar offers secure remote access through firewalls without the need for a separate VPN.
Celestix – Fremont-based Celestix provides secure remote access connectivity to cloud and distributed offices.
CipherGraph – The Pleasanton firm offers secure cloud-based VPN solutions for its customers.
Cisco – Cisco provides its AnyConnect Secure Mobility Client for "per app" VPN support and secure endpoint access to enterprise resources.
Clavister – Headquartered in Sweden, Clavister provides a range of network security solutions including VPN.
Cryptzone – Cryptzone offers a gateway solution that supports a so-called "segment of one" for secure access to the enterprise. Increasingly, secure access products, such as Cryptzone's AppGate, are emerging that are designed in full recognition of the dissolution of the traditional perimeter. These products will integrate with SDN from ISPs into more effective means for handling third party access to company resources.
F-Secure – F-Secure offers the Freedome VPN for Windows, OS X, iOS, and enterprise business.
Huawei – The large Chinese networking firm offers a range of network security products including support for remote access.
IBM – IBM offers its customers the IBM Mobile Connect, a fully featured wireless virtual private network.
Juniper – The large networking firm offers a range of network security products including support for remote access.
OpenVPN Technologies – Headquartered in California, OpenVPN Technologies provides an open VPN solution deployable as software or appliance.
Pulse Secure – Pulse Secure, spun off from Juniper, offers a consolidated access control, SSL VPN, and mobile device security solution for the enterprise.
SecureLink – The Austin-based company offers its SecureLink remote support network for secure remote access by third parties.
Soha Systems – Soha Systems provides an enterprise secure access solution for third parties and employees.
Spotflux – Spotflux offers a secure, managed connection to the Internet for mobile devices and desktops.
SSH – The Finland-based firm offers SSH key management, privileged access control, and identity solutions.
Uniken – Located in Florida, Uniken offers secure virtual private networking solutions.

Verizon – Verizon offers a range of remote access service solutions for business customers with support for strong authentication.
ZenMate – The German company offers a privacy and security-enhanced browser for virtual networking.

Additional VPN/Secure Access Providers

AirVPN – AirVPN provides a VPN based on OpenVPN and operated through community involvement.
CyberGhost – CyberGhost provides downloadable software in support of on-line secure browsing to avoid behavior tracking.
Hideman – Hideman allows unblocking of Websites, hiding IP addresses, and removal of surfing limits.
Hotspot Shield Elite – Hotspot Shield Elite secures connections during surfing over WiFi hotspots.
IPVanish – IPVanish hides IP addresses during surfing and other online resources.
Juniper
NordVPN – NordVPN offers an application for anonymous surfing with no logging policy.
Private Internet Access – Private Internet Access offers high-speed anonymous VPN services for Internet access.
PureVPN – PureVPN delivers a fast VPN service with support for online privacy and security.
TorGuard – TorGuard offers anonymous VPN services in support of end user privacy.
Tunnelbear – Tunnelbear offers a mobile VPN that is designed to unblock and secure Websites.
VyprVPN – VyprVPN offers a secure VPN that runs on Windows, Mac, and other platforms.

17. Anti-Malware Tools

- ⇒ *Traditional Anti-Virus Methods* – Anti-virus software is perhaps the most traditional and well-known technique in the cyber security defensive arsenal.
- ⇒ *Signature Weaknesses* – Attackers have mostly figured out how to develop variants to by-pass traditional signature-based anti-malware security.
- ⇒ *Holistic Malware Prevention* – New advanced algorithms for preventing malware are more holistic and based on improved detection methods.

The presumption is made here that *viruses* are special cases of *malware* that mainly target endpoint personal computer (PC) systems. This definition includes all forms of PC infections including traditional file-based viruses, rootkits, and more modern spyware tools. The types of product features assumed in traditional *anti-virus (AV)*

and *Internet security* products include anti-virus protections, suspicious Website identification, phishing risk reduction, unauthorized Webcam access detection, dangerous WiFi network identification, PC firewall capabilities, password management, safe Web surfing, and many other creative controls.

The concept of PCs becoming infected with viruses is the most traditional and familiar aspect of computer security. The security tools for dealing with viruses have been based on *signatures*, which involve matching patterns of observed behavior with descriptions of known attacks and intrusion indicators. Vendors have had to compete based on the quality and quantity of their signatures. As a result signature databases in most anti-virus products are enormous in size with many millions of attack descriptions embedded in the security detection functionality.

Unfortunately, as the number of known attacks has grown exponentially, and as zero-day vulnerabilities continue to abound, the practical usefulness of signature-based security for PC virus risk reduction has continued to drop. Simply stated: the amount of work required to build a variant around a signature is many orders of magnitude smaller than the amount of work required to surround an attack and its possible variants. In the worst case, as with any signature based on a specific file name, one could argue that the possibility of covering all variants (i.e., all possible file names) is effectively zero.

The trends in the more modern *anti-malware tools* market that CISO teams should understand begin with a period of relative stability for signature-based solutions from the Millenium change to roughly 2003. Significant growth was experienced in the cyber security industry in malware, worms, and enterprise viruses in 2003 with Blaster, Nachi, and other well-known events causing problems worldwide. Since then, the number of viruses and variants has seemed to explode in intensity, rising to the current unacceptable rate. During this time, the health and relevance of signature-based anti-virus solutions gradually decreased.

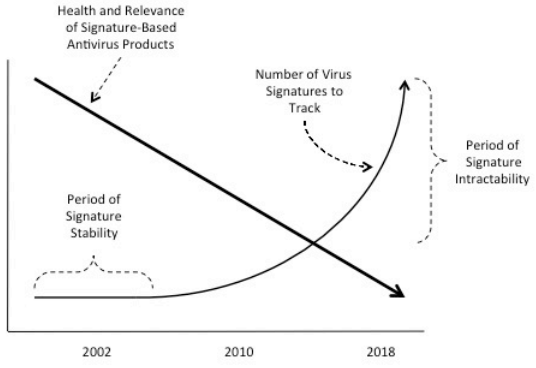

Figure 17-1. Signature Trends for Anti-Malware Tools

To deal with these signature deficiencies, *behavioral analytic* and other creative anti-malware tools have been developed to detect intrusion indicators more

effectively. This more run-time approach compares baseline profiles of empirically normal activity with observed activity from log management or SIEM tools. Measured activity can include operating system processes at the kernel or application layer, or the application-level behavior of a user through an interface. If the baseline and observed behaviors are sufficiently different, then a potential intrusion is flagged. The potential for false positives increases with inaccurate profiles or incorrect log management.

Just as the industry began to effectively write-off static analysis of binaries and code for malware, vendor solutions began to emerge that utilized better heuristic methods for detecting problems. Usually, the better solutions, such as from companies such as Malwarebytes, tend to find creative ways of representing and modeling the structure and behavior of malware. Then, by imposing different types of mathematical and statistical analysis against the models, risk scores of likelihood of maliciousness can be developed. This is a great advance from the more traditional static signature methods.

The outlook for both static and run-time anti-malware products is mixed. As the number, size, and scope of viruses, worms, Trojans, and variants have all increased, traditional and installed anti-virus signature tools have lost some relevance accordingly. If it were not for general inertia of maintaining existing controls, as well as the pressure from auditors to not change environments that have been assessed and certified, the use of anti-virus solutions would have dropped more aggressively in previous years.

As organizations move from traditional PCs to mobile-accessible, cloud-based solutions, however, a continued push will be felt to drive the use of existing anti-virus products to something much more effective on the endpoint. The good news for vendors in this area, however, is that opportunities do exist to create new growth. First, the use of behavioral analytics on the endpoint represents a feasible transition that can reuse existing anti-virus infrastructure such as management and deployment tools. While these controls tend to be run-time versus static, they can still satisfy auditors and reduce real risk.

Second, the transition to mobile device endpoints, combined with an inevitable growth in mobile threats, will drive the need for mobile endpoint anti-virus solutions, presumably using advanced heuristic algorithms and risk scoring. This mobile emphasis will include IoT and industrial control devices, which will require the same intensity of anti-malware protection as exists for PCs and servers today. These solutions can be represented as software libraries to be folded into the code of newly developed IoT devices, or they can be created as software packages that can be run adjacent to the IoT function.

Finally, CISO teams can expect that the traditional static analysis tools in use today for detecting viruses in binaries will continue to improve. Databases such as Google's VirusTotal will continue to help researchers and analysts compare their detected malware against industry baselines. Furthermore, as information sharing mechanisms continue to improve, CISO teams will find it easier to work with other

teams to help determine if something considered suspicious is indeed malicious, not to mention perhaps identifying exactly where it may have originated.

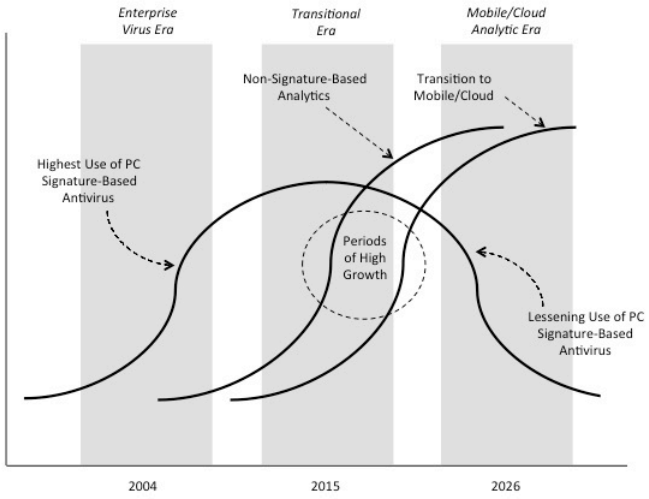

Figure 17-2. Trending in Anti-Malware

It is worth mentioning that anti-virus management tools such as Intel McAfee ePO can be useful for testing add-on tools such as enhanced forensics at the endpoint. This provides an additional powerful incentive for CISO teams to maintain their existing endpoint security infrastructure and will help new and existing anti-malware firms maintain revenue goals while working on new solutions for mobile, IoT, and cloud workloads.

List of Anti-Malware Tool Providers

Several years ago, the computer security industry consisted almost exclusively of anti-virus and Internet security software vendors. As time progressed, however, the signature-based, blacklisting nature of anti-virus software solutions became less desirable for detecting viruses, and the industry began to expand beyond this type of safeguard. In spite of this shift, anti-virus and Internet security, now more often referred to as anti-malware solutions, continue to be one of the most common vendor provided security protections; hence, the list of vendors in this category remains extensive.

In addition, an unusually large number of companies offer free anti-virus software downloads. While I might not recommend free anti-virus for major enterprise, it does provide a good way to evaluate new methods. CISO teams are advised to consider the anti-malware solution vendor list below in close comparison and conjunction with the Endpoint Security provider list, covered in a separate section of this volume.

2017 TAG Cyber Security Annual
Distinguished Anti-Malware Tool Providers

Malwarebytes – Like most cyber security practitioners, I'd begun to lose confidence years ago in the ability of most existing anti-virus solutions to detect the types of malware that were causing operational and compliance issues. I personally first noticed endpoint security provider Malwarebytes about a year ago, based on their popular distribution of a free PC anti-malware and endpoint security tool. Interestingly, this free tool seemed to do a pretty good job cleaning up malware, so I wanted to learn more. What I discovered during my research was a capable firm led by visionary technologists who were applying clever new algorithms to a traditional problem. I am so appreciative of all the time the Malwarebytes team spent helping me re-learn a control area that is so vital to enterprise cyber security.

2017 TAG Cyber Security Annual
Anti-Malware Tool Providers

AhnLab – AhnLab is a South Korean firm that offers V3 Internet security tools for business endpoint protection.
Antiy Labs – The Chinese company offers an anti-virus SDK engine and anti-virus service.
Avast – Czech Republic-based Avast offers standard free and upgraded PC and mobile anti-virus and Internet security tools. Avast acquired Jumpshot in 2013.
AV-Europe – The Netherlands-based firm distributes various security products including anti-virus and Internet security.
AVG – Netherlands-based firm, AVG, offers free and upgraded PC anti-virus and Internet security tools.
Avira – German firm Avira offers a range of free and upgraded PC anti-virus and Internet security tools.
Bitdefender – Bitdefender, headquartered in Romania, offers a range of standard PC anti-virus and Internet security products.
BullGuard – UK-based firm offers the standard set of PC anti-virus and Internet security tools.
Comodo – Comodo offers the standard set of free, downloadable PC anti-virus and Internet security tools.
CrowdStrike – George Kurtz's firm CrowdStrike includes anti-malware solutions in its extensive range of cyber security and response solutions.
Cylance – Founded by Stuart McClure, Cylance uses a variety of advanced heuristic techniques such as machine learning and AI to detect malware in computing endpoints.
Dr. Web Ltd. – Dr. Web Ltd. is a well-known Russian anti-virus and Internet security firm.
Emsisoft – Emsisoft, headquartered in Austria, offers its customer a suite of anti-malware and Internet security tools.

ESET – ESET is a well-known global cyber security company that offers range of PC anti-virus and Internet security tools.
FireEye – FireEye helped invent the run-time virtual detection of malware through safe detonation.
Fortinet – Fortinet includes free PC anti-virus and Internet security tools in its FortiClient offering.
F-Secure – F-Secure, located in Finland, offers online PC scanning and security tools for home and business use.
G Data – German company G Data offers customer a standard set of PC anti-virus and Internet security tools.
GFI Software – The Luxembourg-based firm provides a range of IT security products and services.
Google – The VirusTotal free resource is an excellent service from Google that allows researchers to help identify and understand their malware.
Hitman Pro – Hitman Pro from SurfRight in the Netherlands offers standard set of PC anti-virus and Internet security tools.
Humming Heads – Located in Japan, Humming Heads provides anti-virus and Internet security products.
Ikarus Security Software – The Austrian firm offers a range of virus prevention tools for mobility and cloud.
INCA Internet – The South Korean firm provides security solutions including anti-virus.
Intego – Intego offers a range of PC anti-virus and Internet security tools for Apple Mac users.
Intel – Intel continues to provide world-class capability for enterprise anti-malware controlled by its ePolicy Orchestrator.
Kaspersky – Eugene Kaspersky's Russian firm offers standard set of PC anti-virus and Internet security tools for home and business.
Malwarebytes – Malwarebytes provides advanced anti-malware detection algorithms in its security offering. The company originated with a creative young founder who developed novel detection techniques that grew into a leading anti-malware firm.
Microsoft – Microsoft Security Essentials includes the standard set of PC anti-virus and Internet security tools.
Network Intercept – The Los Angeles-based firm offers anti-malware and keystroke encryption for PCs and Macs
Panda – Spanish firm Panda offers standard set of PC anti-virus and Internet security tools.
Qihoo – The Chinese company's product Qihoo 360 includes PC anti-virus and Internet security tools.
Sophos – Sophos offers standard set of PC anti-virus and Internet security tools for business customers, including its SurfRIght solution.
SUPERAntiSpyware – The Redwood City-based company offers Roboscan, Spybot, and SuperAntiSpyware anti-virus and Internet security tools.

Symantec – Symantec is an industry leader in providing advanced endpoint anti-malware detection solutions based on the famous Norton anti-virus suite. CISO teams cannot ignore the experience and expertise inherent in traditional vendors who know how to push software, make updates, and deal with incidents in ways that minimize business disruption.
ThreatTrack – ThreatTrack offers standard set of PC anti-virus and Internet security tools.
Topsec Science – The Chinese company offers anti-malware tools as part of its suite of security products.
Total Defense – Located in New York State, Total Defense offers anti-malware solutions for PCs and mobiles.
Trend Micro – Trend Micro offers a full range of PC anti-virus and Internet security tools.
TrustGo – TrustGo, part of Baidu, offers customers a full set of mobile anti-virus and Internet security tools.
Trustlook – Headquartered in San Jose, Trustlook offers anti-virus and ani-spyware solutions.
TrustPort – TrustPort from the Czech Republic offers a range of anti-malware security tools for home and enterprise.
Webroot – Webroot, headquartered in Colorado, offers standard set of PC and Mac anti-virus and Internet security tools.

Additional Anti-Malware Tool Providers

Advanced System Care – Advanced System Care offers PC tools for protection, optimization, and other functions.
Agnitum – Agnitum offers Outpost Security Suite with PC anti-virus and Internet security tools.
AppGuard – Blue Ridge Networks offers AppGuard anti-malware and Internet security tools.
Ashampoo – Ashampoo offers standard set of PC anti-virus and Internet security tools.
ClamXav – ClamXav offers a standard set of Mac anti-virus and Internet security tools.
eScan – eScan offers its customer a standard set of PC anti-virus and Internet security tools.
FixMeStick – FixMeStick is a virus removal device to clean infections from user personal computers.
IObit – IObit offers a range of Apple Mac performance and security tools including anti-virus.
Kromtech – Kromtech offers standard set of Mac anti-virus and Internet security tools.
Lavasoft – Lavasoft offers a free Ad-Aware product that includes the standard set of PC anti-virus and Internet security tools.

Norman Security – The Norman Security Suite includes the standard set of PC anti-virus and Internet security tools.
Quick Heal – Quick Heal offers the standard set of PC, Mac, and Mobile anti-virus and Internet security tools.
SecureIT – Security Coverage offers the standard set of PC anti-virus and Internet security tools.
ThirtySeven4 – ThirtySeven4 offers standard set of PC anti-virus and Internet security tools for schools, universities, business, and home.
Valt.X – Valt.X offers its customer a range of non-signature-based anti-malware tools.
VoodooSoft – The company offers VoodooShield anti-virus and Internet security tools.
ZoneAlarm – ZoneAlarm includes PC anti-virus and Internet security tools in its offerings.

18. Endpoint Security

⇒ *Endpoint Protection* – Securing PC and mobile endpoints has always been a fundamental component of every enterprise cyber security program.
⇒ *Variety of Methods* – Many different approaches exist for securing the endpoint including authentication, isolation, and configuration control.
⇒ *Influencing Factors* – Endpoint security will have to address emerging technology initiatives such as BYOD, VDI, IoT, and cloud virtualization.

Endpoint security involves the full range of policy, procedural, and functional controls required to protect enterprise networks from security vulnerabilities that might be introduced by any connected devices. Endpoint security also involves protecting the actual connected devices and their associated information and access from malicious cyber attack. In-scope devices range from the personal computers (PCs), tablets, and mobile phones used by employees, to the packet routers and switches used to operate enterprise networks.

The question of whether servers are considered endpoints is an interesting one, often debated amongst CISO teams. On the one hand, servers are really just computers with hardware, operating systems, and applications, just like a PCs, tablets, and mobiles. As a result, many endpoint security techniques such as integrity checking, patch management, and vulnerability scanning can be applied directly to servers. In contrast, however, most physical enterprise servers are being subjected to virtualization initiatives in the data center at a much greater rate than PCs, tablets, and mobiles. This results in associated cloud security and compliance initiatives for virtual servers that do not look much like an endpoint security program.

So clearly, endpoint security is a complex area, with vendors supporting a plethora of different defensive strategies. For example, CISO teams can focus on

controlling the system administrative and inventory management tasks for endpoints; they can also focus on locking down system configurations for endpoint hardware and software, including how user privileges are managed and how leakage is prevented; additionally, they can protect endpoints through novel techniques such as isolation and containment, sometimes using virtualization. All of these protections augment traditional PC anti-malware tools, with some even making use of traditional PC anti-virus management systems for installation and update.

Corporate IT initiatives that tend to complicate endpoint security deployment include *bring your own device* (BYOD) programs, *virtual desktop initiatives* (VDI), and *cloud virtualization*. All of these initiatives separate management and control of the underlying endpoint hardware from enterprise IT and CISO teams. While this separation might simplify budget and administration, the potential remains for infections to cascade upward from the endpoint hardware and operating system. This separation is also becoming true in industrial control and Internet of Things (IoT) settings, where endpoint devices increasingly rely on the cloud for augmented functionality and control.

Authentication and encryption support tend to be embedded in most endpoint security schemes. This includes traditional device authentication, which has evolved recently from PIN/password to biometrics. Such support can also include certificates used to achieve multi-factor authentication to enterprise applications. Federation of credentials is a growing aspect of endpoint security, especially for mobility-enabled cloud applications. Additionally, compliance requirements have dictated cryptographic controls such as encrypted hard drives on corporate endpoints.

While some might argue that so many diverse endpoint security options improves security by making the cyber attack cascading strategy across multiple endpoints much more difficult to implement, others would claim that such endpoint diversity degrades security through more complex system management and configuration. In the end, both arguments are probably correct since more functionality to stop attacks is always better, but added complexity is also always a significant challenge.

The bottom line is that CISO teams will have to make the effort to achieve the optimal balance in their environment between having a supermarket full of agents on the endpoint with a variety of associated security and management controls – some with full superuser and root privileges to the underlying operating system utilities, and the significant challenge that comes with the management of all this added software.

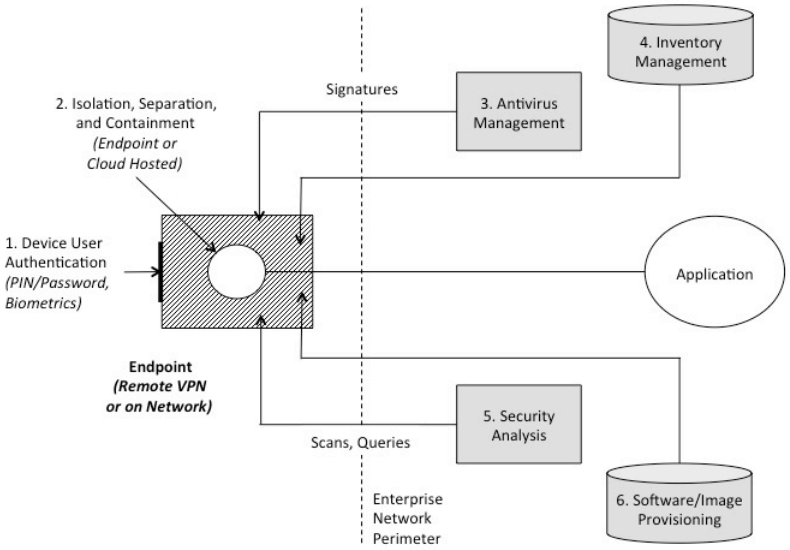

Figure 18-1. Endpoint Security Control Options

The administrative policies and procedures adopted locally to protect endpoints are as important as any vendor-provided functional capabilities. Security training and procedural frameworks are therefore important components in endpoint protection. For example, any experienced CISO team will agree that the majority of enterprise security issues that cause compliance and real break-in risk are the ones caused by system administrators, application owners, or privileged users being sloppy about how that manage and control resources on a server or other endpoint.

To this end, the Center for Internet Security (CIS) establishes a Critical Security Control (CSC) framework that recommends controls for maintaining inventories of hardware and software (CSC 1 and CSC 2), as well as controlling configurations, privileges, access, and accounts (CSC 3, CSC 6, CSC 14, and CSC 16). These controls are best applied through the experience and skills of security administrators. Vendors often map their functionality to the CIS controls, so buyers who use this framework will benefit where applicable.

One area of endpoint security, directly related to security analysis, which receives considerable attention in the community, involves *user behavioral analytics* (UBA). Most UBA schemes work by comparing user activity on the endpoint to some model of what is considered acceptable. This can include esoteric considerations such as process utilization as a function of time, or it can involve more intrusive considerations such as how often an employee checks their LinkedIn account during the day. In all cases, CISO teams are strongly advised to consider the following rules for UBA:

- *Predictable Endpoint UBA* – This type of UBA tends to work well. It is applied in places such as a call or contact center, where employees perform repeat,

predictable tasks. People performing these tasks typically who have a reasonable expectation that their work activities are being monitored.

- *Unpredictable Endpoint UBA* – This type of UBA tends to work less well. It is applied to knowledge workers, such as software developers, who might have less predictable day-to-day endpoint use, and who might be inclined to move to shadow IT solutions such as personal Gmail or personal Box accounts to avoid being monitored.

As alluded to earlier, many endpoint security solutions include client-installed software agents. In most cases, these agents require privileged access to local resources in order to properly monitor, collect, or update the endpoint system. Obviously, these endpoint solutions must have the ability to read information; but a key consideration is whether endpoint agents have the ability to *change* configurations. The case could be made that such powerful remote write capability to a large collection of distributed assets, if hacked, could produce disastrous consequences to the enterprise. So check with your endpoint vendor.

More recently, endpoint security has begun to involve cloud-assisted protections that virtualize functions such as Web browsing and threat intelligence feeds. The progression toward cloud-assisted and isolated endpoint protection follows the growing adoption of public cloud in most enterprise networks. The concept of *cloud access security broker* (CASB) introduces a proxy capability for endpoints trying to access corporate resources. The proxy ensures that endpoints are adhering to security policy without the need for software agents. Isolation of endpoint functions such as browsing to the cloud will revolutionize the endpoint security industry.

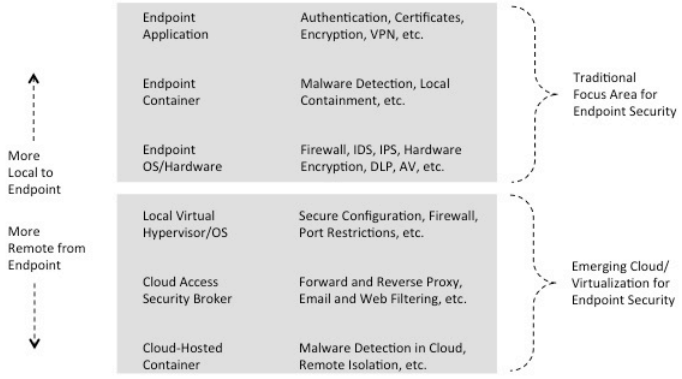

Figure 18-2. Endpoint Security Implementation Options

Trends in endpoint security are tough to predict because so many different initiatives are undergoing dramatic change. Perhaps the best one can do is to predict the relative strength of these various initiatives – BYOD, virtualization, mobility, consumerization of IT, and so on. Such endpoint evolution will be driven by many

different factors, including the inevitable stream of device innovations from companies such as Apple and Google. These will create more choices for endpoints not currently available. Watches, automobiles, and consumer appliances, for example, will emerge as legitimate options for approved enterprise endpoints.

Correspondingly, traditional use of personal computers and workstations on perimeter-protected enterprise LANs will wane as employees move even more aggressively to mobile devices and tablets. Millennials literally *live* on their mobiles, so as they assume more powerful roles in the workplace, they will carry this behavior with them. Furthermore, as traditional enterprise computing shifts to mobile apps and away from enterprise Websites, the endpoint security marketplace will shift accordingly. It is not hard to envision, for example, new businesses starting that create a range of mobile applications, but that don't even bother to create a traditional Website.

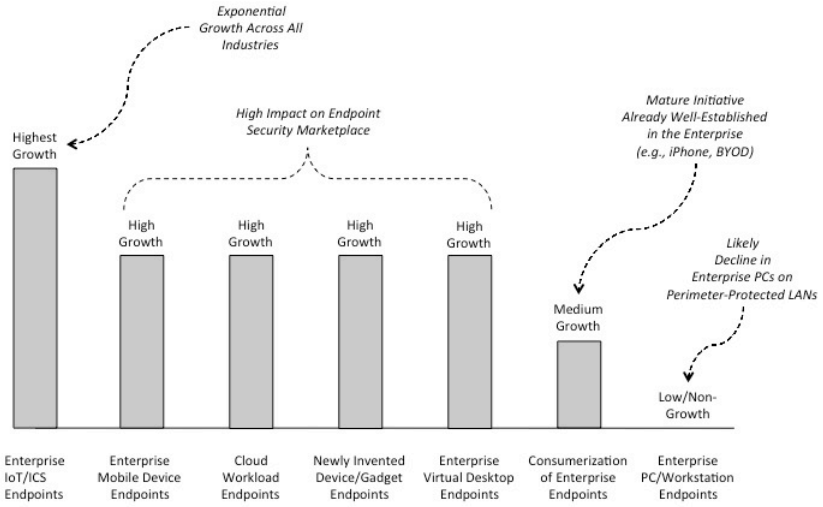

Figure 18-3. Relative Trends in Endpoint Security

With all this change, a number of additional security implications will emerge for supply chain legacy for endpoint hardware and software. The manufacturing of PCs, for example, is now mostly done in some country other than your own, and domestic industries such as defense and energy must include the corresponding security risks as a procurement factor. The most likely trend, however, will be *reduced focus* on such geographic considerations, because the global supply chain has become so interconnected that untangling software and hardware legacies is becoming basically impossible.

Endpoint Security Product Providers

Establishing of list of *Endpoint Security* vendors was hard simply because the field is so scattered across different areas of security technology. For example, two vendors

calling themselves "endpoint security" experts could be working in areas that are not only non-competitive, but that might also be barely complementary. The mobile security marketplace clearly bleeds into endpoint security, and the list below tries to maintain some semblance of separation, since mobile security is dealt with elsewhere in this report, as is anti-malware, which is also so closely linked to endpoint security.

Also, larger mobile ISPs such as AT&T generally include a fine range of managed endpoint security services for the mobile, PC, tablet, IoT, and even set top box device. These types of broad *managed* endpoint services are covered best in the managed security service section of this report since they involve such a broad set of attendant support features. The focus for the extensive list below is more on shrink-wrapped software products and packaged software from technology vendors that can be integrated into an endpoint security solution for the enterprise.

2017 TAG Cyber Security Annual
Distinguished Endpoint Security Providers

Bromium – I've long admired the concept of using virtual containers to isolate an endpoint computing session from the underlying hardware, as exemplified in the Bromium offer. Simon Crosby and his team have spent countless hours helping me understand how this works, never tiring of my endless questions. I had the pleasure of spending some time in New York City recently with the entire Bromium executive team, learning about the wide range of possibilities for containers, CPU isolation, and endpoint protection from advanced cyber attacks. I am so grateful for their kind assistance in advancing my learning and offering support for my research for the past few months.

Cylance – It's impossible to be even marginally familiar with the cyber security industry and not know of the fine technical and business contributions of Stuart McClure. Stu is one of the authors, with George Kurtz (see below), of the best anti-virus signature book ever written. Stu also helped invent the enterprise-scanning tool industry at Foundstone, before creating Cylance. Stu and his team, which includes veteran Malcolm Harkins, were extremely helpful in supporting this work. Discussions with Malcolm, in particular, greatly assisted my understanding of modern endpoint security techniques and algorithms through all phases of this project.

CrowdStrike – George Kurtz, with Stu McClure (see above), is also one of the great luminaries of the cyber security field, and CrowdStrike has developed into a visionary endpoint firm, with advanced algorithms powered by accurate and timely threat intelligence. George and his team, which includes my good friend Shawn Henry, formerly a senior official with the FBI, also integrate cyber forensic investigative capabilities. Readers have probably seen CrowdStrike experts on CBS *Sixty Minutes*, CNN, and other poplar media outlets helping to explain the most recent cyber attack. My thanks are offered to George, Shawn, and the entire CrowdStrike team for supporting this research throughout each phase of the project.

Absolute Software – The Canadian firm provides endpoint security and management solutions.
Atomicorp – The Virginia firm offers advanced security protections for Linux and Windows servers.
AT&T – As mentioned above, larger mobile and Internet service providers manage mobile endpoints in a much larger context than the technology providers listed here. Security services for endpoints are embedded in managed offerings.
Authentic8 – Authentic8 provides secure, authenticated access to Web apps through an isolated securely contained browser.
Autonomic Software – California-based Autonomic provides endpoint management and security plug-ins integrated with Intel ePO.
Avecto – Massachusetts-based Avecto combines privilege management, application control, and sandboxing to provide endpoint security.
Avira– German anti-virus and Internet security provider includes range of endpoint security protections.
Barkly – Boston-based Barkly offers endpoint security that collects real time data to prevent malware attacks.
Beachhead – Beachhead Solutions provides subscription services to secure and manage mobile and PC devices through a Web-based interface.
Black Duck Software – The Burlington-based company offers appliance and container security.
BlueRISC – Located in Massachusetts, BlueRISC provides hardware-assisted endpoint protection.
Bromium – Bromium provides a range of endpoint security protection products that make use of a hardware assisted security container. Containers will continue to grow in relevance to the enterprise as cloud virtualization continues to emerge as a legitimate component of the application-hosting environment.
BUFFERZONE – The Israeli firm provides an endpoint container security solution for enterprise.
Carbon Black – The corporate merger of Bit9 with Carbon Black brings the threat strength of Carbon Black to the endpoint capability of Bit9.
CenterTools – The DriveLock solution from German firm CenterTools includes DLP and encryption.
Check Point Software – Check Point includes endpoint security solutions such as disk encryption for PCs.
Code42 – Minneapolis-based Code42 provides secure data protection for endpoint backup.
Confer – The Waltham-based company offers an endpoint senor that provides early warnings of malware.

CoSoSys – CoSoSys, headquartered in Germany, provides DLP, device control, and mobile device management solution with emphasis on endpoint security protection.
CounterTack – The Waltham-based company provides an endpoint protection solution for active retaliation.
CrowdStrike – CrowdStrike, led by cyber security industry luminary George Kurtz, offers its advanced threat intelligence-based endpoint protection solution via its Falcon platform.
CyberArk – The acquisition of Cybertinel introduced signature-less endpoint security to the CyberArk offer set.
Cybereason – Cybereason combines endpoint security protection with enhanced analysis tools.
Cylance – Cylance offers an advanced endpoint threat detection product using innovative malware detection algorithms. Companies like Cylance provide solutions that bridge the gap between conventional anti-virus and modern endpoint analytics.
Cynet – Cynet collects indicators and supports enterprise analysis for detection and mitigation of threat.
Deep Instinct – The San Francisco-based firm provides intrusion detection solutions for endpoints.
Dell – Dell offers endpoint encryption, endpoint management, and compliance solutions.
DeviceLock – Located in San Ramon, DeviceLock offers endpoint device and port controls.
Digital Guardian – The Digital Guardian offer provides an endpoint security product for data leakage and advanced threat prevention. The endpoint has always been a natural point for DLP security.
Druva – Sunnyvale-based Druva offers endpoint security solutions to support data governance.
Dtex Systems – Located in San Jose, Dtex Systems focuses on insider threat protection using security analytics with behavioral pattern detection. Dtex integrates its offering with various ecosystem partners for product deployment, threat feeds, and other enterprise security functions.
ESET – Traditional anti-virus and Internet security provider ESET includes range of endpoint security protections.
FireEye – The well-known cyber security firm includes a range of advanced endpoint security protections to complement its virtual malware detection and response capability.
Fireglass – Fireglass is a promising start-up from Israel that isolates browser and endpoint sessions using an advanced virtual platform.
Fortinet –Fortinet includes the FortiClient endpoint security solution for its customers.
Great Bay Software – The Minnesota-based firm offers endpoint security solutions for discovery and management of threats.

Guidance Software –The Encase Analytics product from Guidance Software includes EnCase Endpoint Security. The extension of forensic tools into the endpoint protection arena is a natural progression for companies like Guidance.
Heat Software – Heat Software provides unified endpoint management including security.
Identity Finder – New York-based Identity Finder searches computers including endpoints for sensitive information.
Impulse Point – Impulse Point focuses on network access policy enforcement and endpoint security.
Intel Security (McAfee) – Intel includes traditional McAfee endpoint security with popular ePO distribution system for enterprise.
Intelligent ID – The Ohio-based firm provides an endpoint monitoring and protection solution.
InterGuard – Located in Westport, InterGuard offers employee-monitoring UBA solutions for the endpoint.
Invincea – Invincea is one of the pioneering firms at providing a range of advanced endpoint security container technology solutions for the protection and isolation of devices and PCs from the endpoint hardware. Invincea's Norm Laudermilch is one of the cyber security industry's most experienced experts.
iScan Online – The Plano firm offers endpoint scanning and vulnerability detection products.
itWatch – The German firm provides a suite of IT security products including endpoint protection.
Kaspersky – Russian anti-virus and Internet security provider Kaspersky includes a range of endpoint security protections.
Light Point Security – Light Point offers a virtual machine-based browsing solution to contain malware.
Lumension – Endpoint software and management company Lumension offers a range of data protection solutions.
Malwarebytes – Malwarebytes offers world-class anti-malware and complementary endpoint security protections in their offering.
Menlo Security – Amir Ben-Efraim's company, Menlo Security, provides advanced agentless endpoint Web protections through an on-premise or cloud proxy based on novel security isolation technology.
Novell – Novell offers the ZENworks identity-based Endpoint Security Management protection suite.
NPCore – Located in Seoul, NPCore offers a suite of network and endpoint security products.
nTrepid – The Herndon-based company offers a fully-managed virtual machine-based VDI solution for enterprise.
Outlier Security – The Nevada firm provides agentless cyber security solutions for endpoint analytics.
Palo Alto Networks – Palo Alto Networks provides an advanced endpoint protection solution called Traps that focuses on a Zero Trust model to harden endpoints and

applications. The endpoint security solution works on workstations and servers running Windows.
Panda – Spanish anti-virus and Internet security provider Panda includes a range of endpoint security protections for Windows, Mac, and Android.
PFP Cybersecurity – PFP provides embedded integrity verification technology for industrial control and other endpoint devices.
Promisec – The company provides an agentless cloud-based or on-premise solution for securing endpoints.
Quarri Technologies – Austin-based Quarri includes a range of data protection and armored browsing solutions for endpoint control.
Red Canary – The Denver-based firm offers managed endpoint security protections to detect advanced threats.
SentinelOne – SentinelOne is a start-up that provides next-generation endpoint protection products using predictive inspection.
Sirrix AG Security Technologies – Located in Germany, the company offers endpoint security and trusted VPN solutions.
Sophos – Sophos provides a range of protection solutions including endpoint security and control.
Spikes Security – Spikes Security, located in Los Gatos, offers Web security and malware elimination through a browser isolation system.
Symantec – One of the original AV providers includes endpoint security that will become integrated with the Blue Coat portfolio.
Tanium – Tanium provides ultra-fast endpoint scanning, analysis, and discovery through efficient queries. Performance is becoming a bigger issue in endpoint security, especially where live security analysts use the tools to detect malware.
ThreatTrack – GFI spin-off ThreatTrack includes a range of APT detection and prevention solutions for networks and endpoints.
Trend Micro – Traditional anti-virus and Internet security provider Trend Micro includes a range of endpoint security protections.
Triumfant – Rockville-based Triumfant provides an advanced threat detection and remediation solution for endpoints.
Trusted Knight – The company provides browser security protections including keystroke logging prevention.
Trustpipe – Trustpipe offers an advanced endpoint security analytics and protection solution.
Wave – Wave provides the Safend Protector for endpoints, which uses encryption to safeguard data.
Webroot – Webroot offers endpoint anti-malware solutions with related Internet security controls.
Ziften – Austin-based Ziften offers advanced endpoint security solutions with enterprise security analytics support.

Additional Endpoint Security Providers

Arkoon – French company Arkoon merged with Netasq resulting in the Stormshield network and endpoint security protection solutions.
IronKey – IronKey makes encrypted flash drives, external drives, and secure endpoint workspace solutions.
Safetica – Czech firm Safetica offers endpoint security with DLP capability.
SkyRecon – SkyRecon's endpoint protection platform called StormShield offering suite of security features.

19. Hardware/Embedded Security

⇒ *Trusted Execution* – Trusted hardware supports high integrity execution paths to applications through defined interfaces.
⇒ *TPM* – Trusted Platform Modules (TPMs) include cryptographic schemes for assuring integrity in the underlying hardware.
⇒ *IoT and Mobile* – The spectacular growth of IoT and mobile endpoints increases the requirement for trusted, security embedded security.

Perhaps the most basic tenet of computer security from its earliest inception is that *trust* must be built from the bottom up. That is, application software makes use of resources exported upward from an operating system. The operating system, in turn, makes use of resources exported upward from firmware. Correspondingly, the firmware makes use of the underlying hardware. If any of these system layers provides intentionally corrupted information as a result of a malware infection, then any function depending on that information will degrade accordingly.

This layered view of cascading trust suggests that any system will be only as secure as the underlying hardware. Vendors therefore have begun to offer *hardware security* solutions that harden exported services to software. In addition, vendors have begun to provide so-called *embedded security* solutions that can be integrated into devices and other systems. The concept for both hardware and embedded security solutions is that a trusted execution path is assured during production.

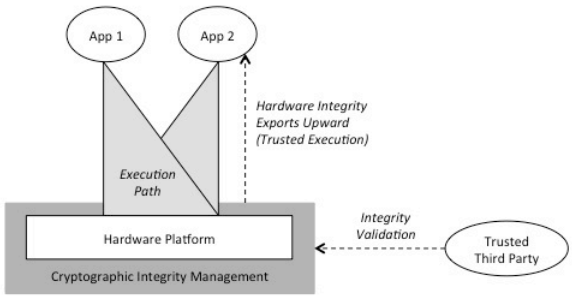

Figure 19-1. Trusted Execution Path Concept

If a system with a trusted execution path is corrupted, then services could still be offered safely from the underlying trusted base to the user. Such protection is especially vital since most cyber attacks gain entry at the application level, as with many browser-based malware infections. If the underlying hardware includes trusted execution paths, then the effects of the application-level attack might be considerably muted, especially in the response and reconstitution phases of recovery after the attack has been either suspected or detected.

The most common implementation of trusted execution in computing involves *trusted platform module* (TPM) functions, which are based on an international standard for security processor design. TPM support in a computing system has been in place for many types of systems, but the coverage is certainly not universal, and the vast majority of applications do not take full advantage of the underlying trust primitives that might be available. Nevertheless, TPM functionality provides a glimpse into the type of trusted execution that will eventually become absolutely required in the majority of computing, especially for critical services.

One of the most common applications of the hardware trusted execution concept is the management of cryptographic keys using trusted hardware. The typical implementation involves a custom-designed device called a *hardware security module* (HSM), which implements the most fundamental cryptographic operations in trustworthy hardware functions that are not easily modified. Many vendors considered part of the hardware/embedded security marketplace include an HSM in their product line.

Future market and enterprise usage trends in hardware/embedded security and trusted execution support will be driven by three on-going shifts in modern computing:

- *Cloud* – The move to cloud is accelerating from on-site servers in enterprise-hosted and managed data centers to off-site hosted infrastructure in third-party managed infrastructure. This changes the amount and type of control that enterprise CISO teams have over the underlying hardware and any associated trust.
- *ICS/IoT* – The number of ICS and IoT mobile endpoints that are connecting to the Internet is accelerating. The underlying trust model on most of these endpoints is non-existent and will require immediate improvements in hardware and embedded security. For specialized ICS or IoT devices still under design consideration, it is conceivable that firmware library functions will be made available to embed into the device at the lowest level. Such libraries are available now for integration at the operating system level, but firmware provision is certainly not common.
- *Mobile* – The security requirements for mobile applications running on Android, iOS, or other mobile operating systems are increasingly referencing some underlying trusted execution model. The likelihood is high that TPM-

like execution support for mobile devices will become more generally available.

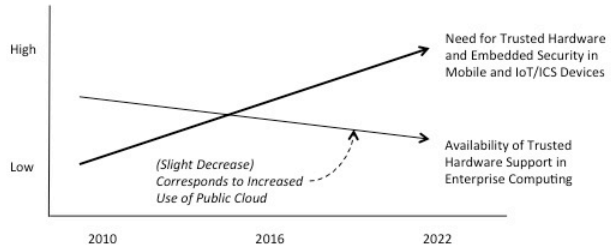

Figure 19-2. Trends in Hardware/Embedded Security

CISO teams should learn about the types of hardware trust that will come with ICS, IoT, and mobile endpoints, and how such trust fits into local security policy and usage requirements. The likelihood that public clouds will offer high assurance underlying trust execution paths remains unclear. Only with pressure from compliance managers, regulators, and CISO teams will public cloud providers begin to seriously offer higher assurance underlying compute and execution support.

A good starting point might be for a cloud service provider to offer higher assurance based on underlying hardware trust for any critical function that is running on a public cloud. By offering "higher rent district" cloud services, providers can improve their profitability accordingly and differentiate services that are increasingly looking more commoditized. This concept is beginning to gain slow traction, perhaps based on more mature requirements that cloud data be resident in certain political geographies to support country compliance requirements.

Hardware/Embedded Security Providers

The vendors below are well positioned, because hardware and embedded security will become more integrated, rather than add-on features. CISO teams should use the list below in conjunction with ICS/IoT providers, since the areas have much in common. Furthermore, the PC and mobile device manufacturing communities will play important roles in promoting trusted execution as part of the normal design of their products. Increasingly, CISO teams are beginning to require basic trusted execution functions such as immutable BIOS in PCs to avoid the effects of malware designed to destroy endpoint systems. This is best done during the design of the hardware systems, rather than as an add-on feature.

2017 TAG Cyber Security Annual
Hardware/Embedded Security Providers

Allegro Software – Allegro makes software toolkits that are used by manufacturers to enable their machines to become embedded participants on the Internet.

BlueRISC – Massachusetts-based BlueRISC offers hardware-assisted endpoint security with anti-tamper features.
Device Authority – D-Factor is an authentication engine that supports trust for IoT applications.
Discretix (Sansa) – Sansa is a leading provider of embedded security technologies for IoT and other devices.
Elliptic Technologies (Synopsis) – Synopsis offers standards-based security solutions for embedded hardware cores.
Gemalto – Located in the Netherlands, Gemalto provides a range of digital security solutions including SIM card, NFC, and other embedded applications.
HID Global – The company is well known for providing devices that manufacture smart cards and other hardware identifiers and tags.
Icon Labs – Icon Labs provides embedded protection for IoT devices that connect via Modbus protocol.
Ingenico – The French firm provides retail secure payment and protection solutions for merchants.
Inside Security – Inside Security provides comprehensive embedded security solutions for mobile, content protection, secure access, and IoT.
Intel Security (McAfee) – Industry-leading platform provider Intel embeds its acquired McAfee security into its underlying trusted execution processing and architecture.
Lynx Software – Lynx focuses on protecting real time embedded operating systems from malware.
NagraID – Located in Switzerland, NagraID makes high-end smart cards for identity applications.
Oberthur Technologies – The traditional French firm includes embedded digital security for transactions and other financial applications.
PFP Cybersecurity – PFP develops physics-based endpoint security solution with processor power consumption protections for IoT.
Secure-IC – Secure-IC offers sustainable embedded technologies that support threat protection.
Sequitur Labs – Phil Attfield and Paul Chenard founded Sequitur to focus on hardware and embedded security for a range of advanced device management functions. The small company is headquartered in the Pacific Northwest.
Skyport Systems – Founded by well-known venture capitalist Stefan Dycherhoff, Skyport provides advanced solutions for hardware and embedded security in servers.
Sypris – The Louisville-based firm offers trusted hardware manufacturing with focus on cyber security.
Tactical Network Solutions – Tactical Network Solutions provides digital forensic snapshots and analysis of memory and firmware on devices and systems.
Trustonic – Trustonic develops a secure environment that executes within smart connected products and devices.

Ultra Electronics AEP Networks – Ultra provides hardware security modules and cryptographic hardware support; the company acquired AEP in 2011.
Watchdata – Located in India, Watchdata offers SIM cards for mobile with capability to support mobile payment.

20. ICS/IoT Security

⇒ *ICS/IoT Risk* – Complex legacy technology and high attack consequences lead to high cyber security risks for most ICS and IoT devices and systems.
⇒ *ICS Architecture* – Cyber security professionals generally have weak technical understanding of ICS and IoT systems, architectures, and security risks.
⇒ *Two-Step Security Integration* – Current ICS, SCADA, and IoT security is focused on traditional controls as a base for later enhancements.

From the perspective of cyber security, *Industrial Control System* (ICS), *Supervisory Control and Data Acquisition* (SCADA), and *Internet of Things* (IoT) represent collectively the most significant new set of threats to global cyber infrastructure. Given all of the various high profile cyber risks identified in the past few years, this is not an inconsequential statement.

The root cause of this intense new risk relates mostly to the complexity of embedded legacy systems that were never originally designed to stop cyber attacks. Legacy heat pumps installed onto the floor of a factory two decades ago, for example, were obviously not designed to address modern cyber security attacks. A related cause of this risk is the degree to which devices and systems in these categories have been automated. As one would expect, the software and systems supporting such automation were never designed with cyber security in mind.

The risk in these areas relates to the highly consequential impact a cyber attack would have on human safety, essential human services, and human life. For example, whereas a virus getting onto an enterprise PC might be a minor nuisance, the same virus getting into an aircraft engine control system could lead to a significant loss of life.

The specific *endpoint* devices relevant to ICS, SCADA, and IoT include, but are certainly not limited to, the following obvious classes:

- *Industrial Devices* – This group of devices is by far the broadest category from a cyber security perspective because it affects so many critical infrastructure systems and essential services. The control elements for ICS are typically referred to collectively as SCADA, and many unique cyber security issues arise in the protection of ICS/SCADA systems from malicious attacks.
- *Medical Devices* – This group of devices relate to medical privacy as well as assuring the integrity of life-critical treatments. Traditional mobility security and encrypted application VPN technology apply here, but medical device connectivity to the Internet introduces problems similar to ICS/SCADA.

- *Connected Cars* – In the next few years, all automobiles will become natively connected to the Internet across mobile service provider (MSP) wireless infrastructure. Infrastructure security issues associated with connected cars are similar to ICS/SCADA, but as autonomous vehicles become more regularly seen across the world, securing the communication protocols between cars will emerge as a new area of cyber security. Academics should be working more vigorously today to establish foundational frameworks for secure inter-vehicle communications.
- *Household and Personal Devices* – This device grouping is included in Internet of Things (IoT) and includes whimsically connected items such as toys and refrigerators, but also bleeds into traditional mobility with items such as wearable devices. IoT generally refers to connected devices that are neither mobile devices, computers, or ICS systems with safety, life, and critical infrastructure implications.

Each of these endpoints can be connected privately to management and control systems through ISP or MSP infrastructure. Alternatively, they might be accessible to users and operators over the Internet, depending on the requirements. When ICS devices are discoverable on the Internet, we refer to the result as an industrial Internet architecture. This type of arrangement is troubling when it combines general accessibility from the Internet with life or safety critical operations. Without careful consideration from a competent CISO team, this can be a recipe for disaster.

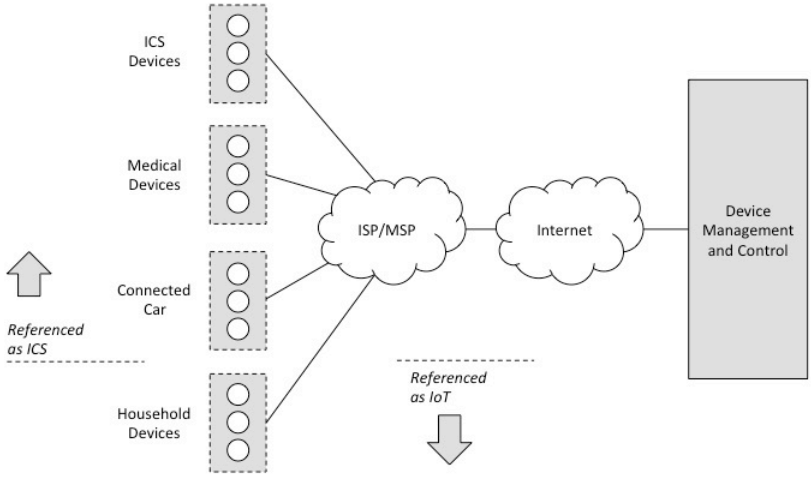

Figure 20-1. Taxonomy of Industrial Control System and IoT Technologies

An irony is that while ICS and SCADA are considered new areas of cyber security, both disciplines are among the more mature areas of technology. In fact, as suggested above, one of the biggest challenges in both ICS and SCADA security protection is that so much of the associated infrastructure will inevitably contain a significant amount of legacy technology. This includes older protocols, mature

systems, and proprietary control components – many of which require comprehensive reverse engineering in order to establish any semblance of cyber security control.

Since ICS/SCADA represents such a departure from the usual sort of training received by CISO teams, it is helpful to examine some of the basics here. In general, the primary functional components in an ICS can be listed as follows:

- *Management System* – Management systems include the consoles and human-machine interfaces required for operators to control and operate an ICS. Many management systems include proprietary software and systems developed long before the industrial endpoints were being considered for remote access. Hackers *obviously* have great interest in finding and owning these systems.
- *Diagnostic System* – Diagnostic systems organize sensor telemetry information for use by ICS operators. Diagnostics have not traditionally included security signatures or profiles, but with increasing attention to cyber security, one would expect this to change.
- *ICS Network* – An ICS network provides wireless or wireline transport and connectivity between ICS components. When this connectivity involves use of the public Internet, the result is often referred to as the Industrial Internet. Private ICS networks should, in theory, be more secure than public ones, but the specifics will always dictate risk posture.
- *ICS Controller* – An ICS controller includes the logic for managing actuators and sensors based on management input. ICS controllers will soon integrate with software defined networking (SDN) from service providers, but this will be harder for legacy and proprietary applications. An advantage of SDN integration is that security analytic processing becomes an important SDN controller adjacency that can help with ICS protection in real time.
- *Actuators* – Actuators include the electronics, motors, and other components for starting and stopping activity in the controlled system and associated processes. These components are usually controlled by legacy and even non-standard protocols designed without much consideration for authentication or encryption. The idea of hackers gaining access to actuators connected to some portion of a nuclear facility is frightening.
- *Sensors* – Sensors collect data from the controlled system and associated processes. Telemetry is one of the main areas of industrial control security that will require confidentiality controls.
- *Controlled System* – The controlled system is the specific, target industrial system that is being managed. Such targets can range from consequential ICS critical infrastructure like nuclear plants to more whimsical IoT devices such as children's toys.

The elements in a basic ICS are typically arranged in a logical architecture as shown below.

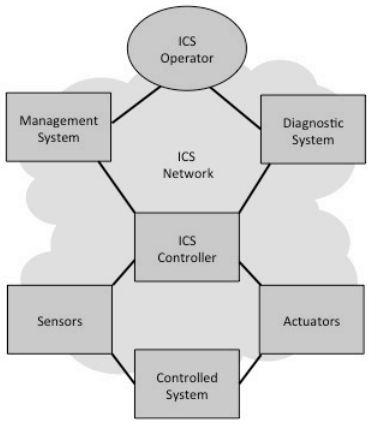

Figure 20-2. Basic ICS Architecture

Embedded in an ICS is the Supervisory Control and Data Acquisition (SCADA), which is designed to control remote elements via centralized data acquisition. Elements controlled by SCADA include water distribution, electricity, transportation, and other embedded electromechanical systems. The obvious criticality of these systems underscores the severe consequences of SCADA cyber attacks. The overall SCADA control function uses a set of component types including the following:

- *Master Terminal Unit (MTU)* – Also known as a SCADA server, the MTU provides remote management of SCADA devices.
- *Remote Terminal Unit (RTU)* – The RTU provides telemetry from field devices often over wireless interfaces controlled by MTUs.
- *Programmable Logic Controller (PLC)* – PLCs perform logic functions by electrical hardware and serve as RTUs.
- *Intelligent Electronic Devices (IED)* – IEDs are smart sensors and actuators required to acquire data and to perform local processing.

A typical SCADA system is depicted in the diagram in the figure below.

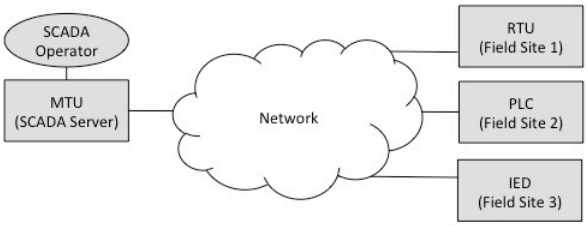

Figure 20-3. Basic SCADA Architecture

The security challenge for ICS and SCADA system architectures is essentially two-fold: First, basic security architectural components are required to bring these industrial systems up to the present state-of-the-practice in network and information system security. This requires familiar integration of components such as firewalls, attack detection and prevention tools, and log management systems. Second, these industrial environments will require advanced functional security mechanisms commensurate with state-of-the-art behavioral analytics, real time virtual protections, and application aware encryption. Many current cyber security product vendors, such as Bayshore Networks, are working hard to bring these previously disparate worlds or ICS/SCADA and modern cyber security together into a more cohesive ecosystem.

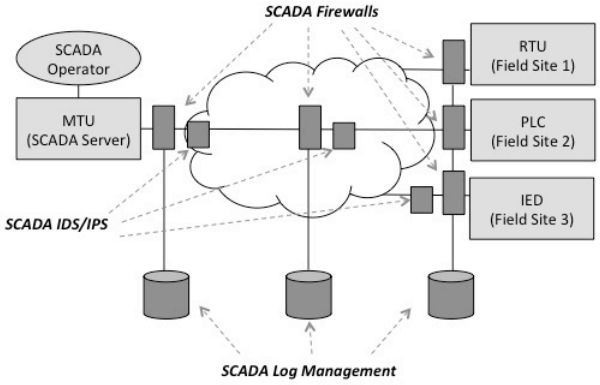

Figure 20-4. SCADA Architecture with Basic Security Functionality

Since ICS and SCADA systems require basic security functionality integration before more advanced cyber security systems can be considered, the trends one should expect in the ICS/SCADA security market will involve the following steps:

- *Basic Protection Step* – Traditional cyber security functions will first be introduced into ICS/SCADA and IoT infrastructure as a baseline set of risk controls.
- *Advanced Enhancement Step* – As hackers quickly gain traction in defeating the conventional controls, newer techniques based on more advanced approaches will find their way into the protection design.

To illustrate the lag associated with this two-step progression, consider that behavioral analytics are already becoming a standard type of offering for standard Internet/Intranet environments. ICS/SCADA behavioral analytics, however, are much less prevalent in the market. Similarly, as services such as penetration testing for standard environments are ubiquitous with many options for buyers, similar security services for penetration testing of ICS/SCADA are less readily available. To

that end, predicted trending in the ICS/SCADA security marketplace for security evolutionary components (perimeter, network, and virtual) is shown below.

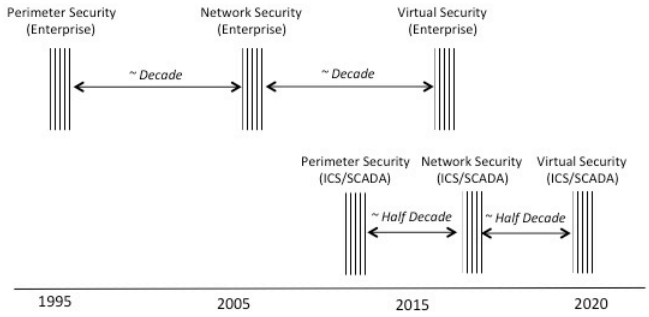

Figure 20-5. Trends in the ICS/SCADA Security Industry

It is worth noting that ICS/SCADA security services will benefit from experiences in more traditional environments. As such, their adoption and evolution to enterprise and even carrier grade should be accelerated from one decade to roughly half that time. ICS/SCADA security will eventually converge, as with enterprise security, on fully virtualized protections architectures. To this end, ICS/SCADA security vendors should have a plan for virtualization with emphasis on integration with SDN services from ISPSs. It is actually conceivable that ICS/SCADA and IoT protections might benefit the most from emerging SDN platforms for service chained security, if only because these applications have less legacy security infrastructure to be replaced or augmented.

Since industry standard protocols are not typically supported in off-the-shelf enterprise security systems such as firewalls and intrusion detection systems, ICS/SCADA security vendors will increasingly be required to demonstrate full compliance with relevant industry protocols. For example, ICS/SCADA firewalls should provide more specific protection for SCADA protocols between MTUs and RTUs than traditional port and protocol-oriented rules that would be implemented in an enterprise firewall.

ICS/IoT Security Product Providers

Given the enormous emphasis on ICS, SCADA, Industrial Internet, and Internet of Things (IoT), it's surprising that there are not more vendors in this area. Many vendors make the *claim* that their product applies here, but few actually have taken the time to address the proprietary, customized, legacy, and unusual protocols inherent here. Of all the vendor lists included in this report, the one below is the one most likely to change in the near term, so CISO teams working on ICS and IoT will need to keep a close watch as new companies emerge to protect electromechanical factory equipment, airplane parts inventory, chemical processing plant safety systems, driverless vehicle road monitoring, and on and on.

It is also worth mentioning that the ISP/MSP plays an important underlying support role in providing safe and secure managed communications for these critical applications. It is much less likely that service providers will natively support protection for the large number of legacy protocols inherent in ICS and IoT, so their solutions will come through managed partnerships with the vendors listed below, rather than through generally available services focused on actuators, heat pumps, wind turbines, refrigerators, and so on.

2017 TAG Cyber Security Annual
Distinguished ICS/IoT Security Providers

Bayshore Networks – Francis Cianfrocca, founder of Bayshore Networks, has become my personal tour guide to the complexities of protecting ICS and IoT systems from cyber attacks. When I meet with Francis and his fine team, I come away with a renewed hope that the security community accelerates its focus in this vital area. I've also learned from Bayshore, however, about the complexities of legacy protocols in operational technology (OT) and how these can be a threat problem for larger industrial entities that cannot easily upgrade. Some of these attack scenarios can cause sleepless nights, honestly. I am so appreciative to Francis for providing such useful technical support to this project, not to mention always showing me demos that are ten times more fun than a trip to the local electronics store.

2017 TAG Cyber Security Annual
ICS/IoT Security Providers

Allegro Software – The Massachusetts-based firm offers ICS/IoT security solutions for embedded devices.
AT&T – Mobile ISPs are well positioned to integrated ICS/IoT product technology into their emerging SDN infrastructure so that CISO teams do not have to do the integration locally. In the best case, ICS/IoT security technologies such as those listed here can be provisioned as part of the virtual MSS.
Bayshore Networks – Bayshore Networks provides an appliance for securing ICS and Industrial Internet protocols for IoT and OT.
Covisint – Covisint originally focused on security products for connected vehicles, has expanded to secure IoT, supply chain, and identity and access management.
CyberX – CyberX provides security solutions for protecting industrial Internet from malicious attacks.
Discretix – Part of Sansa, Discretix provides security solutions for device content protection including support for chip manufacturers and IoT.
Enet 1 Group – Enet 1 Group provides security professional services in the areas of SCADA and critical infrastructure, and mobility.
FireEye – FireEye includes ICS security support as part of its extensive APT protection portfolio.

Fortinet – Fortinet includes ICS security support as part of its larger firewall and gateway security portfolio.
IBM – IBM includes a range of security product solutions for companies in the ICS and IoT space.
Icon Labs – The Iowa-based firm provides security solutions for IoT via portable software for embedded devices.
Indegy – Indegy provides security solutions for protecting industrial Internet from malicious attacks.
Innominate – German firm Innominate provides industrial, machinery, and related ICS security solutions.
IOActive – IOActive is a consulting firm with expertise in hardware and ICS systems including security protection.
Mocana – Mocana provides a mobile application security platform with support for embedded devices in the Internet of Things (IoT).
NexDefense – NexDefense is an expert resource on cyber security protections for automation and ICS systems.
PFP Cybersecurity – The Virginia-based firm offers embedded integrity verification tools for IoT and other devices.
Radware – Radware's cyber security products include industrial control security protections.
Red Tiger Security – Red Tiger is a Houston-based consulting company with expertise in industrial security.
Rubicon Labs – Rubicon Labs provides a secure communications and key management solution for cloud and IoT.
Savant Protection – Part of Digital Guardian, Savant provides endpoint protection that creates per-machine whitelists, which can be used in ICS applications.
SCADAhacker – SCADAhacker provides a range of training and consulting services for SCADA protection.
SecureRF – Located in Connecticut, SecureRF offers security solutions for wireless systems including NFC and IoT.
Securicon – The Virginia-based firm offers a range of security solutions for SCADA and process control.
Security Matters – Located in the Netherlands, Security Matters offers a platform for security protection of SCADA.
Siemens – The major German technology firm offers solutions for energy, automation, and other sectors with ICS security challenges.
Sophos – Sophos provides the Cyberoam network security appliances with support for ICS/IoT systems.
Synopsis – With the acquisition of Codenomicon, the company from Finland has the ability to test ICS/IoT devices and applications.
Tenable – Cyber security firm Tenable markets a range of offerings applicable to ICS/IoT applications.
ThetaRay – ThetaRay provides solutions for detecting threats in critical infrastructure and industrial systems.

Tofino Security – Tofino, a division of Belden, includes a security appliance for industrial network security.
Waterfall – The Israel-based firm provides network security solutions for industrial control.
WISeKey – WISeKey provides digital information security, authentication, and identity management solutions for mobility and IoT.

Additional ICS/IoT Security Providers

Berkana Resources – Berkana is a SCADA integrator offering SCADA security, compliance, and audit services.
Digital Bond – Digital Bond provides professional services with emphasis on SCADA and ICS security.
Inductive Automation – Inductive Automation provides a Web-based and cross platform solution for building SCADA applications.
Wurldtech – Wurldtech is a GE company focusing on cyber security solutions for operational technology.

21. Mainframe Security

- ⇒ *Legacy* – Mainframe computing remains an important component of legacy data processing environments in larger organizations.
- ⇒ *Products* – RACF, ACF2, and Top Secret remain the most popular security products for mainframes, usually from IBM.
- ⇒ *Trends* – The shift across all aspects of modern computing to virtualization is included as an interim feature in most mainframe environments.

Modern *mainframe* computing is characterized primarily by the ability to handle legacy software, usually developed years or even decades ago. Characteristics found in mainframes include high reliability and availability, centralized management and control, and the ability to handle high volume input and output (I/O). Although reliable data is hard to obtain, it is likely that a surprisingly high percentage of business and government data continues to reside on or originate from mainframes.

CISO teams know that *all physical servers* in a modern enterprise environment are of obvious security interest. In fact, many enterprise security teams include a dedicated individual or even staff to coordinate with the server operations group. Specific server protections include scanning, patching, and security administrative tasks, as well as operating system and related middleware source selection and review. But mainframes are a special breed of server with unique protection requirements that are often viewed as legacy and irrelevant to the organizational risk profile. This is a mistake, of course, and the discussion here outlines issues that must be considered in the protection of mainframes.

Interestingly, modern computing capabilities such as virtualization and workload sharing are typically found in most mainframe computing environments, which helps explain their continued use. Nevertheless, the most important and defining characteristic of any mainframe is its ability to support and operate existing, legacy software applications and systems – which saves time, effort, and money, without incurring transition risk. Larger organizations such as banks and government agencies are much more likely to include mainframes than smaller companies.

IBM mainframes remain by far the most popular and dominant underlying platform for enterprise use, perhaps with as much as 90% market share in 2016. As such, most mainframe security products and services focus on providing conventional security controls for platforms such as IBM z Systems. This includes support for the following:

- *Physical Controls* – Mainframes are typically maintained in private data centers with facility protection requirements. Mainframe experts often learned their craft in the context of physical security controls being much more important. As a result, most mainframes exist in well-controlled data center facilities.
- *Penetration Testing* – Though break-ins to mainframes are relatively rare, testing is a typical requirement. CISO teams must be extremely careful in hiring penetration testing services for mainframes. The ability to properly traverse and exercise mainframe systems is an increasingly lost art.
- *Audit and Monitoring* – Financial applications are often found in mainframe environments, which are subject to frequent audit. Auditors usually possess a deep understanding of mainframe systems.
- *Encryption and Policy Enforcement* – Encryption and policy requirements are common in mainframe environments. Mainframe vendors generally have excellent support in this area.
- *Administrative Security* – Mainframe system administration requires knowledge of many non-user friendly tools and mature utilities. The languages and interfaces of mainframes often include input that looks more like old-fashioned line noise from a terminal than meaningful commands.

The most popular security software products for mainframes remain RACF (Remote Access Control Facility) from IBM, ACF2 (Access Control Facility) from CA, and Top Secret from CA. Existing enterprise users of one or the other of these products generally have little motivation to shift from one product to another. Even with corporate mergers, the likelihood that different mainframe systems remain non-integrated post-merger is high. These three primary security products are mature (mostly created several decades ago) and are operated by an experienced community of administrators who are rapidly approaching full retirement age.

It is not important for CISO teams to become experts in the protection of mainframes, but some of the primary techniques employed include mainframe

hosted data governance, data encryption, access control, authentication, log management, and authorization control. As one would expect, these controls correspond to the primary security controls that existed during the era, roughly in the 1970's, in which mainframes were introduced. The clear business usage trends in mainframe security can be summarized as follows:

- *Volumes*: Mainframe usage will continue to decrease at a relatively rapid pace with virtualization of traditionally hosted mainframe applications.
- *Unit Cost*: Mainframe product and service unit costs will increase as the scarcity of trained staff and capabilities grow, especially for mainframe security outsourcing.
- *Business*: Mainframe product and service companies will maintain a neutral business posture by balancing volume reduction with unit cost increases. Mainframe security outsourcing will continue to be a useful service for many businesses to purchase from a professional services company.
- *Threats*: Mainframe security threats will remain constant and relatively low compared to other threats.

These mainframe security industry trends are depicted in the diagram below.

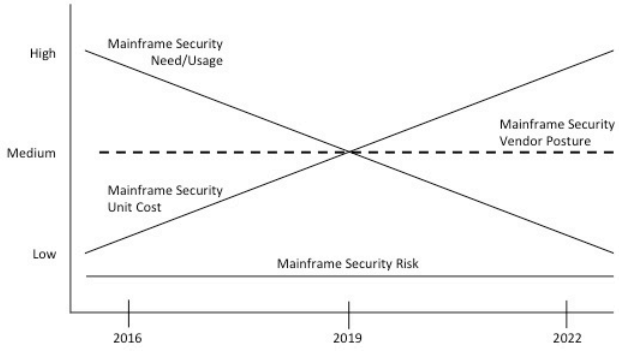

Figure 21-1. Mainframe Security Trends

Enterprise users of mainframe security products and services have the option of maintaining consistency with these trends, which implies gradual reduction of mainframe usage over the next six years, or to accelerate the reduction, which has the advantage of avoiding future higher unit costs. Another option is to lock in deals with mainframe security solution providers in order to avoid higher future unit costs. As mainframes become less prevalent, the skillsets to perform administration, data governance, and related tasks will become more expensive.

Every CIO knows that application and system virtualization carry so much financial and operation benefit for an organization that eventually, the vast majority applications and systems will reside in a virtual data center, often with cloud-infrastructure and front ends. Mainframe solution providers should therefore be

expected to offer a roadmap to deal with this trend for any mainframe hosted applications and systems.

An additional consideration for CISO teams to take into account is the range of career plans, maturity, and future availability of any mainframe security staff. The harsh reality of mainframe skillsets is that the people who learned this technology and continue to perform the functions are moving along in their careers. Young people graduating with computer science degrees rarely possess the skills or motivation to support mainframes. This fact must be taken into account in planning mainframe security support.

Mainframe Security Providers

Contrary to what one hears from IT and network pundits, mainframe computing is alive and well across many aspects of business, especially in larger companies. A management process for moving corporate applications from the mainframe to Linux, from the mainframe to Windows, or even from the mainframe to Android is almost certainly present on some spreadsheet in each of these companies. But the fact remains that mainframe security is a legitimate issue across many companies, hence the list of companies below offering solutions in this traditional area of security focus.

2017 TAG Cyber Security Annual
Mainframe Security Providers

ASPG – ASPG is a Florida-based mainframe software company with a suite of products including security.
Atsec – Atsec is a security consulting firm that provides penetration testing services for mainframes.
CA – CA continues to serve as an industry leader in the area of mainframe security governance, access management, and data protection.
Correlog – Correlog provides log management and SIEM functions, including support for mainframes.
Enforcive – Enforcive supports mainframe deployments and compliance programs for IBM z Security.
IBM – The well-known company, with its associated brand, has been synonymous with mainframe products and services for many decades. CISO teams with mainframes are probably already working closely with IBM in one way or another.
Imperva – Imperva acquired Tomium, which provides a mainframe security solution for continuous auditing.
Infosec Inc. – Infosec Inc. provides professional services specifically in the area of mainframe, including security.
PKWare – PKWare offers software solutions for mainframe including PKZIP and encryption.

Raz-Lee – The New York State-based firm offers audit, monitoring, and related compliance solutions for mainframe.
SafeNet – Part of Gemalto, SafeNet offers a range of mainframe data protection solutions.
Safestone – Part of HelpSystems, Safestone provides a range of IBM server security products.
Software Diversified Services – SDS supports z/OS mainframe software with range of products and solutions.
Voltage – Now part of HPE, Voltage offers mainframe encryption solutions for z/OS users.

Additional Mainframe Security Providers

Ensono – Formerly Acxiom IT, Ensono provides hybrid IT services including support for mainframe.
Interskill – Interskill provides mainframe training with catalog of IBM mainframe and security courses.
Sea – Software Engineering of America provides data center solutions including for mainframe and security.
Treehouse Software – Treehouse Software offers data integration and related solutions for mainframe.
Vanguard – Vanguard provides a range of IBM mainframe solutions including security protections.
Xbridge – Xbridge provides data discovery solutions with coverage for z Systems maintenance and security.

22. Mobile Security

- ⇒ *Mobile Security Controls* – Mobile security controls focus on devices, apps, systems, and mobile device management.
- ⇒ *Mobile Security Threats* – Threats to mobility include gaining access to user credentials, cloud access, enterprise access, and locally stored data.
- ⇒ *Mobile Security Trends* – Mobile security solutions will increasingly rely on mobile device management, adaptive security, and behavioral analytics.

The cyber security threat has *traditionally* been viewed in the context of personal computers, enterprise servers, network components, and enterprise systems. In the past decade, however, the use of mobile devices has added a new dimension to the threat landscape with its unique form factor, operating systems, applications, management systems, protocols, and infrastructure associated with 3G/4G mobile devices and services. The landscape also includes public and private WiFi communications, which is a growing issue as carriers encourage off-loading of data and even voice traffic to WiFi.

Perhaps the more consequential aspect of mobile security risk comes not from the actual devices or ecosystem, but rather from the incredible dependency most individuals and businesses now have on their mobile devices. Ask any executive eight years ago (pre-iPhone) if they would rather give up their PC or their mobile – and the answer would probably be to toss the mobile. Ask the same question today, however, and the answer would be reversed. Such dependency increases security risk, simply because the effects of an attack, especially destructive ones, are now much more significant.

The broad ecosystem for enterprise *mobile security* solutions therefore includes the following protection considerations:

- *Mobile Device Security* – This control is usually implemented by software resident on the mobile device to provide security protections such as anti-virus and lost-device location. Mobile device security methods generally follow traditional PC anti-virus with signature-based protection, but many modern mobile device solutions introduce more modern behavioral analytics and even machine learning techniques.
- *Mobile App Security* – This control is usually implemented as application-level software on the device or in the cloud to increase confidence in mobile app security. A myriad of different methods exists to try to reduce the risk of mobile apps compromising the integrity or privacy of a user's data or access. These include both static and run-time controls.
- *Secure Mobile Communications* – This control is usually implemented as hardware or software encryption functionality to increase mobile-to-mobile secure communications. The trend here, as one would expect, is toward fully software-based solutions, which are cheaper to maintain and often much easier to use.

While the above controls are obviously important, the ever-present *mobile device management* (MDM) function has emerged as one of the most critically important dimensions of the overall security architecture in any enterprise security area. This is somewhat surprising, since MDM was originally viewed separately from cyber security, since functions such as loading software to a device or tracking device inventory were generally viewed as part of conventional IT, rather than security. Furthermore, the use of a mobile device as a means for providing two-factor authentication to systems was originally not very popular.

But all of this has changed. As the mobile device and its corresponding support infrastructure have become more central to enterprise computing, the management of mobile devices and systems has become more central to enterprise security. Furthermore, as two-factor authentication using mobiles and public key certificates becomes more standard, the reliance upon MDM to orchestrate these security functions with mobile access and cloud workloads is rising as well.

The conventional wisdom today around mobile security is that it is the "next big thing" in personal and enterprise cyber security. This view presumes that years

of malware lurking on home and business PCs resulting in identity theft, botnet attacks, and data exfiltration will be soon replaced by similar problems on mobile devices over mobile networks. In truth, this view has *not* materialized through 2016, however, for several reasons.

First, the underlying operating systems for mobile devices have been of higher security quality than their predecessors on PCs. This reduces, but obviously does not entirely remove, the attack surface. For example, security patches must still be pushed occasionally to devices (which is a much more straightforward task, by the way, for Apple given its tight control over all aspects of its ecosystem, versus Google, which does not). Second, the mobile threat is still less attractive to the offense compared with the wide-open nature of PCs and servers that reside on easily accessible local area networks. Attackers know that a botnet can still be constructed trivially from home and business PCs – and this is beginning to include virtual machines in the cloud – without the need to infect anyone's iPhone.

Nevertheless, the mobile security marketplace is beginning to take shape and grow due to increased enterprise adoption of mobile devices and apps in the workplace, and decreased usage and dependency on personal computers both at home and in the workplace. Furthermore, the reality is that if a determined hacker targets your mobile device or supporting infrastructures, chances are high that they will be able to get in. So the threat looms, albeit somewhat quietly in the view of most enterprise teams. The *real* mobile security threats that are likely to emerge and grow in the coming years can be grouped as follows:

- *SMS Trojans* – This is the most visible current mobile threat. It is certainly not to be dismissed, but it is also nowhere near the sort of security problems that would prompt a CISO team to take immediate action – which helps to explain why the mobile security marketplace has not taken off to the degree that most experts have come to expect.
- *IoT/Mobile Attack Weapon* – This threat utilizes access to the mobile in order to construct a directed or distributed attack weapon (as in IoT botnets). Any device with an operating system and a network connection is a target of being maliciously exploited in this manner.
- *Credential Theft* – This threat utilizes the mobile to gain credentialed access to data stored elsewhere. Obviously, if an individual stores data in various cloud services, then the mobile serves as an excellent means for common access to this disparately stored data.
- *Data Access* – This threat utilizes the mobile to gain access to data stored on the mobile. Increasingly, users rely on pictures of important documents such as social security cards, bank forms, employment applications, and the like to text images to contact and support centers. In this sense, stored images on the mobile are no longer just pictures of your children.

The figure below shows the relative expected growth in each of these high-growth, new mobile threat areas.

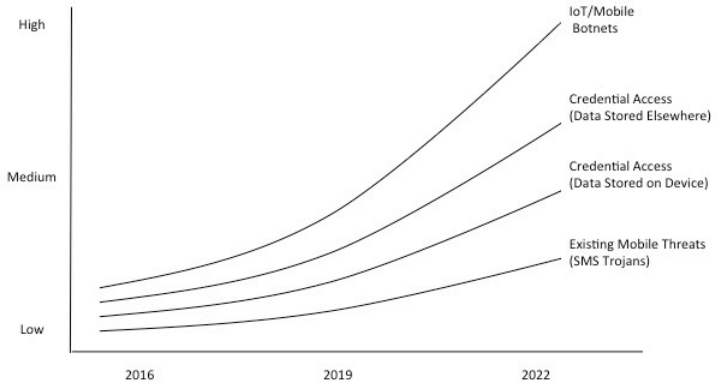

Figure 22-1. Mobile Security Threat Trends

Each of these four mobile threat trends begins with relatively modest intensity and then grows at a rapid rate toward 2022. The intensity of IoT/mobile botnets is likely to be highest, due to the enormous number of IoT devices and the relative lack of embedded security one will find in most Internet connected devices such as sensors, actuators, and other non-smart phone devices. The prospect of billions of IoT devices infected with malware used to overload mobility infrastructure is not something service providers are looking forward to dealing with.

The existing market for mobile security in 2016 is fragmented, with no one vendor, or even area of mobile security, dominating the threat mitigation space. A trend mentioned earlier is that mobile device management (MDM), in many enterprise networks, has begun to serve as the primary means for protecting employee devices and apps. In this context, IT groups utilize MDM capabilities from firms such as MobileIron in order to provide per-app encryption support. The best enterprise security teams will thus learn to take advantage of world-class MDM systems to provide an underlying management framework within which a holistic set of security capabilities can be orchestrated.

In this sense, MDM products and services should be viewed as required security components. But every MDM vendor is quick to point out that their capabilities extend beyond protection of mobile devices. As such, the CIO and IT team often share responsibility for MDM budget planning and source selection. While the existing mobile security marketplace is organized largely around the three areas cited above – mobile device security, mobile app security, and secure mobile communications – each with the corresponding management functions of an MDM, the future of mobile security is likely to be driven by five trends:

- *Mobile Security Signatures* – The conventional use of signature-based anti-malware technology will gradually wane to a modest, on-going level, simply because of the intractability of keeping track of signatures. The best CISO

teams know, however, that signatures will keep their place in the security arsenal and should never be ignored as a potentially useful technique.

- *Mobile Behavioral Analytics* – The use of behavioral analytics to detect security problems is likely to increase as algorithms gradually improve in their accuracy and detection rate. This will require that existing behavioral analytics security tools learn to adapt to mobility protocols and endpoints (e.g., from IP addresses Individual Mobile Subscriber Identifications (IMSI)).
- *Mobile Adaptive Protections* – The use of adaptive, behavioral algorithms to protect devices will become routine. Devices will include technology, for example, that recognizes their owner, and that use learning algorithms to understand how behavior changes with context. Some vendors use the phrases "artificial intelligence" and "machine learning" in their descriptions.
- *Mobile Security Cloud Assistance* – The complementary use of cloud-based intelligence, including from software defined network (SDN) controllers, to assist in detecting and mitigating mobile device and app threats will increase. Mobile service providers are in a good position to offer cloud-based security assistance. In the future, virtually every cyber security protection in the enterprise is likely to include some form of cloud assistance.
- *Virtualized Enterprise Mobile Protections* – Enterprise use of mobile devices, apps, and systems will require transition from LAN-based perimeter protections for PCs to virtualized policy enforcement in the service provider mobility infrastructure. Virtual protections will utilize technologies such as mobile wrappers, which will remain important, but only for developers creating virtual app experiences. Virtual protection can also help provide virtual patching solutions across the mobile ecosystem.

The increases and decreased in these mobile security areas are depicted below.

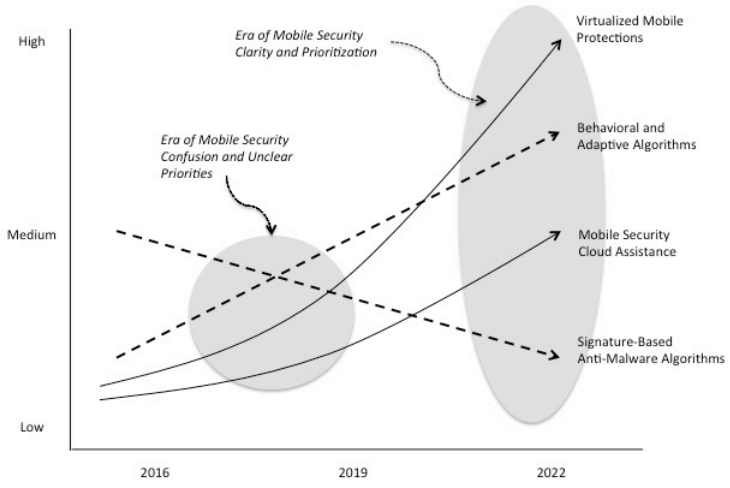

Figure 22-2. Trends in Mobile Security Technologies

The period from 2016 through 2019 is likely to be characterized by a degree of uncertainty and lack of clarity in mobile security methods and prioritization. The wide range of industry offers will likely reflect this lack of clarity, and enterprise buyers might choose to delay long-term arrangements. However, as the 2021 to 2022 period emerges, the proper arrangement and prioritization of mobile security protections is likely to work itself out. Vendors in the areas noted above – cloud-based, virtualized protections based more on adaptive, behavioral analytics – will be more successful.

As service providers roll out their SDN and NFV infrastructures, the mobility industry will be influenced accordingly. Specifically, the idea that security product functions from mobile security vendors could be service chained dynamically into an open, API-accessible MSP infrastructure is an exciting new area of managed mobile security. CISO teams should keep an eye out for emerging security offers in this area from their mobility solution provider. Virtually provisioned mobile security, integrated with the underlying SDN infrastructure is an exciting prospect because it will provide mobile users with access to the best available mobile protections from vendors with the most effective solutions.

One additional area of interest not addressed above is the secure mobile communication marketplace. Today, this is a vibrant area for vendors offering encryption support on a per-app basis for mobile apps for enterprise users with their mobiles. A challenge, however, is that the provision of this technology as an add-on feature, like most PKI-based technologies, will probably be disintermediated by larger offerings from solution providers, including cloud access via mobiles. The requirement for per-app VPN support with encryption is thus likely to become embedded in cloud-mobile communications and should not exist much longer as an add-on product for sale.

Mobile Security Product Providers

The mobile security market has been on the verge of explosive growth for some time, not unlike the similar situation found decades ago with the early personal computer (PC) anti-virus market. As with early PC users, current mobile users expect more malware infections, but are unclear whether to install stronger protections.

As of mid-2016, the vast majority of personal mobile users have not actively selected a mobile security solution, in stark contrast to the vast majority of PC users. The vendors listed below are in an excellent position to take advantage of the inevitable acceleration in use of mobile security solutions for individuals and enterprise users. The question is not whether these providers will experience such growth, but rather *when* this accelerated growth will occur.

As is the case with so many technology areas covered in this report, mobile service providers such as AT&T and their associated equipment manufacturers such as Samsung obviously play a *huge role* in mobile security. Generally speaking, MPSs and manufacturers are to mobile security as ISPs and PC/server manufacturers are

to computer security. CISO teams should therefore view the mobile provider and equipment manufacturer as primary partners in selecting and integrating proper mobile security protections. They will be more than happy to provide assistance through source selection and operational design, perhaps even offering natively embedded protections. Certainly, they play a key role in the design of proper patch processes.

2017 TAG Cyber Security Annual
Distinguished Mobile Security Providers

Lookout Security – My first experience with Lookout several years ago occurred commensurate with my initial concerns about how mobile threats might be best detected and mitigated. After learning more about Lookout, I became convinced – and am still convinced – that their holistic approach to cyber security was correct, combining advanced mobile device protections with accurate threat intelligence and an awareness of the full security architecture. I offer my great appreciation and thanks to Kevin Mahaffey and the Lookout team for their wonderful support of this research and project.

2017 TAG Cyber Security Annual
Mobile Security Providers

Active Mobile Security – Active Mobile Security provides a mobile security solution for data separation and malware protection.
AdaptiveMobile – Located in Ireland, Adaptive Mobile provides mobile threat intelligence, protection, and infrastructure protection (including SS7 security).
AirPatrol – AirPatrol supports location-based content delivery and security management for WiFi and mobile devices.
Appthority – Appthority offers mobile app security analysis to support data loss and privacy risks. Appthority risk scores provide a tangible means for CISO security teams to make decisions about mobile apps desired for use in the enterprise.
Arxan – Arxan protects mobile, desktop, embedded, and server applications including a mobile app assessment.
AT&T – All major MSPs offer a wide range of options for their enterprise customers in the area of mobile security and MDM. Most offerings are provided through partnerships with major mobile security technology providers, and this is likely to continue with SDN deployment, albeit offered via on-demand provisioning.
Avast – Acquisition of Remotium provides Avast with a secure mobile enterprise solution.
AVG – AVG offers anti-virus and optimization for endpoints including Android mobiles and tablets.
BETTER – Enterprise mobile threat defense from BETTER supports detection and prevention of mobile attacks to Android and iOS.

Bitdefender – Bitdefender provides endpoint security protections include support for mobile.
Blackberry (Watchdox, Good) – The acquisitions of Watchdox and Good provides Blackberry with a wide range of secure mobility and mobile device management solutions.
Bluebox – San Francisco-based Bluebox offers mobile app security and management solution to safeguard corporate data.
BullGuard – Anti-virus protections for endpoints from BullGuard include support for Android security.
Check Point Software – Acquisition of Lacoon brings Check Point a mobile threat prevention solution.
eAgency – eAgency is a provider of mobile security products for consumers, business, and carriers.
ESET – Anti-virus and security protection for endpoints from ESET includes support for Android.
F-Secure – F-Secure anti-virus and security solutions include support for smartphones and tablets.
Google – The industry leading mobile operating system developer includes many useful security features in the OS and supporting ecosystem. Google has a more difficult task in security patching than Apple, because it must push source code to all of the mobile device manufacturers using Android. These manufacturer-led software updates must then be coordinated with carriers. The result is a mobile device operating system patch environment that includes quite a few hand-offs between different organizations.
Huawei – The large Chinese technology company offers a range of security products including mobile security.
IBM – The IBM MaaS360 enterprise mobile device management solution from IBM-acquired Fiberlink, includes mobile security capabilities.
Icon Labs – Headquartered in Iowa, Icon Labs provides embedded device security, including support for mobile.
IntegriCell – Washington-based IntegriCell, led by industry expert Aaron Turner, provides a range of mobile security solutions.
Intel Security (McAfee) – Intel offers the McAfee Mobile Security solution for Android and iOS mobile devices.
ITADSecurity – ITADSecurity offers a security risk intelligence solution for mobile devices.
Kaprica Security – Kaprica Security offers penetration testing services with emphasis on mobile security.
Kaspersky – Kaspersky offers mobile device protection including password manager, safe browsing, QR scanning, and Internet security for Android.
Lookout – Lookout provides advanced anti-malware software tools for protection of mobile devices, data, and apps. Important functions included in the Lookout tool are scanning of downloaded apps and mobile device data backup to the cloud.

Marble Security – Marble, acquired by ProofPoint in 2015, offers mobile application security based on cloud threat intelligence.
MobileIron – Mobile device management (MDM) solution provider MobileIron offers a range of security support capabilities in its enterprise product such as certificate exchange for multi-factor authentication.
Mocana – Mocana provides mobile security threat containment through software application wrapping. Mocana was one of the early pioneers in this wrapping concept for mobile applications.
Mojave Networks – Enterprise grade mobile security from Mojave Networks includes cloud-based support.
mSignia – Irvine-based mSignia offers technology to support strong authentication and fraud prevention on mobile apps.
Neohapsis – Part of Cisco, the company provides mobile and cloud security consulting for enterprise.
NowSecure – Illinois-based NowSecure provides mobile security and privacy for Android smart phones and tablets.
NQ Mobile – Anti-virus protection from NQ Mobile is designed for Android and Windows devices.
Pradeo – Located in France, Pradeo offers a suite of mobile application security testing tools and APIs.
Protected Mobility – Protected Mobility, headquartered in Virginia, offers solutions for mobile app security.
Pulse Secure – Pulse Secure, a Juniper spin-off, offers a range of SSL VPN and mobile device security.
Rapid7 – Rapid7 acquired Mobilisafe in 2012, which provided foray into the mobile security product industry.
SAP – SAP Mobile Secure provides a software-as-a-service capability to manage mobile protection.
Sequitur Labs – The small company in Washington State offers mobile security application development tools.
Skycure – Skycure, led by Adi Sharabani, offers mobile intrusion detection and prevention.
SnoopWall – SnoopWall offers malware detection solutions for tablets and mobile devices.
Sophos – Sophos Mobile Security provides advanced security protection for Android devices.
Symantec – Symantec provides a range of mobile device management and mobile security solutions for enterprise and consumers.
Trend Micro – Trend Micro offers security protection for Android including mobile device management.
TrustGo – Part of Baidu, TrustGo offers mobile security solutions for app scanning and other features.
Trustlook – San Jose-based Trustlook offers anti-virus, anti-Spyware, and other security capabilities for Android devices.

Verizon – All major mobile service providers, including Verizon, offer a wide range of protection options for their enterprise customers in the area of mobile security and MDM.
V-Key – Redwood City-based V-Key employs intrusion prevention protection for mobile applications.
VMware – The acquisition of AirWatch brought VMware into the mobile security market; VMware Horizon Mobile involves mobile virtualization and application wrapping. One should expect to see more convergence between cloud operating system vendors such as VMware and mobile security solution offerings that are embedded virtually.
Webroot – Webroot offers SecureAnywhere Mobile solutions for Android smart phones.
Zimperium – Zimperium offers enterprise mobile security solutions supporting BYOD initiatives.

Additional Mobile Security Providers

Apple – The industry leading mobile device provider includes many novel security features in iTunes, iOS, and across the Apple mobile ecosystem.
Box – Box provides mobile security by supporting extending content securely across all mobile devices.
Mobile Active Defense – Mobile Active Defense provides management and security of mobile ecosystem with one solution.
Nubo – Nubo supports BYOD a remote enterprise secure workspace for mobile devices.
Omlis – UK-based firm Omlis supports a range of mobile payment solutions with security.
Phone Warrior – Phone Warrior supports Spam call blocking, text blocking, and Caller ID functions for mobile.
Samsung – Samsung offers the Knox suite of mobile enterprise security solutions for device protection and management.
TekTrak – TekTrak offers a range of mobile application security products for Android.
Workspot – Workspot offers a secure virtual desktop solution for enterprise with cloud support.

23. Password/Privilege Management

⇒ *Passwords* – Passwords are the most resilient, and also the most complained about, aspect of enterprise and personal/consumer cyber security.
⇒ *Password Management* – Modern password management software provides indispensable support for handling access to multiple accounts.

⇒ *Privilege Management* – The improper management of privileges is a commonly exploited weakness in enterprise networks today.

Regardless of the long-standing desire amongst cyber security professionals for *passwords* to be removed in favor of a stronger form of authentication, the simple password construct has remained the most resilient identity validation method ever invented for access to applications, devices, networks, and systems. The main reasons for such continued password use include simplicity, low cost, convenience, interoperability, and cross-platform transportability.

In addition, procurement teams love the use of passwords because the organization typically doesn't have to *buy* anything new to validate users. No system has ever been developed, for example, that included extra fees for inclusion of password authentication. But with password weaknesses leading to so many compliance issues and exploits, the approach has begun to evolve, albeit somewhat slowly.

In particular, *password management* and the associated set of *privilege management* capabilities have begun to emerge with attendant capabilities that increase the accuracy and validity of authentication considerably. Both schemes require an incremental investment by the CISO team in both time and money, but they do improve the security of passwords, and are usually not too difficult to administer for user, server, and mutual authentication schemes.

Advances in this area are especially welcome because password usage remains one of the most complained-about aspects of modern cyber security. The biggest annoyance stems from the difficulty of trying to remember multiple passwords for different systems. Some managers – perhaps trying to make a point to the security team – print out or create laminated sheets with the myriad of user names and passwords required to get through the day. The risk of such laminated sheets, or any other printed list of passwords, getting into the wrong hands is obvious.

So as suggested above, to deal with this multiple password problem for personal and business accounts, password management systems have begun to see greater acceptance amongst CISO teams. The typical design involves a user's passwords, account information, and PINs being dropped into a common, protected vault, which is then enabled for use via a single master password, and integrated into the login and usage process for Websites, servers, PCs, and applications. Password management schemes generally serve two types of users:

- *Personal Use* – Personal password managers help individuals protect their personal accounts, including email and e-commerce sites. This function can be embedded into software such as anti-virus tools or Web browsers. The primary challenge in the management of personal passwords, and the reason it is mentioned here in the context of CISO team concerns, is that employees will almost always choose personal passwords that are similar to, or exactly equal to, passwords they have chosen for work-related access. This might be

one of the most critical weaknesses in any enterprise security protection approach.

- *Enterprise Use* – Enterprise password managers are more complex, feature-rich systems that reduce the risk of sensitive data loss through enterprise or cloud-hosted secure vault capabilities for passwords used by employees, system administrators, customers, and partners.

The primary use case for both types of password management involves securely storing passwords on PCs, mobile devices, servers (e.g., Websites), or service provider cloud systems. The primary access protection for the management system itself involves a master unlocking password or passphrase or use of some multi-factor authentication approach to unlock passwords for sensitive applications and systems.

Obviously, a security weakness results from putting all of one's credentials in one bucket, so to speak. Proper secure storage, handling, and access for password management systems are therefore essential. An additional vulnerability arises when employees reuse the same password for personal and enterprise use. For this reason, it sometimes makes sense for the enterprise team to allow inclusion of personal accounts in an enterprise password management tool. This does introduce some administrative burdens, such as when an employee leaves the organization, but the extra effort might be worth the incremental benefit.

The key functional requirements a CISO team should be looking for in a given password management system include the following:

- *Information Storage* – This usually includes passwords and PIN codes for applications, PCs, servers, networks, and Websites. Mobile devices introduce additional password use cases. Storage can also be portable as in password management software on a USB drive or in a public cloud such as Dropbox.
- *Form Filling* – Good password management systems will automatically and safely enter user and password data onto Website forms.
- *Information Organization* – This usually involves organization of multiple accounts for the user. As discussed above, this might even intermingle personal and business accounts.
- *Password Generation* – This involves automatic generation of complex passwords that are hard for hackers to guess or obtain.
- *Password Protection* – Good password management systems will store your password and account information securely using encryption and secure accessibility through a master password.

The password management market, like all aspects of computer security, has been growing steadily over the past decade. This is *less* due to the strategic value of these systems for consumers and businesses, and more due to the unfettered proliferation of personal and business account access from PCs, tablets, and mobiles. It is also true that passwords will probably never go away completely, in spite of their

predicted demise for many years. Three key trends should be recognized in the context of password management:

- *Traditional Password Management Systems* – Market growth for traditional password management will gradually level off, and even begin to shrink, as adaptive, two-factor authentication solutions become more available.
- *Multifactor Authentication Management Systems* – Integrated multifactor solutions will increase gradually, especially with popular use of thumbprint recognition on mobiles such as iPhones.
- *Integrated, Federated Adaptive Biometrics* – Integrated, federated authentication based on adaptive biometric methods will eventually render password management systems obsolete.

These three password management marketplace trends are depicted in the graphs below.

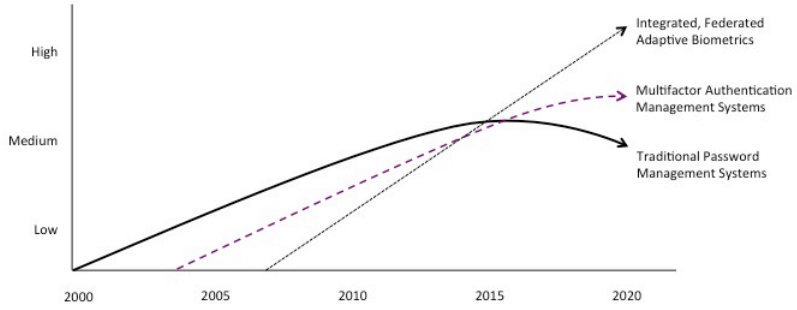

Figure 23-1. Trends in Password and Authentication Management

The use of adaptive technology and biometrics – integrated with the mobile experience – will reduce, but not remove, the need for password management systems in the next decade. In the meantime, password management systems will continue to be useful and the companies providing such tools will continue to thrive financially, especially if they provide an integrated desktop, tablet, and mobile experience.

An additional enterprise security market that is related to password management, but that deals with a more intense threat and more consequential access is known as *privilege management*. Technically speaking, privileges are based on so-called user authorizations, which are part of the ITU X.509 standard. The privilege management function provides registration, issuance, handling, protection, delegation, and inter-domain authorization for privileges, all supported by third party authorities. These authorities digitally sign the underlying privilege, which increases its security, but also increases the underlying complexity.

The handling of privileges, more recently, has gravitated in many environments to the use of Security Assertion Markup Language (SAML), which is

an XML-based open standard for privilege exchange. Web browsers, in particular, utilize SAML to handle the use of single sign-on (SSO) using cookies. This process also requires a complex underlying support ecosystem to include users, identity providers, and service provides. Privilege management trending in the coming years will be driven by these factors:

- *Security Needs* – Applications that absolutely require more security than traditional passwords will drive toward the use of more trusted privileges. Enterprise *least privilege* administration of critical assets such as Active Directory is an example.
- *IoT Scale* – As critical IoT endpoints supplying important telemetry and supporting essential services continue to require authorization and authentication, the use of embedded IoT privilege management will grow dramatically in the marketplace.
- *Inter-Domain Needs* – The plethora of different standards and approaches using passwords, privileges, authorizations, SAML, and so on, will eventually converge on more common standards, but this will take some time.

Many vendors support privilege management and are listed below. The respective approaches used in *identity and access management* and privilege management are so similar that many groups interchange *privilege* with *access*. Hence, the identity and access management market is often viewed as a superset of privilege management, which obviously makes things more difficult for CISO teams to sort out during source selection of vendors. Concepts such as privileged identity management (PIM) and privileged user management (PUM), for example, have emerged and are almost impossible to sensibly differentiate.

Also, while privilege and password management are combined in this section based on the obvious similarity of function, the underlying implementations are so different that vendors have had trouble integrating password and privilege management functions. This might change as virtual technologies introduce greater design and implementation flexibility for the different approaches.

Password/Privilege Management Providers

CISO teams doing review or source selection for password management, privilege management, access management, single sign-on, and the like should combine their review of the vendors listed below with the vendors listed in the identity and access management (IAM) section of this report.

Nearly every IAM vendor includes password and privilege functions, and some of the larger vendors will provide one-stop shopping for password, privilege, and access needs. Obviously, any enterprise design in this area must be closely coordinated with the selection, integration, and use of identity and access management. It goes without saying, furthermore, that if mainframes remain in use, that password and privilege management will be primary data controls.

AgileBits – Canadian company AgileBits offers the 1Password solution for personal and enterprise use.
Avatier – The global firm offers password management as part of its identity and access management suite.
Avecto – Avecto combines privilege management, application control, and sandboxing to provide endpoint security.
BeyondTrust – BeyondTrust provides password management, privileged account management, and vulnerability management solutions.
Bitium – Santa Monica-based Bitium provides password, user, and identity management solutions.
CA – CA offers the Privileged Access Manager product for fine-grained user access controls in the enterprise. Their acquisition of Xceedium provided CA with advanced privilege management capability.
CyberArk – CyberArk provides a range of privileged account management and security solutions for the enterprise. The company acquired Viewfinity.
Dell – Dell provides a range of privileged account management solutions for Unix, Windows, and other environments.
Fischer International – Fischer offers a range of password, privilege, and identity management solutions.
Fox-T – Mountain View-based Fox-T offers access management and password/privilege management solutions.
IBM – IBM includes privileged identity management in its suite of identity and access management solutions. It is not uncommon for large IAM providers to includes a range of integrated password and privilege management functions in its solution suite.
Keeper Security – Keeper Security includes a password manager and secure digital vault.
LastPass – LastPass offers a password manager, auto form filler, random password generator, and secure digital wallet.
Lieberman Security – Lieberman Software includes a range of products related to identity, passwords, and privilege management.
ManageEngine – ManageEngine includes privileged password management and self-service password management solutions.
NetWrix
OneID – Redwood City-based OneID offers identity, access, password, and privilege management.
Oracle – Oracle includes a wide range of password and privileged identity management functions in its popular suite of identity and access management solutions.

Osirium – UK-based Osirium offers identity, access, password, and privilege management solutions.
Symantec – Symantec includes identity access manager capability in its information protection suite.
Thycotic – Thycotic offers complete privileged account management solution for enterprise IT administrators.
Wallix – Wallix provides SSO, password management, privileged user management, and related functions.

Additional Password/Privilege Management Providers

Animabilis Software – Animabilis offers the Aurora, which includes a full-featured password storage and management solution for enterprise.
DataViz – DataViz includes a product called PasswordPLUS for organizing passwords across iOS, Android, Mac, and Windows.
Dashlane – Dashlane offers the Dashlane Password Manager and Secure Digital Wallet products.
Hitachi-ID – Hitachi-ID includes privileged access management in its identity management and access governance solutions.
KeePass – KeePass is an open source password manager that might be considered for use in the enterprise.
Lamantine Software – Lamantine Software develops a password manager and form filler called Sticky Password.
mSeven Software – mSeven Software provides a password manger for Mac and Windows.
MyLOK+ – MyLOK+ offers its customers a secure password manager and data storage capability.
OrangeCat Software – Orange Cat Software offers a password keeper product for its customers.
Password Genie – Password Genie is a data protection and password security solution for Windows, Mac, Android, and iOS.
RoboForm – RoboForm provides its customers with an advanced password manager capability.
SplashID – SplashID supports management of passwords for iPhone Android, Windows, and Mac.

24. Two-Factor Authentication

⇒ *Factor Options* – CISO teams have a plethora of different options for embedding additional factors into the authentication process.
⇒ *Growth Trends* – Two-factor authentication will continue to experience significant growth across all aspects of enterprise computing.

⇒ *Identity Federation* – Stronger authentication allows for a federated experience exported from a two-factor base to application-level needs.

The vast majority of enterprise and personal authentication transactions for applications, systems, devices, computers, and networks continues to be performed with a single password factor. This remains true in spite of the fact that virtually every cyber security expert in the world agrees that authentication for access to anything of reasonable value should be done with at least two different factors. The resulting two-factor authentication process, if designed and integrated properly, is now sufficiently mature, cost effective, and easy to use that few effective arguments can be made against its use.

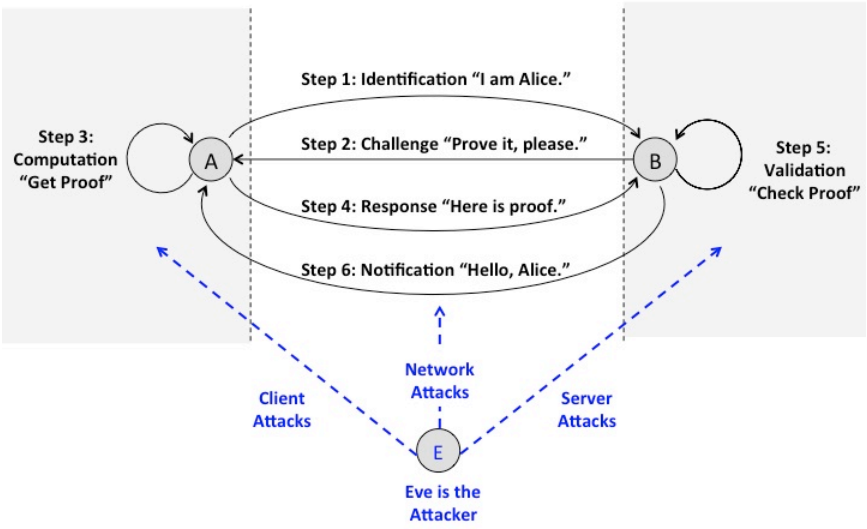

Figure 24-1. General Authentication Schema

Technically, *authentication* involves validation of a reported identity using some set of proof factors, and *two-factor authentication* involves constructing proof using any combination of more than one factor from the following list of validation methods:

- *Something You Know* – This is the most popular method, usually involving passwords, PINs, and passphrases. In the vast majority of enterprise access scenarios, CISO teams will include "something you know" as one of the factors for security, even if it is just a PIN.
- *Something You Possess* – This is usually some sort of tangible security token (hard/physical or soft/software), an electronic certificate, or a mobile device. With iPhone and Android thumbprint unlocking, many enterprise teams are using this as the first factor for secure access.
- *Something You Embody* – This involves biometrics, including voice, thumbprint, and facial recognition. Many security experts hold that

biometrics work especially well in the local, closed environment, as with unlocking a mobile device. Using biometrics in a broader context is still gaining acceptance, but experts worry that a hacked retinal pattern or thumbprint for an individual cannot ever be changed.

- *Someplace You Are* – This factor has traditionally been less reliable, but is now improving based on location from GPS or other means. Privacy experts worry about location as a factor, but many CISO teams are enthusiastic about this method due to its convenience with mobile devices.
- *Something You Do* – This factor involves the use of behavioral or adaptive authentication that relies on patterns to determine if you are who you claim to be. This approach is the most promising of all authentication methods simply because it introduces the possibility of integrating and combining all of the best available factors into a common approach.

While these authentication factors are all "roughly equivalent" in terms of their security strength (ignoring any subtle technical cryptanalytic differences), the vast majority of two-factor authentication usage in the enterprise to date has been a password, combined with a hard or soft token, most likely obtained from RSA.

More recently, however, with such obvious increases in mobile smart phone usage for enterprise applications, the introduction of SMS authentication has become increasingly popular. Companies such as Duo Security are working hard to make these solutions simple to use. Biometrics is also growing in interest as the algorithms for differentiating unique human attributes such as facial features and fingerprints have become more accurate.

CISO teams should review the user registration experience for any two-factor solution. This aspect is essential for success, especially in environments that require scale to a large number of users. If the registration process is onerous – not atypical for many biometric solutions, for example – then application owners, developers, and administrators will shy away from embedding the two-factor solution into their solution. Proof-of-concept deployments are recommended to avoid over-reliance on PowerPoint marketing representations of the expected user experience.

The market trending for two-factor authentication is highly positive since more consumers and businesses recognize the problems inherent in using passwords. Some vendors have also begun making two-factor authentication incredibly cheap – even free – for use in small-scale or personal applications. These factors will combine with the increasingly perimeter-free nature of modern enterprise networking to drive growth in the two-factor market for many years.

That said, different two-factor solutions will see different growth rates. Some enterprise customers, for example, will use MDM for certificates on mobile devices enabled via a device thumbprint. The use of mobile devices as a factor clearly benefits from the obvious social advantage that comes from most individual's desire to never be more than six inches away from their mobile device at any time. The market growth outlook for two-factor authentication solutions is shown below.

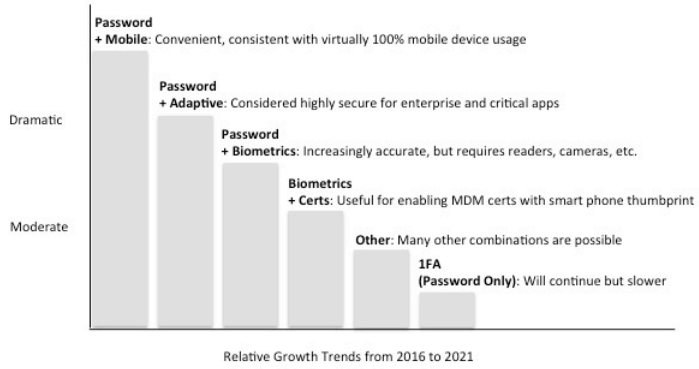

Figure 24-2. Market Trend Outlook for Two-Factor Authentication

As stated above, the good news for any two-factor product vendor is that the market outlook in virtually every aspect of this technology is positive. This is true for mobile, biometrics, and even continued use of tokens. More challenging, however, is the likelihood that this type of two-factor (or even three-factor) solution will become more embedded into cloud-resident applications. Such multi-factor protection will include creative use of biometrics on devices, mobile device management for enterprise, and use of cryptographic certificates for authentication.

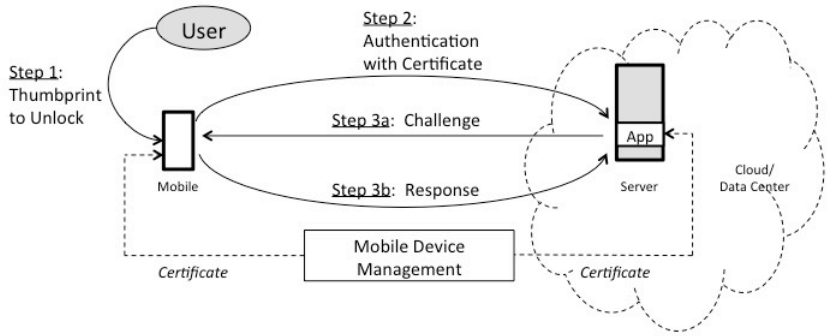

Figure 24-3. Three-Factor Authentication for Cloud App Access

Furthermore, the proliferation of identity federation from larger service and application providers, especially in mobility, downstream to smaller application service providers, will reduce the need in the enterprise, as well as for consumers, for native two-factor solutions. Instead, authentication will become more deeply embedded into the overall experience, perhaps beginning with a hardware root of trust, federated up through the device operating system to a container, which then offers additional validation before the validated user is presented to the desired application, system, network, or cloud. Users will enjoy this experience, since it will reduce the amount of work for them, as well as the amount of information to be remembered.

Two-Factor Authentication Providers

The following companies offer multi or two-factor authentication product or service solutions including biometrics for consumers and enterprise. Vendors who use two factors to authenticate users to their solution are not included here. Many of the listed vendors enthusiastically market their support for the Fast Identity Online (FIDO) initiative. This important market initiative supports and encourages simpler, safer authentication through open, scalable, technical specifications for authentication and related support technologies. CISO teams should have a look at the FIDO alliance Website and consider the advantages of working with a FIDO participant.

The decision was also made to include below only the native providers of two-factor authentication technology, rather than try to list every product or service that includes stronger authentication in their solution. This might change in the future as more services such as social networking or Web-based email include strong authentication as an SSO value-proposition for federation to a broader range of enterprise and consumer services.

2017 TAG Cyber Security Annual
Distinguished Two-Factor Authentication Providers

Duo Security – My good friend Dug Song has been at the forefront of multi-factor authentication for many years. I've always admired his work, and was delighted when he agreed to provide assistance and support for this project. Digging into the Duo Security business model revealed so much to me about how the sincere desire to make the world more secure is always the best way for companies to succeed in a tough cyber security marketplace. Kudos to Dug and his team for combining such sincere purpose with amazing multi-factor authentication technology.
Transmit Security – I was first introduced to Rakesh Loonkar's fine work when he was one of the founding principals at Trusteer, which was purchased by IBM. As Rakesh introduced me to the advanced technical and operational capabilities in Transmit Security, I was impressed by how the team had taken such a holistic approach to authentication, identity, and enterprise security. I am grateful to the entire Transmit team for their assistance throughout this project.

2017 TAG Cyber Security Annual
Two-Factor Authentication Providers

Authentify – Authentify, part of Early Warning, offers phone-based multi-factor out-of-band authentication (OOBA) solutions.
AuthLite – Located in Springfield, AuthLite offers two-factor authentication using a USB key and password.

AuthRocket – Colorado-based AuthRocket provides a user management API to support authentication as a service.
Authy – Authy provides a two-factor authentication smartphone application for individuals and business.
Auth0 – Auth0 supports software developers with single sign-on, token authentication, and related products for integration into apps and APIs.
Behaviosec – Swedish firm Behaviosec provides a biometric authentication solution based on behavioral attributes.
BI2 Technologies – Biometric intelligence and identification technologies firm BI2 technologies is located in Massachusetts.
CA – CA offers strong authentication services embedded in its range of identity and access management solutions.
Celestix – Fremont-based Celestix provides unified remote access to any application on any device using single sign-on.
CertiVox – Now known as MIRACL, the company provides a two-factor encryption and authentication solution, as well as a cryptographic SDK.
Clef – Oakland-based Clef offers secure two-factor authentication solutions with no need for passwords or tokens.
Collective Software – Collective Software provides the AuthLite two-factor authentication system.
Comda – The Israeli firm offers a range of IT security products including biometric authentication.
Crossmatch – Crossmatch offers its DigitalPersona Altus solution for biometric identity verification and enrollment.
Daon – Daon is a biometrics identity management company with an underlying Biometric Trust Infrastructure.
Deepnet Security – Deepnet, located in the UK, offers an authentication platform using multifactor and biometric solutions.
Delfigo – Delfigo develops a range of identity-based strong authentication services for customers.
Delta ID – The California-based firm provides the DeltaID iris recognition solution for strong authentication.
Device Authority – The D-FACTOR authentication engine delivers connected devices for IoT applications.
DirectRM – Located in California, DirectRM provides strong authentication and access management solutions supporting BYOD.
Duo Security – Ann Arbor-based Duo Security provides several different two-factor authentication solutions with emphasis on endpoint visibility protection. Dug Song's team at Duo addresses a large range of customers from Fortune 500 firms to small companies with modest needs.
DynamiCode – Located in Hong Kong, DynamiCode offers strong authentication and secure mobile POS solutions.
Easy Solutions – Easy Solutions includes mobile and strong authentication in its suite of anti-fraud solutions.

ECKey – The Pennsylvania-based firm offers solutions for turning Bluetooth smartphones into access control components.
ElevenPaths – The Madrid-based company provides a range of security products including authentication.
Entersekt – Located in South Africa, Entersekt provides interactive authentication and encryption solutions.
Entrust – Entrust provides a range of identity and authentication technologies using mobile, certificates, and other technologies.
FEITIAN Technologies – The Chinese firm offers IT security solutions including authentication.
Finsphere – Finsphere, located in Finland, provides solutions for using mobile devices for authentication.
Gemalto – Gemalto provides digital security solutions ranging from biometrics, to SIM card development, to protection of near-field communication (NFC).
HID Global – HID Global includes access control and secure identity solutions including smart cards and readers.
Hoyos Labs – Hoyos Labs offers a range of mobile biometric solutions for authentication.
ID Control – Located in the Netherlands, ID Control provides a range of strong authentication solutions.
ImageWare – ImageWare provides biometric solutions to support authentication and identity management.
Imprivata – Massachusetts-based Imprivata focuses on single sign-on, authentication, and related solutions for health care.
Iovation – Located in Portland, iovation supports on-line fraud prevention based on strong device authentication and recognition.
i-Sprint Innovations – Located in Singapore, the company supports identity, credential, and access management solutions.
Keypasco – Swedish firm Keypasco offers secure authentication, multi-factor, and device authentication.
LaunchKey – LaunchKey, headquartered in Las Vegas, provides a next generation authentication platform.
Mi-Token – Mi-Token develops a range of two-factor authentication solutions based on soft tokens.
mSIGNIA – mSIGNIA provides mobile authentication enhanced with biometric device recognition.
Nok Nok Labs – The Palo Alto-based firm provides a streamlined strong authentication protocol based on Fast Identity Online (FIDO).
OneLogin – OneLogin offers cloud-based identity and access management with secure access to cloud applications from mobile devices.
PointSharp – The PointSharp mobile app provides authentication via software-based one time password token.
RSA – Industry leading provider RSA, part of EMC, offers one-time password token solutions that are in use around the world.

SafeNet – Now part of Ingenico, SafeNet provides enterprise authentication as part of its suite of security solutions.
Salesforce Identity – Salesforce Identity provides federated identity services to connect every employee, customer, and partner to any app, on any device. The company acquired Toopher.
Seamoon – Chinese company Seamoon provides a one-time password authentication solution for its customers.
SecSign – Located in Nevada, SecSign provides two-factor authentication, encryption, and related capabilities.
Secure Access Technologies – Secure Access Technologies provides mobile authentication via the SAT Mobile ID solution.
SecureAuth – SecureAuth supports two-factor authentication and SSO for enterprise applications.
SecurEnvoy – UK-based SecurEnvoy offers mobile phone-based tokenless two-factor authentication.
SecureKey – SecureKey, located in Canada, supports identity and authentication needs for online consumer services.
SecurePush – Israeli firm, Secure Push, offers a strong multi-factor authentication platform.
SecuTech – Canadian firm Secutech offers the UniKey and UniToken solutions for USB-based plug-and-play authentication.
SMS Passcode – SMS Passcode, headquartered in Denmark, supports adaptive multi-factor authentication based on mobile phone.
Socure – Based in New York, Socure provides social biometric solutions for identity verification.
Sonavation – Sonavation is a biometrics firm supporting identity authentication and other security solutions.
SSH – Headquartered in Finland, SSH provides SSH key management, access, and authentication support.
Stormpath – The California-based firm offers a user management API for authentication service integration.
StrikeForce Technologies – Headquartered in New Jersey, StrikeForce provides out-of-band authentication.
SurePassID – SurePassID supports next-generation identity and access management with FIDO authentication and secure IoT.
Swivel Secure – UK-based Swivel Secure provides strong authentication for cloud, Web, VPN, and desktop.
Syferlock – Connecticut-based Syferlock offers a range of token-less solutions for multi-factor authentication.
Symantec – Symantec provides cloud-based validation and ID protection services for secure multi-factor authentication.
TeleSign – The California-based company offers mobile identity and authentication solutions.

Transmit Security – The Massachusetts-based company, run by Rakesh Loonkar, offers a range of programmable biometric solutions. Transmit's solution allows for replacement of tokens, passwords, and other traditional factors.
TRUSTID – Located in Oregon, TRUSTID offers automatic caller identity validation capabilities.
2FA – The Austin-based company offers a range of two-factor authentication solutions.
Vasco – Illinois-based Vasco provides solutions for strong authentication, digital signature, and identity management.
Vir-Sec – The Florida-based firm provides multi-factor authentication access to applications.
VU Security – Headquartered in Argentina, VU Security offers two-factor authentication solutions.
WWPass – WWPass provides strong two-factor authentication solutions using cryptography techniques.
Yubico – The Swedish firm provides an open source, USB authentication solution for platforms.

Additional Two-Factor Authentication Providers

Idevity – Idevity supports smart card and identity use with visualization apps for mobile and related products and services.
Nymi – Nymi enables secure, continuous authentication through a wearable, multi-factor biometric device.
OnWire – OnWire includes a FedRAMP, multi-factor authentication platform with cloud based IAM.
Protectimus – UK-based firm Protectimus offers a range of two-factor authentication solutions.
Swivel Secure – Swivel Secure provides two-factor authentication for a range of business applications.
Synaptics – Synaptics supports high-end technology in the touch sensing and display integration area.
Twilio – Twilio provides a range of messaging, voice, and authentication APIs for applications.
Usher – Usher provides biometric, location-based authentication solutions for business and individuals.

25. Voice Security

⇒ *Mobile Voice Security* – The focus of most mobile voice products has been on enhanced confidentiality for mobile communications using encryption.
⇒ *Infrastructure Protection* – CISO teams should select voice security solutions that cover the range of threat considered relevant to the local enterprise.

⇒ *Global Travel* – Protection of voice communications for globally traveling executives is a strong incentive for mobile voice security solutions.

The primary focus of cyber security over the past decade has been toward the protection of data and Internet services. Traditional voice communication services, in contrast, have received relatively minor attention across the entire security community. One possible explanation for this lack of focus on *Voice Security* is the gradually improving encryption that mobile carriers have deployed with each advancing generation of mobile services. Compared with data intrusions, voice-related intrusions have been relatively less intense – or at least relatively less advertised.

As an example, the often-cited threat of fake base station eavesdropping, also referred to as IMSI-catching, has been greatly reduced, if not entirely future-proofed, with the progression from unencrypted 2G/GSM to AES-protected 4G/LTE mobile communications. The remaining confidentiality issues stem from legacy deployment of 2G/3G networks to ensure full wireless coverage, as well as the continued use of Signaling System 7 (SS7) control, which will wane with the progression to Voice over LTE (VoLTE). The dependency wanes further with the deployment of software defined networking. So *time* is clearly on the side of carrier-provided voice security.

That said, several recent developments in our global society have begun to cause a renewed and healthy interest in the provision of more advanced security protections for voice communications, particularly mobile:

- *Expanded Global Business* – With business travel, supply chain, and partnerships expanding globally at an astounding rate, the need to ensure protected voice communications across national boundaries has increased. This is especially true for companies doing business in countries with somewhat dubious underlying telecommunications infrastructure integrity. Voice security companies such as KoolSpan, for example, report a high percentage of their mobile voice security business being driven by global business requirements.
- *Government Surveillance* – The highly visible events over the past few years in the United States and elsewhere with the public exposure of unknown surveillance programs in the Intelligence Community have heightened citizen awareness in the privacy communications to the need for increased encryption. The argument can be easily made that this risk of domestic government surveillance is an international concern, with few if any exceptions.
- *Infrastructure APT Concerns* – With nation states demonstrating the ability to successfully attack anything they target with advanced persistent threats (APTs), the argument that all mobile carriers, including smaller regional providers, can ensure full encryption secrecy from nation-state actors in their infrastructure has begun to be questioned. Users with particularly

sensitive business requirements for voice might be wise to invest in heightened cryptographic protections.

These global societal trends point to increased need for voice security solutions, and in particular, the expanded use of encryption in an over-the-top manner to protect conversations, texting, and related instantaneous communication over traditional circuit switched, IP-based, or mobile networks. Such encryption must be designed specifically to prevent eavesdropping by third parties such as service providers, government agencies, and malicious actors. They must also be easy to use.

The overall ecosystem for a typical encrypted voice communications set-up between two entities is depicted below.

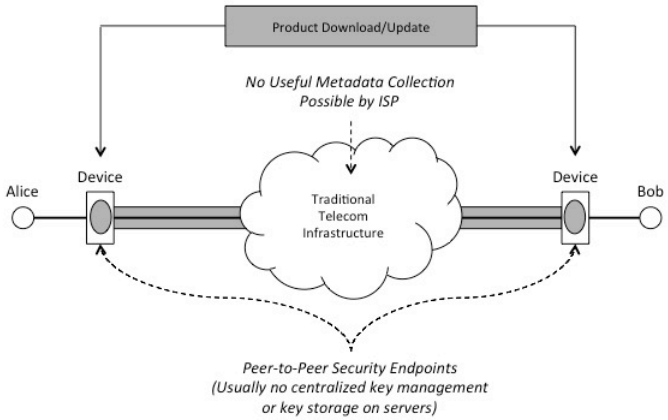

Figure 25-1. Voice Security Ecosystem

An important consideration in the provision of secure voice service is the ease with which users can deploy and utilize the protections. Whether this has been, or will be achieved amongst the leading voice security vendors remains to be seen, but one can expect the norm across the globe in the next few years to include the ability to flip a switch (so to speak) in order to ensure additional encryption if needed. This may be achieved through partnership with the large mobile carriers or mobile endpoint manufacturers, or it may be achieved through ubiquitous apps available on popular app stores. An even more interesting option would be expanded enterprise encryption integrated with, and available through, enterprise mobile device management (MDM) solutions.

Key user and administrative features to look for in a voice encryption solution include the following:

- *Strong Encryption and Security Architecture* – Selected secure voice solutions must have strong underlying encryption algorithms and key management. CISO teams might ask, for example, if a given solution meets NSA's requirements for Suite A (government use) or Suite B (commercial use) –

although this might not really need to be a firm requirement. The Advanced Encryption Algorithm (AES) with key sizes of 128 and 256 bits, as well as Elliptic Curve Digital Signature Algorithm (ECDSA) are examples of Suite B solutions. If the algorithm or key management scheme is proprietary and non-standard, then the vendor should supply evidence that the solution is secure. Recommended minimum key lengths are algorithm-specific, with RSA, Elliptic Curve, and conventional block ciphers each having their recommended size thresholds. CISO teams should keep tabs on the recommendations from the crypto community on minimum acceptable lengths and conversion ratios between ciphers. In practice, the belief here is that basic cyber security issues related to computers, applications, networks, and software are many thousands of times more relevant to enterprise cyber risk than cryptanalysis of surreptitiously collected ciphertext. (Cryptanalysts from Fort Meade might disagree with my view.)

- *Permissions Management via Groups* – Permissions settings usually work by allowing users to create multiple personas, sometimes called workspaces. Each persona will have its own unique app permissions settings, and the best solutions try to use hardware to maintain separation between multiple personas. In addition, permissions management often allows users to investigate the specific settings for each app, often highlighting dubious requests by certain apps for access to resources such as contacts.
- *Integration with Popular Mobile Devices* – If the selected voice security solution is to be used across the enterprise, then support for iOS, Android, and Blackberry is absolutely required. Full cryptographic interoperability between different vendor solutions remains to be determined, and should be reviewed on a product basis, but one can expect to see progress in the coming years.

Some enterprise users also require the ability to route voice communications across secure virtual private networks (VPNs) operated by a secure voice provider. This type of capability will likely become available from mobile service providers in the near future. Obviously, the main consideration is the degree to which any provider maintains metadata, keys, or other information that could be demanded by a law enforcement agency with legal justification.

It is worth nothing that the voice security industry has also come to include infrastructure controls designed to prevent attacks such as telephony-based denial of service (TDOS) and voice over IP (VOIP)-based fraudulent activity. Not surprisingly, such attacks have become more common in the past decade. CISO teams are advised to have a detailed discussion with their voice services provider about the best way to integrate such unique features into the enterprise voice architecture. Companies such as Secure Logix have reported consistent growth in these areas, in spite of the relatively lower level of attention afforded this type of protection.

The trend for secure voice is positive in the near term, with the caveat that most voice security solutions will be best integrated into existing communication services and infrastructure. Cyber security history suggests that encryption is best applied quietly in the background with a minimum of user interaction and hassle. So voice security solution providers are strongly advised to find good partners and integrate. This is especially true for emerging virtual communications over SDN-based carrier infrastructure. CISO teams should keep an eye on this area, especially if auditors and compliance managers begin to include voice security requirements more aggressively in their frameworks.

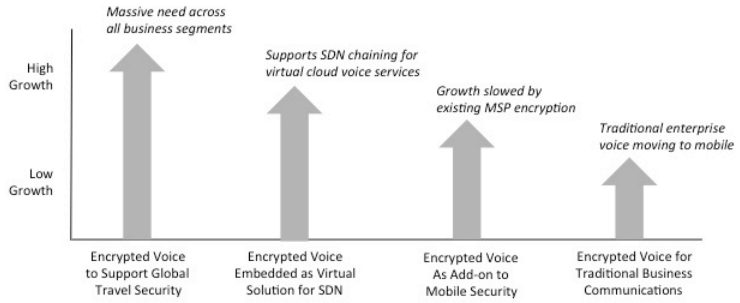

Figure 25-2. Voice Security Trends

One practical benefit *worth re-emphasizing* for CISO teams with the advance of voice security is that it should support streamlined executive travel processes. It is perfectly conceivable that the intensity of executive global travel could drive adoption of secure voice solutions for over-the-top protection of mobile communications to nearly 100% use across larger business. This could provide a massive windfall for secure voice providers, but the timeframe and intensity of this shift might still be a couple of years away. Once enhanced voice products are trivial to deploy with negligible cost and hassle to the user, the general practice of super-imposing encryption to avoid security coverage gaps in international use will become embedded in corporate policies across the globe. In the meantime, it seems irresponsible for CISO teams to not make full use of voice security products in the immediate term for executive traveling to dubious locations.

Voice Security Solution Providers

The voice security solution providers listed below consist mostly of encryption vendors with products, usually software-based, that are designed to integrate with the mobile experience of their customers. Some infrastructure voice security providers are included as well. It obviously makes sense for CISO teams to consult with their mobile and landline carrier to understand the existing protection footprint that will serve as a baseline for their voice security, before decisions can be made about expanded confidentiality solutions. Mobile service providers tend to

offer solutions in this area through partnership with the technology providers listed below. Such solutions are often provided as an overlay to the inherent encryption that is embedded in their mobile communications protocols.

2017 TAG Cyber Security Annual
Distinguished Voice Security Providers

Koolspan – Elad Yoran, who might just belong to the most famous cyber security family in the world, was kind enough to introduce me, over sushi in Manhattan, to the fine technology being developed by Nigel Jones and the technical and crypto team at Koolspan. I've since watched as the company has made the transition from hardware to software-based voice encryption, and Nigel has shared with me many technical insights on the cryptography business that helped me immeasurably in the writing of this section. It was Nigel, specifically, during a couple of different visits to Bethesda, who helped me realize the obvious benefit of voice security solutions for traveling executives.

2017 TAG Cyber Security Annual
Voice Security Providers

AEP (Ultra Electronics) – The UK-based firm provides HSMs for data and voice security protection.
AT&T – The massive ISP/MSP will design a secure voice solution for customers that can integrate with the full range of the carrier's industry leading managed security solutions and threat intelligence product. With SDN deployment will come the possibility to offer cloud workload encryption.
Cellcrypt – Cellcrypt provides a voice security solution with encryption and related protections.
Enigmedia – Headquartered in Spain, Enigmedia provides solutions for secure voice and telepresence.
General Dynamics – General Dynamics offers Sectera Wireless GSM phone for secure communications.
Koolspan – Bethesda-based Koolspan, under the joint leadership of Nigel Jones and Elad Yoran, offers software solutions for voice, texting, and messaging security that are designed for all popular enterprise and personal mobile voice platforms.
SecureLogix – SecureLogix offers secure telephony infrastructure controls for service providers and enterprise users concerned with TDOS and related threats.
Secusmart – Acquired by Blackberry, Secusmart provides a range of mobile solutions including security.
Silent Circle – Silent Circle provides advanced encryption designed by crypto guru Phil Zimmerman with high levels of privacy protection for users.
Sophos – The security firm offers its SafeGuard encrypted voice security solution for customers.

Verizon – The carrier offers secure voice solutions through a business partnership with Cellcrypt.

Additional Voice Security Providers

CellTrust – The company provides a secure voice and messaging security gateway and aggregation solution.
CoverMe – CoverMe is a free download for Android and Apple to encrypt mobile communications.
Ostel – The Jitsi app from Ostel offers encrypted, open source tools resulting in secure voice comparable to Skype.
Nuance – The firm provides a range of advanced knowledge-based and voice biometric solutions.
Phone Warrior – Phone Warrior supports Spam call blocking, text blocking, and Caller ID functions for mobile.
Pryvate – Pryvate offers encryption products for secure voice, video, IM, and related communications.
RedPhone – RedPhone is a free, open source, secure voice application for Android created by Whisper Systems.
SecureGSM – Australian-firm SecureGSM provides a range of communication security solutions.
Secure Mobile – The division of SiRRAN Communications offers encryption-based security solutions for mobile.
Simlar – Simlar is a German-developed app for security mobile with support for Apple and Android.
T-Systems – The large technology and information assurance company offers a voice encryption application.
Twilio – Twilio offers a range of voice and messaging secure infrastructure protection solutions.
VIPole – VIPole is a secure messaging application developed in the United Kingdom for secure business communications.
Voice Security Systems – The California-based company offers technology solutions for voice security protection.
Whatsapp – Whatsapp is a hugely popular application claiming a billion users with embedded cryptographic protections for privacy.
ZoIPer – ZoIPer is a SIP softphone product with a range of advanced encryption-based security features.

26. Brand Protection

⇒ *Monitoring* – Brand monitoring is a mature discipline that has recently integrated cyber security as a factor requiring attention and protection.

⇒ *Brand Abuse* – Most of the security concerns related to brand monitoring deal with the risks of potential abuse and misuse of domains.
⇒ *Role of Social* – Social networking plays an important role in the monitoring of potential brand use activity.

For many years, marketing teams have employed so-called *brand-monitoring* techniques to better understand people's perception of company products and services. These brand-monitoring techniques originally began with manual surveys and polls of the general public pioneered by George Gallop many years ago. They continued through the research-driven period of marketing and advertising pioneered by David Ogilvy in the Sixties. This era was soon followed by the analysis of user clicks on a Website measured by on-line companies over the last two decades. These brand-monitoring methods now include careful collection and analysis of social network content and mobile app usage.

It should therefore come as no surprise that with such careful monitoring techniques in place to understand brand perception that an adjacent means would emerge for understanding brand fraud and misuse. Specifically, the purpose of *brand protection* is to employ active measures to prevent, detect, and mitigate any degradation or theft of a corporate or organizational brand. Viewed in this manner, it is surprising that so many CISO teams have spent virtually zero time working in this area. In fact, if you ask a group of CISOs what sort of protection methods they use to reduce the risk of brand abuse, you should not be surprised if you see mostly blank stares.

More traditional approaches to brand protection have included the use of special visible labels to either overtly or covertly authenticate a given product. This can be done as part of the packaging using optical film, holograms, and high-resolution printing to reduce the likelihood of fraud. The goal in these cases is to reduce the potential for counterfeiting, and it can be done in a manner verifiable by the human eye, or through the use of special equipment.

The primary technical approach used today for online cyber brand protection extends these physical methods to involve monitoring and analysis of data sources such as e-commerce sites, paid search, social media sites, the Dark Web, and mobile app stores. The goal of this analysis is to uncover evidence of the following:

- *Domain Management* – This type of analysis focuses on brand abuse via a domain misuse technique known as cybersquatting using top-level domains (TLDs). This fraudulent activity has become a bigger problem with the growth of e-commerce in the past decade. Nevertheless, CISO teams have tended to be somewhat lax in addressing the issue.
- *Brand Usage Monitoring* – This type of brand protection method includes searching for counterfeit and grey market sales and auctions, false associations, and brand impersonation. Brand usage monitoring can also include focus on the Dark Web in certain circumstances.

- *Partner Compliance* – This technique includes monitoring for improper partner use of brand logos, trademarks, and promotions. Finding your logo being misused on vendor, partner, or even competitor Websites can be a challenge because the metadata might be non-existent or unreliable. Visual inspection is often the only way to notice that some group is using an unauthorized picture of your SOC in their on-line marketing material.

Most current brand protection solutions are offered to the enterprise as managed services with corresponding consulting available to help address more unique circumstances of brand fraud or misuse. Primary focus areas in these brand protection managed offerings include detection and notification of bogus Web presence, spoofed email, and other invalid on-line presence masquerading as your brand. These are all unacceptable scenarios in any business, and the CISO should feel some obligation to reduce risk in these areas.

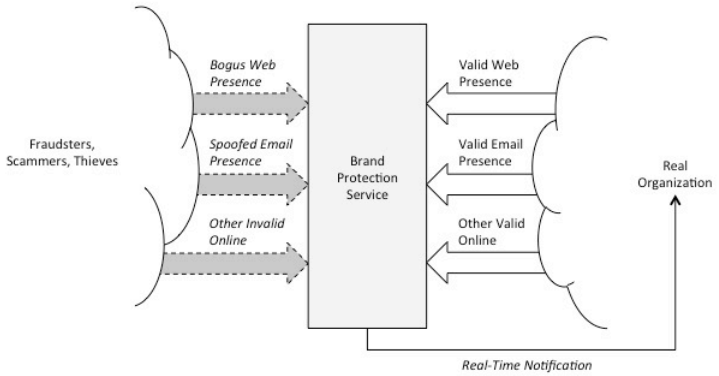

Figure 26-1. Typical Brand Protection Approach

Many of the brand *protection* services available are connected to comparable services focused on the more traditional brand monitoring methods alluded to earlier. Since companies have moved so much of their presence on-line – witness Amazon.com's impact on retail, for example – the degree to which a given brand is perceived on-line has become an important business metric. Companies regularly monitor social media outlets such as Twitter and Facebook to determine the positive or negative views customers have of the brand message.

It was only natural, therefore, for many firms to get into the information security aspect of brand monitoring with protection services focused on detecting and notifying when some fraudster or scammer is intentionally misusing a company's brand. The manner in which this is done is relatively straightforward, which reduces the barrier-to-entry for this industry – and this has a generally negative impact on growth trends.

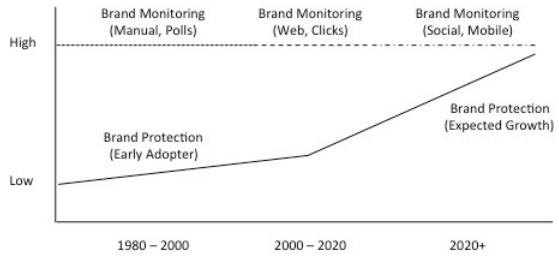

Figure 26-2. Trends in Brand Protection and Monitoring

The expected trend is that as more and more companies shift their brick and mortar presence on-line, this will tend to drive the need for on-line brand protection services. Furthermore, as companies increase their use of mobile applications and cloud infrastructure, the need for brand protection in these areas will grow as well.

In general, the outlook for brand protection services is high, and more CISOs will begin to recognize the benefit. Vendors are advised to look for ways to help CISO teams combine forces with other business units such as public relations teams to share the funding for their combined security and business intelligence brand services. If the marketing team is already doing brand monitoring, for example, then the CISO team might not need to arrange for a new vendor to also check for fraud.

Brand Protection Providers

A challenge for the brand protection vendors listed below is the relatively low barrier to entry for new companies to begin offering these types of services. A large number of companies exist in this category, and many of them will need to find ways to truly differentiate their services from being a commodity offering.

2017 TAG Cyber Security Annual
Brand Protection Providers

Agari – Agari's email security monitoring services provide advanced brand protection enhancement via DMARC solutions for email fraud.
Bouju – Located in Los Angeles, Bouju offers brand protection via data collection and analysis.
BrandProtect – Canadian firm BrandProtect offers a range of brand protection services.
DomainTools – DomainTools provides a range of domain, network, and monitoring tools for look-up, research, investigation, and threat intelligence.
First Cyber Security – The UK firm provides reputational analysis of Website authenticity for reducing fraud.
MarkMonitor – Obtained by Thomson Reuters, MarkMonitor offers solutions for protecting organizational brands.

One World Labs – Owl uses Dark Net threat intelligence to understand risks and protect brands.
Reputation.com – Located in Redwood City, Reputation.com offers brand and personal reputation protection services.
ReturnPath – ReturnPath offers a range of anti-fraud and brand protection solutions for the enterprise.
RiskIQ – RiskIQ uses intelligence driven techniques to scan the open Web for evidence of abuse.
SecureMySocial – The New York-based firm focuses on detection of social media activity that could be considered abusive.
The Media Trust Company – Located in Virginia, The Media Trust Company provides media security scanning for Websites, advertisements, and mobile.
Your Internet Defender – Located in Valley Stream, New York, Your Internet Defender provides a service for managing online reputation.
ZeroFox – Baltimore-based ZeroFox offers a range of social medial risk management and cyber security solutions.

Additional Brand Protection Providers

Brady Brand Protection – Part of Brady Corporation, founded in 1914, Brady Brand Protection provides product authentication labels.
Brandle – Brandle offers its customers a range of social media security and brand protection solutions.
Brandma – Chinese brand protection firm Brandma works closely with top-level domain registrars.
Brandshield – Brandshield supports technology to monitor and protect brands online.
BrandVerity – BrandVerity provides brand protection and monitoring services for paid search, Website content, and coupon codes.
Channel IQ – Chicago-based Channel IQ offers business pricing, media, and brand monitoring services.
CitizenHawk – CitizenHawk is a provider of online reputation and brand protection services.
Identify – Identify provides brand protection to help businesses with online trademark infringements.
Microtrace – Microtrace offers security solutions for brand protection, anti-counterfeiting, and product authorization.
NetNames – NetNames provides domain registration, brand management, name alerts, and consulting services.
OpSec Security – OpSec Security supports anti-counterfeiting, brand protection, supply chain security, and Internet monitoring.
Original1 – Original 1 offers its customers a Security-as-a-Service solution for brand protection.

Sproxil – Sproxil provides a consumer SMS and app product verification service to reduce counterfeit risk.
Stealthmark – Recently acquired by Wellness Center, Stealthmark offers product authorization solutions.
YellowBP – YellowBP provides a range of brand protection and anti-counterfeiting solutions.

27. Bug Bounty Support

- ⇒ *Research Disclosure* – For many years, researchers used ad hoc means to report identified vulnerabilities in products and services.
- ⇒ *Responsible Reimbursement* – Bug bounty programs offer a fair means for reimbursing researchers for responsible disclosure.
- ⇒ *Bug Bounty Services* – The provision of bug bounty support services expands the ability of more companies to participate in this activity.

For many years, when researchers and hackers would find vulnerabilities in vendor products and services, the process for responsible reporting was unclear. Some would post the finding on the Internet; others would send the finding to a conference for publication; even others would send email to the CEO or other ad hoc point-of-contact at the affected company. Obviously, this process – which still exists across many aspects of global business and government – leads to mutual distrust between researchers and purveyors of products and services.

In response to this issue, several companies, including Google, Microsoft, AT&T, and others (including recently Apple), began providing a more specific point of contact for researchers to submit their findings, along with a process for offering some sort of negotiation and interaction with the reporting entity. Larger companies certainly have the ability to assign staff to this sort of pursuit, but middle and smaller-sized companies obviously do not have this financial or staff flexibility. Regardless of company size, however, the benefits of trying to work more closely with researchers and hackers are obvious.

In particular, the purpose of *bug bounty support* from security vendors is to offer the ability for more companies to get involved in the fair reimbursement of security researchers. Specifically, bug bounty support involves the provision of fair financial payment, under controlled circumstances, to security researchers who responsibly find and privately report vulnerabilities in externally visible systems. This can be done directly through internally staffed enterprise programs or through partnership with third-party service intermediaries.

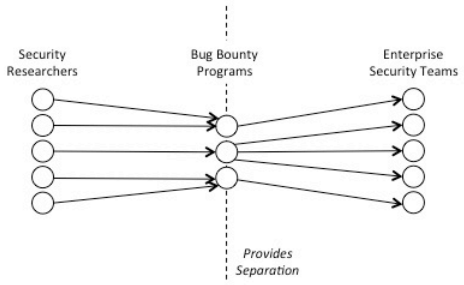

Figure 27-1. High-Level View of Typical Bug Bounty Setup

Bug bounties generally offer a range of monetary incentives for security researchers to report their findings directly and privately to the affected organization, rather than to the general public through industry reporters, bloggers, or pundits. Such reporting has the significant advantage of offering the security researcher monetary compensation. In some countries, the value of a bug bounty payment, which can range from gift cards to tens of thousands of dollars, can become a substantial means for full-time sustenance.

Bug bounties also have the advantage of giving the affected organization time to fix any discovered problems in advance of more widespread knowledge of the vulnerabilities. It goes without saying that bug bounty programs also help companies avoid the usual public relations embarrassment and awkward discussions with customers that come with any externally reported and as yet unfixed security weaknesses.

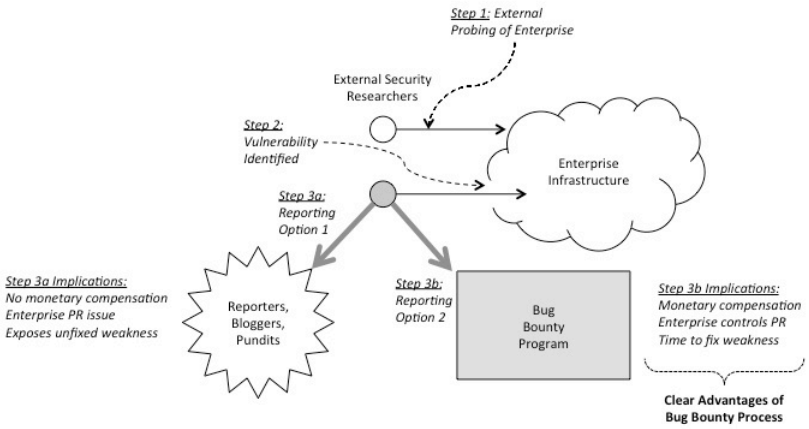

Figure 27-2. Bug Bounty Incentives and Rewards

In spite of the clear advantages of bug bounty reporting for both the security researcher and the enterprise target, the one advantage that comes with reporting vulnerabilities directly to reporters, bloggers, or pundits – and this includes giving presentations at hacker conferences – is the *notoriety* that comes with such

reporting. Many so-called black hats have created strong reputations in the hacking core and driven up their associated consulting fees by following this less controlled reporting path.

The bottom line is that by reporting shocking vulnerabilities that have not been fixed or previously known, researchers create the potential for sensational headlines, but at the expense of exposing problems with serious consequences. This is an unfortunate situation, especially when it involves targets that are part of critical infrastructure such as airplanes, power plants, and automobiles. No responsible researcher wants to expose a vulnerability that could cause serious risk to human lives.

Sadly, two well-known researchers famously staged a cyber attack on a live automobile on a public highway in 2015. They took advantage of the poor communications separation (or lack thereof) that existed on the vehicle between the safety and entertainment systems. While the driver, a writer for Wired Magazine, was fully engaged as part of the demonstration, the potential certainly existed that something might have gone wrong during the test and other real cars with real passengers might have been affected, thus resulting in people being hurt or even killed.

Companies can reduce their external vulnerability risk, improve their public relations posture, and reduce the risk of irresponsible reporting by following these three steps:

1. *Bug Bounty Programs* – By operating an effective bug bounty program either internally or through a third-party intermediary, companies make their policy clear regarding reported weaknesses. They also provide a fair means for researchers to be compensated for their efforts.
2. *Rapid Vulnerability Fixes* – By quickly responding to and fixing reported vulnerabilities, companies remove any frustration amongst researchers that their work is not being taken seriously. Many researchers have claimed to report publicly primarily due to a lack of confidence that the target company will bother to fix their weakness.
3. *Discretion in Hiring Consultants* – By explicitly avoiding ever hiring any security researchers who ignore bug bounty programs and choose to follow more irresponsible reporting processes, companies go a long way toward incenting reasonable behavior across the offensive security community.

Third-party bug bounty services offer companies a safe interface between security researchers and CISO team staff. There are excellent reasons to maintain separation between these groups, including the practical issue of ensuring discretion in any vulnerability discussions. Furthermore, the business economics of negotiating fair and reasonable pricing for vulnerability reporting are currently more art than science. Bug bounty service providers offer a means for creating and managing a good compensation ecosystem, some offering subscription services to companies in order to help make payouts more predictable on an annual basis.

Challenges that emerge with bug bounty programs – many of which are addressed by using a third-party service – include the following:

- *Value of Reported Vulnerability* – The monetary value of a report will be determined based on subjective considerations. For example, a report that identifies a vulnerability that has already been found and is being fixed might have less value than a problem with lesser intensity, but that was not previously know. Third-party providers can arbitrate or adjudicate such issues in a manner that is likely to be trusted by most security researchers.
- *Terms and Conditions of Reporting* – The payment process, including required personal or tax information about the reporter, will vary from one company to the next. This is a good reason to utilize third-party services, which can smoothen the payment process. Some hackers, for example, are not comfortable providing their US social security number for payment.
- *Rules of Engagement for Testing* – If bug bounty programs limit payments to reporting in a certain area, or preclude payment if tests go beyond some specified limit, then companies will benefit from having third-party companies assist in this communication. Bug bounty programs do not provide license for hackers to do anything they desire.

Bug bounty services will grow substantially, as more companies – including small ones – agree to pay for reported weaknesses. One might expect that Bitcoin will become the anonymous currency of choice, which bodes well for anyone willing to be flexible in this regard. Furthermore, block chain-based solutions can help arbitrate the time-value of vulnerabilities by proving who identified an issue first.

The bottom line with bug bounties is that the downside for companies is too great, and the upside too high, for this area of cyber security services not to flourish significantly. The best bug bounty providers will be the ones who focus on maximizing the public relations and early fix potential for companies, while also ensuring that security researchers are paid fairly for their work. They will create a comfortable and trusted ecosystem within which external testers can focus their efforts and receive good compensation.

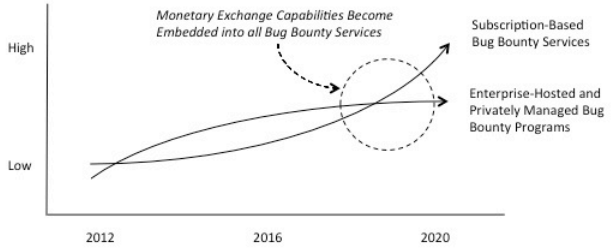

Figure 27-3. Bug Bounty Service Marketplace Trends

A future direction for bug bounties involves monetization of the *intrinsic value* or reported vulnerabilities. By combining anonymous sharing, bug bounties, and monetization using Bitcoin, a *vulnerability exchange* might emerge. Since the value of reported vulnerabilities can range from negligible to high, active trading might emerge as a means for connecting sellers and buyers in the most efficient manner.

One additional interesting development involves offering *premium rewards* for high consequence vulnerabilities. Not all companies think this is a reasonable approach, because it creates an uncomfortable market for vulnerabilities that can have unacceptable consequences for safety, critical infrastructure, and even human life. As an example, penetration testing firm Netragard terminated their program in 2015.

Regardless of the ethical considerations, this more controversial activity, which is likely to increase in prominence, should help prompt companies to work more diligently to *avoid* vulnerabilities either through improved security or through bug bounty programs. The alternative situation – as evidenced with premium rewards programs – is that less secure companies will pay more dearly after problems are found and are being openly marketed.

Bug Bounty Support Providers

My first exposure to Bug Bounties of any sort came several years ago during a discussion with my friend Eric Grosse, then CISO at Google, and previously of AT&T Bell Labs. I'm not sure if Google had the first such program, but it was the first time I'd ever heard of such a thing – and I became a believer quickly. All Bug Bounty vendors are relatively new, so the likelihood that this type of service will evolve is high. The vendors listed below all have excellent positioning as researchers move more and more toward this type of model for vulnerability disclosure. CISO teams might benefit from also looking at existing bug bounty programs publicly available to researchers from companies around the world today. Several good Websites (e.g., bugsheet.com) can be found that catalog these sites with associated statistics.

2017 TAG Cyber Security Annual
Distinguished Bug Bounty Support Providers

Synack – I was recently introduced to the fine team at Synack, and found their approach to be efficient, fair to all involved, and exactly the type of subscription model required to scale this important solution to the masses. I was particularly intrigued at the notion of a vetted, private community of researchers working on behalf of Synack customers. This is a creative approach to vulnerability detection and removal. Thanks to the entire Synack team, especially Aisling MacRunnels, for allowing their enthusiasm for crowd-sourced vulnerability reporting and management programs to hopefully rub off on me – and on the writing in the section.

BugBountyHQ – BugBountyHQ provides a platform and resources in support of Bug Bounty programs.
BugCrowd – BugCrowd offers a crowd-sourced approach. The company was started by its founders in Australia, and has now relocated to San Francisco.
Cobalt – Originally called CrowdCurity, Cobalt involves teams of crowd sourced security researchers.
HackerOne – HackerOne offers a security-as-a-service (Saas) platform for operating a corporate bug bounty program.
Hacking Team – The Italian firm, Hacking Team, (controversially) sells offensive intrusion and surveillance capabilities to governments.
Mitnick Security – The professional services firm operated by Kevin Mitnick includes a zero-day exploit exchange.
Offensive Security – Penetration test training firm Offensive Security operates a bug bounty program.
Synack – Redwood City-based Synack provides an advanced intelligence platform for bug bounty support with actionable intelligence. Synack maintains a red team to support location of exploitable bugs in customer networks.
Zerodium – Zerodium offers an exploit acquisition platform focused on paying rewards for high consequence vulnerabilities.

28. Cyber Insurance

- ⇒ *Insurance Basics* – Cyber insurance is built on the basic insurance industry norms followed by insurers, agents, brokers, and buyers.
- ⇒ *Cyber Risk Transfer* – Cyber insurance involves transferring the risk of a significant cyber breach from the buyer to the insurer.
- ⇒ *Industry Evolution* – Since cyber insurance is so new, the industry is likely to evolve based on early experiences and changing threat patterns.

The only insurance experience most cyber security professionals have involves policies they have purchased for their families. This is not entirely meaningless since ultimately, all forms of insurance provide a means for protecting some entity from financial loss. The industry is based on policyholders choosing to accept small losses in the form of premium payments, in exchange – or as a hedge – against much more significant losses, which would be covered by the insurer. The insurer does the math to make sure the collective premiums exceed the collective payouts. Buying an insurance policy can be viewed as one the purest forms of risk transferal.

In recent years, the decision to transfer cyber security risk to an insurer through a *cyber insurance* policy has become more commonly found, especially in larger organizations. This type of policy is a new entrée to the insurance industry

with still-emerging economics, and CISO teams are advised to learn as much as possible about the pros and cons of cyber insurance – if only because so many board directors and C-suite members have come to view this as an essential component of the information security program.

Listed below are some basics of the insurance industry that might be useful for CISO team members who've been too busy catching hackers, filling out compliance forms, and preventing cyber attacks to have taken the time to learn these simple concepts:

- *Insurance Agents* – Agents represent the interest of insurers by serving as a direct, insurer-paid, distribution channel for the company. Agents sell policies, and it is entirely possible, even likely, that your company will purchase its cyber security policy through an agent. The biggest advantage of working with an agent is the depth of knowledge that individual will bring to you about the specific company and policy options being represented.
- *Insurance Broker* – Brokers represent the client's interest, but also serve as a distribution channel for the insurance company. Brokers are reimbursed through commissions from insurance companies or fees from buyers. The biggest advantage of working with a broker is the range of different insurance company options that will be presented to you.
- *Insurance Company* – The insurer underwrites client risk by providing capital and infrastructure to support the overall insurance business. Insurance companies make money by making sure their underwriting and payout losses are more than offset by premiums and investments.

The way a cyber insurance policy works is easy to describe, but harder to implement. First, your agent or broker will help you select a suitable candidate insurance company and associated cyber insurance policy. The insurance company will then offer generic terms, roughing out how premiums, terms, and payouts might look. This will include details on first-party losses to you, as well as third-party losses to your customers. If you like the initial sketch from the insurer, then a due diligence engagement will ensue to determine the magnitude and type of risks. Obviously, larger companies with more complex needs should expect a longer due diligence process than smaller companies.

During this underwriting process phase, the insurer will want to understand the inner workings of your CISO team, the organizational security posture, and any known vulnerabilities that may exist. CISO teams should naturally be concerned about sharing too much sensitive information with the insurer, who will often put together a team of partner company underwriters to participate in the deal. Once the due diligence has completed, the insurer will then offer a more specific deal, which the legal, business, and CISO teams can review.

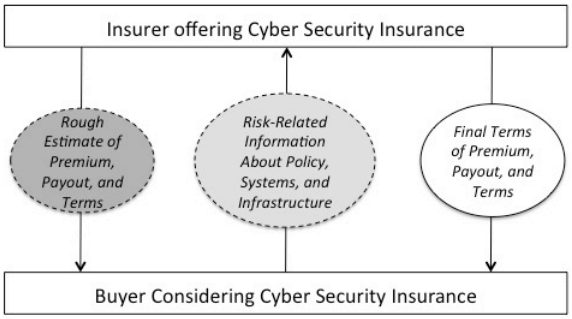

Figure 28-1. Cyber Insurance Process

The challenge in both buying and selling cyber insurance is that – like in a chess game – participants must be careful to make risk moves that will not create a problem later. Since the industry is so new, engagements often create situations that have not arisen before. An example might be an underwriting participant from a country the CISO team is not comfortable sharing information with or an insurance policy with an unclear assumption of what constitutes pre-existing vulnerability conditions.

Typical financial terms for policies are still evolving, but CISO teams should expect three main components to an offer: Annual premium payments, total liability coverage, and provisions on payout in the event of a breach. For larger companies, a typical policy might involve several million dollar annual premiums for roughly a hundred million dollars of coverage, with a thirty million dollar deductible and no payment of government fines for privacy breaches. Smaller companies might just remove a zero from the above example for a less intense policy example. Larger companies might add a zero.

For most firms, the benefits of buying cyber insurance will outweigh the risks, so this is going to be a growing market with enormous impact on how CISO teams operate. CISO teams, in particular, must work to help insurers understand, for example, that levying additional compliance requirements will have little incremental impact on cyber security posture. They must also help insurers understand that virtually every vulnerability found in an organization's infrastructure is pre-existing and that no company on the planet can identify and document all existing problems in their software and systems.

The primary trends in the cyber insurance industry will follow the improved data and experience base collected by the industry. As this base improves, premiums and benefits will also improve, thus increasing the potential size of the market, while also reducing the risk to both buyers and sellers. A caveat is that any major, disruptive global cyber event affecting many companies at the same time, could toss this industry into seriously uncertain territory. In theory, a single worm could wipe out every buyer of cyber security insurance in an instant, so this type of situation would lead to serious debate, negotiation, and swallowed packs of Tums.

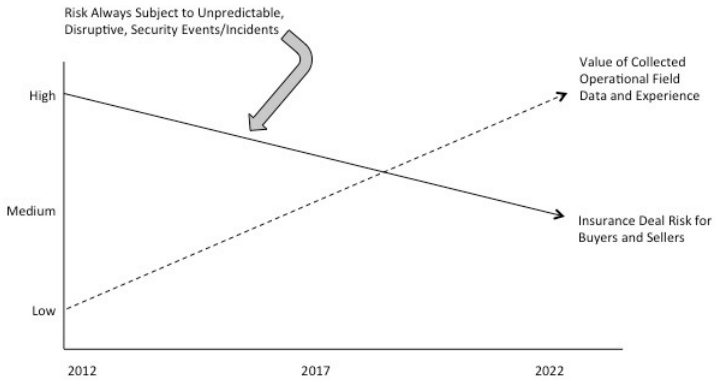

Figure 28-2. Trends in the Cyber Insurance Industry

Some practical tips that potential buyers of cyber insurance might consider are offered below:

- *Insurer* – CISO teams and finance groups should select an insurer that matches their company in terms of size, reach, location, and comfort-level. Large multinational companies will prefer working directly with larger insurers with their teams of legal advisors, procurements specialists, and understanding of scale. Smaller companies, on the other hand, will prefer the intimacy of working with a broker or agent who can tailor several policy options to the unique needs of the buyer.
- *Information Sharing* – CISO teams must be *very careful* about the information being shared during due diligence. Insurance companies often put together teams of smaller participating insurers, and the likelihood that shared files will be misplaced and mishandled is high. CISO teams might consider setting up clean rooms with encrypted storage as a way of sharing information in a more controlled setting – although this will not work when the underwriting participants are small and located around the world.
- *Terms* – The fine print on cyber insurance, like any type of insurance needs to be carefully examined. Payouts of government fines, for instance, could be a sticky point and the specific language on this must be clear in the stated policy. Deductibles can also be a challenge, and CISO teams should make sure that they are reasonable and do not exceed, for example, the maximum financial consequence any member of their sector has ever experienced after a cyber breach.

One caveat on the information shared above is that it is admittedly US-centric. The cyber insurance market, as well as the market and terms of all forms of insurance, will vary globally. CISO teams will need to do the legwork to investigate and learn if they are considering specific policies outside the United States.

Cyber Insurance Providers

The full list of companies providing all forms of business insurance is enormous and completely outside the scope of this report. The vendors listed below represent a small portion of the companies who are aggressively offering cyber insurance. This market will grow significantly and the list of brokers and agents will grow in the coming years as well. CISO teams should use the list below as an early starting point and *small sampling* of companies, brokers, and agents rather than as a definitive guide, because new entrants will be joining the market at an increasing rate.

2017 TAG Cyber Security Annual
Distinguished Cyber Insurance Providers

Aon – Several months ago, I attended a stimulating discussion in Manhattan with the Aon team. During the dinner, I re-connected with my friend Anthony Belfiore, who I'd known while he was with JPMC, and who was now the CISO for Aon. Since then, as I've researched the cyber insurance industry, I've come to recognize the deep expertise at Aon in helping clients understand the risk transferal process, and Anthony has been of great assistance personally, explaining to me in detail how cyber insurance can be a vital, integrated component of a larger cyber security risk reduction approach.

2017 TAG Cyber Security Annual
Cyber Insurance Providers

Aon – Aon is an insurance broker that offers a range of cyber risk insurance policies for business customers. The company has a cyber diagnostic tool on its Website that might be useful for some CISO teams to use in the early conceptualization stages of the insurance process.
CyberRiskPartners – CyberRiskPartners, located in New York, provides a cyber security platform for decision support about risk transfer.
Ridge Global – Founded by former DHS Secretary Tom Ridge, the company provides cyber resiliency assessments and services including insurance protection coverage arranged through Lloyds syndicates.
Marsh and McLennan – Marsh and McLennan claims to be the world's largest insurance brokerage offering a range of cyber insurance policy offerings for companies of different sizes.

Additional Cyber Insurance Providers

AIG – AIG is a large insurance company that is now offering cyber insurance policies to companies. Its policies cover cases of data risk, cyber extortion, and business interruption.

BCS Insurance Company – BCS includes Cyber and Privacy Loss Protection insurance that covers most fines and includes coverage up to $30M. The company, like many others, offers an omissions option to cover the client in case an agent makes some mistake in writing the policy.
Chubb – Chubb is a large insurance company, recently acquired by the ACE Group, that offers a range of cyber insurance policy offerings. Its policies claim to focus on direct loss, legal liability, and consequential loss. Companies buying existing business insurance from a large provider such as Chubb will benefit from the integration of their cyber insurance policy with existing policies.
CoverWallet – CoverWallet is a so-called insurance manager, with an on-line platform that provides broker services to smaller companies who need commercial insurance. The start-up company recently emerged from stealth mode and includes cyber risk options for buyers.
ECBM – Located in Pennsylvania, ECBM is an insurance broker that provides general cyber insurance consulting and brokerage services for every industry. The company's Website has a useful Q&A that helps explain various aspects of cyber risk insurance including the differences between first and third party risk.
IDT911 – Located in Arizona, IDT911 is a broker that provides range of cyber insurance products and concierge professional services through partnership with most of the leading insurance companies fro the US and Canada.
Insureon – Insureon is a broker that will connect small businesses with an appropriate agent for commercial insurance. The company has excellent resources on its Website explaining how cyber liability insurance can be a stand-alone policy or an add-on to an existing policy.
Integrated Coverage Group – Integrated Coverage Group is an example of an independent insurance agent, which essentially provides a brokerage function that helps businesses find the best cyber insurance plan for their needs.
Locke Lord – Locke Lord is a large legal firm with considerable expertise and experience in the insurance industry. As the cyber risk insurance grows, law firms will expand their expertise to deal with the inevitable conflicts that will arise.
Lockton – Headquartered in New York, Lockton is a privately owned insurance brokerage that writes policies for cyber risk management to augment data backup.
Philadelphia Insurance Company – Philadelphia Insurance Company markets a Cyber Security Liability program for first and third party coverage.
John Reed Stark Consulting – John Reed Stark Consulting provides independent consulting services that help businesses understand and purchase cyber insurance.
TechInsurance – TechInsurance is a broker that offers business customer support for buying insurance including cyber through leading insurance companies.
Travelers – Travelers offers a large range of cyber insurance policies for public entities, technology companies, and small businesses.
XL Catlin Group – XL Catlin Group offers policies that cover reasonable customized costs after a breach.
Zurich – Zurich offers data breach insurance protection and data management solutions.

29. Governance, Risk, and Compliance

⇒ *Compliance* – GRC processes and tools in the context of cyber security tend to focus on reducing risk through compliance with security frameworks.
⇒ *Automation* – Embedding automated GRC tools into business processes is an excellent way to ensure optimal compliance and risk management.
⇒ *Cloud Hosted eGRC* – Virtualized eGRC platform in the cloud will extend this capability to a larger marketplace including smaller organizations.

Few topics generate as much debate in the cyber security community as *compliance*. While it stands to reason that sloppy administration of the basics such as inventory and patch management will lead to security issues, few experts contend that strict adherence to compliance frameworks has had much impact on stopping cyber attacks. Some might even argue that the formality and rigid nature of compliance processes could cause an organization to be less flexible, and hence less capable of adjusting in real time to a dynamic, well-orchestrated attack.

Nevertheless, the general consensus among all security professionals is that a well-managed, underlying compliance base is advised for any cyber security program. Furthermore, it is generally agreed that this compliance base must be focused on reducing cyber security risks through disciplined attendance to governance processes that make reasonable sense. This determination can only be achieved through competent management and oversight.

The purpose of *governance, risk, and compliance (GRC)* is the provision of external direction, process management, and fulfillment of demonstrable proof that an organization is operating securely and with high integrity, according to a select compliance framework. This *external direction* can reside within the same company or government agency – as one would find with an internal audit function, for example – but should be sufficiently independent to allow for dispassionate, unbiased assessment of security risk.

Figure 29-1. Assuring Business Process Integrity through GRC

While the control objectives of GRC extend beyond cyber security to issues such as business process assurance, revenue assurance, and regulatory compliance, the discussion here focuses on reducing the risk of malicious actors causing damage, exposure, or harm to an organization. Enterprise security risk management and

security compliance programs are thus viewed here as synonymous with GRC for cyber security. In both cases, risk controls are most effective if they are embedded into business processes, rather than treated as separate frameworks.

Virtually all organizations use some form of governance to manage security compliance goals. Large companies, for example, set aside budgets and employ formal governance teams with full-time experts to address the security frameworks relevant to their business. Smaller companies, on the other hand, will do everything possible to minimize costs by embedding any required compliance into a related activity, perhaps within information technology (IT) or financial support teams.

Not all companies use automation to support GRC initiatives, although newer cloud-hosted eGRC services will increase market usage to a larger number of medium and even small companies. Wherever platform automation is properly introduced, the accuracy, completeness, and efficiency of GRC activities increase dramatically. This includes documenting, directing, controlling, managing, viewing, and measuring the following aspects of cyber security controls:

- *Security Policy Management* – Involves support for documenting and managing organizational security policy requirements.
- *Regulatory Security Management* – Allows analysis of whether organizational security policy requirements satisfy applicable regulations.
- *Security Compliance Management* – Supports analysis of whether organization security policy requirements satisfy applicable external frameworks.
- *Security Risk Analysis* – Provides a means for creating reports that highlight specific risks to the business.
- *Security Process Workflow* – Integrates with and supports business process workflow requirements.

Since the number of available GRC product platforms has grown so quickly, the differentiators associated with the various offerings have become daunting. CISO teams must examine workflow support, access controls, project creation tools, graphical user interfaces (GUIs), deficiency reporting systems, IT integration connectors, and on and on. Offerings will range from simpler, domain-specific GRC tools to integrated GRC platforms with slick screens.

The essence of GRC platforms and services is data management; hence, the CISO should be particularly attentive to the features and capabilities offered in this area. Data import wizards, tools for data reporting and sharing, and support for applicable metrics are example features that are important in the majority of enterprise environments. The CISO team should not have to change their normal security data management and metrics reporting approaches to accommodate the GRC solution.

Another important GRC function for cyber security involves managing, mapping, interpreting, and resolving the respective requirements in all applicable stored policies, frameworks, and regulatory controls. Thus, when an organization

realizes that it must meet some new compliance framework, the GRC tool should assist with making assessments of compliance satisfaction, as well as any requirements gaps that emerge. This automated process should include the cascading of updates to the compliance mappings.

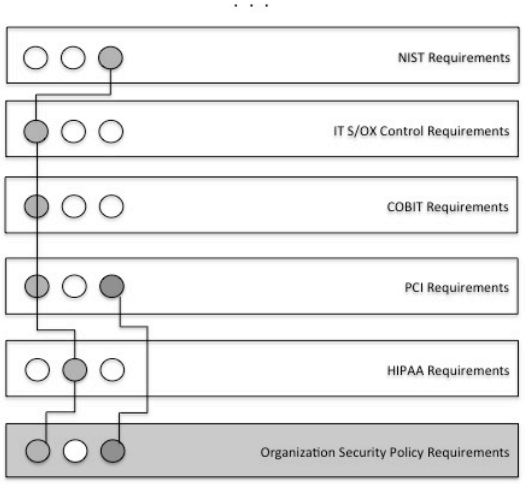

Figure 29-2. Automated GRC Platform Compliance Mapping

Depending on their specific industry, the specific compliance frameworks relevant to the modern CISO team might include (in no particular order) ISO 27001, NERC CIP Cyber Security Standards, NIST Framework, Common Criteria, ISA/IEC 62443, PCI DSS, FCC CSRIC, SANS 20, Sarbanes-Oxley, ISO 17799, (SAS/70) SSAE 16, GBA, HIPAA, FISMA, CSA Open Certification Framework, UL 2825, ISSA GAISP, SSE CMM (ISO 21827), Information Security Forum (ISF), and COBIT. As suggested earlier, teams utilizing GRC platforms should have the ability to generate requirements gap analysis or compliance justifications for all applicable frameworks.

One challenge, however, is that vendor marketing materials, and even the purportedly unbiased analysis reports that come out (e.g., quadrants, waves) will tend to shift their better rankings of GRC vendors based on how broad their support might be for the largest number of compliance frameworks. This makes reasonable sense if the analysts are giving an award for achievement, but the resulting reports could lead buyers to select products that are more feature-rich, and hence more expensive, than they really need. CISO teams are thus advised to be extremely careful in placing too much stock in quadrants and waves.

Modern GRC platforms often include cloud and SaaS-based options. Even for enterprise teams currently focused on perimeter-protected installations, future cloud migration is to be expected as IT and network teams move in this virtual direction. A basic tenet of proper governance, risk, and compliance work is that the associated processes be *embedded* into the target business environment. For example, virtualized infrastructure requires virtualized GRC automation. To this end, on-premise GRC platform vendors should provide a clear migration path to

virtual support, including both architectural changes and evolved data management support.

If a GRC consultant is hired to provide professional services and advice on GRC platform selection, operation, and use, the selected consultant should demonstrate or obtain a working understanding of the business processes of the enterprise. While generic GRC knowledge and expertise is valuable, the nature of compliance work is that domain-specific knowledge of the business is key to successful outcomes. GRC consultants should also possess a working knowledge of enterprise architectures and the shift toward increased mobile, cloud, and virtualization adoption.

If organizational groups beyond the CISO team, perhaps within finance, business continuity, IT, or human resources have a clear need to support governance, risk, and compliance for non-security-related purposes, then selection of the best GRC tool should take the broadest set of requirements into account. Furthermore, CISO budgets are often limited, and to the degree that GRC platform support can be shared expense with other departments, this option should be considered. Holistic support in a GRC platform for various parts of a business will result in better reports and more comprehensive coverage.

If your corporate external auditor agrees to consult with your security team as part of their planning cycle, then a detailed discussion of GRC requirements in the context of audit is advised. Some larger companies guard the external audit relationship closely and keep cyber security staff at arms length from external auditors (except when absolutely necessary), so this might not be feasible in all environments. But if the CISO team can work together with the audit team in the selection and use of a GRC tool and associated process, then this is generally a good idea.

All present indicators suggest that GRC is likely to sustain its role as an important contributor to cyber security programs over the next few years. As such, investments in GRC products and services will likely include multi-year payback, which helps justify near-term expenditure. In fact, CISOs in moderate to large size organizations should view GRC as an essential compliance tool. Security staff in smaller organizations should also consider GRC services in the cloud that require no capital investment.

In spite of this clearly positive outlook for GRC, recent experience does suggest that policy governance, risk management, and compliance are ineffective as a sole or even primary means for preventing attacks. This may seem obvious, but industry emphasis on compliance frameworks such as PCI DSS and the NIST framework has inflated the importance of GRC in tactical security protection. Furthermore, as the enterprise architecture shifts from a perimeter-protected local area network to something more virtual, cloud-based, and mobility connected, the use of all on-premise tools will shift virtual.

As such, the outlook for the overall GRC marketplace, in the context of cyber security, is as follows:

- *GRC Security* – The market should see sustainment of GRC as a component in the cyber security protections of an enterprise. Increased support for management of third-party supplier, partner, and vendor risk will be essential. Smaller companies will begin to use cloud-based GRC services to reduce risk.
- *On-Premise GRC* – The market should experience a gradual slow-down in the current use of on-premise hosted enterprise GRC platforms. Perimeter networks are clearly on the wane, and as such, GRC will be less focused on a well-defined physically bounded enterprise.
- *Cloud-Based GRC* – The market should see a gradual rise in the light deployment of virtual, cloud-based GRC platforms and services. This will include IT services in hybrid and public clouds, as well as telecommunications services in software defined network (SDN) clouds.

These three business market trends in the GRC platform and service marketplace are depicted below.

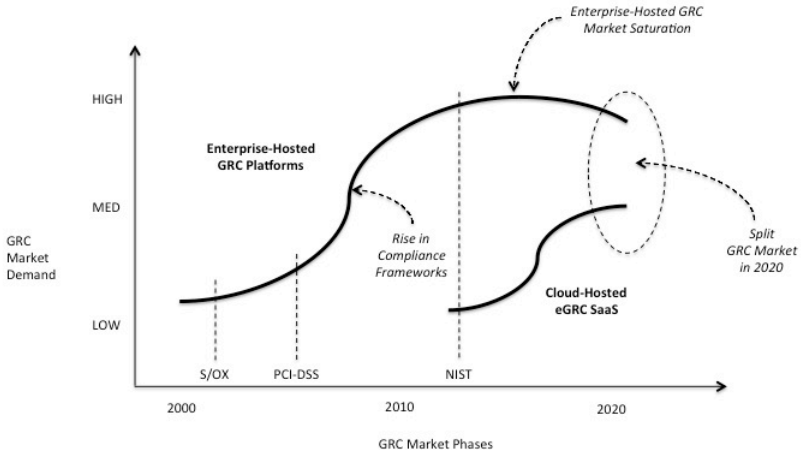

Figure 29-3. Vision for GRC Marketplace

CISO teams will remember a period of *relatively* low GRC intensity for cyber security prior to the inception of Sarbanes-Oxley in the United States in 2002. Since then, the emphasis on security compliance frameworks and the associated impact on the GRC marketplace have grown substantially. While most GRC implementations have been created as enterprise-hosted platforms, there has been modest, early adoption of full cloud-base SaaS eGRC. As confidence in SaaS solutions inevitably increases in the enterprise, significant increases will be seen in cloud-based eGRC.

The likely result is a split marketplace in 2020 with enterprise-hosted GRC and cloud-based eGRC each comprising large portions of the cyber security market. Hosted solutions will continue to be the most common, however, since the cost to

transition hosted GRC content to cloud might outweigh the relative benefits for many groups, especially larger organizations.

It is worth noting that non-security workflow and financial applications for GRC are considered outside the scope of our predictions. These areas should be expected to grow in the coming year as well. The only cyber security implication is that companies are likely to negotiate broader contracts for GRC automated platforms, which could have a positive impact on security budget needs.

Governance, Risk, and Compliance Providers

The vendor community supporting governance, risk, and compliance does include companies that focus specifically on cyber security, in addition to the traditional compliance vendors with more general business focus. Some vendors provide tools that support enterprise risk management, and these were included below if the focus included cyber security. Consultants and analysts providing GRC support were also included in the list.

2017 TAG Cyber Security Annual
Governance, Risk, and Compliance Providers

ACL – Vancouver firm ACL offers products and services focused on governance, risk, and compliance.
Active Risk – Active Risk, previously Strategic Thought Group, provides an advanced platform solution called Active Risk Manager for enterprise risk management.
Agiliance (RiskVision) – Sunnyvale firm RiskVision (formerly Agiliance) offers an integrated governance, risk, and compliance solution for the enterprise.
Alert Enterprise – Located in Fremont, Alert Enterprise, provides a next-generation governance, risk, and compliance solution for enterprise.
Allgress – Allgress provides a governance, risk, and compliance solution with emphasis on business risk intelligence.
ARAMA TECH – Located in Denmark, ARAMA TECH offers a governance, risk, and compliance solution for enterprise.
Aruvio – Aruvio provides a suite of continuous governance, risk, and compliance solutions.
Audit Square – Headquartered in the Czech Republic, Audit Square provides audit and configuration assessment tools for Windows.
AvePoint – Jersey City firm AvePoint offers governance, risk, and compliance solutions.
Bitcrack – South African consulting firm Bitcrack offers services related to governance, risk, and compliance.
Blue Lance – Houston-based Blue Lance provides enterprise solutions for governance, risk, and compliance.
Brinqa – Austin firm Brinqa offers an integrated GRC platform for analysis of business risk.

BWise – NASDAQ firm BWise provides an advanced governance, risk, and compliance solution for enterprise.
Cisco – Cisco offers a governance, risk, and compliance security assessment service for its enterprise customers.
CMT – CMT provides a portfolio of security, compliance, and related solutions for business.
Coalfire – Coalfire provides advisory services on governance, risk, and compliance issues.
CompliancePoint – CompliancePoint performs governance, risk, and compliance assessments and audits with emphasis on call and contact centers.
ControlPanelGRC – ControlPanelGRC offers an advanced governance, risk, and compliance solution for SAP.
Convercent – Convercent provides an ethics and compliance software solution for enterprise.
CriticalWatch (AlertLogic) – Critical Watch provides security risk, vulnerability, and compliance platforms.
Cura Software – Singapore firm Cura Software offers global customers an advanced governance, risk, and compliance solution for enterprise.
Deloitte – Deloitte provides professional services related to governance, risk, and compliance issues.
Delta Risk – San Antonio-based Delta Risk provides strategic advice and consulting in GRC.
Elemental – Las Vegas-based Elemental provides GRC management solutions for enterprise.
EMC/RSA – RSA offers the industry-leading Archer platform, which includes all baseline and advanced GRC functions. Many CISO teams have been introduced to GRC processes, platform support, and methodology through use of the popular Archer platform.
EY – Global consulting firm EY acquired Integrc and offers governance, risk, and compliance services for SAP users.
Fastpath – GRC Studio from Fastpath is an integrated governance, risk, and compliance tool for enterprise.
The GRC Group – The GRC Group is a member organization with resources supporting governance, risk, and compliance programs.
GRC 20/20 Research – GRC 20/20 Research offers governance, risk, and compliance advisory services with advice for buyers. Groups such as GRC 20/20 are particularly helpful since the principal is an industry expert.
High Water Advisors – Consulting firm High Water Advisors offers governance, risk, and compliance advisory services.
Hitec Labs – UK firm Hitec Labs provides governance, risk, and compliance services for customers around the world.
IBM – IBM's OpenPages offers an advanced governance, risk, and compliance solution for its customers.

InfoDefense – The InfoDefense platform includes support for governance, risk, and compliance, as well as IAM and DLP.
IntelleSecure – IntelleSecure is an Indian firm that provides governance, risk, and compliance training.
KPMG – KPMG provides professional services supporting governance, risk, and compliance issues.
Leviathan Security Group – Seattle-based Leviathan offers information security and GRC consulting.
LockPath – The Keylight platform from LockPath is an advanced governance, risk, and compliance solution for enterprise.
Mega – Mega develops tools to support governance, risk, and compliance solution for enterprise.
Metacompliance – Metacompliance provides a range of products and services supporting governance, risk, and compliance.
MetricStream – MetricStream provides an advanced governance, risk, and compliance solution for enterprise. The MetricStream GRC Summit each year is an excellent forum for learning about the industry and its participants.
Modulo – Modulo is a New Jersey firm that provides governance, risk, and compliance services.
Mycroft – Now part of EY, Mycroft includes governance, risk, and compliance consulting services in its IAM suite.
NAVEX Global –Via acquisition of The Network Inc, the company provides an integrated GRC platform.
Nettitude – Nettitude includes consulting services for governance, risk, and compliance solutions in the enterprise.
NextLabs – NextLabs data protection and IAM platforms support governance, risk, and compliance.
Oracle – Oracle provides the Fusion governance, risk, and compliance solution for enterprise.
Paladion – The Risq Vu platform from Paladion is an advanced governance, risk, and compliance tool supporting workflow and audit management.
Pentura – Pentura provides a range of holistic governance, risk, and compliance consulting services.
Pervade Software – Pervade Software, headquartered in the UK, offers security compliance monitoring solutions.
Picus Security – Located in Turkey, Picus Security provides solutions for compliance monitoring and assessment.
Prevalent – The New Jersey-based firm offers a rage of security and compliance consulting services.
Protiviti – Protiviti offers its Governance Portal to support governance, risk, and compliance.
PwC – PwC provides consulting services in support of advanced governance, risk, and compliance.

RiskLens – RiskLens offers a platform and methodology for estimated enterprise security risk.
Rofori – Manassas-based Rofori offers a capability for managing cyber risks consistent with the NIST Framework.
Rsam – Rsam provides an integrated governance, risk, and compliance platform with vendor risk management and capability to build custom apps.
RSM – Former McGladrey firm RSM offers advanced governance, risk, and compliance services.
Quad Metrics – Ann Arbor-based Quad Metrics offers tools for estimating enterprise risk.
SaaSAssurance – Irish firm SaaSAssurance offers a compliance platform for managing GRC.
SAI Global – SAI Global provides SaaS-based, advanced governance, risk, and compliance solution for enterprise.
SAP – SAP provides an integrated set of governance, risk, and compliance features for SAP users.
SAS – The SAS Enterprise platform automates governance, risk, and compliance functions.
Saviynt – Los Angeles-based Saviynt provides a cloud access governance solution for enterprise.
SDG – TruOps is an advanced governance, risk, and compliance solution for enterprise.
Secure Digital Solutions – The Minnesota-based firm offers a range of GRC consulting services.
Security Weaver – Located in The Netherlands, Security Weaver offers GRC solutions for SAP.
SecZetta – SecZetta provides consulting services supporting governance, risk, and compliance.
SignaCert – SignaCert, located in Texas, offers product solutions for automated continuous compliance monitoring.
Software AG – The ARIS platform from Software AG supports governance, risk, and compliance solutions.
STEALTHbits – The New Jersey-based firm provides a range of data access governance solutions.
Symantec – Symantec offers solutions for continuous monitoring of infrastructure for compliance and audit.
Templar Shield – Templar Shield provides a range of security consulting, managed security, and recruiting services including a GRC practice.
Tevora – Tevora supports enterprise risk management solutions using its HydraRisk Model.
Titania – UK-based Titania provides audit compliance tools for enterprise devices, servers, and workstations.
Trace Security – Louisiana-based Trace Security offers IT GRC solutions for the enterprise.

TrustWave – TrustWave GRC is an advanced governance, risk, and compliance solution for enterprise. TrustWave's extensive PCI DSS solutions are directly related to most GRC programs.
Veris Group – Information assurance provider Veris Group includes governance, risk, and compliance-related support for government customers.
VivoSecurity – VivoSecurity, located in Los Altos, provides automated risk calculations.
Winterhawk Consulting – Winterhawk Consulting offers range of governance, risk, and compliance services for enterprise.

Additional Governance, Risk, and Compliance Providers

Compliance 360 – Alpharetta firm Compliance 360 provides an advanced governance, risk, and compliance solution for enterprise.
Enablon – Enablon includes an advanced governance, risk, and compliance solution for enterprise.
FairWarning – FairWarning provides enterprise security and compliance integration across the enterprise.
LogicManager – Boston-based firm LogicManager provides an advanced enterprise risk management solution.
Namtek – Bedford-based Namtek offers a governance, risk, and compliance professional services practice.
Navex Global – Navex Global provides software, content, and services to support governance, risk, and compliance.
OCEG – OCEG is a non-profit group supporting governance, risk, and compliance best practices and solutions.
Resolver – Canadian firm Resolver offers customized governance, risk, and compliance solutions in the cloud.
RSD – RSD offers range of information governance services in support of governance, risk, and compliance.
ThomsonReuters – The Enterprise Risk Manager from Thomson Reuters is an advanced governance, risk, and compliance platform.
TraceSecurity – TraceSecurity offers the Trace CSO governance, risk, and compliance solution for enterprise.
Turnkey Consulting – Turnkey Consulting offers SAP GRC Consulting services for enterprise customers.

30. Incident Response

⇒ *Responsive Security* – Since enterprise cyber attacks have become so inevitable, CISO teams have come to focus resources on reactive response.
⇒ *Process Workflow* – The best incident response tools combine support for hunting by security analysts using enterprise workflow response tools.

⇒ *Response Maturity* – Organizations are evolving in their maturity from manual incident response to automated, tool-supported hunting.

Cyber security professionals understand that cyber attacks are best prevented in the early stages of the threat lifecycle. Such proactive security depends on the ability to detect early warning and indicators in the on-going barrage of information that is presented to a cyber security team – and this must be done before an attack has produced real consequences. The most proactive detection also requires an unusual tolerance on the part of the defense team to accept false positive alerts, since the earlier an organization responds to indicators, the more likely the possibility exists that that indicator is nothing to worry about.

As a result of these challenges in dealing with proactive prevention, the cyber security community has come to accept break-ins as virtually *inevitable*. While this sad conclusion is certainly justified, CISO teams are urged to continue their vigilance in trying to be proactive. It should never be considered acceptable for any organization to be breached – even if the actor is a capable nation state. That said, it is fair to say that a large portion of cyber security attention in the enterprise community has now shifted toward reactive processes initiated after something bad has occurred.

The purpose of *incident response* is to manage required activities after a breach has occurred in order to limit damage, reduce time to recover, and improve the ability of an organization to prevent the next attack. CISO teams drive incident response processes by orchestrating remediation and fostering cooperative interactions between business units, suppliers, partners, vendors, and customers. Since incident response is such a broad activity, virtually *every* cyber security tool, system, and product can be viewed as contributing to the overall response process.

The cyber security industry has thus seen a new category of products and services emerge that focus *specifically* on assisting with the incident response task. Features in such incident response products and services include support for the following four steps:

- *Data Collection* – Involves proactive or after-the-fact collection of data required for response teams to understand the vulnerabilities, timeline, and other attributes of an incident. Clearly, if this data collection process reveals indicators of a newly forming incident, then the lines between reactive incident response and proactive security analysis begin to blur somewhat.
- *Digital Forensics* – Involves the tools, systems, and processes required for expert responders to perform the required forensic analysis on hacked systems to determine root cause and assess damage. This support has evolved from a haphazard collection of available tools from disparate sources to more coherently integrated platforms to support forensic response, now often referred to as *hunting*.
- *Damage Control* – Once a breach has been confirmed, restoration and remediation of any damage to assets are required. These control steps are

considered an essential step in incident response, and they can include many different groups in an organization ranging from the cyber security team to the public relations staff.

- *Root Cause Analysis* – In order to properly learn and benefit from a breach, organizations must perform extensive root cause analysis with the goal of improving security posture. The best management teams will obsess on this important step with the goal of continual process advancement.

The typical sorts of data flows and interaction that occur in an enterprise during these familiar incident response steps can be sketched as emanating from a common incident response core.

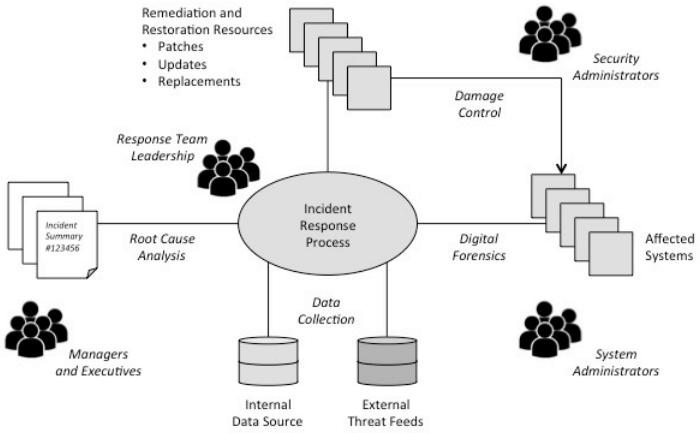

Figure 30-1. Incident Response Data Flows and Interactions

The types of functions supported by incident response product and service vendors are still evolving, with many incident response vendors providing straightforward security consulting and staff augmentation. That said, an industry is beginning to emerge with a standard set of platform support for enterprise incident response. Currently available platforms tend to include the following capabilities:

- *Data Collection* – Many current incident response platforms provide means for assisting in the proper data collection, organization, and interpretation after a breach has occurred. Experienced incident response managers will often claim that data collection is the most important step in the process. Collecting the wrong data in the wrong format with the wrong context is a recipe for wasted time, energy, and money.
- *Workflow Management* – Current incident response platforms typically provide support for process workflow, including automated task coordination, report generation, and management approvals. Such workflow management is essential in larger, more complex organizations where breach investigation could require a high degree of coordination between different

groups in the company or agency. CISO teams should recognize that advanced workflow management of response activities is the primary differentiator between incident response tools and more traditional security analytic tools.

- *Process Automation* – Automation of incident response processes is an important new area for CISO teams. Any task that can be automated, such as periodic report generation, reduces the burden on the response team, which then reduces time to recover. The art of incident response design requires making the correct decisions about which tasks to automate and which to maintain in the hands of the human responder. Automation of human instinct, for example, is unlikely – and any responder will explain that such intangible capability is always essential in a complex investigation.
- *Remote Monitoring* – Many incident response platforms include the deployment of hardware, software, or virtual devices that provide remote monitoring for the purposes of helping to diagnose incident characteristics and detect the remaining presence of advanced threats. Vendors enjoy this capability, because it provides a more sticky relationship with their clients, not to mention offering annuity revenue long after an incident has come and gone.

In addition to automated platform support, many vendors provide response training, tool support, and other professional services in support of incident handling. Such consulting services can include remediation planning and management assistance during investigative phases. They can also include expert recommendations on new countermeasures that might reduce the risk of future events.

The trend for incident response support products and services is significantly positive. This is based on the observation that virtually every organization on the planet has finally come to the realization that they have either already been penetrated or will be soon. This idea that it is not "whether" you will be attacked, but rather "when" you will be attacked, will drive the incident response industry toward dramatic growth. Few companies today have the types of mature processes that are necessary to perform response properly – especially in small and medium sized businesses – and this contributes further toward expected growth in this area.

A crude maturity model can be created for organizations in the area of incident response. By 2010, most organizations had achieved some level of manual incident response process, even if such processes are inadequate. By 2018, one can expect most organizations to reach the next level, which include automated support for incident response. The near-term target in the ensuing years will involve more comprehensive support for integrated, proactive hunting of vulnerabilities, incidents, and indicators.

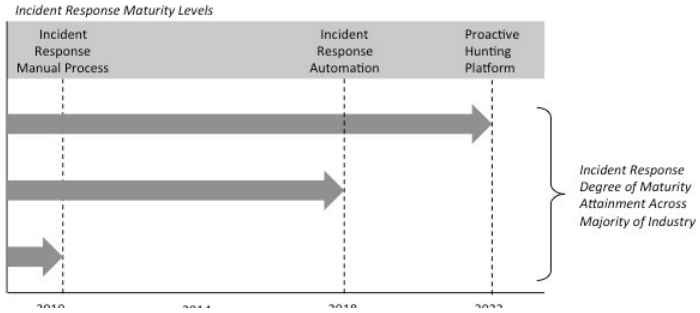

Figure 30-2. Trends in Incident Response Maturity

The trend toward more integrated proactive and reactive support for cyber security in the enterprise is healthy. Incident response providers and security analytics vendors are advised to recognize the obvious synergy between their respective capabilities. Mergers, acquisitions, and joint ventures are thus expected between these participants in the industry.

Incident Response Providers

As mentioned above, all cyber security product and service vendors claim to provide support for incident response – and strictly speaking, this is true. The vendors listed below were chosen because they specifically focus their offerings on improving, automating, and supporting enterprise incident response processes. A very small sampling of consulting firms that support incident response is included below. CISO teams should understand that virtually every security consulting and digital forensics firm in the world would claim to offer support for incident response.

2017 TAG Cyber Security Annual
Incident Response Providers

AccessData – AccessData provides a suite data forensics products and services for cyber security and related purposes including incident response.
Arctic Wolf Networks – Arctic Wolf Networks provides a concierge security-as-a-service (SaaS) cloud-based SIEM with support for incident response.
CounterTack – CounterTack focuses on endpoint security protections for the enterprise with the potential for active retaliation to on-going attacks.
CrowdStrike – CrowdStrike, founded by cyber security expert George Kurtz, offers expert incident responders as a professional service for the enterprise.
CyberSponse – CyberSponse provides a collaboration platform for supporting security incident response.
Cyfir – Cyfir provides an enterprise forensics suite to support computer and network investigations and incident response.
D3 Security – D3 Security provides a platform for incident management and response software.

Emagined Security – Emagined Security provides professional consulting services for information security and compliance.
Enclave Forensics – Enclave Forensics provides incident response and digital forensic services for enterprise customers.
Fast Orientation – Fast Orientation provides software that allows IT organizations to explore IT events in real time as part of a continuous awareness and incident response program.
FireEye – Well-known security firm, FireEye includes the industry-leading Mandiant platform and process for supporting incident response.
4Discovery – 4Discovery provides a range of digital forensics services including mobile forensics, remote forensic collection, computer analysis, and reporting.
Guidance Software – Leading digital forensics firm Guidance Software support incident response activities in the enterprise.
Hexadite – Hexadite provides an automated incident response solution based on intelligent algorithms and tools.
ID Experts – ID Experts provides a SaaS platform for aggregating breach details during response.
Intel – Intel provides security consulting services that include support for incident response.
ISARR – Based in London, ISARR provides a Web-based platform for managing risk, resilience, response, and security intelligence.
Kroll – Kroll offers a range of cyber and physical investigatory services that are useful during incident handling and response.
K2 Intelligence – Founded by Jeremy Kroll, K2 Intelligence support investigations and response before, during, and after a breach.
Larson – Larson Security provides cyber security services including digital forensics and incident response.
LIFARS - LIFARS provides cyber security, digital forensics, and incident response support and services
Maddrix – Maddrix provides incident response professional services including remediation and threat intelligence.
Modulo – Modulo offers a platform that is used frequently to automate workflow management during response.
Palerra – Palerra provides a SaaS platform for threat detection, predictive analytics, incident response, and configuration settings in public cloud offerings.
Praetorian – Praetorian provides professional services in support of enterprise incident response.
Reversing Labs – Reversing Labs provides a platform for advanced threat protection and analytics with support for incident response.
Roka Security – Roka Security provides a range of security consulting services including support for incident response.
RSA – Many enterprise teams use the RSA Archer platform to automate workflow for incident response. This is true increasingly for feature-rich GRC platforms. For this

reason, mergers between GRC firms and incident response providers should be expected in the coming years.
Resilient Systems (IBM) – Resilient, now part of IBM, provides a platform for incident response; company hired Bruce Schneier as their CTO.
SecureState – SecureState is a global management-consulting firm focused on information security with support for incident response.
Security Management Partners – Security Management Partners provides security and IT assurance-consulting services.
Stroz Friedberg – Stroz Freidberg offers professional services for customers who have experienced a breach or require investigative response.
Swimlane – Swimlane offers enterprise support for the incident response and handling process.
Sword & Shield – Sword & Shield provides a range of managed and professional cyber security services.
Syncurity – Syncurity provides incident response solutions for enterprise breach remediation.
Thales Group – The Thales Group is a French multinational aerospace, defense, and space contractor that offers a range of cyber and data security solutions.
Vijilan Security – Vijilan offers a range of managed security services including monitoring and incident response.
Xyone – Xyone provides a range of security consulting including penetration testing, compliance, incident response, and training.

31. Penetration Testing

⇒ *Ethical Hacking* – Penetration testing involves ethical hacking of a target system to find (a small subset of) exploitable vulnerabilities.
⇒ *Controlled Process* – The best penetration testing processes balance the creativity of the tester with control of collateral damage.
⇒ *Trending* – Penetration testing will continue to grow in prominence, especially with new IoT systems that will require advanced testing.

Penetration testing involves ethical hacking for benign purposes to identify select weaknesses, but it is *not* an effective means for offering a clean bill of health on a target system. CISO teams should view penetration testing as a "managed balancing act" between chaotic hacking and controlled analysis. Turn up the offensive crank on the creative hacking, and more subtle problems will be found, albeit with increased risk of collateral damage. Turn up the defensive crank on controlled analysis, and a more stable project will result with more coherent methodological coverage, albeit with a lower probability that hidden weaknesses will be uncovered.

Penetration testing typically involves the use of heuristic methods or brute force automation to identify security weaknesses before malicious actors discover them. The paths taken to identify these weaknesses are then translated into

recommendations for improved security controls and architecture enhancements. Such identification is an excellent way to show business units or stubborn executives that security initiatives are not being properly supported in their areas.

Once a penetration testing team has completed their engagement and developed a list of identified weaknesses, they will write up a report, schedule a series of briefings to explain their findings, and include a proposal for follow-on work. Unfortunately, however, any type of testing will always be ineffective at identifying all problems. As such, the findings from a penetration test will only identify a *small portion* of existing vulnerabilities and an even smaller portion of the potential attack paths toward exploitation of these vulnerabilities.

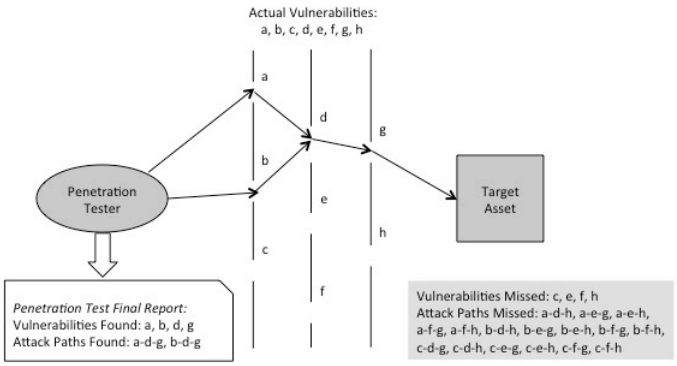

Figure 31-1. Penetration Test Vulnerability and Attack Detection

Experienced CISO teams use penetration testing – which can be done by employees or third-party consultants – to *highlight the existence* of certain vulnerabilities and attack paths in target systems. (Some CISO teams have discovered the somewhat mischievous practice of penetration testing the *finance team's systems* just before budget planning.) Like dipping one's toe in the water, penetration testing provides a means for gaining a rough feel for the ease with which hackers might break into some system. CISO teams should never assume that just because a team of expert white hats cannot break into a target, that the system is truly secure. In practice, the majority of penetration testing engagements, whether done internally or through a hired third-party, will involve the following four steps:

1. *Target Identification* – The best penetration testing projects involve clearly defined targets versus nebulous "hack-my-company" engagements. Without clear definitions of targets, the potential arises for unintended negative collateral damage. It is worth mentioning that less controlled target identification can lead to creative finds, but CISO teams must be very careful with this approach. The risk of collateral damage is high if ethical hackers are given access to anything they desire – and yes, for any Internet-facing applications, this condition already obviously exists.

2. *Ground Rules Establishment* – Penetration testing can cause problems to production systems if careful ground rules are not established in advance. White hat hackers rarely understand the local culture of a company and are highly likely to create problems if allowed to proceed without defined boundaries. Email phishing tests, for example, can sometimes get out of hand.
3. *Execution Oversight* – Insider oversight is recommended during any penetration testing that involves production systems. Such oversight will help ensure that real response activities are properly managed and that response teams are eventually made aware that testing has been done. If the test uncovers something that could affect customers, for example, then an insider must have the ability to step in and terminate the test activity.
4. *Results Interpretation* – After the penetration testing process is completed, management teams must carefully interpret results toward process improvement. Having an unopened final report on the CISO's desk is arguably worse than not having done the penetration testing at all.

Certain threats are not well suited to penetration testing. DDOS attacks, for example, should never be tested in live settings. The same advice goes for any destructive malware testing – this is simply not acceptable in any live setting. Good penetration testers always provide their customers with a baseline process methodology for their testing activities, such as the typical three-phase process shown below.

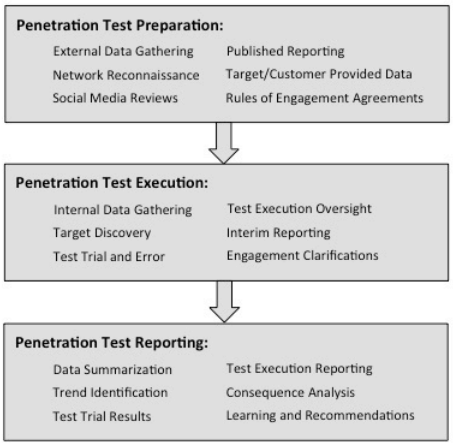

Figure 31-2. Typical Penetration Testing Methodology

In spite of process methodology definition, penetration testers will often reserve the right to deviate in order to more creatively explore possible areas of vulnerability. This artistic license underscores the importance of using penetration testers who have experience. It also suggests extra care in demanding clear definition of rules of engagement, along with processes for unwinding penetration tests that go awry. Penetration testers should list the test tools and platforms used in case information

becomes public at some later time about vulnerabilities in such test support systems.

The state of the practice in *commercial penetration test consulting* is healthy and growing steadily. More companies in all sectors will begin to realize the benefits of live security testing by experts, and the market is likely to shift toward greater emphasis on simulating organized capable threats versus performing simple penetration tests. A balancing force, however, is the increasing shortage of good security testing talent that can be trusted with access to corporate or government systems. CISO team should check carefully with their selected penetration testing vendor, because the contract might be written under the assumption that the actual vendor will be doing the work, only to result afterwards in a chain of subcontracts designed to locate real human beings who can perform the tests.

The trending for traditional penetration testing will involve gradual increases based on growing general cyber security awareness across enterprise sectors. Steep increases will occur in the need for more advanced penetration testing as nation-state attacks increase and expand to non-traditional targets such as retail and other non-military entities. One might also expect compliance standards to emerge for penetration testing so that more common understanding of the assurance associated with an ethically tested system can be obtained.

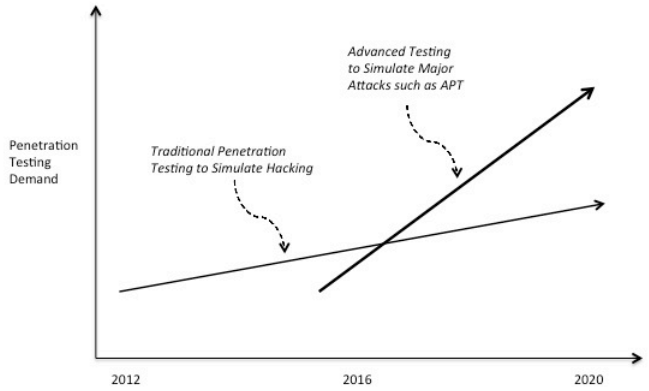

Figure 31-3. Trends in Penetration Testing

An issue that must be factored into any forecast about penetration testing is that as major incidents occur – perhaps for connected cars, industrial control systems, major retailers, or government agencies – the desire and demand for participants in the effected industry to penetration test their systems will spike.

An example is the plethora of retail credit card penetration testing engagements in 2015 and 2016. As a result, penetration test demands in specific areas such as Internet of Things (IoT) will require a bit more due diligence to ensure that the penetration testing team has the requisite skills. For certain aspects of the IoT market, especially in industrial control and operational technology,

knowledgeable penetration testers with specific domain expertise will be extremely hard to locate.

Penetration Testing Providers

Developing a comprehensive list of security penetration testers is particularly difficult because virtually every security consulting firm is willing to accept work in this area. Small start-up cyber security product companies, for example, often have cash flow problems and use penetration testing to pay the lighting bill. Not surprisingly, however, small consulting groups and start-up firms often do an excellent job performing penetration tests, so CISO teams must keep this in mind.

Additionally, the line is blurred between deep penetration tests and high-level security assessments, which are also available from virtually every security consultant. Ultimately, the vendors listed below were selected because they have demonstrated *specific focus* in the area of penetration testing, and continue to improve their capabilities as the cyber threat evolves. The list is quite long simply because the barrier-to-entry for firms to get into penetration testing is so low.

In truth, the list below could have been twice as long if sufficient coverage had been given to all security consultants, managed security service providers, and value added resellers who offer ethical hacking. Vendors performing the related function of supporting bug bounty programs, where external third-parties hack target systems, are listed in their own separate section of this report.

2017 TAG Cyber Security Annual
Penetration Testing Providers

ACROS Security – ACROS is a small, family-owned Slovenia penetration testing and research company.
AppSec Labs – Israeli application security expert group AppSec Labs has emphasis on testing mobile apps.
Atsec – Atsec is a security test and evaluation group with a mainframe penetration testing service.
AT&T – AT&T offers a range of penetration testing solutions through on-staff and outsourced groups.
Atredis Partners – Atredis is a small expert team of penetration testers with presence at conferences such as Black Hat.
Aura Information Security – Part of Kordia, Aura provides information security and penetration testing.
AVeS – Located in Johannesburg, Aves provides IT consulting and penetration testing.
Avnet – Israel-based Avnet provides security consulting and penetration testing with focus on securing databases.
BINAR10 – Peru-based BINAR10 provides ethical hacking and related security services.

Bishop Fox – Phoenix-based Bishop Fox offers security consulting and penetration testing services.
Bitcrack – Located in South Africa, Bitcrack offers security consulting, GRC, and penetration testing.
Bitshield – Located in the Philippines, Bitshield provides security consulting and penetration testing services.
Buddha Labs – The Encino-based firm offers IT security and testing services for clouds including AWS.
BugSec – Located in Israel, BugSec offers penetration testing and security consulting services.
Carve Systems – Carve provides full-stack penetration testing services for IoT devices and other targets.
Cigital – Cigital provides expert application-oriented penetration testing services using multiple testing tools.
Coalfire Labs – Coalfire Labs offers audit, risk, penetration, and scanning services across the US and UK.
Codenomicon – Acquired by Synopsis, the group offers a suite products and services focused on vulnerability testing.
Comodo – Penetration testing is done by Comodo Dragon Labs, which includes staff around the world.
Content Security – Content Security, located in Australia, offers security consulting and testing services.
Core Security – Core Security offers the Core Impact Pro penetration testing platform for networks, endpoints, and Web.
Cyber Alpha Security BV – Located in The Netherlands, Cyber Alpha Security offers consulting and testing services.
Cyber Defense Labs – Cyber Defense Labs provides security consulting and penetration testing solutions.
Cyberis – San Antonio-based Cyberis provides security consulting and penetration testing solutions.
SecureWorks – Penetration testing is offered as part of the SecureWorks Testing and Assessments Services.
Depth Security – Kansas City-based Depth Security provides security consulting and penetration testing solutions.
Encription – UK-based Encription provides security consulting and penetration testing solutions.
Fortego – Maryland-based Fortego provides network operations, reverse engineering, and other advanced cyber test services.
FRSecure – FRSecure offers penetration testing as part of its suite of security consulting services.
GoSecure – Canadian firm GoSecure provides security consulting and penetration testing solutions.
Grid32 Security – Newark-based Grid32 Security provides penetration testing and vulnerability assessment.

Hacking Team – (Somewhat controversial firm) Hacking Team provides offensive attack tools and surveillance capability for law enforcement and government.
HackLabs – Security consulting firm HackLabs specializes in penetration testing and ethical hacking.
Halock Security Labs – Halock Security Labs provides security consulting and penetration testing solutions.
Hedgehog – The UK-based consulting firm provides a range of penetration testing and security research services.
High-Tech Bridge – Located in Switzerland, High-Tech Bridge provides security consulting and penetration testing solutions.
Immunity – Florida-based Immunity provides security consulting and penetration testing solutions.
InGuardians – Washington-based InGuardians provides security consulting, audit, and penetration testing solutions.
ITsec Security Services – Located in The Netherlands, ITsec Security Services provides security consulting and penetration testing solutions.
Ixia – The California-based firm focuses on security and penetration testing solutions for enterprise.
Kaprica – Reston-based Kaprica provides security consulting and penetration testing solutions with emphasis on mobile.
Kernel – Located in Colorado Kernel provides security consulting and penetration testing solutions.
KoreLogic – Maryland-based KoreLogic provides security consulting, application security assessment, and penetration testing solutions.
Kroll – Kroll is a security firm that includes penetration testing as part of their consulting offer.
Krypsys – UK-based Krypsys provides security consulting and penetration testing solutions.
Kyrus – Located in Virginia, Kyrus focuses on reverse engineering, security research, and related testing.
Lancera Security – Lancera is a Utah-based security firm that includes penetration testing as an offer.
Layer Seven Security – Security services group Layer Seven, part of CA, focuses on offering SAP penetration testing.
LBMC Security & Risk Services – Professional services firm LBMC has an information security team with penetration testing capability.
Logically Secure – UK-based Logically Secure provides security consulting and penetration testing solutions.
Lunarline – Virginia-based information assurance firm Lunarline offers penetration testing services.
Maven Security – Maven Security provides a suite of security consulting and testing services.
Meta Intelligence – Virginia-based Meta Intelligence offers risk management and penetration testing.

Mitnick Security – Mitnick security is the security consulting and penetration testing firm of well-known hacker Kevin Mitnick.
NCC Group – NCC Group acquired iSec Partners to integrate penetration testing capability into offers. The company offers a range of testing services from deep technical investigations to higher-level assessments.
Netragard – Penetration testing firm Netragard made news by terminating their exploit acquisition program in 2015.
Nettitude – Nettitude provides penetration testing, risk management, and related cyber security services.
NetSPI – Information security and risk consulting company NetSPI includes a penetration testing capability.
nGuard – Charlotte security consulting firm nGuard includes penetration testing services.
Nisos Group – Nisos Group is a small start-up firm focused on penetration and stress testing to detect advanced threats. The principals have excellent backgrounds in government information assurance.
Offensive Security – Offensive Security is a group of expert hackers running a range of penetration testing courses.
Oneconsult AG – Swiss security consulting firm Oneconsult AG offers a range of penetration testing.
Parameter Security – Missouri-based Parameter Security provides security consulting and penetration testing solutions.
Pen Test Partners – UK-based Pen Test Partners provides a range of penetration testing services for mobile, SCADA, applications, and other areas.
Pentura – Part of InteliSecure, Pentura offers security consulting and penetration testing services.
PivotPoint Security – PivotPoint Security provides a range of information assurance and security consulting services including penetration testing and ethical hacking.
Portcullis – UK-based Portcullis provides security consulting and penetration testing solutions.
Praetorian – Consulting and penetration testing services are available from Austin-based Praetorian.
Provensec – Provensec makes available cyber security and penetration testing focused on mid-sized business needs.
Pwnie Express – Boston-based Pwnie Express provides security consulting, asset discovery, and penetration testing solutions.
Rapid7 – Boston-based Rapid7 offers scanning and penetration testing based on the work of H.D. Moore, inventor of Metasploit.
Reaction Information Security – Reaction Information Security provides security consulting and penetration testing solutions.
Redspin – Redspin is a security risk, compliance, and penetration testing services in California (Redspin was recently acquired by Auxilio).
Rhino Security Labs – Rhino Security Labs includes a range of network penetration, Web penetration, mobile app, and secure code reviews.

Riscure – Located in The Netherlands, Riscure is a global security test laboratory focused on side channel analysis.
RiskSense – RiskSense provides a vulnerability management platform along with a range of security services.
Root9b – The new York-based company provides advanced cyber security consulting, testing, and training services.
SafeBreach – California-based SafeBreach provides a platform for breach execution on a target system.
SAINT – SAINT offers penetration testing through the SAINTexploit scanning platform.
SECFORCE – UK-based SECFORCE offers a range of security consulting and penetration testing services.
Secure Anchor – Virginia-based Secure Anchor offers a range of security consulting and penetration testing services.
Secure Ideas – Florida-based Secure Ideas offers a range of security consulting and penetration testing services.
Security Art – Security Art provides a range of cyber security consulting services including red team exercises.
Security Audit Systems – UK firm Security Audit Systems offers a range of Website penetration testing services.
SecurityMetrics – SecurityMetrics offers PCI and HIPAA compliance services including scanning and penetration testing.
Sense of Security – Located in Australia, Sense of Security offers a range of security consulting and penetration testing services.
7Safe – UK-based 7Safe offers a range of security consulting, training, and penetration testing services.
Sunera – Sunera provides audit, risk, regulatory, and compliance services across US and Canada including penetration testing.
Synack – Synack offers a means for enterprise teams to use continuous Bug bounty exploitation from a vetted team of crowd-sourced experts.
Syndis – Iceland-based Syndis offers a range of security consulting and penetration testing services.
TBG Security – TBG Security provides security consulting services to assist with compliance in HIPAA, PCI, and related frameworks.
TechGuard Security – TechGuard offers a range of security consulting and penetration testing services for commercial and government customers.
Threat Intelligence – Australian firm Threat Intelligence provides managed threat intelligence including penetration testing.
Topgallant Partners – Topgallant Partners offers a range of security consulting, assessment, and penetration testing services.
Trail of Bits – New York-based Trail of Bits provides a range of expert research, training, and testing services.
Trojan Horse Security – Washington-based Trojan Horse Security offers a range of security consulting and penetration testing services.

TrustedSec – Located in Ohio, TrustedSec offers a range of security consulting and penetration testing services.
Trustwave – Trustwave makes available full service cyber security consulting and PCI DSS QSA services including penetration testing.
2-Sec – 2-sec provides a range of security consulting offers including penetration testing and PCI DSS services.
ValueMentor – ValueMentor Consulting provides information security consulting including security assessments and penetration testing.
Veracode – Veracode is an application security firm that includes penetration testing services.
Verizon – Verizon offers a range of penetration testing solutions through on-staff and outsourced groups.
vThreat – Herndon-based vThreat offers a range of test and simulation platform support capabilities for cyber security functions.
Xyone – UK-based Xyone offers security consulting and penetration testing solutions for enterprise.
Yarix – Italian firm Yarix offers security consulting and penetration testing services for customers.

32. Security Analytics

⇒ *Analytic Components* – Security analytics involves data ingest, processing, and analysis to derive actionable intelligence – similar to Big Data Analytics.
⇒ *Improved Methods* – Techniques and methods for security analytics have become more effective and accurate in recent years.
⇒ *Continued Growth* – The market for security analytic products and services will grow considerably in the coming years.

The vital cyber protection task generally referred to as *security analysis* causes considerable confusion amongst security vendors, CISO teams, venture capital investors, and industry observers. The problem is that because so many different techniques, tools, and processes align with this term in their marketing and training materials, it becomes almost impossible for anyone to create a taxonomy that is useful. The popularity of business intelligence-driven Big Data analytics in most enterprise environments also creates some confusion.

Regarding confusion in the cyber security community about analysis, note that the enterprise SIEM, for example, can be viewed as supporting the security analysis task. Similarly, traditional enterprise log management tools can be viewed as supporting security analysis. Network monitoring tools capturing packets at line speed refer to their processing function as security analysis. Even anti-fraud and intrusion prevention systems for enterprise Web services are described as supporting security analysis by enterprise teams. So the term has become sufficiently generic as to be no longer useful.

Nevertheless, the task of ingesting and analyzing data for the purpose of generating "close to real time" actionable intelligence is so important to enterprise protection that we must attempt to create some semblance of order in how we view the market and the attendant tasks for a CISO team. As such, the following observations can be made about this new category of cyber security we will refer to collectively as *security analytics*:

- *Data Ingest* – Security analytics always relies on either an embedded or separately managed process for collecting security-relevant data. Enterprise CISO teams can be opportunistic about this process using whatever means are available or desired. Granted, many new security analytic tools will come with their own means for collecting data, but this might be redundant with other existing collection methods. Relevant data include application and activity logs, system audit trails, network flow information, and other meta-data that could contain evidence of potential or currently active cyber attacks.
- *Data Repository* – Security analytics generally involves tools, techniques, and algorithms that operate on large repositories (often Hadoop-based) of stored, ingested data. This separates the off-line, non-real time security analysis task from the on-line, on-the-fly, network monitoring tools that attempt to report and make mitigation decisions at line speed.
- *Human Analysts* – The security analytic process involves tools that will be used by a human being to derive intelligence. Certainly many automated tools and processes such as intrusion prevention systems will describe their operation as being enabled by security analytic techniques. But our reference here is strict in the sense that we describe security analytics as being done by human analysts. It is common in the security marketplace today to refer to the process of deriving intelligence as *hunting*. The hunter cannot work in true real time, in the strictest sense, but must derive intelligence in as "close to real time" as is possible. Some observers differentiate Big Data analytics from security analytics by this "close to real time" goal.
- *Analysis Results* – The primary purpose of security analytics is for human beings to create actionable intelligence from available data. The idea is that on first glance, the data exposes very little, but with deeper study, the analyst can derive useful causality, relations, and interpretations that will help manage risk. Without clearly actionable results, the hunting task seems a mere academic exercise.

The security analytic task involves a series of monitored sessions as might be represented in a group of captured logs. These sessions on first glance do not expose anything of note; rather they look to be the usual sort of step-by-step progression of computing activity with nothing looking particularly out of the ordinary in the individual session log views.

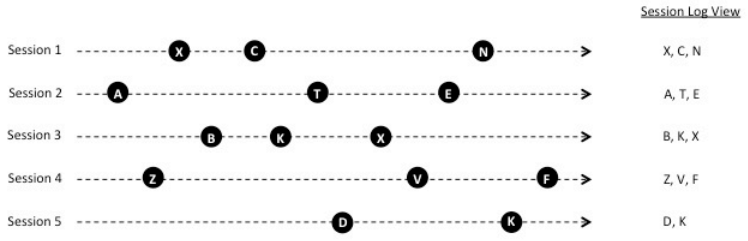

Figure 32-1. Normal Session Log Information

With a security analytic tool, non-obvious relationships emerge that can lead to actionable insights. For the event log example shown in the figure above, a security analytic tool might detect the subtle time-progression of a related series of steps across different sessions. Evidence of enterprise East-West traffic traversal, referred to as lateral movement, is determined in this manner. Advanced persistent threats (APTs) have almost always included some form of lateral movement across the enterprise.

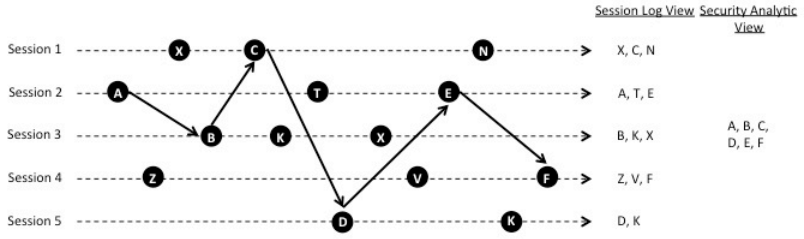

Figure 32-2. Showing Time-Progressed Lateral Movement in Session Logs

Traditional cyber security tools have done a poor job detecting the presence of APTs moving laterally across the enterprise. In many cases, APTs have existed within corporate networks for months or even years. Enterprise security has therefore become increasingly dependent on modern security analytics tools as a means for identifying advanced threats via hunting techniques.

The enterprise architecture of most security analytics deployments can be decomposed into two major components – *enterprise data repositories* and *security analysis tools* – both accessible and utilized by the human security hunting analysts, who are often located in a *security operations center* (SOC). This human performed, tool supported hunting task is intended to produce actionable intelligence from both enterprise ingress data feeds, and external, all-source ingress data feeds. Both the data collected and the intelligence generated can be viewed as local to the enterprise as well as externally relevant to all sources.

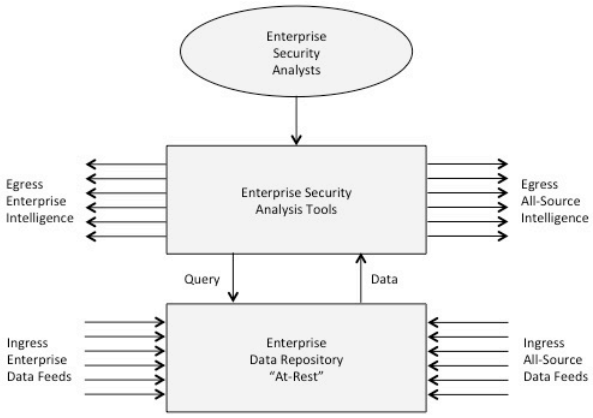

Figure 32-3. Architectural View of Security Analytic Deployment

Many existing security algorithms and tools for analytics will require change to account for more holistic, less uniform data from all sources. The types of algorithms and analysis techniques inherent in modern enterprise security analytics include the following:

- *Traditional Signature Analysis* – While it is common to refer to signature-based systems as useless, this is greatly exaggerated. Signatures such as IP address, domain name, file name, and attack procedure remain highly useful to the security analyst. In spite of the aversion to signature-based methods by pundits and investors, the use of signatures remains absolutely essential to proper detection of cyber security threats.
- *Behavioral Analysis Based on Profiles* – Most new security analytic solutions, including professional services, tend to emphasis behavioral analysis using profiles. The idea is that some computing attribute is established as a baseline profile and deviations create alerts. When this technique is applied to applications, it is sometimes referred to as *watermarking*. Behavioral techniques look for "changes from normal," such as a resource becoming too popular, less popular, more busy, less busy, and so on.
- *User Behavioral Analysis (UBA)* – A special case of the behavior analysis approach focuses on human user behaviors as the basis for comparisons between observed and expected traces. Behavioral analytics usually depend on statistics and machine learning to detect anomalies in collected corporate data. Enterprise CISO teams must be careful not to drive their employees to shadow IT solutions if the UBA is too aggressive. Staff members who believe that their every point-and-click will be monitored for anomalies will be soon motivated to shift to unmonitored private use of cloud services for greater privacy (e.g., Gmail, Box storage, Facebook).
- *Forensic Component Investigation* – Enterprise security analytic solutions will always include the need to support forensics during or after an incident.

While forensics tools are considered a separate area in the CISO toolkit, the enterprise security analysis platform, tools, and capabilities provide important complementary support for the forensics process, often helping to unravel how a given attack might have occurred across the enterprise perimeter.

- *Attack Breakdown and Analysis* – Enterprise security analytics should account for and support the breakdown and analysis of any attack, especially ones that have been recently discovered in the wild in environments similar to the target enterprise. CISO teams will take note that most marketing approaches by security analytic vendors will involve detailed breakdown of how their tool would have stopped some famous attack. This must be taken with a grain of salt, because after-the-fact analysis and breakdown is fundamentally different than proactive prevention.
- *Vulnerability Investigation and Cross Reference* – Enterprise security analytic solutions should account for and support investigation of vulnerabilities including cross-referencing their footprint with corporate enterprise inventories. This is a challenge because few security analytic tools allow for easy integration (even if APIs are present) with identity and access management, enterprise directory, and other IT systems.

All enterprise security analytics solutions include one or more of these types of analysis approaches. Behavioral analytics, in particular, has become a growing area for cyber security vendors and is increasingly referenced in compliance and regulatory requirements. Managed security service providers are also increasingly focused on providing enterprise security analytics support through partnership with a technology vendor as part of their offerings to enterprise and government customers.

The future market and usage prospects for security analytics are influenced by two trends moving in opposite directions. First, the organizational concept of a traditional enterprise behind a perimeter is rapidly becoming less acceptable to CISO teams, especially in small and medium sized businesses. As such, the conventional, on-premise deployment of an enterprise security analytics tool will evolve over time into more virtual, cloud-based solutions.

Correspondingly, however, the need for security analytics to be performed on enterprise data distributed across applications, systems, cloud, and mobility will increase significantly. As such, the market and usage of distributed, virtual security analytics products and services, including managed services, will grow in the coming years. This trend will result in an overall *growing need* for enterprise security analytics, in spite of any enterprise architectural changes away from the perimeter.

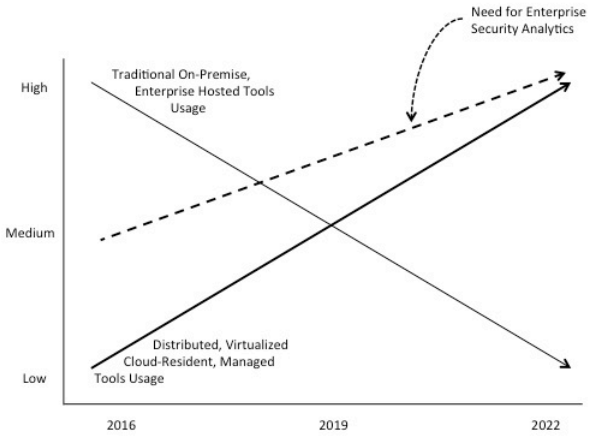

Figure 32-4. Market and Usage Trends for Enterprise Security Analytics

CISO teams should not be confused by the steep decline predicted for traditional, on-premise tools. This does not imply a reduced need for security analytics, but rather underscores the significant shift to all-source, virtual analytics that can blend ingested data from public and hybrid cloud sources into intelligence that can be used locally as well as shared within trusted communities. Security analytics providers should thus be required, during any source selection process, to explain their technology roadmap to support virtualization in the data center and SDN in the wide area network.

Security Analytics Providers

The security analytics vendors selected for this category have all demonstrated a commitment to providing advanced platforms and tools to mine large sets of collected data for evidence of cyber attacks or vulnerabilities. Unlike network security analysis or intrusion detection, the vendors listed below are more focused on the mining of large collected data sets in frameworks such as Hadoop.

It is not uncommon for many of the vendors listed below to find their products operating in parallel with a competing offer on the same collected enterprise data. CISO teams reviewing the lists below should include vendors in the SIEM, IPS, and Network Monitoring sections of this report, since so many similarities exist between the various disciplines – enough so, that some analysts choose to combine the three categories into one "security analytics" grouping.

2017 TAG Cyber Security Annual
Distinguished Security Analytics Providers

Sqrrl – I've been familiar with the Sqrrl team for some time, having followed the progress of principals Adam Fuchs and Ely Kahn as they made the transition from National Security in Washington to Silicon Valley start-up. Technical discussions

with Adam and Ely during the past few months were especially helpful to me in sorting out, and better understanding this complex area of enterprise cyber security. The simplicity and power of the Sqrrl toolset in assisting the analyst/hunter helped me to focus on the salient aspects of security analytics for enterprise security. Thanks to members of the Sqrrl team for their fine support of this research.

2017 TAG Cyber Security Annual
Security Analytics Providers

Alcatel Lucent – ALU offers the Motive BNA Data Miner (BNA) engine for enterprise analysis of network and system data.
Attivo Networks – Attivo Networks provides deception-based attack detection and prevention capabilities that incudes support for advanced analytics.
AxonAI – Virginia-based AxonAI provides AI-based swam technology for anomaly detection.
BalaBit – Located in Budapest, Balabit provides real time intelligence based network security analytics.
Bay Dynamics – Bay Dynamics offers the Risk Fabric predictive security analytics platform.
BrightPoint Security – Formerly Vorstack, the company provides tools for correlating SIEM data into intelligence.
Brinqa – Located in Austin, Brinqa provides an integrated GRC platform that includes extensive security analytic support.
Click Security – Click provides an advanced threat management solution that operates in conjunction with the enterprise SIEM.
Context Relevant – Context Relevant provides state-of-the-art predictive data analysis tools for enterprise cyber security.
CyberFlow Analytics – Based in San Diego, CyberFlow Analytics provides network monitoring and security analytics.
Cylance – Cylance offers artificial intelligence-based analysis tools to detect threats on endpoints.
Cymmetria – Cymmetria provides security analytic-based intrusion detection solutions.
Cynet – Based in New York, Cynet offers enterprise analytic support for detecting cyber threats.
Cyphort – The Advanced Threat Protection platform from Cyphort supports the "single pane of glass" approach to enterprise analytics.
Damballa – The Damballa Failsafe platform collects data from sensors and supports advanced threat analytics across the enterprise.
Darktrace – Darktrace offers a platform that supports so-called Enterprise Immune System technology for advanced analytics.
Dataguise – Fremont-based Dataguise offers solutions for Big Data analysis security processing.

Dtex Systems – Located in San Jose, Dtex Systems focuses on insider threat protection using security analytics with behavioral pattern detection.
E8 Security - E8 security provides a security behavioral intelligence platform to support detection of threats in the enterprise.
Encode – Encode provides a security analytics and response orchestration platform for the enterprise.
Endgame – Virginia-based Endgame provides cyber security support for threat and vulnerability detection.
eSentire – eSentire offers an active threat protection solution with continuous monitoring service.
Exabeam - Exabeam provides user behavioral analytic intelligence from SIEM and log management data to detect insider attacks.
FileTrek – Known as Interset, the company provides endpoint behavioral analytics for enterprise.
FireEye – The popular FireEye platform includes advanced support for enterprise security analytics.
Flowtraq – Flowtraq provides an advanced capability for analysis of network flow data.
Forcepoint – Forcepoint offers a range of content security, advanced analytics, cloud security, firewall, and Web security solutions for the enterprise.
Fortscale – Fortscale provides user behavioral analytics for enterprise security threat detection.
Guardian Analytics – Mountain View-based Guardian Analytics provides behavioral analytic solutions for detecting fraud.
GuruCul – GuruCul supports identity-based behavioral analytics to support risk intelligence.
Hawk Network Defense – Hawk Network Defense provides security analytics for enterprise, service providers, and SIEM enrichment.
Haystax Technology – Haystax Technology provides security intelligence and real-tome situation awareness solutions.
HPE – One of the industry-leading SIEM solutions, ArcSite from HPE, offers a range of security analytics functions.
IBM – IBM includes an extensive range of security analytic solutions as part of its cyber security product offerings.
IKANOW - IKANOW provides Big Data analytic solutions to reduce the risk of breaches and APT attacks.
Informatica - Informatica provides a range of Big Data solutions including a data security offering focused on critical data intelligence.
InterGuard - InterGuard provides employee-monitoring software that records and controls PC activity for loss and misuse.
Jask – San Francisco-based Jask provides an artificial intelligence-based platform for security analytics.
KEYW – KEYW provides the Hexis enterprise security analytics solution with data analysis and SIEM functions.

Lastline – Lastline provides advanced malware detection and threat analysis for enterprise customers as a hosted or on-premise solution.
LightCyber – Located in Israel, LightCyber provides breach detection with emphasis on APTs.
Mobile System 7 - Mobile System 7 provides enterprise security via data protection, identity analytics, and adaptive access controls.
Morphick – Morphick provides security analytic tools for advanced threat detection and response.
Niara – Niara offers an integrated platform for performing analytics and forensics on enterprise data.
NIKSUN – Princeton-based NIKSUN provides network performance monitoring and security surveillance solutions.
Noragh Analytics – Noragh's TAC supports enterprise analysts and managers in their investigation and analysis of large volumes of information.
Novetta – Novetta provides an advanced analytics platform for detecting threat and potential fraud in the enterprise.
Nuix - Nuix provides investigation, information governance, eDiscovery, and cyber security solutions for enterprise.
ObserveIT – ObserveIT provides a software solution for user activity monitoring based on tailored analytics and forensics.
Outlier Security – Outlier Security provides agentless cyber security analytics as a service for endpoints.
Palantir – Palantir provides real time data fusion and intelligence platform solutions for enterprise and other applications.
Pixlcloud – Pixlcloud supports Big Data analytics and visualization in the enterprise with training offers for analysts.
Pravail -
Prelert – Prelert provides an integrated behavioral analytics capability for tools such as Splunk.
Red Lambda – Red Lambda provides a Big Data platform that combines computing and storage with correlation, reporting, anomaly detection, and automation.
RedOwl – RedOwl supports behavioral analytics for information security and enterprise compliance.
Reversing Labs – Reversing Labs provides a platform for advanced threat protection and analytics with support for incident response.
Risk I/O – Rebranded as Kenna in 2015, the company provides a risk intelligence and vulnerability management platform.
RiskLens
RSA (EMC) – The industry-leading security division of EMC has expanded its focus on enterprise security analytics support.
SAS – Advanced analytics from SAS traditionally focused on business intelligence and predictive analysis are being applied to enterprise cyber.
Savvius – Savvius provides advanced network monitoring and security analytics software.

Secnology – Secnology provides a wide range of SIEM, log management, and enterprise security analytics capabilities.
Secure Decisions – Secure Decisions provides cyber security visualization solutions for analysis support of software, networks, and other systems.
SecurityDo – SecurityDo provides a product called Fluency that provides breach detection and response capabilities.
Sophos – Sophos combines endpoint security protection with enhanced analysis tools based on Cybereason acquisition.
SpectorSoft – SpectorSoft provides monitoring software to detect insider threats, employee fraud, and data breaches.
Splunk – Splunk offers an advanced platform for operational intelligence on a network including cyber security threat identification. Splunk acquired Caspida in 2015.
Sqrrl – Sqrrl's Linked Data Analysis supports enterprise security analysis and monitoring of collected data. Former members of the US DoD were involved in the original development of the security analytics tool.
SS8 – SS8 provides advanced enterprise communication security through analysis, correlation, and forensics. The company's heritage in law enforcement-based communication intercept and processing forms a useful base for security analytics.
Sumo Logic – Redwood City-based Sumo Logic provides advanced continuous log management and security analytics.
SurfWatch Labs – SurfWatch Labs provides a risk analytic platform API for translating data to intelligence.
Tanium – Tanium provides high performance, real time endpoint protection through data collection and threat analysis.
ThetaRay – ThetaRay offers enterprise security analytics support for industrial sectors.
ThreatStream – Redwood City-based ThreatStream offers a threat intelligence platform for supporting security data analytics.
ThreatTrack Security – ThreatTrack Security provides a sandbox-based solution for the detection of suspicious or malicious behavior.
TIBCO – TIBCO provides a range of business intelligence and infrastructure solutions, including data security.
Trustpipe – Trustpipe offers endpoint security via network traffic scans and analysis using an attack taxonomy.
21CT – 21CT provides a behavioral analytic fraud detection solution that supports enterprise investigations.
Verint – Verint provides a range of analytic hardware and software products and services for security, business intelligence, and surveillance industries.
Vistronix – Software developer and solutions innovator Vistronix focuses on supporting data analysis.
Yaana – Yanna includes security analytics in its suite of Big Data solutions for enterprise.

Yaxa – Yaxa provides an insider threat protection solution based on user behavioral analytics.
Zettaset – Zettaset provides solutions for securing Hadoop and orchestrating enterprise security analytics.

33. Security Information Event Management

⇒ *Enterprise Use* – Just about every CISO team operates a SIEM as the basis for log and event management in the enterprise.
⇒ *Virtualization* – The trend will be to virtualize the SIEM function and associated infrastructure in a distributed manner across cloud workloads.
⇒ *Cloud Aware* – Evolving enterprise security architecture will require SIEM visibility into public and hybrid cloud activity.

The primary purpose of a *Security Information Event Management* (SIEM) system is to provide real time analysis, correlation, and reporting of security alerts, log information, and events generated by a variety of different sources in an enterprise or network. The marketplace sometimes distinguishes log management and logging-as-a-service as separate functions, but they are assumed here to be enhanced functions provided by the SIEM.

Just about every CISO team today operates a SIEM in their enterprise, with some teams using their SIEM as the basis for real time security operations, and others using it in a more complementary manner as part of the security back office. Surprisingly, not all CISO teams make full use of the features offered by their SIEM vendor, and in companies with a non-existent CISO or a scattered enterprise security team, the SIEM might not play much of a role, if any, in the strategic security protection of the company's most critical assets. So the role of the SIEM in many of these companies is evolving.

The most common architectural view of a SIEM exists as a processing, correlation, and intelligence-generating engine based on structured information that is received via connectors from a variety of devices around the enterprise network. The engine then provides real time support for analysis and incident response, as well as management and reporting through a common interface. The SIEM is often physically constructed as a centralized component on a protected server, but there is no reason why the SIEM function cannot be distributed across several nodes to improve resiliency and performance.

This coordinated SIEM set-up and operation, whether centralized or distributed across the enterprise, with its familiar connectivity to threat feeds, security devices, other SIEMS, other systems, and select applications is depicted in the figure below.

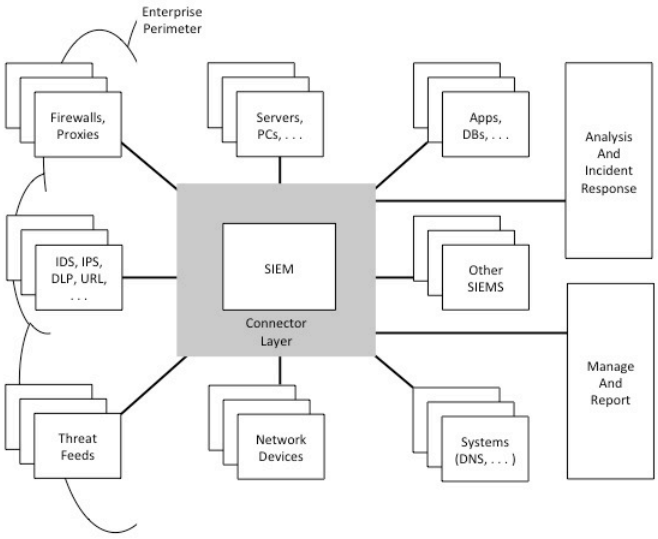

Figure 33-1. Enterprise Use of SIEM

One challenge inherent in *conventional* SIEMs is that they were originally designed to serve a perimeter-protected enterprise. Unfortunately, CISOs are gradually coming to recognize that perimeter-based protections will no longer sufficiently address the needs of private enterprise. Explosive growth in firewall exceptions, partner gateways, remote access, wireless connectivity, and email attachments has made perimeters too complex and leaky to properly protect private information. As such, the familiar concept of collecting information from inside a perimeter for private processing within the enterprise will change.

Specifically, SIEM processing and associated architectures will evolve to support more flexible connectivity, reach, and integration with systems, services, and cloud infrastructure that will exist beyond the perimeter. To this end, future SIEMs will be distributed, virtual, ubiquitous, and cloud-like in their need to decouple from underlying hardware constraints. The now-separate concepts of virtual SIEM and conventional SIEM will no doubt merge.

The first step in this evolution will be SIEM gateways, often just a capability offered in the existing SIEM product, designed to integrate the enterprise SIEM with external collection and analysis functions. This set-up will be required to support CISO teams who remain determined to maintain a firewall-based security perimeter. At some point in the next few years, however, all SIEM functions will likely migrate to fully virtual and cloud-resident architectures as enterprise processing moves virtual and mobile.

The near-term typical arrangement for a SIEM in the coming years will look like the distributed set-up depicted below.

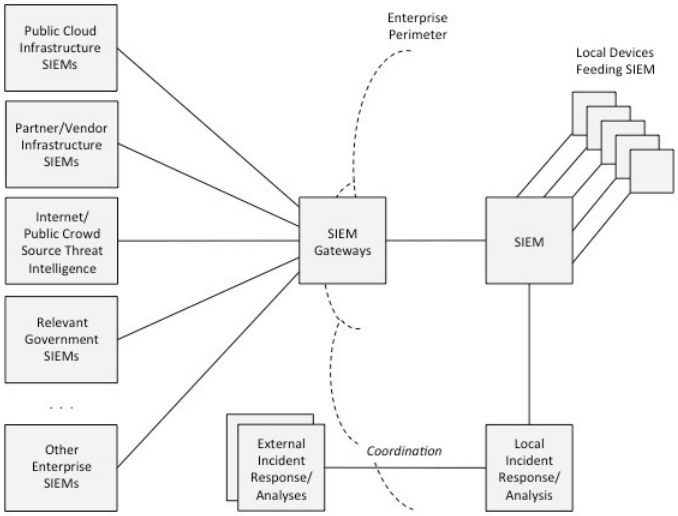

Figure 33-2. Near-Term Use of SIEM

As suggested above, the biggest difference that will emerge in the coming years will be the dissolution of the perimeter, which will result in more machine-to-machine (M2M) communications between different SIEM components. Protocols and communications frameworks such as Structured Threat Information eXchange (STIX) and Trusted Automation eXchange of Indicator Information (TAXII) will thus become examples of automated means for such M2M sharing and coordination between SIEMs.

An additional challenge with respect to a SIEM is the desire of most CISO teams to augment conventional correlation and basic analysis with advanced behavioral analytics engines that use comprehensive profiling of target systems, applications, or networks. One approach is to integrate a separate behavioral analytic engine onto the SIEM, thus leaving the SIEM to focus on its familiar functions.

An alternate approach is to utilize a next-generation SIEM that builds the behavioral analytics directly into the native SIEM. Larger enterprise organizations with business intelligence infrastructure using Big Data collection and analytics should also be integrated into the SIEM analysis and processing. Regardless of the approach, CISO teams will require this type of functionality and will typically adjust their SIEM processes and enterprise security workflow arrangement accordingly as shown below.

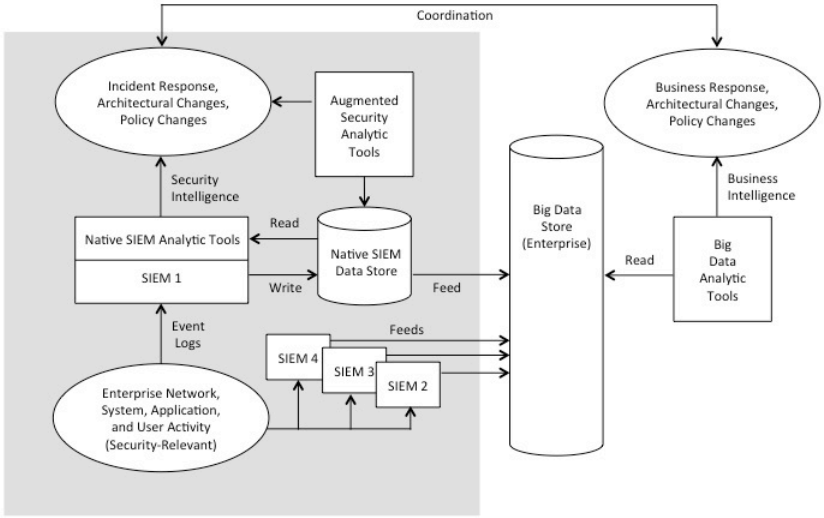

Figure 33-3. SIEM Augmented with Big Data Security Analytic Tools

Additional trends in SIEM architecture, driven by the needs of the CISO team to deal with evolving threats from capable actors will involve the following:

- *Virtualized SIEM* – Virtualization will allow SIEM processing and analysis to be performed closer to the asset and correlation to be done in a distributed manner via network protocols. The potential emerges that a SIEM will become embedded in the SDN control of a data center and wide area network. This will allow the SIEM to have visibility into logs associated with enterprise East-West activity between virtual machines and workloads.
- *Standardized Connectors* – Every newly developed software package or system will have the obligation to demonstrate connectivity into standard SIEM connectors (likely APIs). This issue of coverage has always plagued SIEM operators, because without visibility and information flowing from all relevant aspects of an enterprise, the intelligence derived will miss important contributing value.
- *Standardized Threat Intelligence* – Every SIEM will evolve to accept standard threat intelligence updates using systems and protocols such as STIX and TAXII. The quality of the information will become more important than the quantity, which might be a negative for crowd-sourced SIEM solutions. That said, crowd-sourced intelligence feeds often introduce a diverse mix of information not available from commercially sponsored and vetted feeds.
- *Workflow Support* – As the SIEM function integrates into the incident response process, corresponding support for tiered workflow support will become a requirement. The challenge for vendors will involve balancing the native workflow inherent in the SIEM with having open APIs and connectors to popular workflow tools such as RSA Archer.

- *Analyst Workloads* – One thing that will not change in SIEM processing is that even in the presence of increased automation, analyst workloads will continue to grow as offensive actors become more aggressive. The ability to funnel large numbers of ingested indicators and drive to a manageably small number of work activities will continue to be an important differentiator in the SIEM. Data reduction efficiencies (translated: *work* reduction efficiencies) are as important to security operations staff as any other factor.

The marketplace for SIEMs will evolve gradually from enterprise-resident systems to cloud and externally aware environments with the ability to collect information from a wider variety of endpoints and feeder systems, and to provide better visibility into these systems. This should not cause a near-term reduction in need for enterprise SIEM, but will instead involve pure growth to cloud. Every SIEM vendor should be challenged to offer their planned roadmap to support this evolution, including plans for mobility, virtualization, public cloud, and SDN.

The need for automated support in SIEM processing will also continue to increase, but this will not change the analyst workload as the threat evolves. Crowd sourcing of intelligence will evolve to deal with increased emphasis on quality of data versus quantity. As such, the SIEM marketplace promises to be healthy and growing for the foreseeable future.

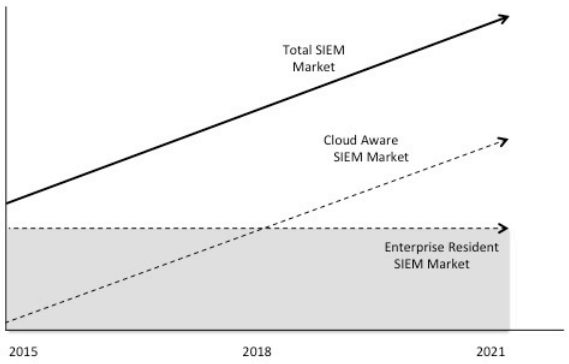

Figure 33-4. Future Trends in SIEM Marketplace

As SIEMs become more cloud aware, the need to recognize and process mobile traffic, IoT traffic, and mobile application-specific security information will grow as well. This will result in richer tools for a greater set of data types including mobile, which uses different endpoint designators, metadata, and so on. Furthermore, SIEM processing will have to deal with the changing landscape that encryption brings to the collection environment. Encrypted traffic will not generate the same types of indicators as clear text data that can be inspected across the enterprise or public network environment. This change might require SIEM connectors to be embedded in the underlying key management infrastructure, which could complicate deployment and operation.

Security Information Event Management Providers

Building a comprehensive list of SIEM providers is a challenge due to the obvious adjacencies with log management, security analytics, and network monitoring tools. CISO teams in the process of source selection for SIEM should use the list below as a starting point, but should recognize that many adjacent components include native or add-on SIEM capability can be obtained in other types of products. Managed service providers such as AT&T also tend to offer SIEM solutions as part of a professional service with attendant human analyst scrutiny on a subscription basis. These are covered in the managed security service section.

2017 TAG Cyber Security Annual
Distinguished SIEM Providers

AlienVault – Roger Thornton, CTO of AlienVault, has been generous in his efforts to help me better understand this vital area. Over breakfast in New York City, and on additional occasions, he's shared his insights with me on the present and future of SIEM, and other aspects of enterprise security. The AlienVault team has also been so helpful in explaining their vision of making SIEM functionality available to security teams of all sizes. Their mission is infectious and deeply influenced the content in this section.
LogRhythm – Mike Reagan from LogRhythm is extremely knowledgeable in all aspects of SIEM, log management, security analytics, and cyber hunting. Discussions with Mike about the impressive LogRhythm platform were invaluable in helping me sort out an area of enterprise security that is both traditional to cyber security, but also fresh and evolving in dealing with modern cyber threats. Sara Czarecki from LogRhythm was also so helpful and accommodating throughout my research.

2017 TAG Cyber Security Annual
SIEM Providers

AccelOps – AccelOps, now part of Fortinet, offers a security information and event management platform, now called FortiSIEM, for enterprise customers.
Alert Logic – Alert Logic provides a managed, cloud-based security information and event management solution for enterprise.
AlienVault – AlienVault offers a unified, flexible security information and event management (SIEM) platform for enterprise customers with support from open source threat feeds. AlienVault includes support for small and medium sized business deployments.
Arctic Wolf Networks – Arctic Wolf Networks provides managed security information and event management service with actionable intelligence.
Assuria – UK-based Assuria sells a cloud-ready security information and event management platform for enterprise.

Astaro – Astaro has a dedicated SIEM function and log management module built into their gateway.
A3Sec – Spanish company A3Sec has a relationship with AlienVault and focuses on SIEM products and services.
BlackStratus – BlackStratus, formerly NetForensics, offers managed SIEM products and solutions for the enterprise.
Correlog – Correlog provides a security information event management component that operates in a mainframe environment.
EMC/RSA – RSA offers the enVision security information event management solution for enterprise.
EventSentry – Chicago-based EventSentry provides a platform for event log monitoring and related real time enterprise security functions.
EventTracker – EventTracker provides SIEM-as-a-Service solution for enterprise customers.
Extreme Networks – Extreme Networks offers its Extreme SIEM based on the Enterasys acquisition.
GFI Software - GFI Software offers IT products and services including email security services, event management, and managed anti-virus.
HPE – HPE offers the industry-leading ArcSight platform, which includes all baseline and advanced SIEM functions. Many of the existing features found in SIEM deployments were either invented or introduced by the ArcSight team.
Huntsman – Huntsman offers the Tier-3 security incident and event management capability.
IBM – IBM offers the QRadar SIEM Q1 through its acquisition and integration of Q1 Labs.
Intel Security (McAfee) – SIEM solutions from the McAfee acquisition remain a component of the Intel portfolio. Nitro Security was acquired in 2011.
Juniper – The Juniper JSA3800 appliance provides both enterprise security analytics and SIEM-like functions.
KEYW – KEYW acquired Sensage in 2012 and offers advanced log and event management solution.
LOGbinder – Delaware-based LOGbinder provides tools for connecting security intelligence to the enterprise SIEM wit focus on Microsoft products.
Loggly – Loggly offers a security and event log management solution for enterprise customers.
LogRhythm – LogRhythm supports SIEM, log management, and network analytics in its enterprise platform. The role of advanced analytics in tools from companies such as LogRhythm is becoming an increasingly important requirement.
ManageEngine – ManageEngine provides the real time EventLog Analyzer, which includes SIEM functionality.
NetIQ – NetIQ provides SIEM-like management functions focused on IAM and operations management.
Prism Microsystems – Prism offers SIEM, IT security, compliance, and log management tools.

SolarWinds – Austin-based SolarWinds offers a SIEM, log, and event management solution on a single virtual appliance. The company bought TriGeo in 2011.
Solutionary – The NTT subsidiary offers a range of managed ActiveGuard SIEM and log management solutions.
Splunk – Splunk offers a set of collection, correlation, and analysis tools for log and enterprise data security investigation.
Sumo Logic – Sumo Logic provides secure, cloud-based log monitoring, management, and analytics.
Symantec – Symantec maintains support for existing SIEM customers through 2017 as it moves focus to other areas.
Tenable – Tenable offers a security information event management solution for enterprise.
TIBCO – TIBCO offers a security information event management solution for enterprise. The company acquired LogLogic in 2012.
Tripwire – Tripwire offers a Log Center solution that includes advanced SIEM functionality.
Trusted Metrics – Trusted Metrics offers a cloud-based security information and event management solution.
Trustwave – Trustwave offers a security information event management solution for enterprise.

Additional SIEM Providers

Logentries – Logentries provides a low cost security information event management product.
Papertrail – Papertrail is an event viewer and log management application available as virtual solution.
Stackify – Stackify offers a developer-centric solution that integrates application log management with Dev Ops.

34. Threat Intelligence

- ⇒ *Actionable* – Cyber threat intelligence provides actionable guidance derived from available security-related data and information.
- ⇒ *Various Methods* – Feeds from trusted sources, sharing among trusted groups, and open, crowd-sourced sharing will drive threat intelligence.
- ⇒ *Growing Need* – All aspects of threat intelligence sharing will grow, limited only by the number of analysts available to interpret collected intelligence.

Threat intelligence services generally involve a real time feed of security-related information to an enterprise for the purpose of supporting preventive or mitigating action. Such intelligence often includes data gathered from the so-called Dark Web, with emphasis on any chatter about a target company, or evidence of stolen

information or customer data for sale by hackers. When threat intelligence services are managed properly, they are tailored to the specific concerns of the enterprise customer and involve sufficient filtering to ensure that the information is both accurate and actionable. When such services are not managed properly, the enterprise receives a useless dump of non-actionable information from potentially dubious sources.

A key insight that most enterprise customers develop after using threat intelligence services for a period of time is that any type of useful intelligence must be *derived* from available information. This implies that the use of threat intelligence services is an *active* derivation process with time, effort, and attention invested by the receiving enterprise. Intelligence is thus not just gathered, but is rather manufactured. Without such enterprise investment of time and effort, threat intelligence service usage often degrades into a *passive* dump of data that has little impact or value to the organization.

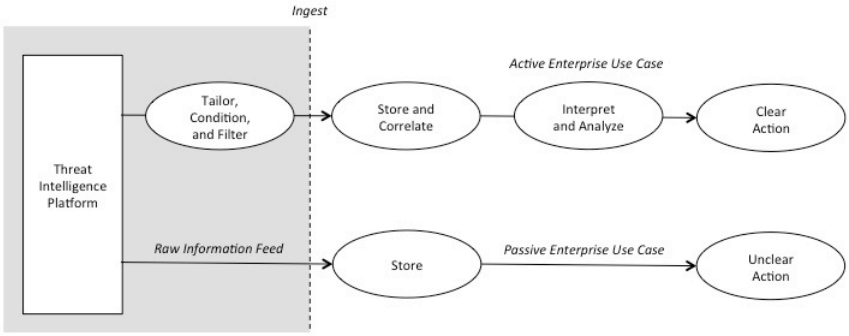

Figure 34-1. Active versus Passive Threat Intelligence Use Cases

Typical features, capabilities, and options one finds in a typical threat intelligence service range from cyber security-oriented services for attack indications and warning, to more business-oriented services that provide competitive intelligence and tracking of partners or other businesses. Many threat intelligence services also provide physical and logistic information for protecting executives or supporting safe employee travel to foreign countries. Ex-Federal Government officials almost always power such services.

Threat intelligence services typically pull a large portion of their data from the Internet, often citing access to the Dark Web. The Dark Net consists of a series of different network clusters of content services that are accessible only with special downloaded Tor software, special configuration, or authorization from the specific Dark Net content provider. The most popular types of information and "services" found on the Dark Net include nefarious sites offering drugs and porn, as well as less disturbing sites focused on hacking and general discussion. It is the hacking and discussion aspect of the Dark Web that is of interest to most threat intelligence firms – not to mention law enforcement.

Some forms of more structured threat intelligence services are embedded into security architectures via live, automated feeds to enhance protection processing. An example would be a structured threat intelligence feed connected in an automated manner to a Web gateway proxy in order to dictate real time information about sites that should be avoided. This type of automated system allows for strong outbound protection in an enterprise for avoidance of exfiltration by advanced malware to uncategorized sites. Such capabilities are usually integrated into the security solution being used, but not always.

Few concepts in cyber security are as universally accepted as the idea of improving the type of cyber threat-related information sharing that occurs between public and private entities around the world. Both preventive security and reactive response benefit from accurate information, telemetry, and signatures about cyber security incidents. Some basic tenets of this information-sharing goal include the following:

- *Sharing Based on Trust* – Senders and receivers need to establish mutual levels of trust for any consequential information sharing. Senders need to know where the information is actually going, and receivers need to know how much confidence to establish in the validity of information being shared.
- *Real Time Sharing* – Timeliness of threat information sharing is generally considered its most important attribute. Staleness grows quickly in signatures, for example, as variants are developed or as offending IP addresses are changed.
- *Structured Process of Shared Information* – The ability to automate the processing of shared information is critical to proper scaling. Any type of structured representation of shared information thus increases the ability of organizations to make practical use of updates, warnings, and signatures.

The US Federal Government – specifically the Department of Homeland Security – has been pushing the idea of standardized threat intelligence feeds for automated consumption. Their proposed approach involves technical specifications such as CybOX (Cyber Observable Expression), STIX (Structured Threat Information Expression) and TAXII (Trusted Automated Exchange of Indicator Information), which define how intelligence is structured for publication, sharing, and automation.

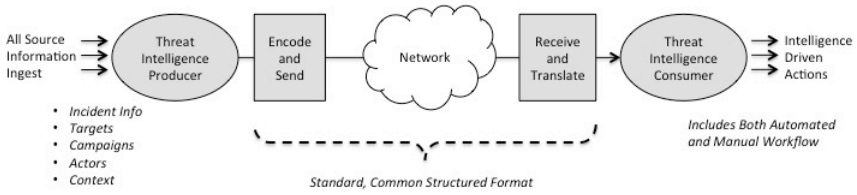

Figure 34-2. Automated Sharing and Processing of Threat Intelligence

The big challenge in the use of automated threat intelligence feeds is the degree of trust that can be placed in the information being accepted. Obviously, in the case of a vendor provided security solution such as a Web security gateway, enterprise proxy, or next-generation firewall, the ingress feed of information is integrated into the product and would thus be as trustworthy as the vendor providing the security solution.

However, in cases where a security team decides to accept peer-to-peer threat intelligence across a grid of participants, questions arise about the validity of the information, the integrity of the sender, and the relevance of information sent from actor A to receiving actor B's environment. Few CISO teams today allow ingested intelligence – other than URL information for proxies or patches downloaded from the vendor – to automatically update equipment and system configurations without attendant human inspection.

An additional question in the automation of threat intelligence sharing is whether the instantaneous nature of indicator sharing is necessary if the recipient uses human-time, manual processes to review and validate received information. In such cases, simple encrypted email would be sufficient for sharing rather than complex, automated protocols.

The market outlook for threat intelligence services is generally favorable, but three distinct market threats should be expected to emerge in the coming years – all with different market paths:

- *Integrated, Trusted Threat Feeds* – The cyber security market will see accelerated growth for integrated, trusted threat feeds from known, vetted sources, especially in the context of cloud integration of feeds from centralized software defined network (SDN) controllers.
- *Feeds for Closed, Trusted Analyst Group Consumption* – The idea that feeds would be created for a closed group of trusted analysts working together is promising. This idea will see steady, linear growth that is limited only by the number and skillset of available analysts globally.
- *Peer-to-Peer Threat Sharing* – Peer-to-peer sharing, with crowd sourced quality control, will see gradual growth, limited by unclear trust models between peers, as well as unclear supply chain legacy for received information.

These three cyber threat intelligence market trends are depicted on the graph below which show emergence from a period of relatively chaotic APT activity with feeds all over the map, to a period of more orderly market clarity with integrated feeds, analyst feeds, and peer-to-peer sharing organized more effectively.

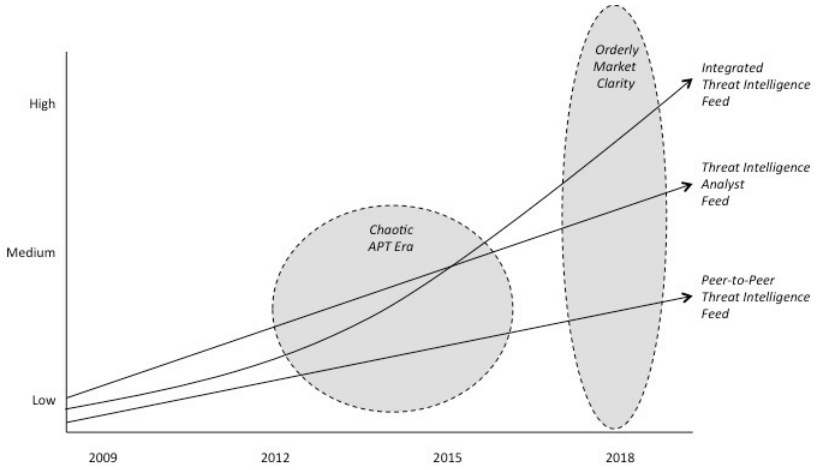

Figure 34-3. Threat Intelligence Market Trends

Certain government agencies, such as the Department of Homeland Security in the US, have created integrated services such as Enhanced Cyber Security (ECS) for commercial entities and Einstein (for government entities) that rely on provision of sensitive, classified threat intelligence. Growth of these types of services will always be limited in their use by the awkward nature of data handling requirements for classified information.

Service providers, for example, are forced to operate the ECS and Einstein functions separately from their normal managed security services. As these services continue to evolve, most likely toward virtual operation, the government's demands that classified signatures be handled in secure facilities will severely restrict the ability of customers to make effective use of these services. Perhaps more important is that commercial entities are gradually reaching the point where their threat intelligence feeds are as good as any comparable provision from the government, even in the presence of classified information.

Threat Intelligence Providers

Inclusion of vendors who provide complementary threat feeds for their products did not seem appropriate here. Instead, the companies listed below are all in the business of providing some sort of threat intelligence product, feed, or service for enterprise customers.

2017 TAG Cyber Security Annual
Distinguished Threat Intelligence Providers

AT&T – Roughly thirteen years ago, AT&T introduced one of the first cyber security threat intelligence services called Internet Protect that was derived from live network telemetry. Marketing that service to CISOs taught me more about the

complex threat intelligence needs of the modern CISO than any inquiry, research activity, and structured investigation ever could have. Now, AT&T has announced a new threat intelligence service called ThreatIntellect that derives its information from the SDN infrastructure. This is a powerful and forward-looking concept, especially in conjunction with AT&T's open sourcing of its SDN controller software. Industry observers should take note of this service, because the direction of traffic management is clearly moving toward SDN controller-centricity in the data center and wide area network.
TruSTAR – My good friend Paul Kurtz, previously one of the cyber security leaders at the White House, was kind enough to share in detail with me the design and operation of his new service TruSTAR. Conceived in conjunction with another industry veteran, Dave Cullinane, former CISO at eBay, the innovative service and supporting infrastructure provide highly secure, community support for automated information and cyber threat sharing. Paul's assistance throughout this project is so appreciated.

2017 TAG Cyber Security Annual
Threat Intelligence Providers

AlienVault – AlienVault includes the Open Threat Exchange crowd-sourced threat intelligence community as part of its range of SIEM and cyber security offerings.
AT&T – AT&T is the first ISP in the world to provide threat information via its virtualized SDN core. The service, called Threat Intellect, is an example of the power of virtualized SDN services for mobile and wireline business support.
BAE Systems – BAE Systems provides a threat intelligence management and analytics platform.
Blue Coat – Blue Coat, not part of Symantec, includes and uses advanced threat analytics as part of its Web security gateway solution.
Blueliv – Blueliv provides an end-to-end cloud-based cyber threat intelligence solution that protects companies from malicious attacks.
Booz Allen Hamilton – BAH provides its Cber4Sight Threat Intelligence offering for the enterprise.
BrightPoint Security – BrightPoint Security, formerly Vorstack, provides real time warning and analytic information related to threats based on peer collaboration, federation, and correlation techniques.
Centripetal Networks – Centripetal Networks provides a real time network protection solution that mitigates attacks at line-speed.
Confer – Confer provides a sensor that is deployed to connect an enterprise to a cyber threat prevention network for early warning and attack detection.
Check Point Software – Check Point Software markets the ThreatCloud IntelliStore threat intelligence platform with live cyber attack threat map.
Corax Cyber Security – Corax Cyber Security provides a range of security threat management and intelligence services using its Corax 360 cyber risk management platform.

CrowdStrike – CrowdStrike bases its endpoint solution on its cloud-based Intelligence Exchange (CSIX) program.
Crypteia Networks – Crypteia Networks provides threat intelligence and related security services to customers across Eastern Europe and EMEA.
CyberInt – CyberInt provides a range of intelligence, monitoring, and consulting services focused on information security and cyber warfare.
CyberUnited – CyberUnited offers enterprise solutions based on threat intelligence, analytics, and machine learning to detect malicious insider behavior.
Cyren – CYREN provides a cloud-based platform that makes threat data available to endpoints.
Cyveillance – Cyveillance uses a proprietary platform and human analysts to develop threat intelligence.
Dell – Dell powers its solutions with threat intelligence from the Counter Threat Unit research team.
Digital Shadows – Digital Shadows offers cyber situational awareness solutions to protect against cyber attacks.
Disrupt6 – Disrupt6 provides threat intelligence based on a subscription feed or from data collected on a deployed sensor network.
Distil Networks – Distil Networks protects Websites from botnets, scraping, data mining, and other fraudulent attacks with advanced threat intelligence.
DomainTools – DomainTools provides a range of domain, network, and monitoring tools for look-up, research, investigation, and threat intelligence.
EclecticIQ – EclecticIQ, formerly Intelworks, provides a range of cyber threat intelligence management solutions.
EmergingThreats – Now part of Proofpoint, Emerging Threats offers security intelligence.
Farsight Security – Farsight Security provides threat intelligence feeds from real time passive DNS solutions.
FireEye (iSight Partners) – Recently acquired by FireEye, has been one of the industry leaders in providing advanced threat intelligence.
Flashpoint – Flashpoint provides cyber ad physical threat intelligence services from the Deep and Dark Web.
Foreground Security - Foreground Security, now part of Raytheon, provides virtual security operations center (V-SOC), managed security services, and threat intelligence.
Haystax Technology - Haystax provides actionable security intelligence and real time situational awareness.
Hold Security – Hold Security is an information security and investigations company providing consulting services and threat intelligence for business clients.
HPE – HPE Threat Central includes actionable threat analysis and intelligence from HPE's cloud-based sharing platform.
IBM – The IBM Security X-Force Threat Intelligence supports IBM platforms with threat data.

Infoblox – Based on acquisition of IID, Infoblox offers a range of threat intelligence services.
Intel Security (McAfee) – Intel offers the McAfee Global Threat Intelligence (GTI) situational awareness service for its Enterprise Security Manager.
Lancope – Lancope, now part of Cisco, provides a StealthWatch platform for providing network visibility and security intelligence for enterprise customers.
Lookingglass – Lookingglass supports threat intelligence management supporting security operations and real time decisions.
Maddrix – Maddrix provides incident response professional services including remediation and threat intelligence.
Malcovery – Now part of PhishMe, Malcovery supplies threat management solutions to support their anti-phishing mission.
Meta Intelligence – Meta Intelligence provides intelligence-based services, cyber risk management, and penetration testing.
NC4 – NC4 provides solutions for sharing and disseminating information related to cyber threats, physical safety, crime, and incident management.
Noragh Analytics – Noragh Analytics offers a data analysis and decision framework for a variety of applications including cyber security.
Norse – Norse is one of the few intelligence providers with capability to report on live network protocol activity such as Border Gateway Protocol.
One World Labs – One World Labs provides enterprise threat intelligence and related security services with emphasis on brand protection.
Pierce Global Threat Intelligence – Pierce Global Threat Intelligence (GTI) provides ranked threat intelligence to help prioritize IT security tasks.
Recorded Future – Recorded Future provides real time threat intelligence to defend an organization.
RSA – RSA FirstWatch involves advanced threat intelligence and security analytics focused on sophisticated threat management.
Security-Database – Security-Database monitors and provides dashboard summaries of vulnerabilities for a variety of products.
Security Tracker – SecurityTracker provides free and premium security threat and vulnerability advisory information.
SenseCy – SenseCy's cyber intelligence provides specific threat information for various sectors.
Soltra – Soltra supports open, automated intelligence with Soltra Edge, consistent with STIX and TAXII specifications.
Spamhaus – Spamhaus is a non-profit organization focused on tracking Spammers and supporting anti-Spam activities across the world through threat intelligence.
SurfWatch – SurfWatch Labs offers comprehensive cyber threat intelligence solutions.
Symantec – Symantec offers DeepSight Intelligence with actionable strategic and technical cyber information.
Taia Global – Taia Global provides a counter-intelligence service that works with a SIEM to provide real time information about threat actors.

ThreatConnect – ThreatConnect consists of a threat intelligence platform (TIP) that empowers large organizations to aggregate and analyze information.
Threat Intelligence – Threat Intelligence provides a range of managed threat intelligence services for the enterprise including penetration testing.
ThreatQuotient – ThreatQuotient (ThreatQ) offers a platform for managing and correlating internal and external threat intelligence.
ThreatStream – ThreatStream offers enterprise class threat intelligence based on data collection, prioritization, and analytics.
Tripwire – Tripwire provides a range of enterprise threat and vulnerability intelligence services.
TruSTAR – TruSTAR provides an anonymous means for sharing of threat and vulnerability information with a community. Former White House official, Paul Kurtz, heads the company.
Verisign – Verisign includes expert cyber threat intelligence services for global enterprise clients.
Wapack Labs – Wapack Labs provides cyber threat analysis, security research, and intelligence services.
Webroot – The Webroot BrightCloud Threat Intelligence Services includes IP reputation services.

Additional Threat Intelligence Providers

OWL Cybersecurity – OWL Cyber security offers a Dark Net threat intelligence platform to allow organizations to better understand their risk.
Silobreaker – Silobreaker provides an app for security and intelligence professionals to keep track of open source data from the Web.
Team Cymru – Team Cymru provides actionable data with the intelligence required to protect an organization.

35. Application Security

- ⇒ *Relevant Area* – Application security has become more relevant and important as attacks have moved up the stack to exploit coding weaknesses.
- ⇒ *Static and Run-Time* – Techniques for addressing cyber security issues in applications involve static and dynamic solutions at compile and run-time.
- ⇒ *Actively Growing Need* – The coming years will see significant growth in application security techniques and methods for enterprise customers.

The purpose of *application security* is to reduce the risk of exploitable software vulnerabilities in application code or its surrounding run-time environment. Some application security methods focus on improving software design and development processes, whereas other methods focus on directly identifying security flaws in the executables. Increasingly, application security controls address the run-time

environment, which complements more traditional software controls that emphasize source code, software process, and compile time safety. All application security methods can be used for the following types of software:

- *Enterprise Applications* – This includes front and back-end applications required for business operations, including legacy mainframe software, physically hosted code in data centers, and emerging virtualized applications. A clear shift is occurring in first or third party developed software from on-premise, enterprise LAN hosting to public, hybrid, or private cloud hosting with mobile access.
- *Web Applications* – This includes front and back-end interfaces, functions, and databases required to provide Web functionality for enterprise marketing, e-commerce, workflow support, and other capabilities. The clear trend here involves Web application virtualization from physical servers to cloud workloads.
- *Cloud Applications* – This includes business and consumer applications being ported to, or developed for public, hybrid, and private infrastructure. Smaller companies, including banks, have already fully adopted publicly accessible cloud applications. As security controls improve for these types of services, larger companies will increasingly move in this direction.
- *Mobile Apps* – This includes the familiar *apps* that businesses and consumers use for entertainment, communication, collaboration, and many other functions. The ecosystem around publicly available apps on app stores from Apple and Google is so mature and accessible that eventually all enterprise application deployment will move to this convenient mobile download model.

Obviously, the best way to reduce application security risk is to prevent flaws from being introduced during design and development – but this is easier said than done. Some methods for preventing application security flaws include investigation of the software process through checklists, interviews, consultations, and data gathering. The resulting information is then synthesized into a score, rating, or maturity level, along with recommendations for process improvement. Example improvements are unit code penetration testing and interim software design reviews. The Build In Software Security (BSIMM) model from Cigital is a prominent example.

Software process improvement is especially useful for so-called *agile development*. Invented to accommodate the unreasonable time pressures placed on the software industry, agile processes involve rapid cycles that are coached along by so-called *scrum masters* who steer the software design and development process on a real time basis with guidance from customers and users. Agile development always results in delivery that is faster than waterfall processes might have produced, but the impact on long-term code quality is debatable.

As a result, application security functionality should be viewed as an essential augmentation to agile development in order to reduce the risk associated

with such process changes. In fact, the case could be made that any organization using agile development methods should introduce application security requirements for functions such as code analysis and process improvement directly into their mandatory security policy.

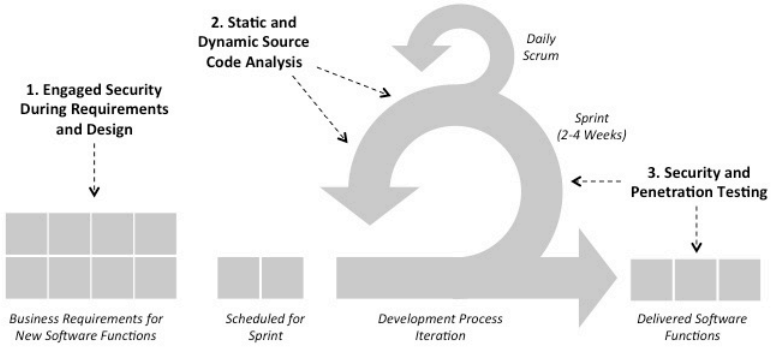

Figure 35-1. Introducing Security Functions to the Agile Software Process

An additional popular approach to application security involves the use of software testing tools to analyze and scan existing code for vulnerabilities. Such analysis can be done statically through design and code reviews, or dynamically through run-time analysis of the application, often in a virtual environment. Both of these techniques are direct descendants of the original Unix *lint* utility developed in the 1970's. Compliance managers are so familiar with application scanning that one should expect this technique to remain in the industry for many years – even if the results from scans are not always perfect.

The challenge with any type of software testing – static or dynamic – is the difficulty in exercising all possible combinations of execution logic that will exist in any non-trivial application. This problem has been a nagging issue in software engineering since its inception, and in spite of vendor claims, significant limitations remain in the ability of any software test environment to demonstrate the *absence* of flaws. Nevertheless, CISO teams are advised to continue making full use of application security testing because they are excellent means for identifying a subset of *existing* flaws. Application scanning and testing will thus remain part of the CISO team arsenal for many more years.

Application security testing methods are often organized into the following two familiar test categories:

- *Behavior Testing* – Involves automated scanning and dynamic assessment based on visible behavior rather than knowledge of the underlying design or code structure. This assessment can and should include both the application and associated run-time environment.
- *Code Testing* – Involves more direct observational assessment of application design with full visibility into software source code to identify potential

vulnerabilities. Companies are increasingly assessing application software executables directly to determine security attributes.

These two types of testing can be performed in unison, but black box testing is best performed in the absence of knowledge about code details. Any insider white box understanding by black box testers can bias the test design and reduce the effectiveness of automated scans. Executable testing requires creative inspection methods, and will sometimes include a quantitative scoring of the application, which is useful for compliance and procurement.

Regardless of the focus, every application security assessment should include structured planning and hierarchical decomposition of all possibilities. The Open Web Application Security Project (OWASP), for example, publishes useful "cheat sheets" for application security assessments to ensure that all possibilities are taken into account.

Application Security Assessment Work Activities:					
Consider Attacks to . . .	Application Platform	Client Software	Network Infrastructure	Server Infrastructure	. . .
Perform Tasks . . .	Binary/Source Analysis	File System Analysis	Runtime Analysis	HTTP/TCP Attacks	. . .

Figure 35-2. Application Security Assessment Work Activities

The market for application security products and services will grow significantly in the coming years as more infrastructure moves from hardware-centricity to software. In fact the designation of the term "applications" will grow from traditional Web or mobile apps to include a much larger set of software including application programming interfaces (APIs), software-defined network (SDN) applications, and virtualized cloud workloads. Furthermore, run-time software validation techniques will merge with network security analytics and other run-time security tools in future deployments so that the inherent security properties of any code to be executed should be analyzed first.

Mobile app security assessment, in particular, will experience steady growth, especially given the complex ecosystem for delivery of mobile apps to individuals and enterprise. Such ecosystem involves the app store infrastructure at companies such as Apple and Google, as well as Web services, embedded browsers, and native code components. Companies specializing in mobile app security are likely to experience significant growth in the coming years, especially as mobile apps find their way to more critical infrastructure usage.

But the most intense hyper-growth will come in the run-time protections required to ensure that applications operate safely and securely during execution.

Containers have been around for a long time, but the trend in run-time application security involves novel techniques designed to inspect, prevent, and contain the operation of an application as it interacts with its environment through execution and function calls.

The resulting technology, often referred to by vendors as *Run-time Application Security Protection (RASP)*, is built with software tools that watch the functional behavior of an application in its environment. If the behavior suggests something that is unexpected or known to be insecure, such as a measurable change in previously profiled function call behavior, then the RASP safeguard might create an alarm to a designated security management function, or might just introduce an in-line functional protection, perhaps using a container to limit any potential damage.

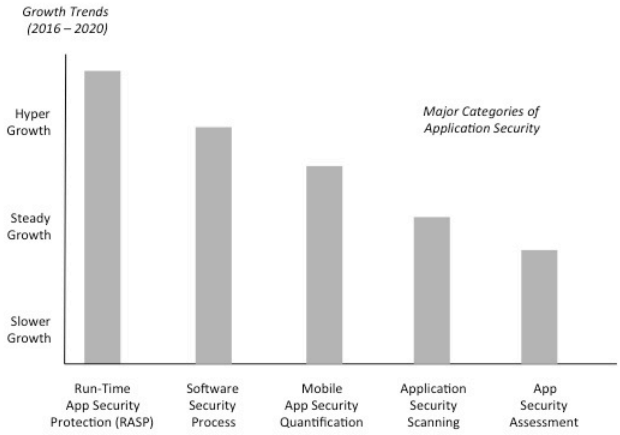

Figure 35-3. Application Security Growth Trends

The intense growth in so many aspects of application security will fuel a busy start-up and venture capital environment. Application security is particularly attractive to smaller entrepreneurs, because the start-up costs for a new business are minimal, with little or no significant capital needs. It is also relatively easy to locate talented programmers who enjoy developing in Java, Python, .Net, and other languages and frameworks. So CISO teams should expect to see a continuing stream of innovative new techniques from companies in this area for many years.

Application Security Providers

The wide range of application security vendors listed below matches the variety of different approaches that can be taken to reduce risk in application software. CISO teams might consider including different solutions in their application security approach, rather than honing in on one to the exclusion of other complementary methods. All security consulting and VAR Security solution providers list application security as one of their offerings, so CISO teams should keep this in mind during

source selection. Requiring application security controls in third party software development and hosting contracts is also recommended for CISO teams. Finally, the mobile security landscape includes vendors such as Appthority who rank applications, and could just as easily be viewed as application security vendors as mobile security vendors. So CISO teams should keep this in mind.

2017 TAG Cyber Security Annual
Distinguished Application Security Providers

Appthority – One of the first experts I called during the initial phase of my research was Paul Stich from Appthority. Paul has extensive management experience in the industry including his time running Counterpane with Bruce Schneier. His company, Appthority, is in the business of helping customers risk score their mobile applications, which requires judgment about virtually every relevant factor in the mobile (and also non-mobile) security landscape. Many thanks are offered to Paul and his team for their support.
Prevoty – One of the most rewarding aspects of researching a massive project such as this 2017 TAG Cyber Security Annual, is the delight one finds in discovering a team of capable individuals doing creative work. Julien Bellanger and Kunal Anand have put together a fine organization focused on developing world-class solutions to improved run-time security, and Roger Thornton from AlienVault serves as an independent director. I certainly enjoyed and benefitted from the several technical deep dives I've had with the company. My interaction with Prevoty has enhanced my research into this growing area – and for this, I express my gratitude.

2017 TAG Cyber Security Annual
Application Security Providers

Appthority – Appthority offers a unique solution for risk-scoring applications based on security factors. The resulting mobile risk management grows in importance as the role of mobile apps grows in the enterprise.
AppSec Labs – AppSec Labs provides research and tool development for mobile application security.
Arxan – Arxan provides run-time protection for applications on mobile, desktop, embedded, and servers.
Aspect Security – Aspect Security provides training, software testing and analysis, and security consulting services to its clients with emphasis on mobile applications.
Beyond Security – Beyond Security offers automated security testing for weaknesses in networks, software, and Web applications.
Black Duck Software – Black Duck Software provides application security, container security, and compliance for open source software management.
Bluebox – Bluebox offers a mobile app security and management solution to protect data.

Capstone Security – Capstone Security offers services in the area of application security, regulatory compliance, and security assessments.
Checkmarx – Checkmarx provides static code analysis tools in support of application security.
Cigital – Software security expert firm Cigital focuses on advancing software security in applications, Web, and enterprise.
Code DX – Code Dx provides tools for static software testing of applications to reduce the likelihood of exploitable vulnerabilities.
Content Security – Content Security provides a software solution for security testing Web applications.
Contrast Security – Contrast Security secures applications from zero day vulnerabilities via interactive application security testing.
Cryptzone – Cryptzone offers secure access, content encryption, and related security solutions useful in protecting the application ecosystem.
Cybera – Cybera provides a secure application defined network (ADN) platform for hosting enterprise applications in the cloud and on-premise.
DBAPPSecurity – DBAPPSecurity provides Web application and database security technology solutions.
Denim Group – Denim Group provides secure software capabilities, including application development, assessment, training, and consulting.
D-Risq – D-Risq provides automated formal analysis tools to improve the correctness of software.
ERPScan – ERPScan offers a suite of SAP security products and services for enterprise customers.
F5 – F5 provides a range of products focused on network security and optimizing the application delivery network capabilities of an enterprise or service provider.
Fortego – Fortego provides computer network operations (CNO) software development, reverse engineering, and cyber security analysis services.
Fortinet – Fortinet offers a range of products including its flagship next-generation firewall for enterprise protection with VPN integration and support for application security.
GreenSQL – GreenSQL provides a database application security solution for data masking, compliance, and database threat protection.
Groundworks Technologies – Groundworks Technologies provides engineering and assessment services including reverse engineering and embedded device security.
HPE – HPE offers the WebInspect dynamic analysis security-testing (DAST) tool for vulnerability discovery and management in Web applications.
IBM – IBM offers the AppScan tool, which tests Web and mobile applications for vulnerabilities.
Include Security – Include Security offers information and application security assessment, advisory, and consulting services.
Indusface – Indusface offers a suite of Web application firewall (WAF), and Web and mobile application testing products.

Klocwork – Klocwork provides secure code analysis tools for software and application security.
Lancera Security – Lancera Security provides a range of services including penetration testing and secure application development.
Layer Seven Security – Layer Seven Security provides a range of SAP security services including application security and penetration testing.
Lookout – Lookout offers a range of mobile and application security solutions for personal and enterprise use.
Marble Security – Marble, acquired by ProofPoint in 2015, provides a mobile application security based on cloud-based threat intelligence.
Metaforic – Metaforic provides technology for software developers to ensure that their code is self-defending.
Minded Security – Minded Security provides software security consulting as well as application security testing tools.
Mocana – Mocana provides a mobile application security platform with support for embedded devices in the Internet of Things (IoT).
N-Stalker – N-Stalker provides a Web application security scanner for enterprise customers through the entire Secure Web development lifecycle.
Onapsis – Onapsis supports protection of SAP applications and processes from vulnerabilities.
Penta Security – Penta Security is an IT security firm offering Web application security, database security, and single sign-on solutions.
Port80 Software – Port80 Software provides Web application security and performance solutions focused on Microsoft Internet Information Services (IIS).
PortSwigger – PortSwigger offers the Burp Suite Web application security testing software solution.
Pradeo – Pradeo provides a suite of mobile application security testing tools and APIs.
Prevoty – Prevoty offers a run-time application security solution for the enterprise. The RASP product includes both application monitoring and dynamic protection.
Protected Mobility – Protected Mobility offers solutions for mobile app security including a secure SMS service.
Quotium – Now part of Synopsis, Quotium provides an automated continuous, DevOps ready interactive application security testing solution.
Radware – Radware offers a suite of security services focused on application delivery and load balancing, web application firewall, and other areas.
Rapid7 – Rapid7, which acquired NT OBJECTives, provides vulnerability management, penetration testing, and application monitoring security solutions.
SafeBreach - The SafeBreach platform executes breach methods on a target system to identify potential weaknesses.
Saviynt - Saviynt provides cloud access governance and intelligence for data protection, privacy, and regulatory requirements.
Security Innovation – Security Innovation provides application security-focused awareness training and related products and services.

Sentrix – Sentrix provides cloud-based Web application security and DDOS solutions for the enterprise.
Sonatype – Sonatype provides open source dev/ops tools including Nexus firewall for software development organizations.
Synopsys – Synopsys provides a range of application security protections from several recent acquisitions.
Trend Micro – TrendMicro provides a range of enterprise and cloud security solutions that are applicable to application security.
TrulyProtect – TrulyProtect provides an encryption-based software data security solution that integrates with various applications to protect IP.
TrustWave – TrustWave provides solutions based on the acquisition of Application Security Inc. in 2013.
Veracode – Veracode offers enterprise, Web, and mobile application security solutions to detect weaknesses.
Virsec – Virsec provides next-generation data breach protection for applications including virtual patching.
Virtual Forge – Virtual Forge offers a range of security solutions for SAP applications.
Waratek – Waratek provides application security through runtime application self-protection for Java as well as containers.
White Cloud Security – White Cloud Security provides blocking of untrusted application executables and scripted malware from running.
whiteCryption – whiteCryption (formerly Cryptanium) provides code integrity protection for apps, as well as a white-box cryptography library.
WhiteHat Security – WhiteHat Security supports discovery and continuous scanning of Web applications.

Additional Application Security Providers

CIX Software – CIX Software is a small promising start-up just emerging from stealth in Weehawken, New Jersey. The CIX team is working specifically in the area of RASP with principals from the financial industry.
Coverity – Coverity provides a range of software application testing tools for static analysis.
Parasoft – Parasoft offers virtualization, API testing, and development testing software solutions.

36. Content Protection

⇒ *Content Value* – Content has value in any context, including enterprise, due to the replacement costs and potential marketability to customers.
⇒ *Protection Approaches* – Digital Rights Management (DRM) protects content through a combination of encryption and access rights policies.

⇒ *Complexity Management* – The future success of enterprise DRM will require improved means for controlling and managing complexity.

Content is generally differentiated from *data* by its human origination. That is, when human beings use their creativity, intelligence, bias, opinion, inspiration, feelings, knowledge, and determination to construct great (or not so great) pieces of writing, music, and film, then the resulting content has value for two reasons: First, human effort went into its creation, so the replacement value can be considerable; and second, customers and users will pay money for that content, simply because the inspiration, knowledge, emotions, and feeling might be transferable.

Sadly, this long-held understanding that customers and users can and should pay money for human developed content is no longer generally accepted by all generations. Youngsters, for example, have grown up with the odd notion that electronic assets are not tangible assets and that the idea of having to pay for music or other creative items is abhorrent. This belief results in teenagers – ones who would sooner die than steal a candy bar from a supermarket – thinking nothing of stealing John Mayer's latest single from an illegal Internet download site.

Great effort has thus gone into developing techniques for protecting content, not only from hackers, but also obviously from the general public. Since businesses also have creatively inspired content – albeit somewhat different from music and film, the protection methods used in all creative industries can be extended to the enterprise for their intellectual property. Most of the time, these techniques make use of encryption, rights management, and policy-based controls. But strong legal consequences can also be a deterrent.

More specifically, the basic security model for *content protection* involves content owners assigning access and usage policy rules for how their content is utilized. Such access and usage policy rules are then embedded into the content usage environment for enforcement. The concept is most frequently applied to the protection of music, entertainment, and books through download to devices such as smart phones and tablets, but as suggested above, it has extended to the enterprise for business intellectual property. Policy rules must be implementable, which means you can't prevent grumpy people from listening to your song or reading your marketing materials. Policies must also be legal, which means you cannot discriminate.

The most commonly used technology for content protection is called *digital rights management* (DRM), and this combines data encryption with third-party support for how content is packaged and used to enforce access policies. Certain types of usage in this context are hotly debated across the global community, with some contending that DRM protects artists from theft and infringement, whereas many others believe it inconveniences legitimate users and stifles innovation. The latter view is more common and the general public often views DRM protected entertainment as evil. This is not the case, however, for enterprise DRM deployed by CISO teams – although the word "evil" is often muttered under the breaths of administrators trying to successfully scale DRM across a complex enterprise.

The technical basis for DRM protection involves a content creator restricting access to only users who have authenticated with some first or third party authority that is managing content licenses. The DRM involves a file header, which includes sufficient information for users to contact the license server and decrypt the file for usage. A major problem is that different DRM providers do not coordinate their technology or protocols, resulting in users having to handle and use content in many different ways across their Android, Apple, Microsoft, and other devices and computers. One might speculate that better DRM standards could result in the general public viewing the technology as less evil, but perhaps this is even too optimistic.

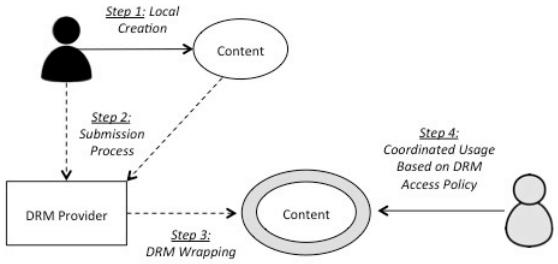

Figure 36-1. Basic DRM Concept

As suggested above, CISO teams typically do not have to take any potentially controversial political or philosophical position on the DRM debate with respect to artistic content. They do, however, have to make a decision about the use of *enterprise DRM* for the intellectual property content created, stored, and shared in the organization and with partners and suppliers. In this age of APT attacks aimed at any form of valuable intellectual property, it is surprising that all CISO teams are not being more aggressive in their investigation of DRM for the enterprise. Furthermore, the topic almost never comes up during corporate security audits.

Enterprise DRM, sometimes also referred to as *information rights management* (IRM), applies to files and documents created using Microsoft Word, Excel, PowerPoint, Adobe PDF, and other common business tools. The use of enterprise DRM focuses on stopping unauthorized distribution, unauthorized copying or modification, and unauthorized printing or screen shots. Enterprise DRM also creates document usage logs and file watermarks to further support the security process.

The challenge with enterprise DRM is not related to the debate about the appropriateness of the technology, but rather the underlying complexity required for proper management (hence the joke earlier about "evil" administration). That is, DRM involves public key infrastructure (PKI) support across sharing domains, and the security community has always had trouble with this method. Even within an enterprise, the underlying rights management and PKI support are difficult to manage, and especially hard to scale across a large organization. If a CISO team

member proposes use of enterprise DRM, it thus pays to focus discussion and questioning around complexity management.

The basic concept for enterprise DRM involves day-to-day creation and sharing of business documents with coordinated assignment of appropriate rights for users. Rights can be defined at the discretion of the users, or constrained by the mandatory policy of the organization. In either case, binding rights to business documents as they travel to external sharing partners is especially difficult. Local users can be trained and provided support for DRM-protected information, but sharing partners might not have the same level of knowledge or assistance.

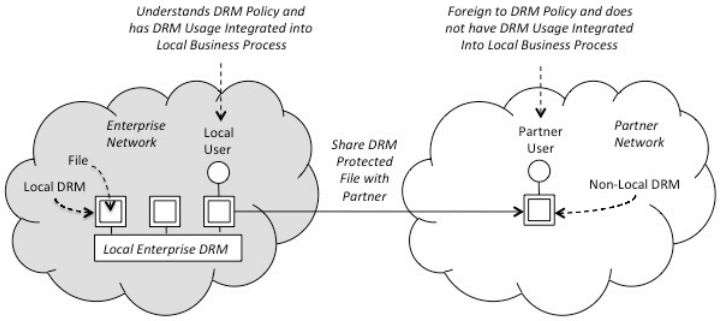

Figure 36-2. Enterprise DRM Concept

The complexity challenges associated with managing and scaling enterprise DRM across an organization and with external partners have been so intense that many CISO teams have simply avoided deployment. This is a shame, because enterprise DRM is an effective means for controlling data leakage, avoiding customer information breaches, and stopping sensitive data theft – all of which have been significant problems for businesses and government agencies over the past decade.

Consider, for example, that a lateral APT attack happening upon a file share with DRM-protected data will probably not result in a data exfiltration. The APT intruder would begin the search phase of the attack after having gotten internal access, only to find that the interesting intellectual property requires DRM-related authorizations – hence the exfiltration process, in theory, would stop. So the cyber security motivation should be sufficiently present to make DRM work in the enterprise.

The future of enterprise DRM will be mostly dependent on how easily the technology can be integrated into day-to-day usage and sharing within the organization and across external domains. It will be a technology that requires integration with secure file sharing, public and hybrid cloud usage, and mobile device management – each of which also share their own complexity challenges. The vendors that will succeed in the enterprise DRM market – which must be viewed as having *significant upside growth potential* – will be the ones that focus on ease of installation, maintenance, support, and usage within the organization and across external usage.

Content Protection Providers

The content protection vendors listed below, most of which provide some form of DRM, include vendors who focus on protection of artistic content, as well as one providing enterprise DRM for intellectual property. The technology for both cases is closely related, but the underlying infrastructure and user support in each case are fundamentally different. Moving forward, the distinction between DRM for user content and DRM for enterprise files will grow more significant based on the need to focus on infrastructure support in enterprise DRM.

2017 TAG Cyber Security Annual
Content Protection Providers

Amazon Web Services (AWS) – Amazon offers a range of different DRM options for content users as well as for AWS infrastructure services.
Armjisoft – Armjisoft provides a range of digital rights management (DRM) solutions for license protection, watermarking, and related protections.
Arxan – Arxan provides two-tiered software-based application and key protection for digital media.
ContentGuard – ContentGuard provides a range of digital rights management (DRM)-based content management technology solutions.
Content Raven – Content Raven provides cloud-based solutions for protecting the distribution of files to internal and external groups for enterprise customers.
docTrackr – docTrackr, from Intralinks, provides a solution for controlling and managing document security in Gmail extensions, Web applications, for API-based and custom solutions.
Fasoo – Fasoo supports continuous encryption, permission control, and enterprise DRM solutions.
FinalCode – FinalCode provides an encryption-based solution for secure file sharing in enterprise.
GigaTrust – GigaTrust offers its customers a range of pervasive content management solutions.
Google – Google includes Widevine DRM protections in its device, application, system, and content ecosystem.
HoGo – HoGo provides a digital rights management (DRM)-based solution for protecting and sharing documents.
Inside Secure – Inside Secure provides a range of embedded security solutions for mobile payment, content protection, secure access, and IoT.
InterTrust – InterTrust Technologies invents, develops and licenses software and technologies in the areas of content protection, cryptography, and digital rights management (DRM). Dave Maher, formerly of AT&T Bell Laboratories, is a principal in the firm.

Microsoft – Microsoft provides computer software, consumer electronics, and personal computer services including IT security and content protection.
NextLabs – NextLabs supports a range of enterprise digital rights management solutions.
Rightsline – Rightsline provides a digital rights management (DRM) solution for tracking and managing contract and royalty rights with emphasis on media and entertainment.
SafeNet – SafeNet, now part of Gemalto, acquired Alladin and Beep Science to integrate software digital rights management protections into their range of content protection offerings.
Sansa – Sansa, formerly Discretix, provides embedded security solutions for device content protection, platforms, and chip manufacturers supporting IoT.
Terbium Labs – Terbium Labs provides a fingerprinting solution that can detect stolen intellectual property.
Trend Micro – Trend Micro describes its endpoint and related security solutions as content security.
Vitrium – Vitrium provides document security and digital rights management protection for PDF files.
Watchful Software – Watchful Software provides DRM-based data security solutions for enterprise customers.

Additional Content Protection Providers

Adhaero – Adhaero Doc supports encryption and control of Microsoft Office and Microsoft Outlook documents throughout their lifecycle.
aegisDRM – G-Tech offers aegisDRM product that supports security control for Microsoft Word documents and other Office products.
Apple – Apple supports DRM for its range of devices, computers, systems, applications, and support. Many Apple users complain about the tight DRM controls inherent in the access and use of content.
Appligent – Appligent supports a range of enterprise DRM protections for PDF documents.
Araloc – Araloc offers a range of secure content management, distribution, and file sharing for board management, sales management, and related applications.
Artistscope Copysafe – Artists Copysafe offers a Web plugin in all popular Windows Web browsers to protect media from unauthorized copy, printing, or screen capture.
Axinom – Axinom offers a multi-DRM service in the cloud built on MPEG and supporting Microsoft PlayReady, Apple FairPlay, and Google Widevine.
Aspack – Aspack provides its ASProtect solution for software protection with registration keys.
Bisantyum – Toronto firm Bisantyum offers distributed DRM management using block chain technology.

CryptKey – CryptKey provides a range of software licensing and software copy protection options.
Defective By Design – Defective By Design is a grassroots organization that opposes DRM and provides on-line support in opposition of the technology for devices and media.
Dubset – Dubset offers secure distribution solutions for artists, labels, and producers.
DRM NZ – DRM NZ provides DRM support services for content creators, managers, and owners.
EditionGuard – EditionGuard consists of a secure eBook distribution platform with selling tools and DRM.
EMMS – Emacs Multimedia System software supports the playing of multimedia files from Emacs using external players. It is delightful to see tools such as Emacs continue to find use in a new generation.
EZDRM – EZDRM provides a digital rights management solution to protect digital media.
Fadel – Fadel supports management of intellectual property via digital asset rights in the cloud.
FileOpen – FileOpen consists of an Adobe Acrobat plugin that ensures that digital publications are not redistributed.
Foxit – Foxit offers its customers a range of secure PDF protection solutions including readers.
GiantSteps – Management consultancy GiantSteps focuses on protection for the content industries.
Haihaisoft – Haihaisoft offers the DRM-X digital rights management solution to protect digital content products.
Identify3D – Identify3D provides intellectual property protection, quality assurance, and data security through all phases of digital manufacturing.
Link Data Security – Link Data Security provides copy protection for CDs, DVDs, USB, and Web.
Liquid Machines – Liquid Machines develops enterprise rights management software to protect corporate assets.
Locklizard – Locklizard provides DRM software for complete document security and copy protection.
Lockstream – Lockstream offers DRM solutions for ringtones, music, and mobile games.
OpenText – OpenText provides a rights and content management platform for cloud, Oracle, Microsoft, and other software suites.
Rchive – Rchive consists of a copyright protection system for securely sharing, tracking, and revoking access to screenplays.
SecureMedia – SecureMedia provides a security system for encrypted distribution of digital content.
Sealedmedia – Sealedmedia offers a range of digital rights management software solutions.

Sofpro – Sofpro offers a range of software copy protection and licensing solutions for Windows and .NET framework applications.
Softwarekey – Softwarekey supplies Protection PLUS software licensing and server licensing automation technology.
Source3 – Source3 provides an advanced platform and licensing and distribution of 3D content.
Valve – Valve develops Steam, which is an Internet-based solution for games and software that are DRM-free.
Vaultize – Vaultize supports enterprise secure file sharing solutions through DRM support.
X-Formation – X-Formation offers a range of software license management solutions in its suite.

37. Data Destruction

⇒ *Destruction Emphasis* – CISO teams have not sufficiently prioritized emphasis on assuring that data is physically destroyed in a secure manner.
⇒ *RIM Policies* – Records Information Management (RIM) policies are often so convoluted as to degrade the organization's willingness to destroy records.
⇒ *Destruction Methods* – Several secure methods exists for safely and efficiently destroying data from potential theft and abuse.

Data destruction is a critically important security function in every enterprise organization, but is rarely treated as an explicit, strategic component of information security programs. Instead, IT systems and operations managers will generally perform ad hoc management of data destruction, perhaps not even taking thoughtful steps to properly dispose of data no longer needed in an organization. The resulting risks are often invisible, since it is so hard to track and trace lost intellectual property to equipment and media that were not properly destroyed after their period of usefulness expires.

Specifically, the destruction of unneeded data from disks, tapes, and other storage media must be performed by enterprise IT or security managers in one of three different manners:

- *Software Overwriting* – This process involves overwriting applicable memory to ensure that target files for removal cannot be retrieved.
- *Media Degaussing* – This process involves magnetic destruction of stored data using appropriate field strengths.
- *Media Shredding* – This process involves mechanical destruction usually with shredders that render the storage media irretrievable.

The two biggest advantages of the software solution to data destruction over physical media shredding are the environmental impact reductions and the

hardware replacement cost avoidance. A major disadvantage of the degaussing solution is that it cannot be used for optical and solid-state storage devices. These three practical methods for destruction of data from storage media are depicted below.

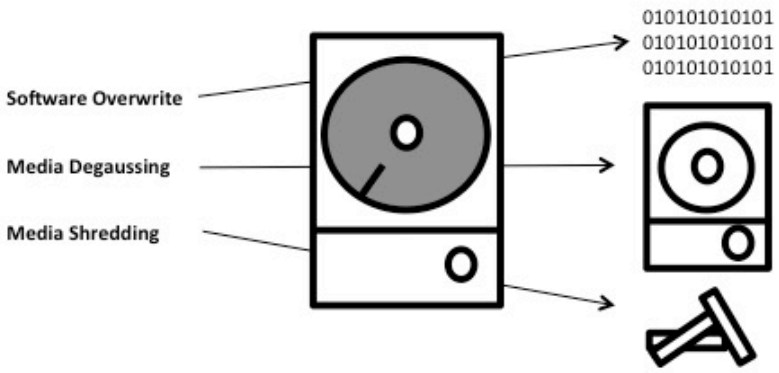

Figure 37-1. Data Destruction Options

Companies generally view data destruction as consisting of two basic activities: (1) data center administrators (usually not including input from the CISO team) *maybe* following one of the three data destruction options shown above to get rid of old, unnecessary data and to reduce storage costs, and (2) employees making local decisions about what to delete and what not to delete from directories on PCs, cloud services, file shares, and other accounts.

In the first case, it is not uncommon in many companies for old PCs and media to be sitting in closets or storage areas, perhaps in poorly marked cardboard boxes. With the rise of mobility, older cell phones are sometimes even prominently displayed in offices and cubicles as a visual tribute to the progression of technology with time. Furthermore, bags or boxes of scattered memory sticks are often found in desks, drawers, and closets in many organizations. The decision to not properly destroy this older media – including the decision to not securely wipe, reimage, and reuse the media – is a clear security risk that exists far too often.

In this second case, two specific problems emerge. First, normal deletion of a file from memory on a typical machine does not, in fact, actually remove the file. Instead, typically the memory containing the deleted file would be released, but not overwritten. As such, advanced persistent threats could actually retrieve deleted information using commercial recovery tools. This underscores the importance of proper software overwriting as the optimal way to remove information without corrupting or destroying hardware.

Second, most organizations include a specific IT policy on records and information management (RIM) that dictates what type of data should be retained and what type of data *can, should, or must* be removed. The problem with most RIM policies is that they do not dictate proper data destruction and they leave the "*can,*

should, or must" decision to the employee, rather than just demanding that unnecessary data should be removed. As any CISO team member knows, if such policy is left up to lawyers, all data would be maintained forever – and this becomes a security disaster.

The recommendation here is that CISO teams take the time to ensure that proper technical means are being used for data destruction, and if possible, to codify such action into organization security policies, especially for records and information management. To the degree that practical guidance is needed for the groups or individuals performing the data destruction, the following tips might be included in policy or training materials:

Threat Assessment – Organizations destroying data from stored media will have different threat vectors. Retail companies, for example, will have a different set of threats than a government intelligence agency, which will have more formal, legal obligations for data destruction. Organizations with a less intense threat will have the luxury of making decisions based on cost, convenience, and environmental impact more easily than groups under more intense threat pressure.

Media Reuse – The overwriting method is optimal for reuse of media. Degaussing can, and destruction will, render media non-reusable after data destruction. CISO teams should consider this factor carefully when selecting a suitable data destruction method. This is an especially important consideration if mobile devices with application credentials and passwords are recycled or sold for external use. Policies should be in place from the CISO team that any piece of equipment with storage of, or access to, critical infrastructure components, must have its data destroyed in the most secure available manner.

Given the growing need for enterprise organizations to create more stringent practices around all aspects of data destruction, future trends in this area suggest greater attention to the following:

- *Enterprise RIM Policy Emphasis* – More companies will include proper data destruction as a component of their records and information management (RIM) policies. It seems negligent that so many security programs do not have direct influence on the local RIM policy. CISO teams need to start working with their legal team to make sure data retention policies do not go too far in demanding storage forever. If the lawyers control this decision, then the security risk to the organization will almost certainly be too high.
- *Proper Data Destruction Methods* – More companies will begin to recognize the threats of recycled equipment and will begin paying closer attention to proper destruction methods. The US National Security Agency (NSA) has developed standards for how data and equipment are properly destroyed. The National Association of Information Destruction (NAID) also provides procedure certification. CISO teams should seek compliance with these standards from their data destruction vendors.
- *Required Removal of Unnecessary Data* – More third party buyers, partners, suppliers, and agencies will find themselves subject to stringent

requirements for proper data destruction of equipment to reduce the disclosure risk. As such, third party controls for development, customer support, or other activities will begin routinely including secure data destruction and handling requirements for any equipment related to the supported or outsourced service.

The progression of these three data destruction trends is depicted below from present to 2020.

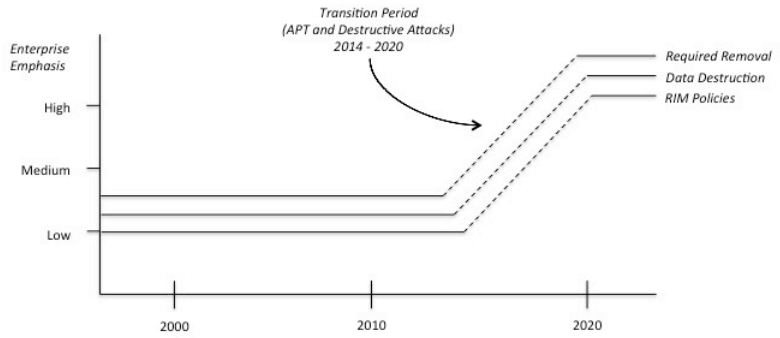

Figure 37-2. Trends in Enterprise Data Destruction

The outlook for companies providing data destruction products and services is generally positive for the next decade. Increased emphasis from CISO teams will lead to new sales, increased practical usage, and more intense pressure to integrate data destruction and RIM into security policies and practices. One can also expect government and federal regulations in this area to intensify as well. The result is that data destruction product and service vendors are likely to thrive and grow in the coming years. One point of differentiation is that with many data destruction companies following somewhat clumsy processes such as sending a large truck to the customer site for the manual destruction, companies that can find a more efficient way to do this will have a great business advantage.

Data Destruction Providers

The following companies provide data destruction product and service solutions for the enterprise. Many of them include on-site services where information, media, documents, and equipment can be destroyed securely, albeit somewhat clumsily (i.e., staff carrying bags and boxes of paper to the parking lot). Small local businesses supporting data destruction abound in virtually every city or every country, so the list below is just a small percentage of the full list of global data destruction providers. CISO teams should ask around to get a good list of local businesses that might be suitable for their needs. By the way, virtualized solutions for data destruction have not been generally available (perhaps not yet invented), so

innovation in this area is expected and welcome. CISO teams should also note that data destruction, digital forensics, and data recovery products and services are often related and offered by a common vendor. This observation might provide some assistance in the source selection process and might offer opportunity to negotiate data destruction as part of an existing forensic or recovery contract with a vendor.

2017 TAG Cyber Security Annual
Data Destruction Providers

Altep – El Paso-based Altep provides digital forensic and data destruction services with an associated consulting practice focused on cyber security.
Applied Magnetics Lab –Baltimore-based Applied Magnetics Lab manufactures military security and data destruction equipment.
Data Devices International – Located in San Marino, Data Devices International provides secure data destruction, degaussing, and hardware destruction services.
Data Security Inc. – Located in Lincoln, Nebraska, Data Security provides products for securely erasing and destroying data stored on hardware media.
4Secure – 4Secure provides security consulting and training for clients across Europe. The company also provides a hardware data erasure tool.
Garner Products – Located in Roseville, California, Garner Products includes professional data destruction for high security wiping.
Guardian Data Destruction – Long Island City-based Guardian Data Destruction specializes in on-site data destruction, computer system decommissioning, and data logistics.
Heshengda Information Security – Beijing-based HSD is a manufacturer of information destruction devices including degaussers, data disintegrators, and data erasers.
Iron Mountain – Located in Boston, Iron Mountain is an industry leading information disposal, destruction, and management firm. Iron Mountain seems to stand out for its wide range of products and services for enterprise customers in this important area.
LSoft – Canadian firm LSoft provides a suite of tools for data recovery, security, and backup.
Secudrive – San Jose-based Secudrive provides USB data leakage prevention and advanced data security solutions including disk erasure.
TechFusion – Cambridge-based TechFusion offers data forensics and eDiscovery services including erasure verification and evidence preservation.

Additional Data Destruction Providers

All Green – All Green provides secure and certified data destruction and on-site hard drive shredding services.

Brass Valley – Brass Valley is a comprehensive IT solutions and services firm with solutions for data destruction.
Corporate Business Services – Corporate Business Services provides hard drive shredding and related services.
CloudBlue – CloudBlue provides IT asset disposition, on-site data destruction, and IT lifecycle support.
Data Destruction – Data destruction offers hard drive shredding, paper shredding, and electronic recycling.
Data Killers – Data Killers includes on-site shredding and degaussing of tapes and hard drives.
4thbin – 4thbin provides a range of certified and secure data destruction services in New York.
IntelliShred – New Jersey firm, IntelliShred, offers a range of on-site shredding services.
Kroll Ontrack – Kroll Ontrack includes a range of recovery, restoration, collection, review, discovery, and erasure services.
Nexcut – Nexcut provides its customers with hard drive and digital media shredding services.
Phiston – Phiston offers high security data destruction including hard drive destruction.
ProShred Security – ProShred Security provides on-site shredding in the New York area.
ProTek Recycling – ProTek Recycling offers hard drive and data destruction including desktops, laptops, and servers.
Rockland IT Solutions – Rockland IT Solutions provides data destruction, data erasure, and document shredding.
Seagate – Seagate is a major American storage company offering a range of business products and services.
Securis – Securis provides a range of IT asset recycling and data destruction services for businesses.
Shred-it – Shred-it offers a range of hard drive destruction services for obsolete data storage.
Sims – Sims offers several on-site data destruction services for magnetic and solid state devices.
Solstice Technologies – Solstice Technologies supports degaussing of USB, SD card, flash, and other media.
Systems Maintenance Services – Systems Maintenance Services includes IT asset disposition as part of its range of services.
TBS Industries – TBS Industries is a full-service computer recycling company supporting data destruction.
Verity Systems – Verity Systems is a manufacturer of magnetic media bulk erasers for data destruction.
Whitaker Brothers – Whitaker Brothers supplies paper shredders, folder, and other business equipment.

White Canyon – White Canyon offers solutions for wiping hard drives and recovering files.
Wise Data Recovery – Wise Data Recovery offers a range of freeware for recovering deleted files.
World Data Products – World Data Products delivers refurbished equipment based on sales of used hardware.
ZLOOP – ZLOOP offers a range of data destruction and hardware recycling products and services.

38. Data Encryption

⇒ *Enterprise Use* – Encryption is more vulnerable in practice to sloppy administration at the endpoint than cryptanalytic code cracking weakness.
⇒ *Taxonomy* – A large selection of different data encryption solutions exists for the specific data protection needs across an enterprise.
⇒ *Growth Trends* – Encryption solutions will continue to grow in relevance and need across the global cyber security community.

The most fundamental and traditional means for data security is *cryptography*, which can be defined loosely as the science of making codes. The corresponding means for breaking data security is *cryptanalysis*, defined loosely as cracking codes. Most CISO teams will never have to worry about making or breaking codes. The emphasis in practice is much more on the selection and operation of systems that make use of existing cryptography, rather than on the design of new ciphers.

Academics and researchers tend to way over-emphasize the importance of rock-solid cryptography with domain sizes for keys that ensure full protection from the best crackers. In practice, cryptanalysis is almost never an issue at the enterprise level (other than having to deal with vocal academics and researchers demanding better cryptography). Rather, poor endpoint administration and set-up are much more common means by which bad guys gain access to protected data. If your crypto scheme was broken, then the chances are much higher that you were just plain sloppy with system or network administration, than that your encryption algorithms were too weak or key sizes too small.

Data encryption and decryption (herein referred to collectively as *encryption*) allow for scrambling and descrambling content, usually via algorithms that rely on managed keys for secrecy and proper handling. Data encryption can be applied to many different applications including the following:

- *Stored Data* – Includes personal or enterprise data that resides in files, databases, or other storage media. The encryption can be done at the application level, system level, or even hardware level – as is found in hard drive encryption solutions. Software applications provide access to this data from work centers, customer support groups, development teams, and so on.

- *Network* – Includes encryption of data in motion across a wide area, local area, or mobile network. The intent of encrypting network traffic is to reduce the threat of man-in-the-middle eavesdropping attacks.
- *Video* – Includes encryption of traditional video broadcast transport as well as IP-based provision of video over data networks. Video traffic types can range from entertainment content to live security surveillance.

Encryption in these areas requires key and certificate management support at the local and infrastructure levels. A conundrum of modern security certification and regulation is that auditors rarely ask how and where keys and certificates are managed and protected. Companies like Venafi offer valuable enterprise protection solutions in this area, and CISO teams are advised to stay ahead of this vital task. Not knowing where your keys are located, or having weak means for validating certificates, are examples of sloppy enterprise security.

Weaker scrambling such as data masking or suppression also play a role in some contexts. Contact centers, for example, sometimes provide too much information to operators, especially in outsourcing deals. Masking portions of sensitive customer records on operator screens can reduce this risk. The likelihood of cryptanalytic attack in this case is low, so CISO teams can select whatever method is easiest, as opposed to the normal obsession security experts are forced to have around assurance of the highest level of security in all cryptography usage.

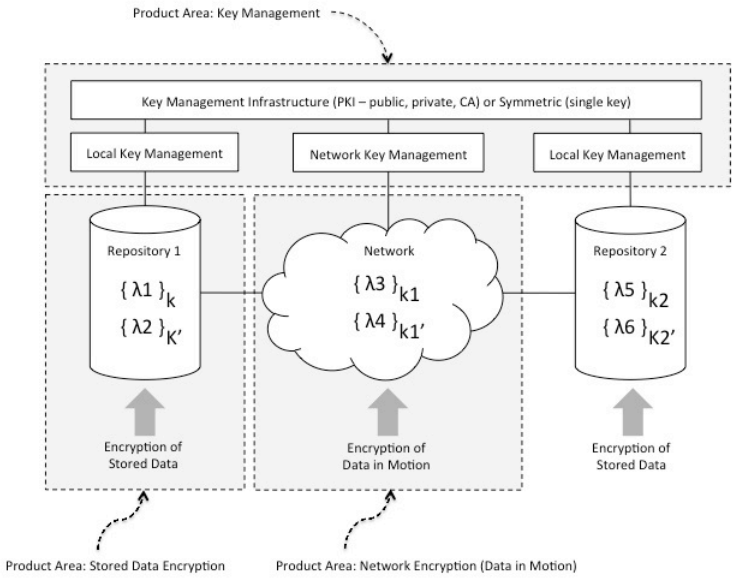

Figure 38-1. Encryption Product Areas Addressed

To date, the availability of high-quality encryption and key management technologies has not been an issue in any sector; rather, individuals and enterprise teams have had more trouble *integrating* different existing encryption tools and

systems into coherent, practical methods. In addition, large-scale infrastructure, technology, and software providers have not had sufficient motivation to offer broad key management infrastructure solutions across industrial, political, and government sectors.

This implies that the most useful innovation in encryption has corresponded to improved usability, broader interoperability, and ease of integration, rather than on pure cryptographic strength. Furthermore, key management continues to serve as a nagging barrier to many types of innovations such as secure business-to-business email communications. As such, innovations in key management infrastructure are welcome and will serve as important differentiators moving forward.

An additional factor worth noting is that as Big Data applications continue to expand in virtually every business sector around the world, the need will increase for super-fast cryptographic solutions that can operate on enormous quantities of data with the ability to focus on record or field levels of obfuscation. Many encryption product vendors are already beginning to focus on these performance needs of larger data sets.

CISO teams should make sure to investigate the eDiscovery and forensic implications of any selected data encryption solution. Many organizations have strict enough requirements or regulations on eDiscovery and data forensics to warrant additional investigation into selected encryption methods. Some solutions simply do not provide sufficiently flexible support for enterprise discovery. Teams should also recognize that a large assortment of free encryption software is available – Silver Key Free, VeraCrypt, Kryptelite, DeepSound, CloudFogger – that might be sufficient for lower intensity file encryption needs. The obvious advantage here is much lower cost.

The data encryption marketplace includes so many different products and services that it is instructive to create some structure around what is available. The taxonomy below provides a reasonably comprehensive view of encryption solutions, including both enterprise and consumer focus, as well as SSL/CA. The taxonomy includes technology, tools, and services that focus on encryption, rather than products and services, which happen to use encryption, such as secure file transfer.

Product	*Primary User*	*Description*	*Sample Products*
File encryption	Consumers	PC data protection for user files and folders	Folder Lock, Advanced Encryption Package Pro, Dekart Keeper
Disk encryption	Enterprise	Hard drive protection for PCs and other devices	CheckPoint Full Disk Encryption, BitArmor, McAfee SafeBoot
Data encryption	Enterprise	Data protection for business applications	Symantec (email, file, drive), Sophos SafeGuard
Database encryption	Enterprise	Database protection for fields and records	Vormetric, Microsoft, Oracle TDE
Encryption toolkits	Developers	Encryption toolkits for software developers	PKWare, Cryptlib, Dmoz, Lantronix
Email encryption	Enterprise, Consumers	Encryption toolkits for encrypting email	HP SecureMail, DataMotion, Proofpoint, EdgeWave, Privato
Cloud encryption	Enterprise, Consumers	Encryption solutions for encrypting cloud	Boxcryptor, CipherCloud, Vormetric, nCrypted Cloud
Enterprise DRM	Enterprise	Enterprise digital rights management (DRM)	Fasoo, LockLizard, Documentum, WatchDox

Figure 38-2. Taxonomy of Encryption Products and Services

As can be seen from the taxonomy, some encryption products are embedded into the domain they serve, such as database encryption, whereas others are add-on solutions, such as encryption in some cloud storage services. In all cases, however, the goal should be *ease of implementation* and *simplicity of operation*. Any encryption solution being considered that cannot offer good stories in these two areas should be immediately dismissed. Expensive deployments, followed by complicated key management processes, are the scourge of crypto in the enterprise.

The trends in the encryption marketplace will be almost entirely positive as the data theft and leakage challenge intensifies, especially with respect to nation-state advanced persistent threats. As such, requirements for increasing encryption coverage, improving and streamlining key management tools, and integrating encryption into applications and systems will grow. The view here is that encryption solutions for business will grow at the most rapid pace, particularly as enterprise users require more on data protection in the cloud than on firewall perimeters.

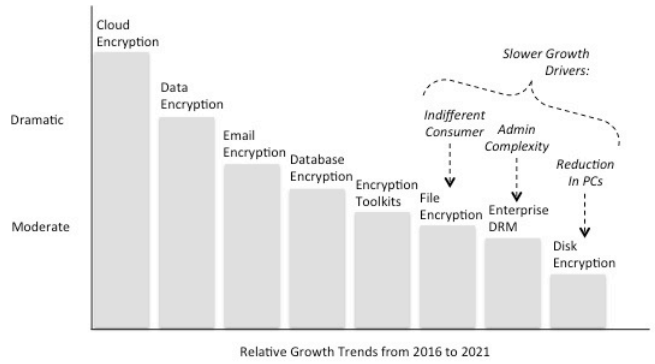

Figure 38-3. Encryption Product Marketplace Trends

Providers of encryption tools often express concerns about export restrictions in the United States and other countries. Such concerns are justified, although the likely direction of export restrictions will be toward more lax controls rather than the reverse. Excellent cryptography is available in all countries and export restrictions simply handicap domestic providers while offering only incremental support for local law enforcement.

One final point on encryption deployment: When an encryption solution is integrated into an application such as a database or Big Data repository, the auditors are generally pretty happy, but users might not be. If, for example, the encryption solution breaks native functions such as simple data search, then while security has been improved, the overall system quality has not. So CISO teams must be practical in this regard and not just assume that integrating encryption is always a good idea.

Data Encryption Providers

The data encryption vendor market is pretty mixed, with pure-play encryption solutions, infrastructure providers, application specific solutions, open source libraries, and on and on. Data encryption has also become a major component in adjacent solution areas such as CA/PKI solutions, secure file sharing, voice security, VPN/secure access, cloud security, and content protection/DRM. CISO teams analyzing the data encryption market as part of source selection should include these adjacent areas in the investigation.

2017 TAG Cyber Security Annual
Data Encryption Providers

Absio – Absio provides a data security solution that allows organizations and private users to securely store and share email messages and data externally, while maintaining control of its use.
AgileBits – AgileBits provides a range of security applications for password protection and file encryption.
Alertsec – Alertsec offers a Web-based service to deploy and administer Pointsec disk encryption software on PCs. The company is a spin-off of Pointsec, which was acquired by Check Point Software.
Boldon James – UK-based Boldon James provides data classification, secure messaging, and a range of related security products.
Boole Server – Italian vendor Boole Server provides data security and DLP through its encryption and support for sharing.
Boxcryptor – Located in Germany, Boxcryptor provides file encryption tools for use with public cloud services such as Dropbox and Google Drive.
CA Technologies – The large software and technology company includes data encryption solutions for its customers.
CENTRI – Seattle-based CENTRI provides an encryption-based solution for data protection.

Certes – Certes Networks provides software-defined, encryption-based security for enterprise applications.
Certicom – Now part of Blackberry, Certicom provides a range of cryptographic solutions using elliptic curve cryptography (ECC).
CertiVox – Now known as MIRACL, the authentication company offers open source, distributed security and encryption solutions.
Check Point Software – Check Point provides a range of data encryption solutions based on its Pointsec acquisition.
CipherCloud – CipherCloud provides cloud security monitoring, encryption, and key management solutions.
CloudLink – Previously Afore Solutions, the company provides data security and encryption management products.
CloudPrime – Now known as Cloak Labs, the company provides end-to-end encryption of application data from the enterprise to partners.
CORISECIO – CORISECIO provides a range of encryption solutions for Microsoft SharePoint.
Cryptography Research – Part of Rambus, Cryptography Research develops and licenses cryptographic technology solutions for semiconductor chips to reduce security risk across many industries.
Cryptomathic – Cryptomathic provides security solutions for eBanking, PKI, ID and ePassport, card issuance, and related key management applications.
Cypherix – Cypherix markets drag-and-drop personal data encryption software and network security tools.
DataLocker – Kansas-based DataLocker includes USB-based DLP protection solutions with digital rights management.
east-tec – Located in Romania, east-tec offers encryption-based products that protect sensitive information by secure erasure and other means.
Echoworx – Echoworx offers advanced email and desktop encryption products to secure data at rest.
EgoSecure – EgoSecure provides data protection solutions based on encryption, control, filtering, and management.
Encryptics – Encryptics provides a data privacy and protection software platform including encryption that can be embedded into applications and processes.
Entrust – Entrust provides a suite of authentication, identity, PKI, certificate, and mobile security solutions.
Fasoo – Fasoo offers a range of continuous encryption, document security, and DRM solutions.
Futurex – Futurex offers a range of encryption solutions include hardware security modules.
Gazzang – Now part of Cloudera, Gazzang offers encryption solutions for Big Data deployments.
GigaTrust – GigaTrust provides enterprise rights management solutions built on the foundation of Microsoft's Rights Management Services (RMS).

Guardtime – Guardtime provides a family of security solutions based on its keyless signature infrastructure (KSI) that enable data integrity, protection, and governance through block chain.
HPE – The acquisition of Voltage provided HPE with strong capability in data and email encryption marketplace.
InfoAssure – InfoAssure provides a solution for data owners to protect their assets through a combination of cryptography and content-based access controls.
InterCrypto – Seattle-based InterCrypto provides data encryption tools for files, disks, and media.
InterTrust – InterTrust Technologies invents, develops and licenses software and technologies in the areas of content protection, cryptography, and digital rights management (DRM).
Ionic Security – Ionic Security provides a unified cloud and mobility-based security platform focused on data protection, single sign-on, and analytics.
Krimmeni Technologies – Krimmeni Technologies provides a secure communications and key management solution for cloud called Rubicon.
Linoma Software – Linoma Software focuses on providing enterprise customers with data security solutions including encryption, backup, and secure file transfer.
Network Intercept – Network Intercept provides a suite of Internet security and keystroke encryption products for PCs, Macs, and mobiles.
Pawaa – Now part of Cisco, the Indian firm offers secure on-premise, encrypted file sharing capabilities.
Penta Security – Penta Security is an IT security firm offering Web application security, database security, encryption, and single sign-on solutions.
PKWare – PKWare provides an encryption solution for securing data files at rest and in transit.
Porticor – Porticor provides cloud security, encryption, and key management for public and private clouds such as AWS.
Protegrity – Protegrity markets comprehensive data security including tokenization, encryption, and policy enforcement.
Quintessence Labs – Quintessence Labs develops security products for cryptographic purposes including quantum key cryptography.
RSA (EMC) – This name is synonymous with public key encryption, but the corporation also focuses in many other aspects of cyber security.
SafeLogic – SafeLogic supports integration of Suite B and FIPS 140-2 validated encryption into mobile devices.
SafeNet – Now Gemalto, the company provides data protection solutions using authentication and encryption technology.
Secure Channels – Secure Channels provides a range of data encryption solutions for various types of systems and applications.
Senetas – Australian firm Senetas provides defense-grade encryption solutions for government and commercial customers.
Sophos – The UK-based security firm offers encryption solutions, including full disk encryption, for its customers.

StrongAuth – StrongAuth offers encryption, tokenization, and key management for compliance and security.
Symantec – The large technology and cyber security company includes data encryption solutions for its customers.
TecSec – TecSec provides information assurance solutions for access control enforced through encryption and key management.
Trustifier – Trustifier provides kernel-level security protections including mandatory access controls for UNIX systems.
Vaultive – Vaultive encrypts Microsoft Office 365 documents and other SaaS application by encrypting data before it is transmitted to the cloud.
Venafi – Venafi provides a protection platform to secure the keys and certificates required for secure storage and communications. Too much emphasis is placed in the community on key strength, and not nearly enough emphasis on protection of infrastructure. CISO teams must therefore review (and improve) the security of their keys and certificates.
Virgil Security – Virgil Security provides developers with cryptographic software and services.
Vormetric – Vormetric deploys high performance data encryption for cloud, Big data, and other enterprise applications.
Wave – Massachusetts-based Wave provides a range of data security solutions for the endpoint including a virtual smart card.
whiteCryption – whiteCryption (formerly Cryptanium) provides code integrity protection for apps, as well as a white-box cryptography library.
WinMagic – WinMagic provides full-disk encryption software to protect sensitive information on desktops and laptops.
WolfSSL – WolfSSL offers its customers an extensive SSL/TLS library for software developers.
Zettaset – Zettaset develops enterprise class data protection and encryption for Hadoop and other Big Data databases.
Zixcorp – ZixCorp provides a range of email encryption, BYOD, and DLP solutions for enterprise customers.

39. Digital Forensics

⇒ *Purpose* – Digital forensics involves preserving and analyzing data for the purposes of a cyber security investigation.
⇒ *In-House Versus Contracted* – The difficulty of keeping forensic expertise in-house drives many CISO teams to develop third-party relationships.
⇒ *Progression to Cloud* – With virtualization of applications, systems, and data comes the need to evolve data forensics approaches and tools.

The time will eventually come, if it has not already, when your CISO team will need to perform (or have someone perform) digital forensics, and the likelihood is high

that this task will be done under great management stress – usually just after or during a painful security incident. It pays therefore to make certain that your enterprise security managers and staff familiarize themselves with the basics of digital forensics and to arrange for the best available analysis tools, recovery processes, and technology experts to be deployed when needed.

The specific purpose of the *digital forensics* process at the enterprise level is to preserve, recover, and analyze artifacts from digital devices such as smart phones, computers, and storage in order to gain evidence and insights into a suspected malicious intrusion. Law enforcement and national security contexts are similar, but obviously are driven by slightly different sets of motivating forensic objectives.

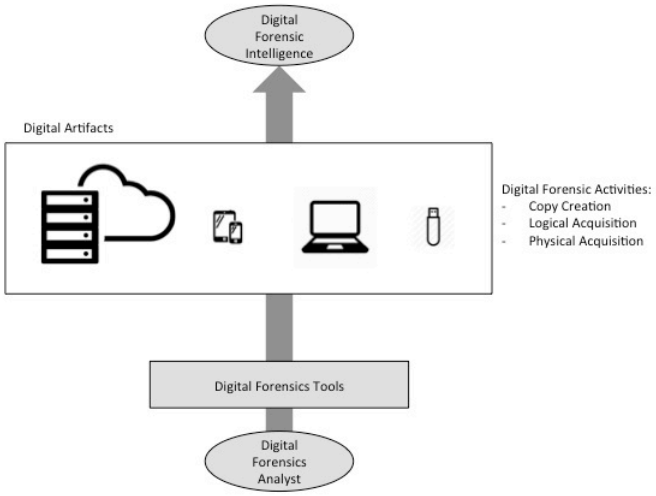

Figure 39-1. Digital Forensics in the Context of Cyber Security

The more specific motivations for digital forensics in an enterprise can range from a brief targeted analysis of malware on an endpoint, to a comprehensive root cause analysis of a major wide scale intrusion. Typical digital forensic activities include physically acquiring suspect devices, preserving copies of systems, interpreting stored memory, and drawing technical conclusions.

When the motivation for such work involves support for legal initiatives such as legal compliance checking or response to corporate litigation, then we refer to the corresponding forensic process as *eDiscovery*. Usually, eDiscovery tasks are less concerned with malicious activity than with organized collection of information for the purposes of some legal process; however, it is common for the CISO team to get involved here simply because the required skill set matches so directly.

It is beyond the scope of this report to get into the computer science details of how digital forensics experts interrogate NAND flash on a smart phone or the solid-state drive of some computing device to identify evidence of cyber attacks. Suffice it to say that the techniques are increasingly mature, and the best digital

forensic analysts will often joke that they can recover "anything from anything." So while enterprise security managers should be aware of the highest-level basics of how this is done, they probably won't ever find the need to develop expertise with a hex editor.

Every member of an enterprise cyber security team should therefore have a working knowledge of how, when, and why digital forensics should be used, as well as the types of issues that can be identified using forensics approaches. Furthermore, with the plethora of different digital forensic product and service options, security experts and managers need to understand the digital forensic and eDiscovery marketplace. Two practical decisions that CISO management teams will need to make regarding enterprise digital forensics for cyber security are as follows:

- *Insource or Outsource* – Employees can perform digital forensics with tools and infrastructure procured and managed internally. Alternatively, digital forensics work can be fully outsourced to professional consultants who can obtain and manage the best tools and expertise in the field. Outsourcing might seem the simplest approach, but keep in mind that this involves exposing organizational secrets to an external entity.
- *Proactive or Reactive* – Organizations can take a reactive approach, and perform digital forensics only in response to confirmed security events or business conditions. This certainly saves money and avoids wasting time on potential false positive conditions. Alternatively, the digital forensic process can be applied proactively to search for early indicators of cyber attacks. This technique begins to merge with the common technique known as hunting, which involves use of security analytics and SIEM tools.

These two decisions on digital forensics result in a simple taxonomy for management of the process. That is, by creating a matrix of the possible decisions regarding insourcing or outsourcing, and proactive or reactive, managers can look at all four possible choices in the context of the consequence and frequency of expected intrusions. For example, a public middle school is likely to see less consequential and less frequent intrusions than a power company, so they might make a fundamentally different decision about planning for the forensic process.

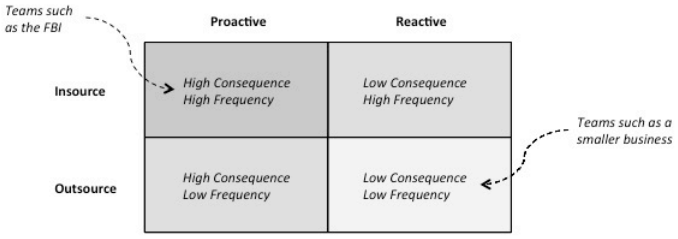

Figure 39-2. Taxonomy of Digital Forensics Approaches

Modern digital forensics platform and service vendors and consultants make available a plethora of features, capabilities, extensions, interfaces, ratings, case studies, services, and options. CISO teams will typically turn to vendors for automated tools that assist in the extraction, analysis, reporting, and storage of collected artifact data. Some teams have done well using free or open-source software forensic tools from organizations such as the United States Department of Defense. As these digital forensic tools are being used in support of the organizational digital forensic process for cyber security, several practical considerations should be taken into account by CISO teams.

Whether digital forensics is performed in-house or by third parties, the level of expertise associated with the forensic analysts is an important factor. While it is hard to gauge expertise without being overly subjective, there are various certifications that can be used to ensure a level of acceptable training. Applicable certifications include ISFCE Certified Computer Examiner and IACRB Certified Computer Forensics Examiner. Expert consultants should have experience with a variety of different endpoints, systems, and data. Mobile forensics, for example, is a relatively recent area of deep expertise, and must take into account a rapid technology development cycle as new devices are introduced.

Third-party security consulting companies who perform forensics make their money through references, which increases the likelihood that if a digital forensic expert performs some task on your behalf, that others will hear about it. If you are concerned about exposing security incidents in your company, then you should be concerned about this marketing practice, which might even include seeing your company logo displayed prominently on the Website of a company specializing in performing digital forensics.

Security protections for collected data are essential to the digital forensics process, especially in cases where the target of investigation involves sensitive or critical information. If collected data is to be transferred to an external, public cloud service, then the specifics of this transfer and how data is protected must be made available. In general, collected data should not be sent unencrypted to public cloud storage services.

The provision of forensic services should not be connected to some mitigation product offering that the forensics company is selling. When such bias enters the picture, one can be certain that the final results will almost certainly be consistent with, and supported by, the company's mitigation feature offerings. This is not to imply that mitigation services, post-forensic analysis, are a bad idea; rather, staff that can help select and use the best available tools for the organization, independent of any marketing or sales goals, should be the ones performing the digital forensics process.

While some environments might normally avoid virtual handling of sensitive data, forensic platforms should offer the option to run securely in the cloud. Such an option should include the ability for experts to be deployed quickly to perform an emergency data analysis from a remote location. This is especially useful in environments where certain applications (e.g., SCADA) require detailed, domain-

specific expertise that may not be immediately available locally. Virtual appliances for digital forensics support will also be important as more organizations move in the direction of virtual, cloud-based infrastructure.

Regarding future trends, most experts in digital forensics recommend that their work become more proactive in advance of breaches. While this might occur in certain instances, the predominant bulk of digital forensics will remain reactive for the foreseeable future. As a result, tools that analysts procure and learn to use on known suspicious or known-compromised targets will be the predominant solution in the marketplace. This is also true for legal eDiscovery.

As a result, any *significant* changes in the digital forensics marketplace are likely to come as a result of changes in how data and networks are designed and operated. Such changes will more than likely involve a shift toward greater adoption of cloud services – including public and hybrid – with emphasis on using mobile devices to access cloud data.

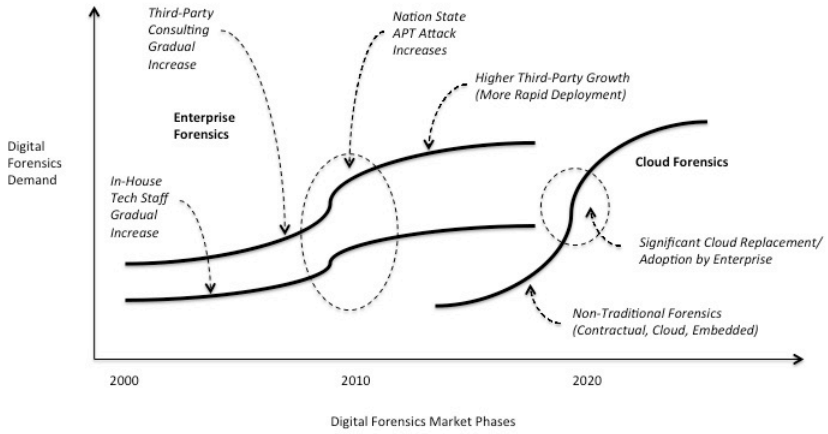

Figure 39-3. Digital Forensics Marketplace

The trend from 2000 to roughly 2010 was a gradual increase in this area for cyber security response as (1) technology usage increased in business, and (2) nation-state sponsored APTs increased considerably across the enterprise. During this period, the use of external consultants was common, especially in smaller organizations with limited resources. Consulting firms specializing in digital forensics for cyber security thus flourished during this era.

Moving forward, however, it is likely that as enterprise users adopt the cloud more aggressively, and as cloud providers embed forensics into bundled packages offered to customers, that more of this marketplace will find its way to the cloud. This stands to reason, because if data moves from on-premise enterprise servers to off-premise, cloud based systems, the forensic discovery process will virtualize accordingly. With this transition to cloud, the massive size of the digital forensics marketplace is likely to reduce as cloud service providers embed the capability into their offerings.

Digital Forensics Providers

The digital forensics solutions marketplace for enterprise, legal, or law enforcement customers is unfortunately *massive*. The intensely litigious nature of modern business is one of the reasons for all of the eDiscovery work and digital forensics requirements driving so many vendors offering solutions in this area. CISO teams considering digital forensics platforms or services should use the list below as a sampled starting point, cross-referenced with local requirements such as geographic location, size, and particular area of expertise. CISO teams should also keep in mind that virtually every security consultant advertises capability in digital forensics, so checking credentials before hiring is imperative.

2017 TAG Cyber Security Annual
Distinguished Data Forensics Providers

Guidance Software – I first met Patrick Dennis, CEO of Guidance Software, at a dinner sponsored by West Coast venture capitalists. I was so excited to hear about how Patrick was injecting new and creative energy into a security firm that was so well established in the digital forensics marketplace. Just about every forensic analyst in the business had, for example, spent some time with the Encase platform. So it would be easy for a company like Guidance Software to rest on its success and reputation. Technical discussions with Patrick and his team proved otherwise, as the company is clearly evolving its digital forensic and endpoint security offerings to support the evolution of the enterprise to mobility, cloud, and virtualization.

2017 TAG Cyber Security Annual
Data Forensics Providers

AccessData – AccessData provider of eDiscovery, computer, and mobile device forensics.
Altep – Altep offers certified data forensic investigators, emergency response technicians, and data privacy consultants.
Asgard Group - Asgard Group provides a range of wireless RF-based and communications security solutions for counterintelligence and cyber investigations.
Atlantic Data Forensics – Atlantic Data Forensics offers digital forensics, eDiscovery, and witness services.
Azorian Cyber Security – Azorian Cyber Security provides a range of cyber security services for enterprise customers.
Belkasoft – Belkasoft develops the its Evidence Center for digital forensic investigative support.
BitSec Global Forensics – Maine-based BitSec Global Forensics provides computer forensic support.

Caveon – Caveon includes data forensics in its suite of fraud testing and investigative services.
Cellebrite – Cellebrite offers an extensive portfolio of advanced and easy-to-use mobile forensics for analysis and extraction supporting law enforcement and military users.
Cyber Diligence – Cyber Diligence provides professional services in the area of combatting and investigating cyber crimes.
Cyfir – Cyfir provides its customers with an advanced enterprise digital forensics platform.
Elcomsoft – Russian company Elcomsoft focuses on password and system recovery software.
Enclave Forensics – Enclave Forensics offers expert incident response and digital forensic services.
FireEye – Through its Mandiant unit, FireEye offers incident response and network analysis to support forensics. FireEye has been a leader in the forensic analysis of enterprise incidents for many years.
4Discovery – 4Discovery offers computer forensics, computer security, and incident response.
FTI – Global business advisory firm FTI includes a range of digital forensics services for the enterprise.
Global Digital Forensics – Global Digital Forensics supports data forensic investigations including eDiscovery.
Guidance Software – Guidance Software is an industry-leading provider of the Encase forensic and analytic solution. Companies such as Guidance, with deep forensic capabilities, have come to recognize the adjacency of their tools and business to endpoint security.
Hacking Team – Italian firm Hacking Team provides expert digital forensics and investigative tools for government and law enforcement. Hacking Team has been a somewhat controversial vendor for its role in providing offensive tools used in government.
ID Experts – ID Experts supports recovery services including identity theft protection and credit monitoring.
Kroll – Kroll provides a team of computer forensics experts to assist in digital evidence collection and analysis.
K2 Intelligence – K2 Intelligence is an investigative and risk analytics consultancy founded by Jeremy and Jules Kroll.
Larson Security – Larson Security provides cyber security services including digital forensics and incident response.
LIFARS – New York City firm LIFARS provides data forensic and investigative capabilities.
Magnet Forensics – Magnet Forensics offers computer forensic and investigative tools for examiners.
NowSecure – NowSecure includes digital forensics in its mobile security suite of capabilities.

Nuix – Nuix offers search, investigative, and information management analytics capabilities supporting digital forensics.
Oneconsult AG – Oneconsult AG provides data forensic and investigative capabilities along with its testing and auditing suite.
The Oxman Group – Dallas-based Oxman Group includes data forensic and investigative capabilities in its response offering.
Paraben – Paraben provides a range of mobile data forensic and investigative capabilities.
Parameter Security – Missouri firm Parameter Security provides penetration testing, audit, and digital forensics specializing in the financial industry.
Stroz Freidberg – Stroz Freidberg offers computer forensics, investigations, expert witness, and electronic discovery services. Firms like Stroz Freidberg combine response, investigations, and forensics into an integrated offering.
Sylint – Sylint provides expert services in data forensics, eDiscovery, and compliance.
Symantec – Symantec supports digital forensics capabilities across its product and service suite.
Tactical Network Solutions – Tactical Network Solutions supports a range of digital forensic solutions.
TCS Forensics – Western Canada firm TCS Forensics supports eDiscovery, forensics, and risk management.
TechFusion – TechFusion is a certified expert computer forensics firm located in Boston.
US Data Forensics – US Data Forensics provides computer forensic examination, fraud investigations, and litigation support.
Wetstone – Wetstone, now part of Allen, offers a suite of forensic tools including WiFi Investigator and StegoHunt.
X-Ways Software Technologies AG – X-Ways provides hex file, disk, and RAM editor and other software for data recovery and computer forensics.

Additional Digital Forensics Providers

ACE Data Group – Philadelphia firm ACE Data Group provides data recovery and forensics services.
AC-Forensics – Kentucky firm AC-Forensics provides data recovery and forensics services.
Advanced Discovery – New York-based Advanced Discovery supports legal eDiscovery.
ASR – ASR provides expert supports in digital forensics for customers with Linux-based systems.
Axiom – Axiom provides forensic accounting, investigative, and expert witness services.
Barrister Digital – Barrister Digital offers a range of litigation and digital discovery support.

BIA – BIA offers expert digital forensics, eDiscovery, and witness services for enterprise.
Binary Intelligence – Binary Intelligence specializes in forensics of computers, cell phones, and chips.
Burgess Forensics – Santa Monica-based Burgess Forensics offers digital forensics, eDiscovery, and witness services.
CBL Data Recovery – CBL Data recovery provides a range of data recovery capabilities for failed hard drives.
Crane Engineering – Crane Engineering includes data forensics in its suite of technical and engineering consulting services.
CyberEvidence – CyberEvidence trains computer investigators in art of data recovery and analysis of evidence.
Data Recovery Labs – Florida-based Data Recovery Labs specializes in expert data recovery.
Data Forensics Group – Data Forensics Group supports data acquisition, data recovery, forensics analysis, and eDiscovery.
Datarecovery.com – Datarecovery.com supports a range of expert data recovery services.
Data Rescue Labs – Canadian company provides recovery for mobiles and computers.
DataTriage Technologies – DataTriage Technologies offers computer forensics, recovery, and eDiscovery capabilities.
Data Triangle – Data Triangle offers computer forensics, recovery, and eDiscovery capabilities for litigation support.
Deedoc Consulting – Small Raleigh computer repair company Deedoc Consulting offers recovery services.
D4 eDiscovery – Rochester-based D4 eDiscovery includes managed eDiscovery services.
Digital Detective Group (BLADE) – UK firm Digital Detective Group develops digital forensic software.
Discovia – Discovia delivers managed eDiscovery services to companies and law firms.
Disklabs – Disklabs is a provider of computer forensic services for legal firms, law enforcement, and enterprise groups.
DisputeSoft – DisputeSoft provides litigation support and expert testimony in New York.
Drivesavers – Data recovery firm Drivesavers support recovery for hard drives, RAID, SSDs, and phones.
D3 Forenics – Located in Asia, D3 Forensics provides data forensics and litigation support.
DTI – DTI supports a range of expert legal eDiscovery services for enterprise customers.
Eco Data Recovery – Florida-based Eco Data Recovery offers a range of recovery services.

e-fense – Colorado firm e-fense provides the Helix platform for digital forensic analysis.
Elite Forensics Investigators – Elite Forensics Investigators supports digital forensics and paper discovery.
Epiq Systems – Epiq Systems is a public company trading on the NASDAQ that supports technology services for the legal profession.
Expert Data Forensics – Small Nevada-based Expert Data Forensics supports recovery and forensics.
Flashback Data – Flashback Data offers data recovery and computer forensics for hard drives.
Forensic Data Services – Forensic Data Services offers computer forensics, recovery, and eDiscovery capabilities.
Forensic Risk Alliance – FRA is a consultancy that provides expertise in electronic forensics.
Forensic Strategy Services – Forensic Strategy Services supports collection and preparation of evidence for legal proof.
Fulcrum Data Forensics – UK firm Fulcrum Data Forensics offers computer forensics, recovery, and eDiscovery capabilities.
G-C Partners – G-C Partners offers computer forensics, expert testimony, and eDiscovery capabilities.
GetData Forensics – GetData Forensics supports data recovery, email recovery, and file repair.
Global CompuSearch LLC – Consulting firm Global CompuSearch supports computer forensics, computer security, and incident response.
Group-IB – Group-IB provides a range of expert data forensic and investigative capabilities.
Hawaii Data Forensics – Hawaii Data Forensics specializes in investigations of computer forensics and network intrusion.
Helios Data Forensics – Helios Data Forensics offers computer forensics, computer security, and incident response.
Iris Data Services – Iris Data Services provides a range of managed eDiscovery services.
kCura – kCura develops advanced eDiscovery software for electronic evidence collection.
Kessler International – Kessler International offers forensic accounting, intellectual property investigations, digital forensics, and investigative services
Lighthouse eDiscovery – Seattle-based firm Lighthouse eDiscovery supports legal eDiscovery.
Microforensics – Microforensics offers computer forensics, computer security, and incident response.
Northeast Ohio Forensic Data Recovery – Northeast Ohio Forensic Data Recovery supports digital forensics and litigation.
NTI Associates – NTI Associates offers computer forensics, computer security, and incident response supporting litigation.

NuVida – NuVida offers consultation, digital forensics, litigation, and expert witness services.
Optimo IT – Optimo IT includes legal support services in its range of technology consultation services.
OSForensics – OSForensics offers a range of forensic solution supporting discovery and extraction
Peak Forensics – Peak Forensics offers computer forensics, eDiscovery, and expert witness services.
PwC Forensics – Consulting group PwC Forensics includes support for digital forensics dispute and related services.
Responsive Data Solutions – Responsive Data Solutions provides electronic discovery services and software for law firms.
St. Johns Data Consulting – St. Johns Data Consulting offers digital forensics, consulting, and expert witness in Jacksonville area.
Thumbtack – Thumbtack provides a range of data recovery and digital forensics services.
Tri-State Data Recovery and Forensics – Pennsylvania firm Tri-State Data Recovery and Forensics provides RAID and hard drive recovery.
UnitedLex – UnitedLex provides legal and business services that integrate consulting and technology.

40. Identity and Access Management

⇒ *Primary Control* – Identity and access management has emerged as a primary cyber security control in de-perimeterized enterprise security protection.
⇒ *Responsibility* – Identity and access management responsibility should be placed with the CISO team given its central role in protecting the enterprise.
⇒ *Cloud Migration* – Future trends in identity and access management center on supporting migration to virtualization and public cloud support.

The purpose of *Identity and Access Management (IAM)* is to manage and enforce the lifecycle policies around *who* can access *what* resources and under *which* conditions. To support this IAM goal in any non-trivial organization requires a surprisingly complex set of functions and associated processes that can be roughly grouped into the following categories:

- *Managing Identities* – This includes the technology, interfaces, and processes required to register new users, assign credentials, track user activity, and support audit and governance requirements for user account management. An important aspect of identity management involves integration with corporate systems such as directories and human resource (HR) systems.
- *Federating Identities* – This includes the necessary agreements, interfaces, and protocols for passing and receiving identity credentials across different

domains. This can include domains that cross an organizational or company boundary. The most critical aspect of identity federation involves trust relationships between federating entities. If your company is small, for example, you might be willing to trust and accept identities from Google, but the reverse might not be true.

- *Managing Access* – This includes the policy-based decisions around which privileges and roles are sufficient to access which types of resources. Typically, resources will be arranged into groupings based on criticality, priority, or other attributes. Auditors spend a substantial amount of time making sure all these access groupings and policy decisions are correct and properly enforced.

The core architectural components in an identity and access management (IAM) system include a combination of technical IT controls and interfaces, security components, business processes, and workflow elements. This results in what is often the most complex system in the entire organization – and this is not just a statement about security. Rather, the IAM system is often the most complex system in an entire organization, including all IT and operational support systems.

The components supporting the identity and access management lifecycle start with a core IAM system, most likely purchased from a vendor. This core system includes an interface to some *user management* system, which includes support for provisioning, managing, and managing attributes of users, including their roles and privileges. The core also includes an interface to *authentication* systems that might involve technology from separate vendors. In fact, with the transition to more adaptive two-factor authentication, the likelihood is high that the IAM must include connectors for single sign-on (SSO), biometrics, voice authentication, one-time password (OTP) and other functions, probably coming from multiple vendors.

The IAM components also include interfaces to other major IT systems such as LDAP servers, workflow automation support, and customer resource management (CRM) systems. The idea is that the IAM must co-exist with these IT and business systems, simply because it provides a central means for making security decisions. These decisions are usually managed by an *authorization* component that manages access decisions, supervisor approvals, and other business workflow requirements. These decisions must be integrated tightly with the specific applications being managed, thus further complicating the overall IAM function.

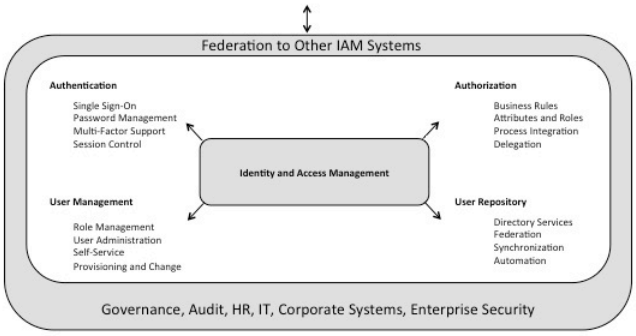

Figure 40-1. Identity and Access Management Ecosystem

Providing an overview of the detailed underlying architecture and operation of an identity and access management system is somewhat beyond the scope of this report. Suffice it to say that integrating IAM into an enterprise, especially one that is evolving to cloud virtualization, is a significant technical and operational challenge. The reason for this is that IAM plays such a central security, business, and administrative role in registering and managing user identities, supporting access policies including role based or adaptive authentication, providing continuous evidence of compliance support for numerous different internal and external auditors, and even supporting the performance needs of supporting sign-ups for customers of new on-line services.

Given the central nature of IAM, CISO teams are advised to learn as much as possible about the present and future states of commercially available IAM tools, platforms, and professional services. This is a priority for CISO teams, even if the responsibility for IAM currently resides in another area of the business. The learning emphasis should be placed by CISO teams on how evolving IAM systems in the enterprise will have to adapt to shifting security needs across the corporate network in the coming years. This includes support for automated cloud workloads, IoT and other mobile devices, complex Big Data access policies, and increased virtual computing.

An initial challenge for IAM in the enterprise is the wide assortment of decisions made by businesses around *who exactly* has responsibility for the function. Some companies place IAM in the hands of the IT operations team, citing the importance of high availability and reliable operation. Others place IAM in the hands of the CISO team, citing its fundamental role in protecting critical assets. Still other companies (especially service providers) place the function with their digital group citing the close experiential ties that exist between IAM, user registration, customer provisioning, and application usage.

Each of these decisions has its pros and cons, but the position held here is that IAM is a *primary cyber security control* and should therefore be managed by the CISO team. This will ensure that IAM data is always sent to the SIEM, that provisions remain in place for IAM security analytics, and that attention is always paid to least privilege and segregation of duties. Regardless of where the IAM function resides,

however, several major challenges must be kept in mind during product and system procurement for any IAM infrastructure components supporting the enterprise.

The first challenge involves the *uniformity* of IAM platform design. A surprisingly high percentage of non-trivial enterprise networks currently include more than one IAM system, perhaps even ones that are home grown from Excel spreadsheets. This complex situation was improved slightly for financial systems in American public companies with Sarbanes-Oxley, but most companies have not made the full investment to combine their IAM systems onto a common platform. As enterprise computing continues to virtualize, the need to simplify IAM onto a one uniform platform will increase.

The second challenge involves supporting IAM operations. Providing robust day-to-day operations support for IAM is challenging since it resides in the middle of all IT applications and system operation. When enterprise single sign-on (SSO) breaks, for example, the impact on business operations will cascade to all applications reliant on this persistent feature. This often creates organizational stress because the best *security* IAM staff is not always the best *operational* IAM staff, and these are different. The result is that in so many organizations, the CISO team has little to do with day-to-day IAM operations, and this can cause serious seams in security coverage.

The third challenge involves enterprise migration of IT and operational systems to pubic clouds. Few CISO teams can describe a clear migration path from current enterprise-resident IAM to virtual IAM systems supporting cloud. This is unfortunate since IAM is essentially swapping roles with the firewall as the primary control in the enterprise. Once auditors, regulators, and compliance manager recognize this shift, they will begin to demand information on planned cloud migration, and this will not be easy to manage since so many critical IT systems connections, such as to Microsoft Active Directory, will probably remain on the enterprise-hosted LAN.

This type of arrangement, by the way, provides a great market advantage for IT systems providers such as Microsoft that are also cloud providers. Moving the IT systems to the cloud makes for an easier migration path to moving IAM to the same cloud. Watch for this type of offering to become more common from IT and cloud providers.

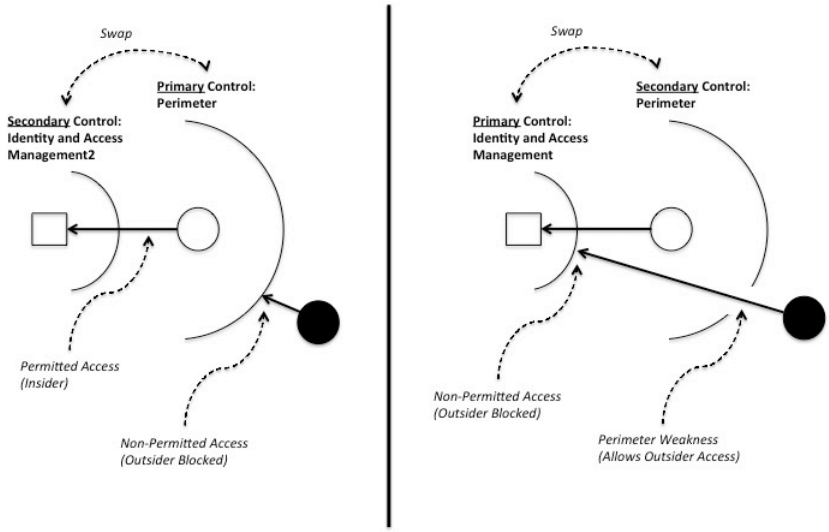

Figure 40-2. Evolution of IAM as a Primary Control

If you ask most IAM experts how they spend the majority of their time today, they will tell you that compliance processes demand more time and effort than any other function. Auditors have come to understand elements of IAM in recent years, certainly enough to be overly focused on IAM to the exclusion of many other critical security functions. When, for example, was the last time an auditor demanded more information on the underlying mathematical models in your security analytics toolkit? The answer is that this doesn't happen.

A common compliance scenario might involve an auditor demanding evidence of support for a requirement such as segregation of duties. Perhaps the organization does software development and the auditor wants to see that development and production staff cannot access the same software. This task would be accomplished by having the IAM team provide evidence of proper user credentials, correct assignment of roles (developer or administrator), and proper enforcement of the separation policy. If any of the audit tests fail, then the IAM staff would be engulfed in a project to fix the problem, and deal with the barrage of compliance documentation implications that would follow.

The belief here is that in the coming years, IAM will gradually transition from this compliance-motivated set of functions and processes to a more operationally critical cyber security control. This shift in emphasis will be more by necessity than anything, because enterprise teams will need to focus on IAM excellence to keep intruders out of systems. For enterprise virtual and cloud systems, this will be more intense than for the perimeter-based systems in use today. As such, the following trends will emerge for IAM:

- *Decrease in Enterprise-Hosted IAM* – The deployment of complex IAM infrastructure inside an enterprise perimeter will gradually level off simply because the perimeter protected enterprise will soon disappear. IAM

functions will have to virtualize, but this will require coordination with vital components such as Microsoft Active Directory and internally hosted Human Resource (HR) systems.

- *Increase in Two-Factor Authentication for IAM* – Requirements for IAM systems to a wider variety of two-factor and adaptive authentication solutions will increase. This will introduce higher percentages of mobile and biometric authentication tools in the enterprise. In some cases, the transition to two-factor authentication will provide an excuse to completely redesign the IAM system.
- *Increase in Cloud IAM* – As the enterprise becomes virtualized, and as young Millennials enter business, the use of cloud infrastructure for *everything* will increase. As such, third-party companies offering cloud IAM will thrive. This will be throttled somewhat by the slow virtualization that might occur for enterprise infrastructure support.

These emerging trends in the IAM platform and service marketplace involve a shift from an era of large, multi-year enterprise deployments of IAM systems into a period in which cloud-hosted IAM is complemented by technology support for stronger and adaptive authentication. Most new IAM vendors recognize this shift in their product designs, but the practical implementation by enterprise teams will be nonetheless difficult.

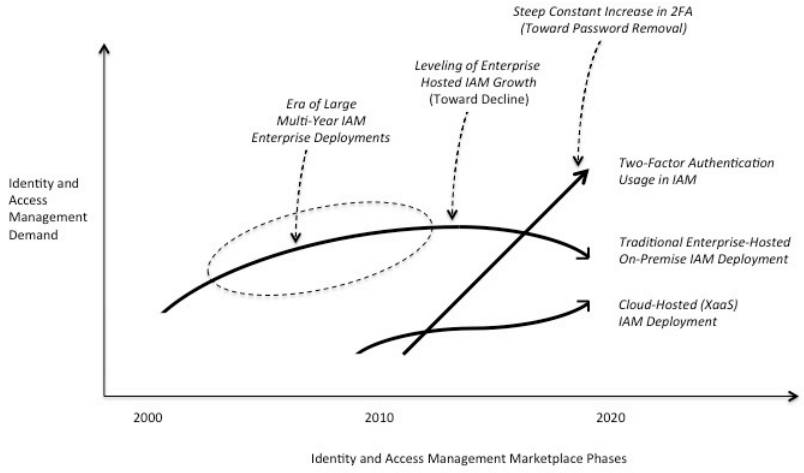

Figure 40-3. Vision for IAM Marketplace

Given the relative importance of cloud to IAM strategy, examination of how cloud-based IAM systems will integrate with IT and security ecosystems is instructive. In the coming years, the major endpoint, system, and network components for IAM integration will include the following:

- *Existing and New Endpoints* – This set of endpoints will include corporate-provided and BYOD PCs, mobile, tablets, and other devices such as gaming systems and wearable devices.
- *Existing Enterprise IT* – This IT infrastructure will include the set of on-premise enterprise systems and applications in use today in the physical or virtual data center.
- *Emerging Cloud IT* – This virtualized IT infrastructure will include the set of off-premise enterprise systems and applications being added today in the cloud.
- *Existing Enterprise IAM* – This includes the existing IAM infrastructure currently embedded in the enterprise, and protected by a firewall.
- *Emerging Cloud IAM* – This new area includes emerging cloud-based IAM services offered by providers or platform vendors supporting off-premise hosting.

The resulting integration of these endpoints, systems, and networks will be part of the challenge in establishing next-generation IAM in the mobility-enabled, cloud based enterprise.

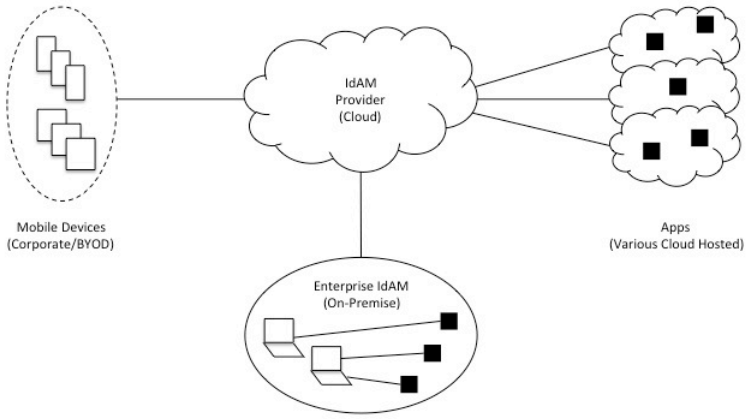

Figure 40-4. Cloud-Based IAM Configuration

Some larger organizations will perpetuate the use of the enterprise perimeter through sheer determination and budget. They will continue to cite the stubbornness of internal and external auditors who demand that IAM functions *not change* and certainly never move to a public cloud. This represents a real challenge for CISO teams, especially in industries such as financial services where the regulatory pressure in particularly intense. The result will be slower adoption of cloud IAM in regulated industries in favor of avoiding the obvious risks that emerge with change to any new infrastructure approach. Ironically, the risk of maintaining infrastructure inside a perimeter might be higher.

Identity and Access Management Providers

The *Identity and Access Management* market includes a large number of vendors that can roughly be grouped into traditional vendors with enterprise solutions moving to cloud and new entrants designed specifically for cloud support. CISO teams should consider both types of vendors in source selection, as both bring unique skills to the table. Vendors offering adjacent functions such as identity validation services are included below as a convenience for CISO teams desiring such support.

2017 TAG Cyber Security Annual
Distinguished Identity and Access Management Providers

Ping Identity – During the early stages of my research, I was intrigued by the design elements embedded in Ping's IAM solutions. Having had decades of practical experience in this area, I was able to differentiate between hype and reality, and I liked what I saw in the Ping design. So I went and spent time at their Annual Conference in New Orleans (dealing with balmy one hundred and five degree temperatures) and I thoroughly enjoyed learning more about the work Patrick Harding and his IAM team had going in this area. I am so grateful to the entire Ping team for their kind assistance and support throughout this project.

2017 TAG Cyber Security Annual
Identity and Access Management Providers

Aegis Identity – Aegis Identity offers an identity management solution focused on the education market.
Alert Enterprise – Alert Enterprise provides infrastructure protection through governance, risk, and compliance (GRC) management, situational awareness, and continuous monitoring
Amazon Web Services – AWS includes extensive identity and access management capability for securely controlling access to its cloud services and resources.
Aujas Networks – Aujas Networks provides security solutions in risk and vulnerability management, data protection, and identity and access management.
Auth0 – Auth0 provides a product that allows developers to add identity federation to their apps.
Avatier – Avatier automates IT operations and compliance of user provisioning, access management, and related functions.
Avecto – Avecto focuses on providing Windows-based privilege management for desktops and servers.
Axiomatics – Axiomatics provides a suite of attribute-based access control and dynamic authorization solutions based on the XACML 3.0 standard.
BeyondTrust – BeyondTrust offers a range of enterprise security products with focus on privilege and identity management for servers and other IT software.

Bitium – Bitium provides a cloud-based platform for managing passwords, users, and SaaS application access.
CA – CA offers its Identity Suite, Privileged Access Manager, Identity Manager, Identity Governance, and related SaaS solutions for enterprise IAM. CA acquired Xceedium in 2015.
Centrify – Centrify offers an identity and cloud management platform supporting Identity-as-a-Service solutions.
Certified Security Solutions (CSS) – Certified Security Solutions (CSS) provides security solutions in the areas of PKI, encryption, and identity, with emphasis on securing IoT.
Core Security – Formerly Courion, Core supports identity and access management solutions with self-service password management and automated access reviews.
Covisint – Originally focused on connected vehicle, Covisint has expanded to secure IoT, supply chain, and identity and access management.
Cross Match Technologies – Cross Match technologies provides identity management and biometric identity verification solutions.
CyberArk – CyberArk focuses on locking down privileged accounts to reduce security risk, especially advanced persistent threats (APTs).
Daon – Daon offers platforms, tools, and applications focused on identity assurance and biometrics for enterprise and government customers.
Deep Identity – Located in Singapore, India, and the UK, Deep Identity offers a layered approach to identity and data governance.
Deepnet Security – Deepnet Security provides multi-factor authentication and identity and access management solutions.
Dell Software – Dell provides a suite of identity governance, access management, and privileged management for enterprise.
DirectRM – DirectRM provides strong authentication and access management solutions supporting BYOD.
Evidian – Evidian supports IAM for single sign-on, user provisioning, and related functions for enterprise and cloud.
Exostar – Exostar offers identity and access management and cloud collaboration solutions.
Fischer International – Fischer offers identity management software for outsourced and on premise environments with emphasis on higher education.
ForgeRock – ForgeRock provides identity and access management for cloud, mobile, and enterprise.
FoxT – FoxT provides a suite of network security and access management solutions for the enterprise.
Gluu – Gluu provides an open source or on demand, standards-based identity and access management capability for enterprise.
Google – The famous technology firm offers identity services that federate Google login to other cloud identity and access applications and services.
HID Global – HID Global provides a range of identity and access solutions including smart cards, readers, RFID tags, and software.

HPE – HPE offers its Cloud Identity Service supporting secure IAM for the Helion Public Cloud.
IBM – IBM offers capabilities based on early acquisition of Tivoli for identity and access management.
Identacor – Identacor enables secure, one-click access to corporate applications via SaaS identity management and SSO.
Identia – Identia provides next-generation identity and access focused on cloud use and integrated with PKI technologies.
Identiv – Identiv offers a range of identity solutions including uTrust supporting premises access, information access, and credential management.
i-Sprint Innovations – i-Sprint Innovations provides identity, credential, and access management solutions.
iWelcome – iWelcome supports identity and access management for European government applications.
Jericho Systems – Jericho Systems provides support for access management with emphasis on XACML implementation.
Lieberman Security – Lieberman Security includes a range of products related to identity, passwords, and privilege management.
Mycroft – Now part of EY, Mycroft provides managed and professional services in IAM.
NetIQ – NetIQ, offered by MicroFocus, includes full-featured IAM and security management.
NextLabs – In addition to data and rights security, NextLabs offers XACAML policy server solutions.
neXus Group – neXus Group provides a range of products and services in identity management, certificate and key management, and authentication.
9Star – The company offers its Elastic SSO software solution for federated access technology.
Okta – Okta offers a cloud-based solution for identity and access management services.
Omada – Omada offers identity management, governance, compliance, and user provisioning.
OneID – OneID focuses on the management of on-line identities without the need for passwords.
OneLogin – OneLogin supports cloud-based identity and access management with secure access to cloud applications from mobile devices.
Oracle – Oracle provides a full featured, industry-leading capability with large and small customers.
Osirium – Osirium provides privileged user account management and protection solutions for the enterprise.
PerfectCloud – PerfectCloud offers range of cloud security solutions including SmartSignin with SSO and federated IAM.
Ping Identity – Ping Identity supports the full range of enterprise identity and access management for internal and SaaS applications. This includes support for multi-

factor authentication, single sign-on, access security, directory support, and user provisioning. Ping Identity, like many other IAM vendors, is well aware of the need to support these functions as customers move to SaaS applications in the cloud.
Protected Networks – Protected Networks is a German company that provides server access rights management solutions.
Radiant Logic – Radiant Logic supports identity, federation, and directory services through virtualization and cloud technologies.
RSA – RSA offers a range of identity and access management solutions building on the Aveksa acquisition and the industry-leading RSA token for 2FA.
Sailpoint – Sailpoint offers on-premise and cloud-based identity and access management platform.
Salesforce Identity – Salesforce Identity includes extensive IAM functions to provide SaaS protections for Salesforce.
Saviynt – Saviynt provides cloud access governance and intelligence for data protection, privacy, and regulatory requirements.
SecureAuth – SecureAuth provides an IAM solution that supports enterprise requirements for SSO and 2FA for mobile, web, and cloud applications.
SecureKey – SecureKey offers identity and authentication solutions for online consumer service providers.
SecZetta – SecZetta provides security consulting services specializing in IAM implementation and privileged account management.
Simeio – The company offers the Simeio Identity Orchestrator platform and Identity Intelligence Center solution.
Soffid – Soffid offers an open-source identity and access management solution with support for SSO.
Stormpath – Stormpath provides a user management API that allows developers to integrate authentication for users and roles.
SurePassID – SurePassID provides cloud-based identity and access management for mobile and hybrid cloud use.
Syntegrity – Syntegrity provides a range of security products and professional services including support for identity and access management.
2Keys – 2Keys provides a range of managed and professional services with emphasis on user authentication and identity attributes.
UnboundID – UnboundID offers identity and preference management through the UnboundID platform.
White Cloud Security – 2Keys provides a range of managed and professional services with emphasis on user authentication and identity attributes

Additional Identity and Access Management Providers

Atos – Atos offers the DirX portfolio of identity and access management product solutions.
Coreblox – Coreblox is a premier provider of identity and access management for enterprise, federation, and cloud.

Ellucian – Ellucian provides range of education industry software with identity and access management consulting services.
Equifax – Equifax supports credit reporting via identity assurance for personal, small business, and larger business applications.
Experian – Experian supports identity and credit access, as well as related data management solutions.
Hitachi-ID – Hitachi-IS provides identity and access management including support for governance and password management.
Identicard – The company manufactures ID, access, and security cards and accessories.
Identigral – Identigral offers consulting services and solutions for clients working on identity and access management.
Identropy – Identropy provides a range of information, resources, and services in support of IAM.
OnWire – OnWire includes a FedRAMP, multi-factor authentication platform with cloud based IAM.
Tools4Ever – Tools4Ever offers identity governance and administrative tools and enterprise solutions.
Transunion – Transunion provides fraud, identity, and credit-related services. Transunion acquired Trustev in 2015.

41. PCI DSS/Compliance

- ⇒ *Compliance Standards* – PCI DSS and other security compliance standards follow a similar assurance lifecycle for enterprise teams and businesses.
- ⇒ *Representative Case Study* – Even CISO teams with no retail responsibility can benefit from studying the PCI DSS environment as a relevant case study.
- ⇒ *Compliance Trends* – Future compliance programs will tend to shift from specific frameworks to more holistic compliance concerns.

With *so many* cyber security frameworks in use today, a segment of the security consulting industry has emerged to support the compliance lifecycle. Popular frameworks – and this is a tiny subset – include Payment Card Industry (PCI) Data Security Standard (DSS), International Standards Organization (ISO) 27001, National Institute of Standards and Technology (NIST) Framework, Sarbanes-Oxley, Health Insurance Portability and Accountability Act (HIPAA), and Federal Information Security Management Act (FISMA). Each defines a set of functional and assurance requirements to establish, maintain, and demonstrate compliance.

Because the compliance requirements across different frameworks are similar (if not exactly the same), security consultants, auditing firms, and GRC platform providers tend to provide support across the full spectrum. Granted, some frameworks such as FISMA have unique process and attestation requirements; but *the establishment of compliance is similar, if not essentially the same, across different*

sets of framework requirements. This has major consequences for CISO teams, because compliance with one framework will usually go a long way toward compliance with another. This saves money in security deployment work, but wastes money in repeat attestation of the same controls.

A good example of this commonality across frameworks involves the retail point-of-sale (POS) and payment card handling industry. The number of recent breaches in this sector has grown so much that the industry is in crisis. Break-ins at Target, Home Depot, and Wendy's have raised questions about the industry's ability to protect card information. In response, the sector has reaffirmed its existing standards and compliance process to deal with this intense threat. It has also demanded adoption of more rigorous security technology, including the migration of all POS to chip processing, with either PIN or signature factors. The United States has lagged many other countries in this use of tokenized security.

The purpose of PCI DSS consulting is to provide support and attestation for retail industry participants to comply with the PCI DSS requirements. But this is no different than HIPAA teams helping clients support that framework or government consultants helping agencies support FISMA. In each of these cases, organizations will do an early assessment, which helps smoothen the subsequent more formal attestation process. Also in each of these cases, an attested result follows, which will dictate remediation tasks required to achieve formal certification. The best news of all is that security controls put in place for one framework, such as PCI DSS, will likely apply directly to other frameworks such as HIPAA.

To make the discussions here more concrete, we will highlight PCI DSS in this section as a working compliance example. We begin with attention to the underlying principles of PCI-DSS, which can be roughly organized into six different categories of twelve control requirements.

PCI DSS Control	Requirement Grouping
1. Firewall Management	Construct and Maintain Secure Network
2. Vendor Default Controls	
3. Data Protection	Protect Cardholder Information
4. Data Transmission Encryption	
5. Anti-virus Control	Maintain Vulnerability Management Program
6. System & Application Security	
7. Data Access Controls	Implement Strong Access Control Measures
8. Personal Access Controls	
9. Physical Access Controls	
10. Data and Network Access Controls	Monitor and Test Networks
11. Security Testing	
12. Information Security Policy	Maintain Security Policy

Figure 41-1. PCI DSS Requirements

A taxonomy such as for PCI DSS is found in every security compliance framework. This has the advantage of orderliness and completeness, but it has the disadvantage of leading to comprehensive reviews of large lists of compliance areas. If a taxonomy includes one hundred requirements, for example, then compliance must address each of these, even if the assessor knows that fifty or sixty of the requirements are not going to be an issue. Cyber security compliance review and attestation must be complete and orderly – and this can take considerable time to get right.

As a result, a consulting industry has emerged for security compliance – with PCI DSS being perhaps the largest and most intense example of this information security sector. There is even a special designation for consultants who are properly training in PCI DSS known as a Qualified Security Assessor (QSA). Obviously, CISO teams considering PCI DSS consulting services would be wise to stick to QSA consultants. This is true for other frameworks as well; CISO teams must be diligent in checking background qualifications of consultants. Never hire a FISMA consultant, for example, who does not understand Washington.

By way of brief history, PCI DSS was developed in 2004 by the Payment Card Industry Security Standards Council to ensure consistent security practices amongst merchants processing credit cards. PCI DSS compliance thus emerged as a key consideration for any company accepting American Express, Visa, and Master Card. In fact, it was designed for any group processing, storing, and transmitting credit card-related information. The requirements require a mapping from company practice to the intended PCI DSS control, which explains why so many companies are in the business of providing security consulting support in this area.

When the PCI DSS requirements were created, and as they have evolved, few in the industry would have expected the rise of advanced persistent threats from nation-state actors being directed at credit card and related personal information from customers. This shocking increase in APT attacks is found in virtually every sector, and has rendered most compliance standards ineffective in dealing with the break-ins occurring. Retail POS attacks seem to happen every month, and all of the targets are fully PCI DSS certified.

The result is that new technologies have emerged in every sector to address these more intense attacks. In retail POS, for example, a new EMV standard is being put in place for protecting card data. EMV is based on an improved cryptographic protocol that is used in conjunction with encrypting card readers to reduce fraud risk. As such, direct retail attacks to POS terminals will wane as the EMV standard is deployed in retail environments across the United States, following more aggressive deployments in other areas such as Western Europe.

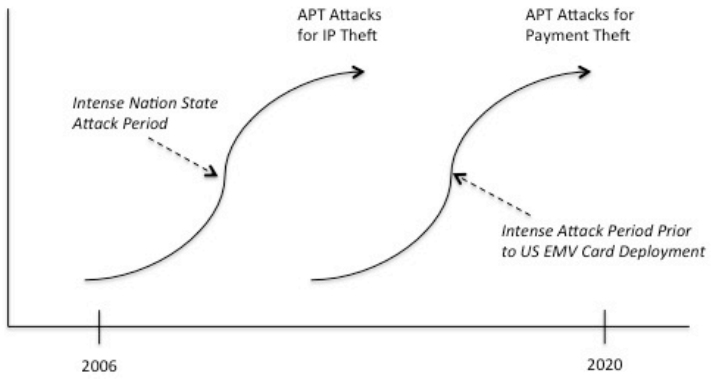

Figure 41-2. APT Techniques for Cardholder Attacks

The implication of the APT attack vector from nation states, with continued targeting of retail companies, is that simple compliance programs, even with EMV transition, will no longer be sufficient to stop theft. This is an important point: *EMV and compliance will not be sufficient to stop cyber theft of credit card information*. Rather, just as in other sectors that have been dealing with APT attacks for many years, the retail sector is forced to significantly improve the overall cyber security ecosystem and lifecycle in order to more effectively stop these advanced attacks.

As a result, any observer would be forced to expect a drop off in *primary emphasis* on PCI DSS standards usage and consultation. This industry shift will parallel similar changes in "quality management" that ballooned in the nineties and leveled off afterward. This is not to imply that PCI DSS or any other form of security standards consulting will go away, but the number of companies involved and the growth of engagements will shift to more holistic cyber security initiatives as shown below.

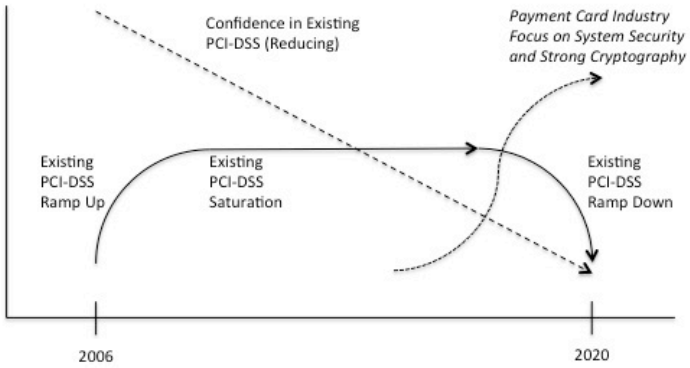

Figure 41-3. Trends in PCI DSS Emphasis

The good news for security compliance consultants is that their relationship with existing customers can be parlayed into more general consulting opportunities. Organizations will be looking for more secure means to shift applications securely to cloud, or to virtualize their workflow securely, or to share information with third parties more securely. Each of these new focus areas represents growth opportunities for the more flexible compliance consultants. Buyers of security consulting services should therefore be on the lookout for partners and vendors with ability to adapt their consulting services to more general issues, especially as they relate to APT risk reduction.

PCI DSS/Compliance Providers

The list below includes both PCI DSS and other security compliance standards consultants. Regarding PCI specifically, the PCI Security Standards Council (see https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php) provides a current and accurate list of QSA Companies, as well as a plethora of related information. CISO teams can use the companies listed below as a starting point in selecting a PCI DSS QSA or security compliance services vendor. Source selection in this area should also include attention to governance, risk, and compliance (GRC) solution providers, as well as security consultants.

2017 TAG Cyber Security Annual
PCI DSS/Compliance Providers

Above Security – Above Security includes PCI DSS and compliance consulting as a complement to its managed security service and security audit offerings.
ANX – ANX is a global provider of managed payment, compliance, and security services.
AT&T – AT&T includes a wide range of expert compliance and PCI DSS QSA support in it global consulting offering. The company acquired the Verisign security consulting team, led by Todd Waskelis, several years ago.
Attack Research – Attack Research is a PCI-QSA certified consulting group located in Los Alamos.
Avnet – Avnet is a consulting firm in Israel includes range of compliance and PCI services.
BAE – Acquired SilverSky, which offers a managed, GSA-approved PCI compliance solution for preventing breaches in retail environments.
Bell Canada – Bell Canada includes compliance and PCI consulting as part of its services.
Blackfoot – Blackfoot is a UK firm offering a range of PCI and compliance consulting services.
The CISO Group – The CISO group offers information security consulting with an emphasis on PCI DSS compliance issues.

Clone – Clone Systems is a Managed Security Services Provider (MSSP) that focuses on continuous monitoring, secure private cloud, security scanning, and consulting.
Coalfire – Coalfire provides cyber risk management and compliance services for enterprise and government organizations.
CompliancePoint – A PossibleNOW Company, CompliancePoint offers information security consulting.
Comsec Consulting – Information security consulting Comsec Consulting offers services with emphasis on risk management and compliance.
Content Security – Content Security includes a range of PCI DSS consulting in its service suite.
Contextual Security – Contextual Security offers IT security services including PCI and HIPAA consulting.
ControlScan – ControlScan provides a range of PCI compliance and self-assessment services.
Deloitte – Deloitte serves as an approved Qualified Security Assessor (QSA) for its global enterprise clients.
Enterprise Risk Management – Security consulting firm Enterprise Risk Management includes compliance management services.
Espion – Based in Dublin, Espion provides a range of security consulting and PCI DSS services.
Ground Labs – Ground Labs provides security and auditing software in support of PCI DSS compliance.
Halock Security Labs – Halock Security Labs includes compliance services along with penetration testing and risk assessment.
The Herjavec Group – The Herjavec group is an information security firm with QSA services and PCI-compliant managed services.
IBM – IBM's global enterprise consultants are available to support PCI DSS assessments for customers.
KPMG – KPMG includes PCI compliance and QSA consulting services in their professional service offerings.
Nettitude – Nettitude offers penetration testing, risk management, and PCI consultancy services.
nGuard – nGuard is a security consulting and testing vendor that also serves as a PCI QSA vendor.
NTT Communications – NTT Com Security includes PCI DSS in its range of consulting and managed security services.
NTT Security – Operating in Ireland and Italy, NTT Security offers the ZeroRisk PCI portal for PCI compliance.
Optiv – Security solutions provider Optiv includes PCI support as part of its professional services.
Orange Consulting – Orange Consulting includes focus on governance, risk, and compliance assessments.
Paladion – Information risk management firm Paladion offers professional services including compliance.

Praetorian – Praetorian offers a range of risk consulting and compliance advisory services.
Protiviti – Protiviti provides customers with PCI planning, readiness, and compliance capabilities.
PwC – PwC includes PCI services in its suite of global technology and consultation offerings.
RavenEye – RavenEye provides a range of security consulting services including ethical hacking, PCI DSS QSA services, and penetration testing.
SecureState – SecureState includes compliance in its suite of information security services.
SecurityMetrics – SecurityMetrics provides PCI DSS, HIPAA, and data security compliance assessments.
Sera-Brynn – Sera-Brynn serves as a PCI QSA and includes compliance in its suite of information security services.
Solutionary – Part of NTT Group, Solutionary includes security compliance consulting services.
Stickman Consulting – Stickman Consulting includes compliance in its suite of penetration testing and information security services.
Sunera – Sunera addresses HIPAA and other compliance suites in its suite of information security consulting.
Sword & Shield – Sword & Shield includes PCI assessments in its suite of security services.
Sylint – Sylint offers customized services for PCI, HIPAA, NIST, and ISO compliance and audit.
Sysnet – Sysnet provides a range of PCI, cyber security, and compliance solutions for business.
TBG Security – TBG Security provides security consulting services to assist with compliance in HIPAA, PCI, and related frameworks.
Tevora – Tevora provides security consulting, risk management, and governance/compliance solutions for enterprise customers.
TrustedSec – Information security consulting firm TrustedSec, located in Ohio, offers PCI QSA services.
Trustwave – Trustwave offers an extensive range of PCI DSS professional services, and was one of the first companies to truly embrace PCI as a consulting focus. Singtel acquired the company in 2014.
2-sec – 2-sec provides a range of security consulting offers including penetration testing and PCI DSS services.
Veris Group – Veris Group serves as a PCI QSA for customers as part of its GRC assessment and advisory services.
Verizon – Verizon includes compliance in its suite of managed and information security consulting services. Verizon acquired the consulting team of CyberTrust several years ago, which included the National Cyber Security Association team originally led by cyber security pioneer, Peter Tippett.

Additional PCI DSS/Compliance Providers

Ather Technology – Trading as Cianna technologies, Ather is the only PCI DSS registered in the Kingdom of Saudi Arabia.
Cadence Group – Cadence Group is an advisory and compliance consulting firm offers support for PCI and other frameworks.
Cadre Information Security – Cadre Information Security consulting firm in Cincinnati provides compliance and PCI assessments.
CNS Group – UK consulting firm CNS Group offers information assurance, IT security and compliance solutions.
Compass IT Compliance – Compass provides IT compliance, security, and audit services.
Continuum Security Solutions – Information security firm Continuum is engaged in compliance, assessments, and governance.
ControlCase – ControlCase is an information technology, GRC, managed compliance software, and services company.
ControlGap – ControlGap is an approved Canadian QSA company for PCI DSS compliance.
CrimsonSecurity – CrimsonSecurity includes compliance services for PCI DSS, ISO 27002, NIST 800-53, GLBA, and HIPAA.
Crossbow Labs – Crossbow Labs provides enterprise-consulting services for PCI DSS compliance.
Cybercom Group – Cybercom Group is a Swedish consulting firm that includes compliance services.
Dara Security – Dara is a security firm of advisors, assessors, and ethical hackers with experience in PCI DSS and other standards.
Dimension Data – Dimension Data is a New Zealand group supporting PCI based on its Security Assessment acquisition.
DirectDefense – DirectDefense offers a range of security consulting services including compliance and PCI DSS.
ECSC – UK firm ECSC offers managed solutions for customers including PCI services and consultancy.
Galix Networking – South African information security firm Galix Networking includes PCI compliance in its specialties.
Geobridge – Geobridge focuses on security, compliance, and payment services, which is fundamental to the PCI DSS process.
Grant Thornton – Accounting firm Grant Thornton includes enterprise PCI DSS QSA consultants.
GRC 360 – GRC 360 is a consultancy with PCI DSS capability operating in the Middle East region and UK.
GRSee Consulting – GRSee Consulting is an Israeli consulting firm that includes PCI DSS assessments.
Intersec Worldwide – Newport Beach firm Intersec Worldwide specializes in PCI compliance professional services.

IRM – IRM is a UK-based firm that provides a range of consulting services including PCI DSS.
Lazarus Alliance – Arizona firm Lazarus Alliance provides security, risk management, audit, and compliance.
Megaplan-IT – Megaplan-IT offers a PCI consultancy, including an on-site pre-PCI gap assessment service.
NetWorks Group – NetWorks group includes compliance services for PCI, HIPAA, and other frameworks.
Novacoast – Novacoast is a professional services company that includes compliance services for PCI, FISMA, HIPAA, and other frameworks.
Panacea Infosec – Indian firm Panacea Infosec provides information security services including PCI DSS certification.
Parameter Security – Parameter security includes compliance audits in its range of professional services.
Pentest Partners Compliance – Pentest Partners Compliance offers QSA and PCI forensics services.
Pondurance – Pondurance is an information security firm that includes security compliance services.
Redhawk Network Security – Redhawk Network Security specializes in information security with PCI QSA services.
RedIsland – UK-based consulting firm RedIsland offers information security and governance with PCI.
Security Risk Advisors – Security Risk Advisors includes compliance in its suite of information security consulting.
SISA – SISA is a payments security specialist firm located in India with capability in PCI DSS.
True Digital Security – True Digital provides a suite of network security, application security, and compliance/audit services for customers.
Truvantis – Truvantis offers authorized PCI QSA services as part of its professional services suite.
Westnet Consulting Services – Westnet Consulting Services offers IT network security, compliance, and PCI QSA services.

42. Vulnerability Management

⇒ *Process* – Vulnerability management must be a holistic organizational security process rather than a simple scanning and patching function.
⇒ *Approaches* – Vulnerability management can be done using hosted enterprise scan tools or through cloud-based subscription services.
⇒ *Trends* – Future vulnerability management processes will be less enterprise-centric and more focused on hybrid information collection across the cloud.

Vulnerability management involves the organizational processes, enterprise platforms, and security tools required to detect, document, scan, discover, patch, track, and manage security weaknesses in target systems. Most of the larger CISO teams include an enterprise vulnerability management group, usually armed with either an in-house scanning system or a partner vendor offering scanning services, assigned to this function. Smaller CISO teams usually rely on either subscription or outsourced support to provide vulnerability management. Internal and external auditors demand that vulnerability management programs be comprehensive and well documented.

The day-to-day responsibilities of every vulnerability management team, big or small, usually include the following activities:

- *External Vulnerabilities* – Good CISO teams collect and analyze externally reported vulnerabilities, categorizing and managing these vulnerabilities for local process improvement. Teams must be especially careful, however, to factor in the high likelihood that popular media reporting of security incidents will be inaccurate. Obtaining vulnerability information from popular consumer Websites is usually a bad idea.
- *Software and System Patch Management* – In all cases where the CISO team has not signed up for automatic patching, reported patches for applications, systems, and devices must be analyzed and determined if necessary for deployment. Patching across the enterprise has gone from spotty coverage in the early 2000's to highly efficient processes in most modern organizations. It's a shame, however, that software engineering remains in such a sorry state that every large software system continues to exhibit some set of exploitable vulnerabilities.
- *Internal Vulnerabilities* – These represent a particularly tough challenge for CISO teams, because it is difficult to manage vulnerabilities that have not been noticed. Discovery tools can help, but the risk of unknown, exploitable internal weaknesses may be the most challenging aspect of enterprise cyber security. Bug bounty and penetration testing initiatives can be helpful here, but CISO teams must expect that from time to time, ad hoc operation of the business will uncover vulnerabilities that can range from minor annoyances to horrific problems with potentially disastrous consequences. In regulated environments, some of these vulnerabilities will have to be reported, which has the odd effect of reducing the incentive for them to be found.

Many vulnerability management vendors offer subscription access to what is claimed to be a comprehensive list of relevant vulnerabilities. This can only be partially true, because proprietary misconfigurations, corporate system administrative errors, and local infrastructure design flaws will not be visible to a generic product or service from a vendor. Instead, proprietary vulnerabilities can sit dormant for months, years, or even decades until they are discovered through some means – usually by accident. Every CISO team knows that the vulnerabilities that

will cause *real* problems are rarely the famous ones that are reported publicly and discussed widely. Instead, the more intense problems come from something subtle introduced locally in a way that makes it difficult to detect.

Vulnerability management processes always include some form of automated *vulnerability scanning* and the goal is increased visibility across the enterprise. Many pundits and industry observers will equate vulnerability management to scanning (and perhaps patching), and this is partially correct, because scanning is an important component of the process. A danger, however, that must be managed in the enterprise is the informal interpretation non-technical managers and auditors might make regarding the concepts of "scanning." The term itself connotes a thorough examination of some entity in order to draw clear conclusions about the existence or absence of some concern. While this might be true in medicine, it is not true for the vast majority of vulnerability scanning.

Scanning is always done with an automated platform focused on visibility, and the types of vulnerability scanners found in a typical enterprise include the following:

- *Network Vulnerability Scanners* – These scanners focus on finding and examining visible computing resources at reachable locations (usually IP addresses) on target networks. Many of these products and services focus on inventory, as well as detection of security vulnerabilities. Firewalls often limit the reachability of network scanners. Several of these types of tools offer excellent visual representations of what was found.
- *Host Vulnerability Scanners* – These scanners focus on examining accessible resources on physical servers and endpoints. Host scanners often run at the application level, which limits their ability to detect kernel resident vulnerabilities. Scanners are emerging now that can help deal with virtual infrastructure.
- *Application Vulnerability Scanners* – These scanners target software components, systems, or applications. This type of scanner is often used to assess the security of Web applications. Scanners for proprietary or legacy software require a special build, which would only be attempted in an environment with significant resource, motivation, and consequence – as in, for example, a software application controlling safety in a nuclear power plant.

Security administrators must determine how deep and penetrating a given scan should be. More intense scans discover and collect more information about a target, whereas lighter scans provide less relevant and detailed information. On the flip side, however, deeper scans can create or disrupt target systems, whereas lighter scans probably will not. For example, simple network scans might do nothing more than a simple TCP protocol *open*. More involved scans would check to see which TCP or UDP ports are listening for inbound connections. They would then establish the

connections to see how far the test might go. The diagram below depicts the relative focus, typical depth, and reachability of each type of vulnerability scanner.

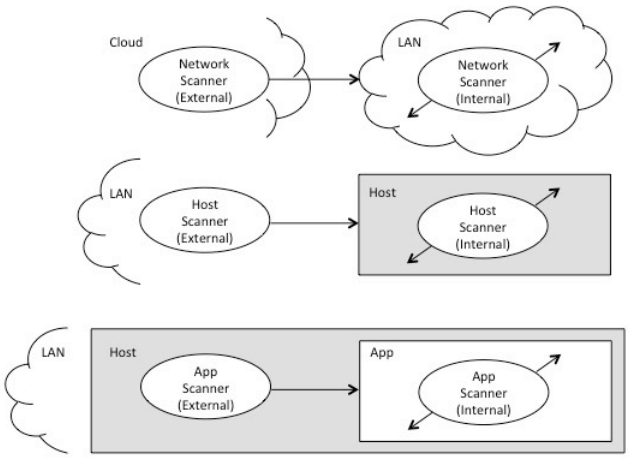

Figure 42-1. Vulnerability Scanning Approaches

In each of these cases, the scanning can be done continually at scheduled intervals, or manually on demand. Furthermore, the vantage point of the scanner is determined by its location on a network, host, or application environment. Scanners placed in some network segment might not, for example, be capable of detecting or scanning resources on another network segment separated by a firewall. The visibility in such cases is limited.

Companies today are evolving their infrastructure with transition to hybrid, multi-vendor cloud architectures filled with mobile devices and apps. They are also virtualizing their data center infrastructure, resulting in more vague enterprise perimeter delineation. To deal with this evolution, future scanners will need to perform more intelligent reachability and data gathering functions across private clouds, hybrid clouds, legacy enterprise LAN resources, and public clouds.

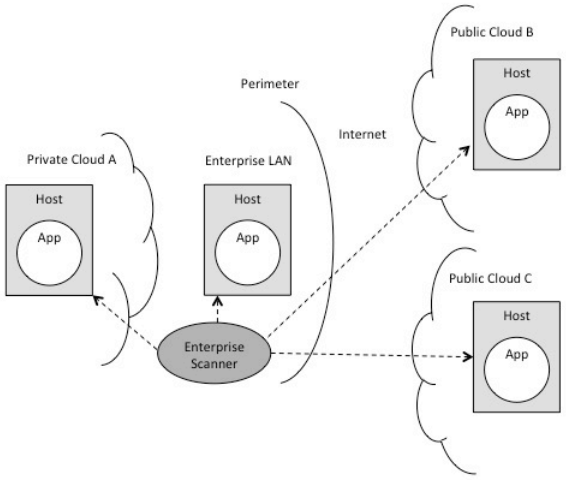

Figure 42-2. Expected Enterprise-Hosted Scanning Arrangement

The process of vulnerability scanning can also be done in unusual contexts such as using a search engine to scan for publicly advertised or accessible information. Many illegal and unethical methods for scanning are also well known (e.g., ones utilizing social engineering components), but certainly not considered within scope here. Scanning vendors or security consultants who even hint at such questionable activity should be quickly dismissed.

CISO teams need to be particularly mindful of licensing models for scan targets, especially in larger environments. A major issue in larger network environments is that budgets often cannot support scanning the entire target range of IP addresses, servers, and other resources. The result is a partial scan with gaps in visibility of the enterprise. Virtualization of servers and infrastructure will complicate licensing and increase the size of gaps as well. Negotiating scan license terms is thus an important consideration for any CISO team.

The CISO must take time to *clearly explain* to senior management and compliance auditors that scanning is not synonymous with security. Scanning requirements in compliance and audit-related projects often presume that to "run a scan" is to ensure security. This misconception is important to correct, since many scans do little more than open a TCP port to detect that some device is actually connected to a target IP address. CISO teams should prepare technical white papers and reports explaining the exact nature and function of all vulnerability scanning being performed.

The key points of differentiation for vulnerability scanners can be summarized in the following product and service attributes:

- *Discovery and Categorization* – Scanners should offer a suitable range of discovery and categorization options for endpoints on a network, processes or applications on a host, or code attributes in an application. This includes the ability to detect virtual systems.

- *Threat Information Base* – The scanning vendor should have sufficient access to best-in-class threat information generated internally, collected through partnership, or aggregated via crowd sourcing. Without good threat data, scanners will miss many of the most common techniques being employed by advanced attackers.
- *Compliance Monitoring* – Most enterprise security teams utilize scanners in the context of security compliance monitoring requirements for PCI DSS, HIPAA, and other frameworks. This implies that specific types of reports and formats are required in the scan output.
- *Product versus Service* – Enterprise security teams should determine if a managed service or an internally operated product is best for the local set of requirements. With the transition to cloud for most companies, a cloud-based managed service is increasingly acceptable.

The outlook for vulnerability scanning products and services in the near term is positive, but the likely targets of scanning will be less enterprise network-centric. Instead, vulnerability scanners will needed to operate in heterogeneous hybrid clouds, mobile applications, and legacy perimeter-protected applications. They will also need to have capability to handle increased use of data encryption, which can complicate visibility. As for more targeted scanning on hosts and applications, the function is likely to become more embedded and native to the enterprise virtual data center, rather than requiring of installation as a separate overlaid hardware or appliance product.

The biggest shift in the vulnerability scanning business, with the shift to virtual, will be greater emphasis on ensuring that *automatically provisioned virtual systems* have the proper security configuration, rather than trying to determine – after the fact – whether systems are configured properly. Keep in mind that a virtual machine can be created, used, and decommissioned in such a short period of time as to hide from a periodic scan process. More centralized provisioning in cloud and virtual data centers will change the face of enterprise-hosted scanning in the long term, rendering the process less relevant; but this will take some time – perhaps close to a decade, before it reduces the need for separate scanning as a control in a meaningful way.

These trends in the vulnerability-scanning marketplace can be represented in terms of market demand across different usage phases since 2000. Enterprise-hosted scan platforms saw significant rise during the past two decades, but now cloud-hosted solutions focused on hybrid infrastructure will begin to see a more significant rise. Companies with a network-hosted vantage point, will have an advantage, simply because can optimize the operational model to cloud.

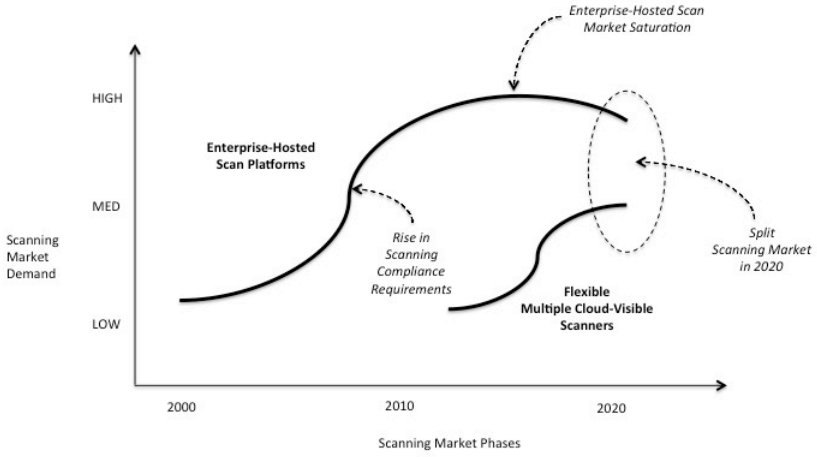

Figure 42-3. Trends in Vulnerability Scanning Marketplace

Vendors providing all forms of vulnerability scanning are going to grow and make money in the near term, but they should immediately begin to adjust their strategy to address cloud and virtual systems. In the long run, however, automated centralized provisioning will remove the some portion of the need to separately scan systems to detect sloppy system administration. This will be replaced, obviously, with the need to scan for other types of issues in virtual environments.

An area of future growth for scan vendors worth mentioning is industrial control and IoT. In both cases, the explosion of connected devices will create a market for discovery, search, and scanning, but R&D is required to determine how to actually find these systems. Unfortunately, advanced hackers are already beginning to perform such work as evidenced by the famous Stuxnet case.

Vulnerability Management Providers

Most CISO teams equate vulnerability management with vulnerability scanning, and the case can certainly be made that these functions are closely related. But some vendors go above and beyond the provision of scanners by offering platforms for creating structure in collected vulnerability data with connectors to SIEMS, integration with GRC, and other extended features. The vendors listed below generally offer both products and related services for scanning, but this decision might shift with the progression to cloud-based scanners, which will be managed on-demand by the owner without the need for deployed appliances. CISO teams investigating vulnerability management tools should also review the application security and Web security vendor lists in this report since there are so many similarities in focus. Managed security service providers and value added resellers also tend to include scanning as an option, and these groups are covered in a separate section.

2017 TAG Cyber Security Annual
Distinguished Vulnerability Management Providers

Lumeta – I've gotten to know Reggie Best and his fine Lumeta team quite well in the past few months during my research. Reggie has been generous with his personal time, helping me understand the vulnerability management process and the best techniques for establishing visibility into an enterprise. Many readers who enjoy the popular and visually striking Internet maps that Lumeta generated years ago will be happy to know that the company has gone far beyond these original scan processes with their current suite of vulnerability management and enterprise visibility products. Thanks again to Reggie and his team for their help throughout this project.
Qualys – When I started this research, Philippe Courtot, CEO of Qualys, was one of the first experts I contacted. I not only benefited from his fine technical knowledge, but also from his business experience and expertise. Qualys clearly nailed the concept of network-based vulnerability management before anyone else in the industry, even when security compliance managers were complaining that to deal with Qualys required opening in-bound ports on the firewall. The Qualys team knew that a cloud-based vantage point was best, and to that end, the company continues to be well positioned to provide expert vulnerability management and scanning capability to enterprise teams moving toward SDN, cloud, mobile, and virtual environments.

2017 TAG Cyber Security Annual
Vulnerability Management Providers

Acunetix – Acunetix provides a vulnerability management solution for Websites and Web applications.
Allgress – Allgress provides a suite of products and solutions focused on governance, risk, and compliance (GRC) and vulnerability management.
Audit Square – Audit Square provides a Microsoft Windows security, configuration, and audit assessment tools for desktops and servers.
Aujas Networks – Aujas Networks provides security solutions in risk and vulnerability management, data protection, and identity and access management.
Beyond Security – Beyond Security offers the AVDS automated security test suite for detecting weaknesses.
Contrast Security – Contrast Security provides a continuous application security tool to detect vulnerabilities and ensure compliance.
Core Security – Core Security provides a solution for consolidating and prioritizing vulnerability data.
Defence Intelligence – Defence Intelligence (Defintel) combines global threat data, research partnerships, analysis and tools to provide advanced malware solutions for customers.
Detectify – Detectify performs Web vulnerability scans through cloud-based tools that audit site security.

ElevenPaths – ElevenPaths provides a range of security products and services including authentication and vulnerability detection.
enSilo – enSilo provides data exfiltration detection solutions for enterprise customers experiencing a breach.
eSentire – eSentire provides active enterprise cyber security threat protection solutions including scanning, log centralization, and traffic capture for forensics.
Firebind – As part of its voice and video performance offerings, Firebind provides a passive, continuous network security and performance-monitoring tool.
FireMon – FireMon provides a security management platform with advanced security intelligence capabilities for enterprise, government, and service providers.
GroundLabs – GroundLabs provides software tools for sensitive data discovery to support compliance and avoid breaches.
HPE – HPE offers the WebInspect dynamic analysis security-testing (DAST) tool for vulnerability discovery and management in Web applications.
IBM – IBM offers the AppScan tool, which tests Web and mobile applications for vulnerabilities.
Indusface – Indusface supports security testing of Web, applications, mobile, and enterprise software.
Infocyte – Infocyte provides a solution that scans networks for evidence of exploitable vulnerabilities.
Intel – Intel continues to support existing customer base with legacy scanning solutions as they approach end-of-life.
ISARR – ISARR provides a Web-based platform for managing risk, resilience, response, and security intelligence.
iScan Online – iScan Online scans and detects vulnerabilities on enterprise endpoint and mobile devices.
Kenna – Formerly known as Risk I/O, the company provides a risk intelligence and vulnerability management platform.
Lumension – Lumension provides endpoint management with emphasis on patching, vulnerability management, and application whitelisting.
Lumeta – One of the original scanning companies, Lumeta has a rejuvenated team providing a combination of vulnerability discovery with visualization. Lumeta achieved great fame developing some of the most impressive and colorful network maps, showing entity relationships in small and large-scale environments that were not observable in any other manner.
Lunarline – Lunarline offers a range of cyber security and vulnerability management products and services including SOC operation, penetration testing, and privacy.
The Media Trust Company – The Media Trust Company provides media security scanning for Websites, advertisements, and mobile.
MyAppSecurity – MyAppSecurity provides security risk management solutions for designers and developers via threat modeling tools.
NETpeas – NETpeas provides an SaaS marketplace with a payment interface front-end to a variety of security solutions including vulnerability management.

NopSec – Nopsec provides an on-premise or cloud-based unified vulnerability risk management solution collects and manages scanning output.
N-Stalker – N-Stalker provides a Web-application security scanner that includes a free downloadable edition.
Onapsis – Onapsis provides a behavioral-based approach to detecting anomalies against business critical applications with emphasis on SAP.
OPSWAT – OPSWAT provides IT security products that protect devices, as well as secure and track data flows via malware scanning.
Outpost24 – Outlier Security provides agentless cyber security analytics as a service for endpoints.
Pwnie Express – Pwnie Express provides a range of penetration testing, security testing, asset discovery, and vulnerability.
Qualys – Qualys provides an industry-leading vulnerability management platform with the original virtualized, cloud-based solution. Qualys committed its approach to network-based cloud access long before most in the industry.
Rapid7 – Rapid7 offers AppSpider and integrates good hacking talent on the team with its products and services. Rapid7 acquired NT OBJECTives in 2015.
RiskIQ – RiskIQ provides solutions that scan the open Web to ensure security outside the firewall-protected enterprise, including on-line advertisements.
RiskSense – RiskSense provides a vulnerability management platform along with a range of security services.
SAINT – SAINT offers vulnerability management, penetration testing, and compliance solutions.
SAVANTURE – SAVANTURE provides managed security and consulting services including SIEM, log management, vulnerability management, and authentication.
SecludIT – SecludIT provides continuous vulnerability detection and management solutions.
SecPoint – SecPoint provides IT security products including a vulnerability scanner, UTM firewall, and Web scanner.
Secunia – Now part of Flexera, the company provides a vulnerability management platform for enterprise.
Security Scorecard – Security Scorecard provides a threat management system for collecting security-related information on the enterprise.
Shavlik – Shavlik provides patch management solutions for operating systems, virtual systems, and applications.
6Scan – 6Scan provides automated vulnerability detection and mitigation of malware on Websites.
Skybox – Skybox collects data from all network devices and systems and creates a model for analysis and response.
SolarWinds – In addition to network performance, application, and database monitoring, SolarWinds offers IT security and compliance solutions.
Solutionary (NTT) – Solutionary, an NTT Group Company, provides MSS and consulting for enterprise security using its cloud-based ActiveGuard platform.

Sucuri – Sucuri provides protection for Websites, malware removal, and network asset security.
Symantec – Symantec offers the Control Compliance Suite vulnerability management solution.
TaaSera – TaaSera build runtime behavior detection solutions to proactively identify vulnerabilities.
Tenable – Tenable provides the Nessus vulnerability scanner for advanced detection of weaknesses.
Tinfoil Security – Tinfoil Security offers a developer-friendly service for scanning a website to detect vulnerabilities.
Tripwire – One of the original security companies in the scanning and discovery business, Tripwire offers WebApp360 for the enterprise.
TrustWave – TrustWave offers a behavior-based scanning technology acquired via Cenzic in 2014.

Additional Vulnerability Management Providers

Buguroo Offensive Security – Spanish firm Buguroo offers a range of platforms and solutions including vulnerability management.
GamaSec – GamaSec provides malware detection and Web vulnerability solutions via the GamaScan platform.
Grendel-Scan – Grendel-Scan offers an open-source downloadable tool for supporting automated testing.
ITrust – Luxembourg-based information security company ITrust offers an online multi-anti-virus scanner platform.
Mavituna Security – Mavituna Security offers the Netsparker tool for automatically detecting vulnerabilities and security flaws.
MileScan – MileScan provides an intelligent scanner that simulates hacker attacks and identifies security risks.
Nikto – Nikto consists of an open source Web scanner for detecting vulnerabilities in servers.
NRI Secure – NRI Secure offers the automated GR360 Website security scanning solution.
Orvant – Orvant uses multiple proprietary and open source scanning tools to detect vulnerabilities.

43. Industry Analysis

⇒ *CISO Team Use* – CISO teams should learn to make use of cyber security industry analysis materials in their enterprise solution planning.
⇒ *Approaches* – Analysts tend to compare different vendors based on their range of security capabilities, which may or may not be locally relevant.

⇒ *Trends* – The role of the industry analyst for CISO teams is likely to mature, hopefully through more in-depth and accurate, practical analysis reports.

Cyber security industry analysis provides CISO teams with expert reference and comparative information about cyber security vendors and their offerings. The modern CISO team needs to learn how to use industry analysis in the same manner as threat intelligence or any other form of useful information sharing across a trusted community. Industry analysis can be written by experts with operational experience, or by career analysts who specialize in designing frameworks useful for practitioners.

Industry analysis can come from firms that focus only on analysis, or ones that combine analysis with consulting services, preferably offered behind a business "firewall," in order to maintain some semblance of impartiality. Analysis results can be made public or kept private, depending on the report circumstances. Analysis results are often embedded in vendor marketing literature to distinguish and differentiate security offerings. Analysis can target working CISO practitioners, such as this 2017 TAG Cyber Security Annual, or can focus on the needs of senior corporate executives and board directors.

The best cyber security industry analysis will take into account CISO team usage feedback, vendor marketing data, personal experiences with specific products and services, interviews with vendor principals, and quantitative comparative assessments. Analysis criteria will vary, but should always include the depth of features offered by a given vendor, the future roadmap and vision of the vendor, the experience of the management teams, and other tangible and intangible factors. Subjectivity is involved in all analysis, with some analysts basing their work exclusively on their own critical judgment. Bias is not a bad thing in good security analysis, as long as the bias is recognized and transparent.

Certain analysts like Gartner and Forrester create competitive structures as a means for explicitly comparing vendors. Vendors are actually *ranked* by these analysts into hierarchical groupings based on the evaluated criteria, and buyers are encouraged to weave such ranking into their source selection process. While rankings provide great fodder for cyber security industry gossip and discussion, they must be used with discretion, because the criteria for a high ranking might be poorly reflective of local usage needs. The idea that a CISO team should purchase the product of a vendor that is given a higher ranking than another is misleading and might even weaken the security posture of the purchasing team.

Competitive vendor rankings tend to be provided as a series of two-dimensional waves, boxes, and quadrants that place cyber security vendors into predetermined classes. In spire of all the legal disclaimers, the clearly implicit understanding is that vendors in desirable categories offer superior solution to vendors less desirable categories – or worse, in no category at all. Waves, boxes, and quadrants are typically published in an unusual manner, where the reports must be either purchased at great expense to the CISO team, or obtained from vendors who like the analysis.

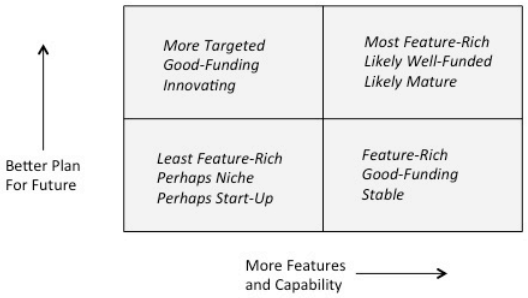

Figure 43-1. Competitive Structure for Cyber Security Industry Analysis

The primary advantage of waves, boxes, and quadrants is that recommendations are certainly clear. That is, vendors placed in higher classes are purported to provide superior solutions to ones placed in lower classes. Furthermore, the larger analysts have considerable reach across the CISO community, and can gather information about specific usage. So waves, boxes, and quadrants are not to be discounted. They do include useful information based on a great deal of work by the analysts.

Nevertheless, a conflict emerges between the published ranking of a given vendor and their *real suitability* for a specific CISO team. Smaller vendors, for example, with less impressive rankings might be perfectly suited and priced to their target segment, and with no need to scale up to a set of product features that would result in a better ranking. Furthermore, the criteria for certain vendors such as global reach and in-house staffing, might be irrelevant to buyers who are fine with domestic focus and outsourced services.

Perhaps the most controversial aspect of waves, boxes, and quadrants is the unregulated and poorly understood business firewalls, or lack thereof, between analysts and their consulting work. Clear conflicts of interest emerge when an analysis firm demands large consulting fees from a ranked vendor with the implicit understanding that the higher the fees, the higher the rankings. On the other hand, accepting reasonable administration fees from vendors to support analysis and research seems like a fair practice, as long as readers of the analysis understand the specifics of what is going on.

The process followed with this 2017 TAG Cyber Security Annual was to include and list every vendor we could identify in each of the TAG Cyber Fifty Controls categories in Volume 1 of this report. Vendors who were willing to sponsor the research, provide technical assistance, and submit for a detailed interview in Volume 2, were designated as *distinguished* and thanked for this assistance in a clear and transparent manner. Detailed listings of all vendors, including smaller ones, are included in Volume 3, so that CISO teams can use the information as a starting point for their own source selection. No rankings, boxes, quadrants, or other scoring mechanisms are included. As such, this report never makes the claim *anywhere* that vendor A is preferable to vendor B.

An additional point of debate in the analysis business is whether published research should be free or not. Most of the waves, boxes, and quadrants are not available free of charge, which has the effect of increasing the perceived value. On the other hand, free research might be worth exactly what a reader is paying, so CISO teams must take all of this into account. It seems reasonable for analysts to request and obtain fair payment for their research efforts, but some of the prices being asked for security research reports today seem excessive.

It is worth mentioning that investors and venture capitalists also perform a great deal of expert industry analysis. In some cases, CISO teams might get their hands on this material, usually as thick PowerPoint decks with lots of charts, graphs, logos, numbers, lists, and predictions. Practitioners should beware this type of analysis, because it is written to support investment models rather than the real needs of CISO teams. Furthermore, the backgrounds of the analysts producing this information can be spotty, so the material in many cases could be dead wrong. CISO teams must be *very careful* if they choose to read investment-related cyber security industry guidance.

Finally, a great number of academic think tanks exist, often with government or academic focus, who will comment on various aspects of the cyber security industry. These groups are only as good as their experts, so CISO teams would be wise to trust these reports based on the background of the writer performing research, regardless of the reputation of the firm. Retired senior government officials, for example, often provide excellent analysis once they are free of the public affairs constraints that maybe kept them quiet during their years of service.

Trending in the cyber security industry analysis area is highly positive with traditional and new entrants continuing to find a huge audience for their reports and analysis. A great deal of growth will come from senior executives and board directors who will want more quantitative seals of approval for selected vendors. It is unclear whether this expands to procurement teams limiting purchase options to vendors receiving the best "ratings" from analysts, but one can speculate that such an approach might be inevitable. Let's hope it doesn't happen.

2017 TAG Cyber Security Annual
Industry Analysis Providers

CSIS – CSIS is a well-known government think tank and public policy research institution that includes the respected and experienced expert, James Lewis, covering issues in cyber security.

Cybersecurity Ventures – Cybersecurity Ventures provides a comprehensive market report, which includes the popular Cybersecurity 500 list researched and edited by Steve Morgan.

451 Alliance – 451 Alliance is an analysis firm offering excellent research and information on the technology, telecommunications, and security industries. The group also sponsors conferences and working sessions on various topics.

Forrester – Forrester provides the well-known Forrester Wave in various business, technical, and security areas. The Forrester Wave is unabashed in offering specific judgment about the relative strengths and weaknesses of difference cyber security vendors.
Gartner – Gartner offers its famous Magic Quadrant in many different areas of business, information technology, and cyber security. Having a favorable Gartner magic quadrant rating can mean millions of dollars of new revenue for a vendor (and the reverse is true as well).
HfS Research – HfS Research offers blueprint reports and other research that focus on the "as-a-service" marketplace in technology and business.
IDC – IDC is well-known analysis firm with teams of expert analysts who provide a wide range of excellent research, commentary, and analysis on technology, including cyber security.
Light Reading – The fine team of analysts, writers, and experts at Light Reading are a valuable asset to the entire cyber security community.
Markets and Markets – Markets and Markets is a group that sells its Cyber Security Market Global Forecast as a download on the Internet.
Radicati – The Radicati Group is a technology market research firm that publishes a market quadrant report on cyber security that is similar to the Gartner Magic Quadrant.
Securosis – Securosis is an independent security research and advisory firm offering insights into Web 2.0, APT protection, and security investment.
TAG Cyber LLC – TAG Cyber provides this 2017 TAG Cyber Security Annual as a technical and market reference guide to CISO teams. The report, written by Dr. Edward G. Amoroso, highlights distinguished vendors who provide assistance in producing the report, but specifically avoids any vendor ranking, ratings, and recommendations.
TechSci Research – TechSci Research is an independent research and consulting firm that offers a wide assortment of market research.

44. Information Assurance

- ⇒ *Government Origin* – Information assurance solutions originate with government customers, and are migrating to commercial markets.
- ⇒ *Operational Focus* – Real time operational focus and situational awareness are the salient aspects of information assurance solutions for cyber security.
- ⇒ *Growth Trends* – The US market will expand into commercial, but will be limited in the specific international buyers that can be served.

Information Assurance (IA) services are integrated offerings of professional services and customized offensive and defensive tools offered to government and commercial customers. IA services frequently originate in the defense industry and expand to commercial usage after years of successful operation in military settings.

Many times they will overlap with similar commercial offerings with different legacy, but the salient aspects of IA services can be summarized as follows:

- *Government-Related Origin* – Virtually all IA services originate with some government or military project, and many of them remain there. The US Federal Government's Enhanced Cyber Security (ECS) email and DNS filtering service are examples of government-originated capabilities that are now commercially available IA services. The term "information assurance" itself was developed as the defensive response to "information warfare."
- *Large-Scale Infrastructure Focus* – IA services typically provide solutions for large-scale infrastructure organizations dealing with broad threats, rather supporting solutions for smaller companies or consumers. Governments purchase IA solutions to obtain this broad infrastructure focus, and larger commercial customers are attracted to this as well.
- *Cyber Offensive and Defensive Operations* – IA services usually provide technology support and guidance for large-scale cyber offensive and defensive operations. Cyber operations for IA implies large infrastructure.

Obviously, since IA services originate from vendors to government, defense contractors tend to dominate this industry, using long-standing relationships with government as a marketing differentiator. Many IA services, however, as alluded to above, follow a lifecycle path from inception to large-scale delivery to *commercial* customers. The size of the market and intensity of adoption generally falls as the IA services depart from their initial government market, but the allure to IA vendors is the perceived unbounded growth in the commercial market.

This process can be successful if the commercial buyer leans toward situation awareness, real time protection, and the tactical controls that characterize high-end IA services. But IA vendors will usually fail if they do not learn that *government program managers measure the success by the money they spend, whereas commercial project managers measure the success by the money they save.*

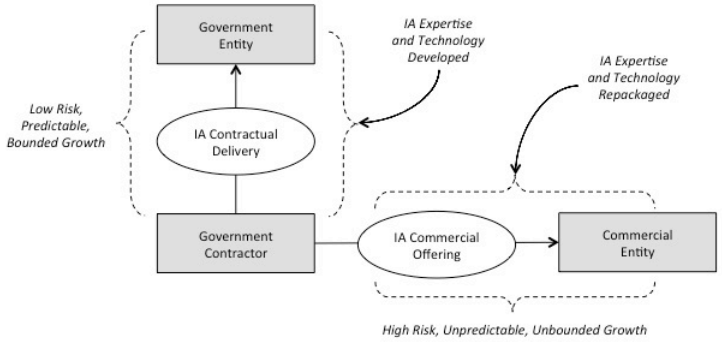

Figure 44-1. Information Assurance Commercialization Lifecycle

IA vendors who succeed in selling to government, but never recognize the incentive difference between government and industry, will fail in their efforts to grow their business commercially. This is not intended as a political statement, but is rather an observation of fact. IA vendors know that government agencies demonstrate their power and reach through size, scope, and budget. Thus, the ability for an IA vendor to partner with a government customer to lobby for and obtain funding is in the interest of both parties. This concept rarely exists in industry, where the goal is always to obtain the greatest service at the lowest cost.

The staff associated with many IA service companies will often maintain active clearances with some government agency, and might even support programs or services that include active participation from the Federal Government (as in, for example, the ECS offering from various commercial entities with involvement from the US Department of Homeland Security (DHS)). CISO teams visiting vendors with an IA focus who are offering commercial solutions will often find the development or SOC staff to be former government employees. Representative IA service capabilities commonly found in this category include the following:

- *Cyber Security Program Management Office (PMO) Services* – Many IA services will originate from PMO activity in government. The PMO is then extended, adapted, and repurposed for some other project or customer. This works well within government entities in a given country, but is not easy to accomplish from government to commercial operation where the regulatory, certification, and competitive pressure are often quite different.
- *24/7 Security Operations Center (SOC) Services* – The use of 24/7 SOC services in the government IA space is frequent and almost obligatory. Commercial entities, on the other hand, are more likely to outsource these functions to managed service providers. As such, SOC adaptation for commercial use is more difficult than reusing a SOC between one government customer and another (where the issues will be more political than business or technical).
- *Large-Scale Data Fusion for Cyber Operations* – This is an area of IA services where adaptation from government to commercial has the most promise. Commercial entities tend to admire (perhaps even over-estimate) the data fusion capabilities found in government. This implies that data fusion operations originating in government can generally be adapted for commercial use without great difficulty.

Obviously, many of these capabilities align with similar commercial offerings from consulting companies, penetration testing firms, managed security service providers, and other groups that never had anything to do with IA. The salient aspect considered here, however, is the common government and military origination of these services and support areas.

The outlook for the IA marketplace will remain stable with only modest overall growth. The pressures are as follows: Government use of IA will remain an important part of program management and requirements; commercial adaptation

will continue to provide a growth outlet for IA companies; and the large-scale cyber threat will continue to grow. Additionally, domestic US IA firms generally shy away from doing business in countries that might negatively affect their own government business. For example, a US defense company developing IA solutions for the US Government might be fine selling to a domestic bank, but not fine selling to a Chinese one. This marketing pressure can limit their growth considerably.

As government programs continue to feel pressure to find more efficient ways to handle the cyber threat, commercial adaptation of IA will see more competition than ever (thus driving down prices). This is tough for vendors, but good for buyers, especially because IA solutions tend to be excellent. In theory, with more IA focus, businesses and infrastructure operators should have more success countering cyber risk as they adopt tactics that are more military-oriented. The resultant IA marketplace will see a slight overall growth trend as shown below.

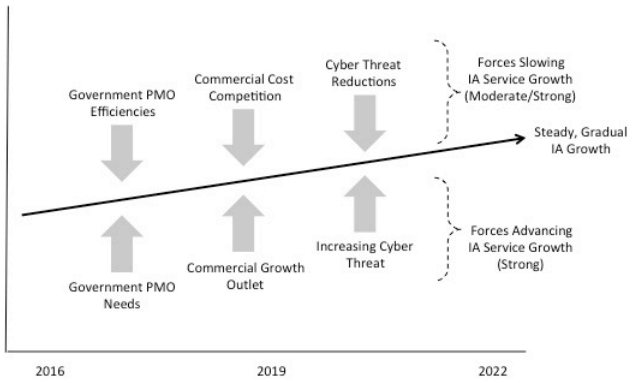

Figure 44-2. Information Assurance Marketplace Trend

Decisions will have to be made in the next decade about how international use of IA services proceeds. As suggested above, defense companies, for example, are currently very careful about how they market capabilities developed with the US Federal Government to customers outside the United States. This is particularly sensitive when such customers are in fact foreign governments. One country that has been unabashed about exporting government-originating technology to foreign buyers is Israel, where virtually every new start-up in cyber security boasts its legacy connections to Israeli Defense. More countries might move in this direction.

Information Assurance Providers

The Information Assurance providers listed below are companies with explicit programs of IA products and services. Virtually every defense company on the planet claims to be in the IA business, so CISO teams can expect to see offerings from defense and government contracting firms they might not expect to be in the business. Furthermore, every consulting firm and managed security service provider (MSSP) will claim to be an IA services vendor, so most of them are not

included here, unless they offer explicit IA services such as ECS. The list provided here serves as a good starting point for CISO team source selection.

2017 TAG Cyber Security Annual
Information Assurance Providers

Accenture – Accenture provides global professional services, consulting, and outsourced services, including cyber security.
Airbus Defence/Space – Airbus is a large aerospace company that includes a wide range of information assurance solutions.
AirPatrol – AirPatrol, part of Sysorex, provides platforms and tools for enterprise delivery of software and wireless protection based on the location and context of the users, with emphasis on serving US Federal Government customers.
Applied Physics Lab – The non-profit technology and research group, affiliated with Johns Hopkins University, provides IA services to the Federal Government.
ApplyLogic – McLean-based ApplyLogic specializes in cyber security and information assurance.
Assevero – Assevero is a unique virtual company offering information assurance services to the government.
AssurIT – AssurIT is an information technology (IT) services and solutions provider that specializes in cyber security.
AT&T – AT&T includes a mature Government Solutions unit that provides a wide range of information assurance, cyber security, and telecommunications protection solutions, including ECS, to government customers.
Axxum Technologies – Axxum Technologies is a minority and woman owned firm providing IT security and IA solutions.
BAE – BAE is a large British aerospace company that includes a range of information assurance solutions.
Boeing – Large American aerospace company Boeing includes a range of information assurance solutions.
Booz Allen Hamilton – Traditional professional services company BAH offers information assurance capabilities to its clients.
CACI – CCI is a defense contractor that provides a variety of technology and information assurance solutions.
Carahsoft – Carahsoft provides value added solutions including security and information assurance for the Federal Government.
CGI – CGI provides global IT consulting, systems integration, and outsourcing, including a practice in cyber security.
CSC – CSC is a traditional technology and professional services company that offers information assurance capabilities.
C3IA – UK-based small enterprise firm C3IA specializes in security solutions for defence applications.
Cyber Defense Agency – Sami Saydjari's consulting firm includes information assurance for government.

CyberDefenses – Consulting firm CyberDefenses includes a range of information assurance capabilities.
Cyber Net Force Technologies – CNF Technologies provides a range of cyber operations and systems engineering solutions with emphasis on network defense and intrusion detection.
CyberPoint International – Consulting firm CyberPoint International includes a range of information assurance capabilities.
Cybersalus – Cybersalus is a consulting firm in Reston that includes a range of information assurance capabilities.
Chertoff Group – Former US Homeland Security Secretary Michael Chertoff's consulting firm includes a range of information assurance capabilities.
CSRA – Government solutions provider CSRA formed from (CSGov and SRA) provides a variety of technology and information assurance solutions.
Delta Risk – Delta Risk is a consulting firm that includes a range of information assurance capabilities.
EWA-Canada – Canadian consulting firm EWA-Canada includes a range of information assurance capabilities.
Fidelis Cybersecurity – Fidelis Cyber security provides information assurance and cyber security solutions for enterprise customers.
4Secure – Data diode firm 4Secure offers information assurance-related solution for UK-based customers.
General Dynamics – Defense contractor General Dynamics provides a variety of technology and information assurance solutions.
Good Harbor – Former White House security expert Richard Clarke's consulting firm includes a range of information assurance capabilities.
Harris – Defense contractor Harris provides a variety of technology and information assurance solutions.
Hex Security – Hex Security provides security and information assurance consultation services toward both strategic and compliance objectives.
IBM – IBM is a large technology and professional services company that offers information assurance capabilities.
InfoDefense – InfoDefense provides security consultation services focused on regulatory compliance, information assurance, and response.
KEYW – HexisCyber, formed by KEYW through acquisition of Sensage, provides information assurance solutions.
Kroll – Kroll provides investigations, risk, and cyber security consulting services for business clients.
Leidos – Leidos offers solutions in national security, health, and engineering including cyber security.
Lockheed Martin – Large aerospace company Lockheed Martin provides an impressive portfolio of information assurance solutions including support for ECS.
Lunarline – Arlington-based firm Lunarline offers products and services with information assurance capabilities.

Magal S3– Defense contractor MagalS3 provides a variety of technology and information assurance solutions.
Mandalorian Security – Mandalorian Security provides a range of information assurance and information security advisory services in EMEA and Asia Pacific.
ManTech – Mantech is a consulting and sourcing firm that includes a range of information assurance capabilities, including active gateway traffic analysis.
Merlin International – Merlin International is a provider of IT and cyber security solutions for Federal Government.
MITRE – MITRE is a Federally-funded Research and Development Center (FFRDC) includes a range of information assurance capabilities. The Federal Government tends to rely heavily on FFRDCs to support their initiatives.
NCC Group – NCC Group offers a range of security testing and information assurance services including escrow, consulting, and domain services.
Network Security Systems Plus – Network Security Systems Plus provides information assurance solutions focused on Federal Government.
Newberry Group – Newberry Group is a provider of IT and cyber security solutions for Federal Government.
NEXOR – NEXOR provides security solutions for information exchange and information assurance.
NJVC – Virginia-based NJVC is a provider of IT and cyber security solutions for Federal Government.
Northrop Grumman – Defense contractor Northrup Grumman provides a variety of technology and information assurance solutions.
Patriot – Patriot provides a range of cyber security and information assurance solutions including infrastructure protection and mobile security solutions.
PivotPoint Security – PivotPoint Security provides a range of information assurance and security consulting services including penetration testing and ethical hacking.
QinetiQ – British defense contractor QinetiQ provides a variety of technology and information assurance solutions.
Raytheon – Defense contractor Raytheon provides a variety of technology and information assurance solutions.
Referentia – Referentia provides a range of information assurance product, and managed solutions with emphasis on government customers.
Renaissance Systems – RSI provides a range of solutions including cyber security/information assurance, cloud integration, network design, and other services.
SAIC – Defense contractor SAIC provides a variety of technology and information assurance solutions.
SecureNation – SecureNation provides IT security, compliance, and information assurance solutions through value added resale partnerships with technology vendors.
SecureWorx – SecureWorx provides secure data centre solutions for Australian government customers.

Sotera Defense Solutions – Defense contractor Sotera provides a variety of technology and information assurance solutions.
Strategic Cyber Solutions – Strategic Cyber Solutions provides US Government with cyber intelligence and cloud data analytics.
Swain Techs – Swain Techs provides a range of engineering, managed services, and cyber security/information assurance consulting services.
Tangible Security – Tangible Security provides a range of security consulting services including assessments and virtual CISO for government.
TASC – Defense contractor TASC provides a variety of technology and information assurance solutions.
TDI – Security consulting firm TDI provides a variety of technology and information assurance solutions.
TechGuard Security – IT services firm TechGuard provides a variety of technology and information assurance solutions.
TecSec – TecSec provides information assurance solutions for access control enforced through encryption and key management.
Telos – Cyber security solutions and secure mobility firm Telos offers information assurance solutions.
Templar Shield – Templar Shield provides a range of security consulting, managed security, and recruiting services.
Tenacity Solutions – Reston-based IT services firm Tenacity Solutions offers information assurance solutions.
Thales – The Thales Group is a French multinational aerospace, defense, and space contractor that offers a range of cyber and data security solutions.
Unisys – Unisys is a technology company that includes cyber security solutions for enterprise customers and government.
Van Dyke Technology Group – Van Dyke Technology Group is a consulting firm that offers information assurance solutions.
VariQ – VariQ is a Washington-based IT and cyber security consulting firm that offers information assurance solutions.
Vencore Labs – Formerly known as ACS, this division of Vencore focuses on R&D projects including information assurance.
Veris Group – Veris Group provides a range of cyber security/information assurance consulting services with emphasis on Federal Government customers.
Verizon – Verizon includes information assurance solutions for Federal Government customers in its portfolio.
Vistronix – Vistronix specializes in Big Data analysis solutions including a specialized focus on cyberspace and SIGINT operations.
Widepoint – Widepoint provides mobility, telecom, and cyber security services for Federal, state, local, and enterprise customers, with emphasis on identity management.
ZRA – Longtime government cyber security expert Lee Zeichner's consulting firm includes information assurance services for Federal Government and commercial clients.

Additional Information Assurance Providers

Decisive Analytics – Decision Analytics is an employee-owned engineering firm in Arlington includes a range of information assurance capabilities.
EmeSec – Consulting firm EmeSec includes a range of information assurance capabilities for government customers.
Information Assurance Solutions – Information Assurance Solutions Ltd. is a consultancy providing information assurance solutions.
Netwar Defense – Netwar Defense is an SBA provider in Maryland of IT and cyber security solutions for Federal Government.
Northstar Group – Northstar Group is a provider of IT and cyber security solutions for Federal Government.
SphereCom – SphereCom is an IT services company in Manassas that provides a variety of technology and information assurance solutions.

45. Managed Security Services

⇒ *Traditional MSS* – Managed security services emerged in the 1990's as a means for the enterprise to gain access to SOC-based capabilities.
⇒ *Network-Based* – Network-based security allows for advanced protections to be located upstream from the enterprise perimeter edge.
⇒ *Future Virtual* – Clear trends point to virtualized, on-demand MSS with support for self-provisioned enterprise mobility and SDN security.

Managed Security Service Provider (MSSP) solutions involve outsourcing select network security functions to an external third-party, usually offering 24/7 security operational support. An MSSP markets and sells to customers their centralized expertise and control, along with the ability to maintain the best available technologies and tools for protection. Companies of all sizes have tended to make use of MSSPs for perimeter security management. Internet service providers are natural participants in this market, given the type of work required.

MSSPs came into existence for enterprise use in the Nineties and grew in popularity afterward. Specifically, during that era, AT&T created the first managed security solution for packet filtering firewalls in partnership with BBN, ushering in the modern era of managed security services. The industry has grown considerably since then, with the business and security value propositions offered by MSSPs now including:

- *Monitoring of Security Devices* – As the use of security devices to guard perimeters became an essential component of enterprise protection methods, the tedious nature of device monitoring soon became apparent.

MSSP offerings filled this gap with the ability to provide up/down support for firewalls, intrusion detection systems, and so on.

- *Log Management and Analysis* – The volumes of user, event, and system logs generated from security devices provided an opportunity for MSSPs to expand their value proposition toward what is now referred to as SIEM analysis.
- *Centralized, 24/7 Support* – By amortizing multiple customers within a common Security Operations Center (SOC), MSSPs could feasibly support 24/7 operations in a cost-effective manner. Most enterprise organizations found that they could not create sufficient financial justification to build their own 24/7 support centers.
- *Expert Analyst Staffing* – Finding and keeping expert, trained staff for security management and operations functions is a challenge for enterprise groups, but more tractable for MSSPs that offer a wider range of challenges, exposure to different technologies, and more vibrant career paths for security professionals.

For these reasons, the original MSSP model flourished through the 90's and well into the mid-2010's. The traditional MSSP architectural and operational support model is shown below.

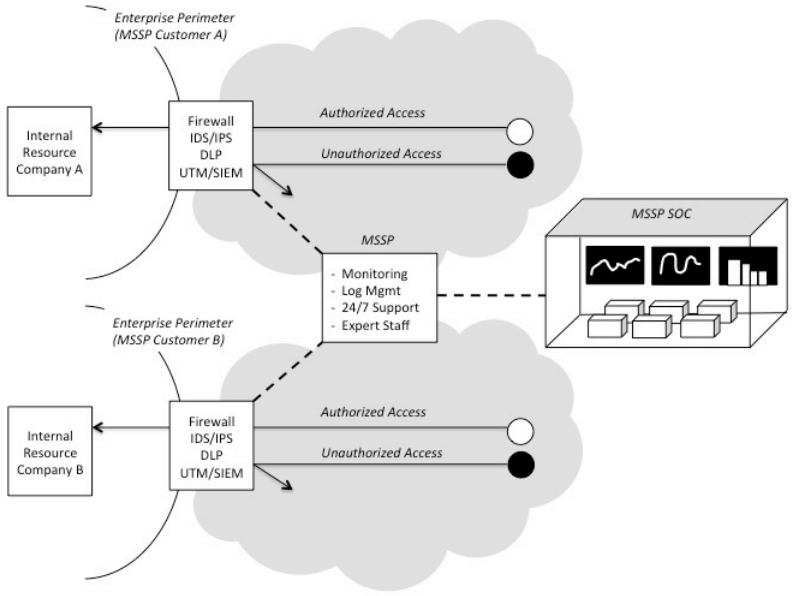

Figure 45-1. Traditional MSSP Model

In selecting an MSSP, customers should keep in mind that while MSSPs rarely refer to SOC support as a professional service, this is *most definitely* what is being performed. To that end, customers of MSSP offerings should demand specific information about the backgrounds and expertise of the individuals who will be

working on their account. This can make the difference between successful and unsuccessful MSSP engagements.

Internet service providers and telecommunications companies have been attracted to the MSSP model because it is compatible with their broader operational services. This compatibility includes interaction with the network perimeter edge, which is both the natural choke point for traditional security and the point of management presence for many carriers. It also includes the ability of an ISP or telecommunications provider to scale their operations and staff as business grows.

As the enterprise perimeter continues to vanish due to size, scaling, and complexity issues associated with maintaining trust inside an enterprise, many MSSPs have begun to rely on *network-based* protections virtualized either into the provider core or the public Internet. These virtual, network-based security services can be provided in-line for active mitigation, or off-line for passive security telemetry. In either case, the protection is offered "north" of the enterprise perimeter and does not rely on fixing the porous nature of firewalls and other demilitarized zone (DMZ) devices. The general approach to providing network-based security services is depicted below.

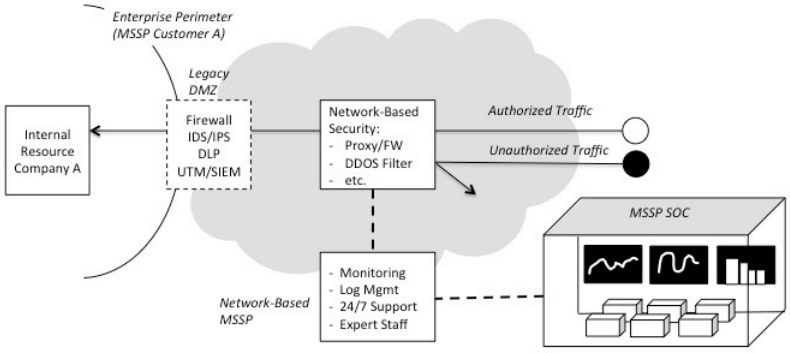

Figure 45-2. General Network-Based Security Approach

Once again, ISPs and telecommunications companies have a huge advantage in this type of arrangement because network-based nodes can be easily integrated with managed virtual private networks (VPNs) and amortized across multiple customers to reduce unit costs. This network-based VPN security node method, pioneered at AT&T in the late 1990's, thus looks to enterprise users as a normal node on the network, accessible through routing, and usually supportive of the Internet-facing and perimeter gateway functions.

Future MSSP offerings will begin to take advantage of the power of virtualization and its ability to efficiently create, expand, and manage computing power. As organizations untether security dependency from the perimeter, they will need the ability to create a virtual perimeter across heterogeneous, hybrid cloud infrastructures. The likely endpoint migration to BYOD and mobile devices for most companies will also require secure, containerized, virtual private networks (VPNs)

across diverse networks. This virtualization is best done in the presence of some chain of trust to trusted platform module (TPM)-like hardware integrity, but this might only be required for the most secure environments.

As such, MSSP offerings will need on-demand, customized virtual security provision for dynamic objects. This is likely to emerge as a virtual cloud marketplace for security, where users select on a portal the security services they need as part of the creation, use, and release of cloud services. In this model, vendors create virtual appliances that are selected at provisioning time from a menu of different options. Furthermore, as users access cloud resident apps over mobile infrastructure, a new type of mobile security service will emerge, most likely integrated with the mobile service provider's IP infrastructure.

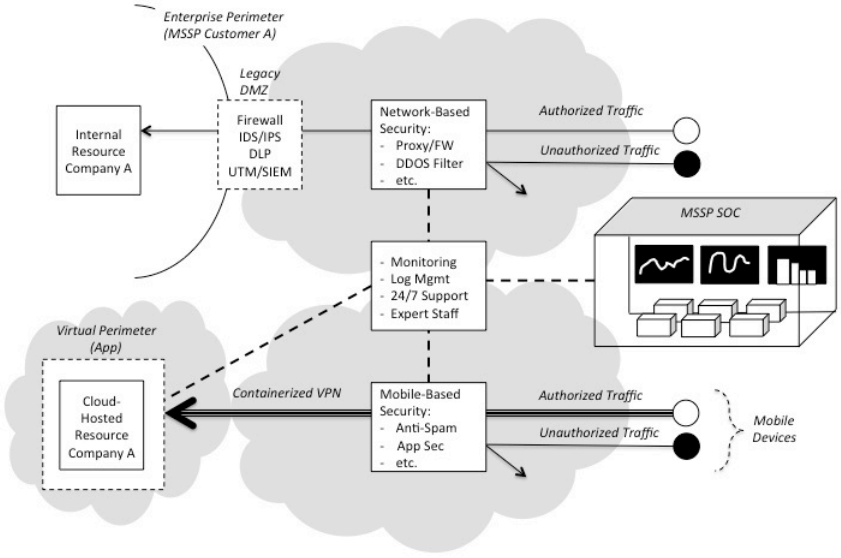

Figure 45-3. Cloud and Mobile Security Services

In many cases, the enterprise VPN is peered by the service provider directly to the public cloud infrastructure as in AT&T's NetBond offer. This allows for more secure access to cloud applications without the need to visit the public Internet. The virtual cloud perimeter is still required, however, because the enterprise perimeter has long since lost its ability to block malware, APTs, and deal with compromised insiders. The specific trends one should expect in MSSP services include:

- *Perimeter MSSP* – Enterprise CISO teams must expect continued reduction in the need for traditional customer premise equipment (CPE)-hosted perimeter-based MSSP services. Such hosting of CPE security hardware will be replaced by virtual security services.
- *Network MSSP* – CISO teams should expect gradual slowing of need for network-based services as the perimeter erodes. The network-based

approach will continue to be important for Web and email solutions, but will also be supplanted by virtual security services.

- *Cloud MSSP* – Every indicator suggests a *rapid escalation* in the need for virtual, public cloud-based managed security services. Smaller organizations will move to this model more quickly, with larger companies such as banks focusing on private and hybrid cloud arrangements.
- *Mobile MSSP* – CISO teams should expect a growing need for mobile infrastructure managed security services. This will require integration with cloud MSSP services, as well as with enterprise mobile device management (MDM) solutions.
- *SDN-Based MSSP* – The provision of software defined network (SDN) technology creates the possibility that SDN service providers such as ISPs and MSPs can offer dynamic service chained provisioning of security functions. The result will be point-and-click set-up of a security architecture in an enterprise. It will also help support IoT devices on a mobile network.

CISO teams *should not* assume that the same MSSP market leaders for perimeter and network will simply inherit leadership into the cloud and mobile spaces. The core competencies, especially for cloud managed security, are different from those required for more traditional MSSP offerings. Thus, only the most forward-looking MSSP participants will have a well-formed roadmap for guiding their clients into cloud and mobility-based infrastructure, including the use of public, hybrid, and private cloud services connected via SDN. While some may disagree, the belief here is that the ISP model, combined with an open, API accessible SDN core, will provide the best capability for future MSSP services.

Managed Security Solution Providers

Managed Security Service Providers (MSSPs) listed below include the most obvious participants. Some smaller consulting firms that list MSSP as a capability were not included because they often support only one or two customers. Furthermore, product vendors who include a managed support option were not included, because this somewhat limited offering does not constitute a full service MSSP. The list of MSSPs is surprisingly large, given the high cost of operations to maintain currency with modern cyber security technology and threat.

Note that many value added resellers often market support for managed services, but this is covered in a separate VAR section of this report, so most VAR solution providers reselling MSS are not listed below. It is my belief that with SDN deployment, the value proposition for VARs to be in the MSS business will shrink in comparison to the opportunity for VARs to help enterprise customers optimize integration of their virtual infrastructure. Related sections such as information assurance and security consulting should be folded into any CISO team source selection planning for MSS, especially for groups associated with Federal Government work.

2017 TAG Cyber Security Annual
Distinguished Managed Security Service Providers

AT&T – It is my sincerely held belief that AT&T's bold plan to virtualize its telecommunications support and operations based on an open-source, API-enabled SDN core, will enable a fresh new generation of flexible cyber security capabilities provisioned through an on-demand managed security services marketplace. Where so many industry analysts view the area of managed services in the context of support and operations models, they miss the critical nature of the decision to virtualize, and how this will prove to be the most important factor in the long run. The AT&T team continues to provide great friendship and support through my TAG research activities, and I am certain that the work being done now in the company to support virtualization will be referenced in the next generation as one of the major positive turning points in the fight against APT attacks.

2017 TAG Cyber Security Annual
Managed Security Service Providers

Above Security – Canadian firm Above Security delivers customized managed and IT security services including NIDS, HIDS, and log analysis for protecting enterprise customer infrastructure.
Accenture – Accenture Operations offers managed cyber defense, managed identity, and managed compliance as part of its managed security service offerings. The acquisition of FusionX provided capability in cyber risk management.
Alert Enterprise – Alert Enterprise provides infrastructure protection through governance, risk, and compliance (GRC) management, situational awareness, and continuous monitoring.
Alert Logic – AlertLogic, headquartered in Houston, offers 24 by 7 monitoring and a research team as part of its managed cloud security services.
Allstream – Ontario-based Allstream is a Canadian telecommunications company offering a range of voice, IP, and unified communications, including managed security services.
Arcon – Brazilian firm, Arcon, is a managed security services provider serving enterprise customers in Latin America.
AT&T – AT&T currently provides a full range of managed security services including network-based protections for email and Web. AT&T has made the bold decision to aggressively virtualize and even open source its SDN core. This push to an SDN-enabled infrastructure will enable a plethora of new on-demand capabilities in MSS.
Aura Information Security – Aura Information Security, acquired by Kordia in 2015, offers security consulting and managed security services in New Zealand.
Bell Canada – Bell Canada markets managed network protection services for Web, email, DDOS, and identity.

BinarySEC – French firm BinarySEC, provides a managed security solution to reduce the threat of attacks to Websites.
BT – BT Managed security includes DDOS, cloud, firewall, and event monitoring. In 2006, BT acquired one of the pioneer managed IDS companies, Counterpane, which had been founded by industry expert Bruce Schneier.
CenturyLink – CenturyLink Business provides two levels of managed security. The basic level includes managed firewall services, and the comprehensive level introduces email and URL security.
China Telecom – China Telecom is a large state-owned telecommunications provider of phone, Internet, mobile, and application services, including managed security.
Clone – Philadelphia-based Clone Systems is a managed security services provider focused on continuous monitoring, secure private cloud, security scanning, and security consulting.
ControlScan – Located in Alpharetta, Georgia, ControlScan provides a range of managed security services and compliance support solutions.
CSC – CSC supports traditional managed security services for data center, endpoint, network, and applications through its Risk Management Centers.
Cyber Engineering Services – Cyber Engineering Services is a small firm in Columbia, Maryland that provides managed data protection services for small and mid-sized companies.
DarkMatter – DarkMatter offers professional and managed security services and solutions in Abu Dhabi.
Datapipe – Jersey City-based Datapipe offers a range of managed, hosting, and cloud services, including managed security, compliance, and resale services.
Deloitte – Deloitte is a professional services company that focuses on audit, finance, tax, and consulting, including enterprise risk and compliance services as well as MSS through its acquisition of Vigilant.
Deutsche Telecom – Deutsche Telekom is a German telecommunications provider offering a range of managed and network-based security services. The company also offers cyber security through its T Systems unit.
DMX Technologies - In addition to its digital media, ICT, mobile SaaS, and managed services, Hong Kong-based DMX Technologies offers a range of managed security solutions and consulting services.
Earthlink – Earthlink provides Internet services including security services for residential and business customers in the US.
EWA-Canada – EWA-Canada provides information assurance services in Canada including IT risk management and managed security services.
Foreground Security – Foreground Security, now part of Raytheon, provides virtual security operations center, managed security services, and threat intelligence.
GBprotect – GBProtect is a managed security service provider located in Colorado offering security operations and applications management as well as consulting.
The Herjavec Group – The Herjavec Group is a Canadian technology firm specializing in network security managed services and consulting. Robert Herjavec, Founder of The Herjavec Group, is one of the stars of the ABC television program, Shark Tank.

IBM – IBM offers a range of managed security services accessible to customers through a common Security Operations Portal.
Igloo Security – Igloo is a Korean company that provides managed security services including SIEM management.
Kernel – Located in Colorado, Kernel provides a range of security services including managed and network security as well as penetration testing and security audit.
Level 3 – Colorado-based telecommunications firm Level 3 offers a range of traditional managed security services.
Masergy – Plano-based Masergy provides a range of enterprise networking solutions including advanced managed security.
MegaPath – MegaPath provides voice, data, and broadband telecommunications including managed security services.
My Digital Shield – My Digital Shield (MDS) provides enterprise network security-as-a-service solutions focused on the small and medium-sized business market.
Netsurion – Netsurion provides managed security services, mobile access, and compliance solutions for enterprise customers.
NTT Communications – Japanese telecommunications firm NTT Communications provides a range of managed security services.
Orange Business Services – Headquartered in France, global integrator Orange Business Services includes a managed security service offering.
Paladion – Located in India, Paladion offers managed security services and a range of risk management-based consulting services.
Proficio – Proficio offers advanced cloud-based managed security services with SIEM and SOC-as-a-service.
Quadrant Information Security – Quadrant Information Security provides a range of security consulting, managed security, and enterprise security management.
Rook Security – Rook Security provides advisory services, managed security services, and solution integration.
SAVANTURE – SAVANTURE provides managed security and consulting services including SIEM, log management, vulnerability management, and authentication.
SecureWorks – SecureWorks issued an IPO in 2016 from its parent company, Dell. SecureWorks, which has been in the MSS business since 1999, bases its services on its Counter Threat Platform.
Security on Demand – San Diego-based Security on Demand offers managed security solutions for enterprise and cloud.
Sentor – Swedish company, Sentor, provides a range of IT security services including network protection, log management, and vulnerability monitoring.
SilverSky – SilverSky, now part of BAE Systems, provides cloud-based enterprise managed security services including secure, hosted email.
Solutionary – Nebraska-based Solutionary operates as a separate subsidiary of NTT, offering managed security services.
Sword & Shield – Sword & Shield provides a range of managed and professional cyber security services.

Symantec – Symantec includes managed security services in its extensive security portfolio.
TaTa Communications – Internationally based TaTa is an outsourcing and technology firm that includes managed security services.
Tech Mahindra – Tech Mahindra is an Indian IT outsourcing and services company that includes an information security services practice.
Telefonica – Telefonica is a Spanish broadband and telecommunications company that includes a managed security services offering.
TELUS – TELUS is a global telecommunications company in Canada that offers a range of managed security services.
TrustWave – TrustWave is a leading security compliance firm that includes a range of managed security services including support for SMB.
2Keys – 2Keys provides a range of managed and professional services with emphasis on user authentication and identity attributes.
Verizon – Large US-based telecommunications firm Verizon includes a traditional range of managed security services offers. The company acquired security professional services firm CyberTrust in 2007.
Vigilant – Vigilant provides a range of cyber security services including managed network security, managed endpoint, and consulting.
Vijilan Security – Vijilan offers a range of managed security services including monitoring and incident response.
Wipro – Outsourcing and technology firm Wipro includes a range of managed security services.
XO Communications – XO Communications is a telecommunications services provider that offers a range of managed security services.

46. Security Consulting

- ⇒ *Consulting Areas* – Cyber security consulting ranges from high-level management guidance to more technical assessments by experts.
- ⇒ *Final Report* – Every security consulting engagement includes the obligatory final report as a documented record of the assessment work done.
- ⇒ *Practical Considerations* – CISO teams must be careful to match their selection of security consultant to their actual project needs.

An important management consideration for CISO teams is whether to hire full or part-time staff to accomplish its cyber security task objectives, or to engage a *security consultant*. Third party consulting expertise can be more carefully matched to a specific task, and does not require the costly overhead of benefits, office space, and other employee requirements. Furthermore, the consulting option is becoming more popular than ever as a large security professional services industry has emerged to meet the growing need for external cyber security support in the

enterprise. CISO teams should therefore give source selection of consultants at least as much consideration as other security controls.

Security consulting specifically involves paid experts – and many do not come cheap – providing guidance on cyber security-related issues to their clients. Such engagement might involve senior, experienced cyber security executives offering high-level guidance on risk and governance issues to business clients. Or it can involve cyber security subject matter experts, even white hat hackers, providing more focused technical insights to a client. Services considered in-scope to the security consulting designation include the following:

- *Security Policy and Architecture Reviews* – Involves expert review of organizational policies and architectures with attention to cost effectiveness and security risk reduction. The consumer of such reviews can range from IT teams to security policy writers. This task is deceptively complex, because while the result might not always require deep technical expertise, it does require sufficient local knowledge to create feasible plans. Too many security policy and architectural reviews make academic recommendations from textbooks that cannot possibly be implemented in the actual environment.
- *General Security Posture Assessments* – Includes high-level assessment of overall effectiveness of security programs in protecting organizational assets from attacks. The consumer here tends to be management, but working level staff can benefit as well. Posture assessments are also deceptively complex and can suffer from unrealistic, academic treatment if done by ivory tower teams.
- *Automated Security Assessments* – Involves testing, probing, scanning, and even hacking to provide insights into the security posture of an organization. Penetration testing, PCI DSS/compliance, and bug bounty services are included in this designation, but are addressed separately in this report. CISO teams must beware of the automated assessment that generates a report showing many thousands of vulnerabilities in some area. While it is possible that some enterprise environment might actually be this bad, usually large volumes of vulnerabilities in an automated assessment suggest a repeat occurrence of the same problem.
- *Security and Business Risk Analysis* – Includes estimating and calculating risk with recommendations for risk reductions in new and existing security programs. Business and financial risk models are increasingly being applied here, but this is often a force-fit. Many CISOs like to keep this task simple, preferring that consultants provide a basic summary of the top ten cyber security risks, with straightforward recommendations on mitigation.
- *Security Strategy and Planning* – Includes short and long-term security strategy creation, planning, and implementation. The consumer here is almost always upper management including the CISO and CIO. The danger in such engagements is the production of a high-level plan with no grounding in

reality. CISO teams must keep a close watch on consultants brought in to do security strategy and planning.

- *Mergers and Acquisition (M&A) Assessment* – Includes recommendations and pro/con analysis of potential targets of acquisition in the cyber security industry. Offering this type of guidance requires experience and expertise in business, financial, and cyber security areas. Very few cyber security consulting firms have the maturity to provide this type of service.
- *Regulatory and Compliance Management* – Includes management planning for local, state, and federal regulatory requirements compliance. This is a niche type of consulting that is valuable wherever the compliance or regulatory environment is so complex that it inherently introduces risk just by its very existence.

Perhaps the unifying aspect of all security consulting service engagements, whether they involve automated scans or business risk formulas, is the so-called *final report*. Buyers of security consulting services have come to expect this report as the tangible output and proof that the consultant has accomplished something useful. Without a final report, buyers have no means for recording work performed or sharing recommendations among team members.

Given the sensitive nature of a final report, document protection and sharing are important throughout the lifecycle of a security consultation. Too many CISO teams agree to a detailed data collection, analysis, and assessment from a consultant, followed by a truly sensitive document being passed around with maximum cringe on the public Internet as an unencrypted attachment to clear text email. If your security consultant appears comfortable with this sort of document sharing arrangement, then you have probably selected the wrong consultant.

In fact, a consultant's document sharing norms during source selection might help differentiate between providers. The consultant who handles your proprietary request for proposal (RFP) best should be given an edge over others – at least in the important category of information handling. Obviously the content of their responses should be the *primary* consideration, and as mentioned above, the structure of responses is almost always the so-called *final report*.

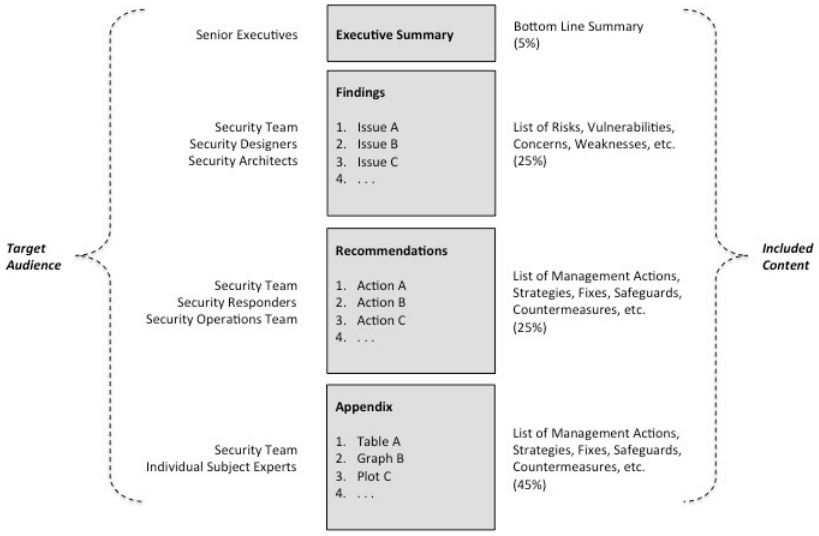

Figure 46-1. Security Consultant's Report Structure

As shown in the diagram above, the vast majority of security consulting projects end with a final report delivered to management with the obligatory executive summary, detailed findings usually numbered and listed in priority order, set of management recommendations usually offered with a proposed set of deliverables, milestones, cost estimates, and schedules, and a detailed appendix with charts, graphs, and tables summarizing the research, scanning, and interviews that were used to create the report.

While it is easy to poke fun at this repeat structure, it should be emphasized that this approach to documenting security findings is so common because it generally works. Organizations who contract to have such a report generated should ensure that the specifics are developed in phases, with reviewed input at various steps during the process. Information included in the report should be relevant and specific to the target organization, and should be specific enough to direct action. All of these reports should be written in a no-boiler-plate zone.

One exception to the final report rule involves so-called staff augmentation projects. In these cases, the consultant is hired to become part of the local day-to-day team, behaving essentially as an employee. While this practice has many human resource (HR) implications related to legal matters, benefits, longevity, and training, the staff augmented approach has advantages for the security team. It introduces fresh blood into a team, and allows for fine-tuned matching of skill sets to specific phases of projects. Government agencies seem to especially enjoy this model, which is why virtually every information assurance firm also provides staff augmentation. Like ketchup and cooked meat, the two offerings are made quite differently, but the buyer likes to consume them together.

Regardless of the work being performed, the *most important factor* in selecting a security consultant is the collective background of the firm being hired,

and the specific and relevant background of the individuals doing your analysis or project work. Experience and expertise in your organization's specific domain is also essential. Energy companies, for example, should demand that their consultants actually know the difference between transformation of electric power and transformation of business processes.

When reviewing proposals from different security consulting firms for a given project, buyers are advised to address the cross product of the consultant's general level of expertise in cyber security (ranging from modest to high) with the correlated focus of their expertise in your organization's area of expertise (ranging from low to high). The resulting value for a given consultant, such as high security experience and low domain correlation, or modest security experience with high domain experience can be matched to the needs of the project.

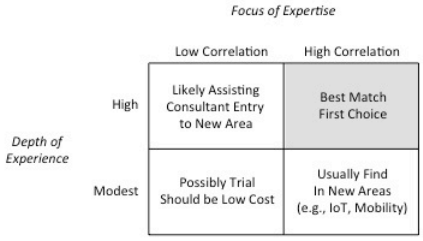

Figure 46-2. Handy Guide for Security Consultant Assessment

One commonly cited factor that should *not* influence buy decisions for security consulting services is the size of the firm. Larger consulting firms will certainly have more resources for more extensive efforts, but a small firm with experienced personnel who understand the target domain of operation can also do a fine job. In fact, smaller firms often provide more customized, personalized, and friendly service than a larger company.

Many professional security consultants market their expertise in physical security, personnel security, travel security, political security, equipment security, and other business areas where "security risk" is an issue. Some of these areas, such as investigations and asset management, do have overlap with cyber security, but CISO teams should be careful to check the credentials of any consultant. Former police officers are awesome for helping to optimize safety and logistic support, but might have less experience with software vulnerabilities in your virtualized data center. So be careful if you are easily swayed in your selection process by consultants with former law enforcement association. This is sometimes great, but sometimes not. You have to check.

Market trending for security consulting services will involve continued steady increases in both revenue and engagements for the foreseeable future. For firms currently performing security consultation, the extremely low barrier to entry for new participants will throttle individual growth. In fact, product companies who are struggling to generate revenue from their offering will use professional services

to help pay the rent. Sometimes great deals can be had through such an arrangement, but the long-term commitment of the company to consulting might be somewhat questionable.

Regardless of the growth throttling in this area, certain types of security consulting will see hyper-growth in the coming years. These include security architectural assessments and support for cloud and virtualization migration, IoT deployment, and mobility adoption. Very few companies know how to transition to cloud and SDN, for example, so security consultants who can help them manage risk through this process will be quite successful. Other security consulting areas will see more muted growth as the enterprise becomes less coherently organized around a perimeter-protected local area network and as compliance projects become more and more redundant.

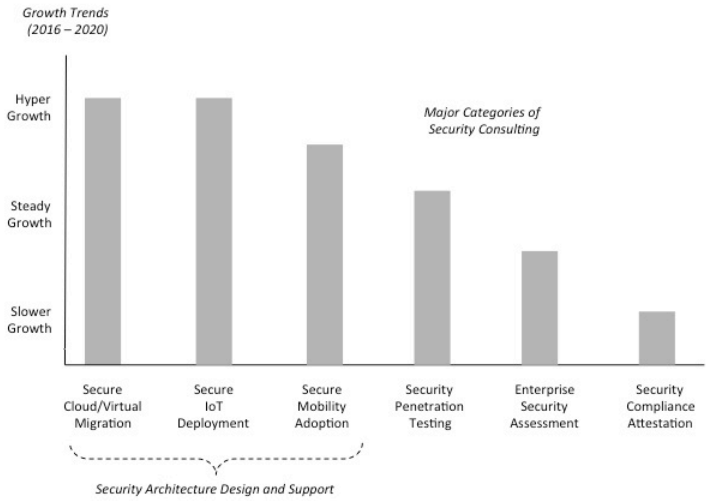

Figure 46-3. Trends in Security Consulting Areas

The implication of slower growth in compliance assessments might come as a surprise to some, but this is a healthy response to the unreasonable burden numerous compliance assessments place on CISO teams. Doing compliance once, and doing it well, is highly preferable to doing multiple compliance assessments with a high degree of redundancy. Cyber security compliance consulting should therefore evolve to more focused, higher value engagements at much lower volume. This issue is addressed in more detail in the PCI DSS/Compliance section of this report.

Security Consultants

The list of cyber security consultants below cannot possibly be complete, simply because a CISO could retire tomorrow, hang out a consulting shingle, and provide excellent consulting services. CISO teams should therefore use the not-surprisingly

large list below as a very small subset of the potential market and as a starting point in source selection. Penetration testing, PCI DSS, and vulnerability management vendors often provide theses services as part of security consulting engagements, and are addressed in separate sections.

ABR-PROM – ABR-PROM provides value added reseller (VAR) security solutions and IT outsourcing to customers in Poland.
Accenture – Accenture provides global professional services, consulting, and outsourced services, including cyber security.
ACROS Security – ACROS Security is a Slovenian provider of penetration testing and related information security, application assessment, and research services.
Advent IM – UK-based Advent IM is a cyber and physical security consulting company.
ANX – ANX provides a range of managed compliance and collaboration services including PCI DSS compliance and secure connectivity.
Aon – London-based Aon provides risk management and insurance brokerage services, including cyber insurance.
Ascentor – UK-based Ascentor offers its customers a range of information risk management consulting services.
Assure Technical – Assure Technical, located in the UK, provides a range of cyber and physical security consulting services including training.
Assuria – Assuria provides security solutions, security software, and managed SIEM services supporting security operations and enterprise security needs.
AsTech Consulting – AsTech provides a range of security consulting services in the areas of discovery, remediation, software development, and training.
Atredis Partners – Atredis Partners provides software security research, embedded security, and penetration testing services.
Atsec – Austin-based atsec provides laboratory and consulting services in the area of information security.
AT&T – Large telecommunications firm AT&T includes a team of expert security consultants to complement MSS offering. The acquisition of Verisign's consulting team in 2005 complemented AT&T's managed security service offerings.
Attack Research – Attack Research provides a range of security consulting, assessment, and training services.
Aujas Networks – Aujas Networks provides security solutions in risk and vulnerability management, data protection, and identity and access management.
Aura Information Security – Aura Information Security, part of Kordia, offers a range of information security consulting and managed security services for enterprise customers.
Aurora Information Security & Risk – Aurora Information Security & Risk provides a range of security consulting solutions for enterprise customers.

AVeS – AVeS provides a range of IT consulting focused on digital information and information security.
Avnet – Avnet provides security consulting services with emphasis on helping companies secure their databases.
Axxum Technologies – Axxum Technologies is an IT security services and solutions company focused on government customers.
Azorian – Azorian Cyber Security provides a range of cyber security services for enterprise customers.
Bambenek – Bambenek is a cyber security investigations and consulting group located in Illinois.
Banff Cyber – Banff Cyber provides a solution for Web defacement along with complementary security consulting offers.
BHC Laboratory – BHC Laboratory provides independent security consultation and advice for business customers.
Bishop Fox – Bishop Fox provides cyber security consulting, assessment, and testing services to enterprise customers.
Bitcrack – Bitcrack provides a range of security consulting services for business customers including penetration testing.
Bitshield Security – Bitshield security provides IT security consulting services and professional training for customers in the Philippines.
BitSight – BitSight provides a security posture assessment and rating for organizations based on their visible behavior.
Blackfoot – Blackfoot provides a range of security consultants including risk, PCI, security awareness, and other areas.
Booz Allen Hamilton – Technology services and consulting firm BAH includes cyber security and information assurance.
BugSec – Located in Israel, BugSec offers cyber and information security technical services.
Burns and McDonnell – Burns and McDonnell makes available a vast array of engineering services in many different areas including integrated security focused on compliance.
Caliber Security Partners – Caliber Security Partners provides security technical and strategic advisory services, as well as staffing services, for enterprise customers.
Capstone Security – Capstone Security offers services in the area of application security, regulatory compliance, and security assessments.
Carve Systems – Carve Systems provides security consulting and penetration testing services for IoT devices.
Certified Security Solutions – Certified Security Solutions (CSS) provides security solutions in the areas of PKI, encryption, and identity, with emphasis on securing IoT.
CGI – CGI provides global IT consulting, systems integration, and outsourcing, including a practice in cyber security.

Chertoff Group – Former DHS Secretary Chertoff's consulting and advisory services firm offers high end services including advice on M&A. The Chertoff Group tends to employ senior officials with deep government management expertise.
Cigital – Cigital provides consulting services in the areas of application and software security design, development, and maintenance.
Cirosec – cirosec provides security consulting and information security support for enterprise customers in Germany.
The CISO Group – The CISO group offers information security consulting with an emphasis on PCI DSS compliance issues.
CMT – CMT, now DataEndure, provides a portfolio of security, compliance, and archiving solutions for protecting business sensitive information.
Coblue – Coblue offers a security benchmark platform that allows organizations to assess security posture.
Comda – Comda provides a range of IT security products and services including biometrics, access control, consulting, and VAR integration.
CompliancePoint – CompliancePoint provides a range of compliance assessments, consulting, and managed IT.
Comsec Consulting – Comsec Consulting provides a range of security professional services for business customers.
Content Security – Content Security provides security consulting and professional services for enterprise customers.
ContextIS – Context Information Security (ContextIS), part of Babcock, provides security consulting and professional services for business clients.
Contextual Security Solutions – Contextual Security Solutions provides IT security, regulatory, and compliance consulting services for enterprise customers.
CriticalStart – CriticalStart provides information security services as well as resale of select security products for enterprise customers.
CryptoNet – CryptoNet offers security consulting, hardware, and software solutions for risk analysis, network security, and application security to Italian customers.
CSC – Technology services and outsourcing solutions firm CSC includes cyber security offerings.
Cyber Alpha Security BV – Cyber Alpha Security provides a range of security consulting services including ethical hacking.
Cyber Defense Agency – Longtime cyber expert Sami Saydjari's cyber security consulting firm Cyber Defense Agency is located in Wisconsin.
Cyber Defense Labs – Cyber Defense Labs provides a range of security consulting including vulnerability assessments, penetration testing, and cyber forensics.
CyberInt – CyberInt provides a range of intelligence, monitoring, and consulting services focused on information security and cyber warfare.
Cyberis – Cyberis provides information security, risk management, and assurance consulting services and solutions.
CyberPoint International – CyberPoint International provides security professional services and information assurance to commercial and Federal Government clients.

DarkMatter – DarkMatter provides a range of professional and managed security services and solutions.
Datashield – Datashield provides a range of security consulting, professional services and managed services with emphasis on RSA/EMC products.
Day Zero Security – Day Zero Security provides a range of security services and solutions for customers ranging from residential users to police services.
Déjà vu Security – Déjà vu Security provides information security research and consulting services for enterprise customers.
Deloitte – Traditional consulting and accounting services firm Deloitte includes cyber security. Deloitte 's experience in audit is an advantage for compliance assessments such as PCI DSS pre-audits.
Delta Risk – Delta Risk provides strategic advice, cyber security consulting, and risk management solutions to government and business clients.
Delphiis – Delphiis provides an IT security application and services suite for enterprise customers, including risk management as a service.
Depth Security – Depth Security provides security consulting with focus on penetration testing, Web application security, and network access control.
Deutsche Telecom – Deutsche Telekom is a German telecommunications provider offering a range of managed and network-based security services.
Digital Defense – Digital Defense Inc. (DDI) provides a range of managed and on-demand SaaS risk assessment solutions, as well as security professional services.
Digivera – Digivera provides information security, managed services, and technology consulting services.
DMX Technologies – In addition to its digital media, ICT, mobile SaaS, and managed services, DMX Technologies offers a range of managed security solutions and consulting services.
Emagined Security – Emagined Security provides professional consulting services for information security and compliance.
Enet 1 Group – Enet 1 Group provides security professional services in the areas of SCADA and critical infrastructure, and mobility.
Enterprise Risk Management – Enterprise Risk Management provides a range of security consulting and training services including risk management and IT security.
Espion – Espion provides a range of security consulting services including information governance, forensics and eDiscovery, training.
EWA-Canada – EWA-Canada provides information assurance services in Canada including IT risk management and managed security services.
EY – EY includes a range of cyber security, audit, and cyber advisory services for clients. EY acquired Mycroft in 2015.
Fortalice – Fortego provides security consultation and training services for business and government.
4Secure – 4Secure provides security consulting and training services to corporate and public sector clients across Europe. The company also provides a hardware data erasure tool.

FoxIT – Fox-IT combines human intelligence with technology to provide security solutions and training for customers.
FRSecure – Cyber security consulting firm FRSecure specializes in compliance, standards, and regulatory solutions.
FTI Consulting – FTI is a global business advisory company with a practice in forensic consulting and eDiscovery services.
Galois – Expert team Galois uses advanced mathematics and computer science to solve problems in technology and cyber security.
General Dynamics – General Dynamics is a traditional defense contractor with cyber security and information assurance capability.
Global Cyber Risk – Global Cyber Risk (GCR) provides advisory services to business and government in privacy, security, and related areas.
Good Harbor – Richard Clarke's cyber security management consulting and advisory firm Good Harbor offers higher end services including M&A.
GoSecure – Canadian firm GoSecure provides a range of security consulting and managed security services.
Guidepost Solutions – Guidepost Solutions provides a range of consulting services including investigation, compliance, and monitoring. The company has expertise in the installation of physical security.
Halock Security Labs – Halock Security Labs provides security consulting services including penetration testing and security assessment.
H-Bar Cyber Solutions – H-Bar Cyber Solutions provides a rage of security consulting, compliance, and security training services.
The Herjavec Group – The Herjavec Group is a Canadian technology firm specializing in network security managed services and consulting.
Hex Security – Hex Security provides security and information assurance consultation services toward both strategic and compliance objectives.
Hold Security – Hold Security is an information security and investigations company providing consulting services and threat intelligence for business clients.
IBM – IBM includes outsourcing, technology development, and consulting solutions including cyber security in its suite of products and services.
Immunity – Florida-based Immunity provides security consulting services including assessments and penetration testing.
Include Security – Include Security offers information and application security assessment, advisory, and consulting services.
InfoDefense – InfoDefense provides security consultation services focused on regulatory compliance, information assurance, and response.
InfoGuard – InfoGuard provides ICT security products, professional services, and managed security for business customers.
infoLock – infoLock provides information security consulting, integration, and value added resale (VAR) services.
Infosys – Infosys provides IT consulting, technology and outsourcing services including a range of information security solutions.

InfoWatch – InfoWatch is a group of information security companies – InfoWatch, Kribrum, EgoSecure, and Appercut – that operates across Eastern and Western Europe, Asia, and the Middle East.
InGuardians – InGuardians is a vendor-independent security consultancy offering audit, penetration testing, and related services.
Intellect Security – Intellect Security provides value added data security and encryption solutions for enterprise and cloud using a network of partners.
Interhack – Interhack provides a range of computer-related professional services with emphasis on security assessments.
Intrinium – Intrinium offers, in addition to cloud and network services, a range of cyber security consulting and managed security services.
IOActive – Security research group IOActive focuses on hardware, software, and systems.
IPV Security – IPV Security provides a range of security consulting services focused on compliance, monitoring, management, and audit.
IRM – IRM is a UK-based firm offering security consulting and risk management services.
ITsec Security Services – ITsec Security Services provides IT security-related consultation services in the Netherlands.
IT Security Experts – IT Security Experts is a UK-based security consulting organization focused on audits and training.
Jacadis – Ohio-based Jacadis provides a range of security consulting services to business clients.
justASC – justASC provides advanced security consulting focused on threat management, secure architecture and incident response.
Kindus – Kindus is an IT security and services consulting firm located in the United Kingdom.
KLC Consulting – KLC Consultants offers security assessments, third-party risk management, and security engineering.
KoreLogic – KoreLogic provides a range of security professional services for business customers. Services include penetration testing, application security assessment, and threat modeling.
KPMG – KPMG provides professional services to business clients, including information security.
Kroll – Kroll offers a range of information, physical, and investigative security professional services.
K2 Intelligence – K2 Intelligence provides investigative, integrity, and analytic consulting including forensics.
Larson Security – Larson Security provides cyber security services including digital forensics and incident response.
LBMC – LBMC Information Security offers a range of security consulting services including penetration testing.
Leidos – Formerly part of SAIC, Leidos offers a range of information assurance and cyber security services.

Leviathan Security Group – Leviathan Security Group is an information security and risk management consulting firm.
Mandalorian Security – Mandalorian Security provides a range of information assurance and information security advisory services in EMEA and Asia Pacific.
Marsh – Marsh provides a range of insurance products and related professional services including several cyber security offerings.
Maven Security – Maven Security provides a suite of security consulting services including Web and network security assessments.
McKinsey – McKinsey offers a range of technology and business advisory services including enterprise and IT security risk consulting.
Minded Security – Minded Security provides software security consulting as well as application security testing tools.
MindPoint – Information security consulting and engineering services company MindPoint is located in Virginia.
MKA – MKA provides a range of security consulting services including SOC and vSOC capabilities for public and private sector customers.
Navixia – Navixia provides a range of security technical and advisory services including audit and training.
NCC Group – NCC Group is the parent company of several cyber security firms including iSec Partners.
NetSPI – NetSPI provides security professional services and penetration testing for its customers.
nGuard – nGuard provides a range of professional services including penetration testing and security assessment.=
Nisos Group – Nisos Group provides penetration testing, risk advisory, and cyber security consulting services.
Northcross Group – Northcross Group provides management and technology consulting including cyber security.
NTT Security – NTT Security provides PCI QSA services, secure software consulting, and compliance support.
NuHarbor – NuHarbor is a cyber and information security consulting services firm located in Burlington, Vermont.
Obsidian Analysis – Obsidian Analysis provides management consulting and professional services in the area of homeland security and intelligence, including cyber security.
One World Labs – One World Labs provides enterprise threat intelligence and related security services with emphasis on brand protection.
Optimal Risk Management – Optimal Risk Management provides a range of risk and security consulting services for business and government clients.
Optiv – Value added reseller security solutions provider Optiv includes security advisory consulting services.
Orange – Orange Business Services is a global integrator of communications solutions including cyber security services.

The Oxman Group – The Oxman Group provides cyber security management consulting and data forensics.
PA Consulting – London firm PA Consulting specializes in consulting, technology, and innovation.
Paladion – Risk advisory and consulting firm Paladion provides integrated SOC management, risk, and compliance.
Palo Alto Networks – Security consulting services offered by Palo Alto Networks includes best practice training, validation testing, proof of concept testing, configuration audit, organizational health check, architecture consulting services, migration consulting services, resident engineering services, and additional cyber security professional services.
Parameter Security – Parameter Security is a technical security audit and ethical hacking firm specializing in financial services.
PatchAdvisor – PatchAdvisor provides security consulting services, including penetration testing, to enterprise customers.
Patriot Technologies – Patriot Technologies information and network security services firm is located in Frederick, Maryland.
Pentura – Pentura, now part of InteliSecure, provides a range of security consulting services included penetration testing, managed services, and GRC services.
Phirelight – Phirelight offers a suite of IT security consulting and cyber security protection solutions.
Phish Labs – Phish Labs provides a range of security services focused on detecting and preventing phishing-related threats.
Phoenix Data Security – Phoenix Data Security provides security consulting services with focus on data loss prevention.
PivotPoint Security – PivotPoint Security provides a range of information assurance and security consulting services including penetration testing and ethical hacking.
Portcullis – Portcullis provides a range of security consulting services including penetration testing and threat analysis-based response.
Praetorian – Praetorian offers a range of security consulting services focused on applications, mobile, and network.
Prevalent – Prevalent provides a range of security consulting solutions with emphasis on compliance and third-party vendor risk management.
ProactiveRisk – ProactiveRisk provides cyber security professional and managed services including security testing and response planning.
ProfitStars – ProfitStars provides a range of professional services and solutions for financial services companies including information security and risk management consulting.
Protiviti – Protiviti provides a range of business consulting services included GRC, audit, and risk management.
Provensec – Provensec provides a range of security consulting and penetration testing services for mid-sized businesses.
PUNCH – PUNCH is a boutique cyber consulting firm offering security analytic support for threat management.

PwC – PwC is a multinational professional services company that includes a cyber security consulting offering.
Quadrant Information Security – Quadrant Information Security provides a range of security consulting, managed security, and enterprise security management.
RANE – The Risk Assistance Network (RANE) connects subject matter experts, including in cyber security, with subscribers requiring assistance.
RavenEye – RavenEye provides a range of security consulting services including ethical hacking, PCI DSS QSA services, and penetration testing.
Razorpoint Security Technologies – Razorpoint Security Technologies provides a range of security consulting, professional, and managed services including penetration testing.
Reaction Information Security – Reaction Information Security provides security consulting services with emphasis on penetration testing.
Redspin – Redspin, now part of Auxilio, provides a range of security consulting services including penetration testing, application security, and audit services.
Red Tiger Security – Red Tiger Security offers security consulting and training services with emphasis on ICS/SCADA security.
ReliaQuest – ReliaQuest offers a range of security consulting services focused on assessment, protection, and management.
Rhino Security Labs – Rhino Security Labs provides security consulting services including penetration testing.
Ridge Global – Ridge Global provides a range of security professional services including cyber security insurance protection solutions for business.
Risk-Based Security – Risk Based Security provides security and risk consulting services including vulnerability intelligence, training, and cyber risk analytics.
RiskSense – RiskSense provides a vulnerability management platform along with a range of security services.
Rofori – Rofori provides a capability for managing cyber risk in the enterprise consistent with the NIST Cybersecurity Framework.
Roka Security – Roka Security provides a range of security consulting services including network reviews, vulnerability assessments, and support for incident response.
Root9b – root9b provides advanced cyber security training and consulting along with regulatory risk mitigation services.=
SafeCipher – SafeCipher offers a range of security consulting services including PKI solutions, PCI services, and encryption.
Sage Data – Consulting firm Sage Data offers its nDiscovery Log Analysis service for enterprise.
sandSecurity – sandSecurity offers a range of security consulting services including assessments and risk mitigation.
Seccuris – Seccuris, now part of Above Security, provides a range of security consulting, managed security, and security educational services.
Secure Anchor – Secure Anchor provides a range of security consulting services including vulnerability assessment, penetration testing, and forensics.

Secure Digital Solutions – Secure Digital Solutions provides a range of IT security, and governance, risk, and compliance (GRC) consulting services
Secure Ideas – Secure Ideas provides a range of security consulting solutions including penetration testing.
SecureState – Consulting firm SecureState specializes in compliance, information security, and incident/breaches.
SecureWorx – SecureWorx provides a range of security/information assurance and consulting solutions with emphasis on the Australian Government.
Securicon – Securicon provides a range of security solutions including assessments with emphasis on SCADA, process control, and other areas.
Security Art – Security Art provides a range of cyber security consulting services including red team exercises.
Security Audit Systems – Security Audit Systems provides a range of security consulting services including penetration testing.
Security Compass – Security Compass provides a range of security consulting services including application security assessment and secure development advisory.
Security Management Partners – Security Management Partners provides security and IT assurance-consulting services.
SecurityMetrics – SecurityMetrics provides PCI DSS, HIPAA, and data security compliance assessments.
Security Risk Solutions – Security Risk Solutions provides information security and compliance consulting services.
Secur1ty – Secur1ty provides a social platform for connecting customers with security experts on demand.
Sense of Security – Information security services provider Sense of Security is located in Australia.
Sentor – Sentor provides a range of IT security services including network protection, log management, and vulnerability monitoring.
Sera-Brynn – Sera-Brynn provides PCI DSS QSA services as well as security risk management consulting.
7Safe – 7Safe provides information security consulting, penetration testing, training, and related services.
Singular Security – Singular Security provides a range of risk analysis, vulnerability assessment, and cyber security services.
Spohn – Spohn is a professional services company offering security audit and assessment services in addition to telecommunications and training.
Spyders – Spyders is a Canadian firm providing IT and network security consulting and advisory services.
Stickman Consulting – Stickman Consulting is a security consulting firm that specializes in PCI DSS compliance.
STI Group – STI Group provides a range of strategic and tactical information security services for clients.

Stratum Security – Information security consulting firm Stratum Security is located in Washington, DC.
Stroz Friedberg – Stroz Freidberg provides investigation and response-based consultation services for enterprise.
S21sec – S21sec is a multinational firm that provides a range of cyber security services and technology across many industries.
Sunera – Sunera provides IT and risk advisory, information security, and corporate/regulatory governance consulting services.
Sword & Shield – Sword & Shield provides a range of managed and professional cyber security services.
Symosis – Symosis helps customers manage risk on emerging application, mobile, and cloud platforms through assessments, gap analysis, and due diligence.
Syndis – Syndis is a security think tank offering a rage of services including penetration testing.
Synercomm – Synercomm is an IT, mobility, infrastructure, audit, testing, and security consulting firm.
SystemExperts – SecurityExperts is a boutique provider of IT compliance and security consulting services.
Taino Consulting Group – Boston-based firm Taino Consulting Group specializes in security risk management.
Tangible Security – Tangible Security provides a range of security consulting services including assessments and virtual CISO for government.
TBG Security – TBG Security provides security consulting services to assist with compliance in HIPAA, PCI, and related frameworks.
TDI – TDI provides a range of security technology, policy compliance, and audit consulting services.
Tech Mahindra – Large Indian outsourcing and technology firm Tech Mahindra includes cyber security consulting.
Telos – Telos provides cyber security, secure mobility, and identity management solutions.
Templar Shield – Templar Shield provides a range of security consulting, managed security, and recruiting services.
Tevora – Tevora provides security consulting, risk management, and governance/compliance solutions for enterprise customers.
360CyberSecure – Security consulting and assessment services firm 360CyberSecure is located in Bellaire, Texas.
Tiger Security – Tiger Security provides a range of security consulting services including offensive, investigation, and intelligence.
Tiro Security – Tiro Security provides staffing and consulting services with emphasis on security assessments and virtual CISO.
Topgallant Partners – Topgallant Partners provides a range of security consulting services including assessment, audit, and risk analysis.
Torus Technologies – Torus Technologies provides valued added resale security solutions along with a range of security consulting offerings.

Trojan Horse Security – Trojan Horse Security provides a range of security consulting services including penetration testing and compliance assessments.
TruSec Consulting – TruSec provides a range of security consulting services including IT compliance assurance and IT risk management.
TrustedSec – TrustedSec provides a range of security consulting services including penetration testing.
TrustWave – Cyber security firm TrustWave includes PCI DSS, managed security, and security consulting capabilities in its extensive portfolio of security offerings. Like most QSAs, TrustWave has extensive expertise in compliance assessments.
TwelveDot – TwelveDot provides a range of security consulting with emphasis on mobile and cloud.
2B Secure – 2B Secure is a security consulting firm that provides a range of value added reseller solutions in the area of information security.
2-sec – 2-sec provides a range of security consulting offers including penetration testing and PCI DSS services.
Urbane Security – Urbane Security provides information security consulting services including defensive, offensive, and compliance offerings.
ValueMentor Consulting – ValueMentor Consulting provides information security consulting including compliance and assessments.
VariQ – Security consulting company VariQ covers IT, cyber security, and software development.
Varutra – Varutra offers a range of information security consulting and training services for enterprise customers.
Veris Group – Cyber security company Veris Group offers a range of cyber security consulting services.
Verizon – Verizon acquired a large group of experienced security consultants via acquisition of Cyber Trust to complement its MSS offering. The acquired group included the early visionary bunch at the NCSA in Carlisle, Pennsylvania led by industry pioneer Peter Tippett.
Vigilant – Vigilant provides a range of cyber security services including managed network security, managed endpoint, and consulting.
VigiTrust – VigiTrust provides security training, compliance readiness, GRC, and related security professional services.
Voodoo Security – Voodoo Security offers a range of security-related professional services for enterprise customers and security technology vendors.
Wipro – Wipro provides IT services, consulting, and outsourcing, including a practice in IT security services.
Wizlynx Group – Wizlynx Group provides a range of IT security services based on its Information Security Competence Center.
Xyone – Xyone provides a range of security consulting including penetration testing, compliance, incident response, and training.
Yarix – Yarix provides a range of security consulting services including penetration testing, forensic analysis, and audit.

Additional Security Consultants

Accellis Technology Group – Professional services firm Accellis Technology Group is located in Cleveland, Ohio offering managed IT, legal consulting, and cyber security/compliance.
Anchor Technologies – Business management consulting firm Anchor Technologies is located in Annapolis.
Axis Technology – Security consulting firm Axis technology focuses on governance, entitlement, and business risk.
BDO Consulting – Accounting, tax, audit, and consulting services firm BDO Consulting includes information security and compliance services.
BH Consulting – Information security consulting firm BH Consulting is located in Ireland.
The Cyber Security Agency – The Cyber Security Agency offers information security consultants with ethical hacking and penetration test experience.
Cyber Shield Consulting – Information technology firm Cyber Shield Consulting offers cyber security consulting.
Grant Thornton – Large accounting firm Grant Thornton offers professional services including cyber and compliance.
The Knox Corps – The Knox Corps provides consulting solutions with emphasis on regulatory compliance.
Imagine Cyber Security – Information security assessments are available from private firm Imagine Cyber Security, which was founded in 2014.
London Cyber Security (LCS) – Cyber security consultancy firm London Cyber Security serves global insurance markets.
Rook Security – Rook Security is a security and advisory consulting firm with managed security services and solution integration.
Stealth Entry – Stealth Entry offers an experienced cyber security and network assessment team in Columbus, Ohio.
TSG Solutions – TSG Solutions offers infrastructure security and technology solutions including risk management.

47. Security Recruiting

- ⇒ *Selection Decision* – CISO teams should choose recruiting firms based on a selection decision matrix that includes focus areas and coverage.
- ⇒ *Retained Search* – CISO teams should consider engaging in retained search deals with the better, more experienced cyber security recruiters.
- ⇒ *Integrated Recruiting* – An integrated recruiting approach is recommended, with recruiter, university, and other resource partnerships.

Since the ultimate purpose of a CISO team is to reduce security risk, it follows naturally that the lifecycle management of human resources is an essential

component of every enterprise security program. Failure to attract or retain capable cyber security data analysts, for example, will render even the best threat analysis tool essentially useless. Not attending properly to people management on a CISO team is thus a substantive security risk that should be avoided at all cost.

As a result, every modern CISO team, regardless of size, should create appropriate business relationships with *security recruiting* companies who can assist with human resource management at various points in the lifecycle. Good recruiting firms can help to bring new talent into the CISO team at the front end of the lifecycle; they can aid with filling in staff talent during the operational stages of a project or mission; and they can also provide confidential, private assistance to CISO staff and executives who are ready for career changes.

The urgency of building this relationship is heightened by the obvious skills shortage that exists in cyber security today. This shortage exists across all ranges of the cyber security landscape, although finding capable mid-level managers with technical, business, and compliance expertise is a particular challenge. Certainly, nurturing and growing staff organically is a wonderful goal and must be part of the equations, but the practical situation in cyber security today is that staff will be transient – and CISO teams must be mindful of this fact.

Cyber security recruiting firms tend to differentiate based on their level of focus – that is, *senior executive focus* versus *subject matter expert* focus, as well as *regional coverage* versus *global coverage*. Boutique agencies tend to combine the best elements of these factors into a customized set of services for clients. CISO teams should thus never ignore smaller, more focused recruiting service providers in lieu of the larger global search agencies with more recognizable brands. It is also important to highlight that a security manager or subject matter expert can and should consider engaging privately and directly with a security recruiter for the purposes of *obtaining* a new security position. The more mature CISO teams will encourage staff to do this, since a team is only as strong as its members feel connected.

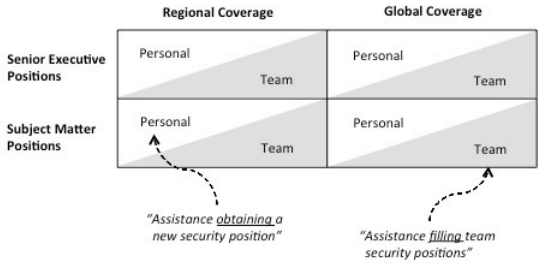

Figure 47-1. Decision Matrix for Selecting a Recruiter

The cyber security skills most recruiters handle include the full range of capabilities found in most enterprise CISO teams. It is worth mentioning that this underscores the need to be especially careful in providing detailed "needs descriptions" for recruiting agencies – especially ones that might be new entrants into the market.

The sensitivity of such information cannot be under-estimated, as it provides a roadmap to the staff weaknesses in an organization. This information is obviously of great use to an adversary. *Only share the details of your specific cyber security skills requirements with a recruiter you know and trust*. In any event, the relevant cyber security skills handled by recruiting firms include the following:

- *Senior Cyber Security Executive* – Includes CSO, CISO, and Deputy CISO positions. Candidates should have demonstrated experience managing teams and dealing with external entities such as regulatory groups. The larger search agencies will tend to focus more on these positions simply because the fees are more substantial.
- *Security Compliance and Audit* – Includes the skills required to manage compliance initiatives, audit systems against security requirements, and negotiate results with compliance and audit authorities.
- *Regulatory and Security Policy* – Includes the skills for regulatory and policy interpretation and negotiation with authorities including state, local, and Federal Government agencies.
- *Enterprise Security* – Includes endpoint security skills such as anti-virus/Internet security for laptops, mobiles, and tablets. Also includes enterprise LAN protection skills such as scanning, integrity monitoring, and system administration.
- *Cryptography and PKI* – Includes email, file, database, and system-level encryption skills for both symmetric and public key cryptography. Also includes data masking skills.
- *Identity and Access Management* – Includes skills for selecting, designing, and setting up identity and access management systems as well as operating authentication and authorization systems for enterprise and customer use.
- *Network Security* – Includes skills for perimeter devices such as firewalls, intrusion detection and intrusion prevention, data leakage prevention, and other network security solutions.
- *Security Analytics* – Includes skills for analyzing Big Data repositories from SIEMs and log management systems for evidence of threats and vulnerabilities.
- *Incident Response* – Includes skills for understanding vulnerabilities, tracking and logging their impacts, and managing response activities including restoration and patching.
- *Mobility Security* – Includes skills for managing mobile threats on Apple iOS, Android, Blackberry, and Microsoft for mobile phones and tablets. IoT is an important new component of this cyber security area.
- *Cloud Security* – Includes skills to manage threats on public, private, and hybrid clouds from a compliance and enterprise perspective. Knowledge of how virtualization works is an important new skill for cyber security.

- *Secure Software Development* – Includes the skills required to reduce risk in software lifecycle processes through agile and waterfall protections and controls.
- *Security Awareness and Training* – Includes skills for advising and training employees to exercise caution and to understand relevant security policy issues.
- *Government Security Program Management* – Includes special skills and background – including clearances – that support government programs focused on information assurance.

Cyber security recruiting firms generally provide hiring organizations with what is known as a *retained search*. The hiring organization works with a project team at the recruiting company to define their staff needs, relocation issues, and specific skills wanted. The project team then utilizes their "people network" to identify candidates, which are pre-screened and offered for review by the client. The process is more intense for higher-level retained searches such as the CISO position simply because so many more business, technical, administrative, and salary considerations come into play.

Fee structures vary across the industry, but typically the hiring company should expect to pay a percentage of the starting salary upon hire. These fees will vary based on the level of the hired candidate – perhaps in the 10-15% range, although larger corporate procurement teams will try to negotiate this percentage down dramatically. Some recruiting firms will require a portion of the estimated payment to be made up front, but this also varies. Many recruiting companies differentiate themselves by only taking payment when someone is actually hired.

While it can be misleading to generalize specific salaries for cyber security executives and subject matter experts, some anecdotal information can be offered here – with the full disclaimer that the total annual compensation estimates (salary, bonus, and incentives) listed below are based on confidential discussions between the lead author and roughly thirty-five CISOs, CSOs, government officials, and security experts in the United States in mid-2016:

- *Corporate CISO/CSO*: Total annual compensation packages tend to range from a low of $150K to a high of roughly $1.75M. Such positions often include creative retention components such as performance shares or options. Many positions are also offered in a so-called "two-plus-two" arrangement, where a contract is signed by the executive to work for two years, after which both the executive and the hiring firm have the option to continue or terminate the relationship.
- *Senior Government Official – Cyber Security*: Total annual compensation packages tend to range from a low of $75K in state or local positions to higher salaries in the $175K range for Federal Government positions with broader reach. These salaries are insufficient to attract suitable talent – roughly ten times lower than their commercial equivalent, so government

officials are often individuals who are in the latter stages of their career, or those rare people with the sincere desire and willingness to perform public service.

- *Senior Manager – Cyber Security*: Total annual compensation packages range from $100K to $800K. This wide range reflects the differences in senior manager positions, with some carrying low responsibilities and others carrying heavy operational and risk management burdens. Larger companies tend to pay more than smaller ones.
- *Group Manager – Cyber Security*: Total annual compensation packages for individuals who have several years experience and are in supervisory roles range from $80K to $350K. The higher salaries are only found in industries such as financial services with larger budgets.
- *Cyber Security Subject Matter Expert*: Total annual compensation packages for individual contributors range from $75K to $250K. Seasoned experts with track records command the higher compensation.
- *New University Recruit*: Computer science graduates or the equivalent can earn $50K to $80K in their first positions doing cyber security work. Information systems or business degrees tend to earn slightly less than more technical, scientific degrees. Start-up companies in cyber security compensate in more creative ways, often with equity (and free junk food).

For the estimates listed above, the northeast tends to pay higher wages than other parts of the United States; the financial services industry tends to pay higher wages than other sectors; government clearances, where applicable and desired, tend to drive up compensation, especially for more experienced staff; and physical and corporate security positions tend to receive much lower compensation than their cyber equivalent.

From a practical perspective, CISO teams should weave security recruiting services into an overall, integrated recruiting approach, making use of multiple resources such as local universities, contacts of team members, security working groups, and other business contacts. The better boutique agencies will welcome such a holistic approach and will even provide assistance in establishing contacts in local universities and groups. Usefulness of these different strategies vary, but in general – retained search is better for finding senior executives, whereas university recruiting is often better for entry-level cyber staff.

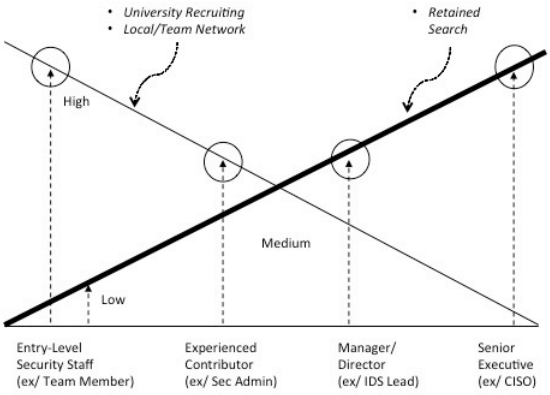

Figure 47-2. Integrated Cyber Security Recruiting Approach

The market outlook for cyber security recruiting services is positive with high likelihood that businesses, government agencies, and vendors will continue to need retained talent searches at virtually every level. CISO teams should pay particular attention to agencies with experience and track records over time. Alta Associates, for example, has been in business offering cyber security recruiting for over three decades, and is an example of a firm with a strong people network. Newer entrants might be perfectly capable and helpful, but CISO teams should ask around and check references before engaging with a recruiter.

As the pool of recruiting companies thus grows, CISO teams should remember that the best recruiters have personal relationships with available talent and hiring employers. This is particularly important in regions such as New York City and Washington, which tend to require specific expertise and access to individuals with unique attributes such as security clearances held by the appropriate government agency. In such areas, it helps to ask around locally for the best recruiting firms with the best available contacts.

Cyber Security Recruiters

The list of cyber security recruiters below is focused on those companies and individual recruiters with specific focus and a demonstrated track record in cyber security job placement. CISO teams and individual security professionals might find, however, that some excellent positions do become available from time to time through any number of recruiting firms, including ones with little or no background in this area. This is obviously different than other participants in the cyber security community; one is not likely, for example, to find a good firewall solution from a company with no background in firewall development.

That said, CISO teams must be very careful in their selection of, and partnership with, cyber security recruiters – if only because in retained search, clear descriptions are offered into potential weaknesses in the local cyber security team. Security managers should therefore use this list below as a starting point, but

should also ask around, check references, and consult peers during the selection process. The effort will turn out to be well worth the time.

2017 TAG Cyber Security Annual
Distinguished Cyber Security Recruiters

Alta Associates – My friend and New Jersey neighbor Joyce Brocaglia is one of the great pioneers in information security recruiting and retained search. She and I shared a wonderful lunch recently, where we discussed the issues, trends, and challenges associated with professional recruitment services for enterprise information security teams. I've learned from Joyce that experience and expertise matter, and that when a team decides to partner with a search firm, that they should put as much care and thought into that selection as they might with any other aspect of their cyber security arsenal. I offer many thanks to Joyce for her many contributions to our industry and for her kind support of this research.

2017 TAG Cyber Security Annual
Cyber Security Recruiters

Acumin – Acumin is part of Red Snapper Group with executive search reach across the UK (headquartered), Europe, and the US.
Alliance Resource Network – Alliance Resource Network has offices in New York and New Jersey with focus on broad set of C-suite positions including cyber security.
Alta Associates – Boutique executive search agency Alta Associates focuses on information security, risk management, GRC, and privacy. Joyce Brocaglia is one of the more well-connected and experienced search executives in the business.
Ashton Search Group – Ashton Search Group offers engineering and technical recruiting including cyber security.
Assevero – Assevero offers a range of cyber security services including security recruiting.
Barclay-Simpson – Search firm Barclay-Simpson, located in the UK, specializes in IT security and audit positions.
Benchmark Executive Search – Benchmark Executive Search firm includes a practice in cyber security and secure communications.
Blackmere Consulting – Blackmere Consulting offers specialized recruiting services with a focus on information security and enterprise risk.
Brandon Becker – Brandon Becker focuses on placement in networking, cloud, security, and virtualization.
Bridgen Group – Executive search firm Bridgen Group specializes in filling positions for senior to C-level and cyber response teams.
Caliber Security Partners – Caliber Security Partners provides security technical and strategic advisory services, as well as staffing services, for enterprise customers.
Cyber Search West – Cyber Search West is a search firm specializing in the managed security services sector.

Cyber Security Recruiters – Cyber Security Recruiters performs recruiting services for information security professionals from CISO to analyst.
CyberSN – Boutique recruiting company CyberSN specializes in identifying and placing cyber security talent in companies around the world.
Cyber 360 Solutions – Cyber 360 Solutions provides information security search and recruiting services.
Direct Recruiters – Recruiting firm Direct Recruiters has many areas of staff specialization including an IT Security practice.
Egon Zehnder – Major global executive search firm Egon Zehnder focuses on C-suite and board level positions.
Heidrick & Struggles – Major executive search firm Heidrick & Struggles focuses on executive and senior leadership positions including CISO and CSO.
Lenzner Group – Lenzner Group is an executive search group focused on enterprise security, risk management, and cyber intelligence.
LJ Kushner and Associates – LJ Kushner and Associates is an executive search and recruiting firm focused on information security.
Manta Security Management Recruiters – Florida-based search and recruiting firm Manta Security Management Recruiters focuses on security management positions.
McIntyre Associates – Boutique search firm McIntyre Associates focuses on cyber security positions.
Momentum Security Recruitment – Momentum Security Recruitment specializes in recruiting security professionals across the UK, Europe, Middle East, and Africa.
Pinnacle Placements – San Francisco firm Pinnacle Placements addresses security industry recruiting and search opportunities.
Russell Reynolds – Russell Reynolds specializes in senior executive and board-level opportunities around the world.
Sabat Group – New Jersey-based recruiting firm Sabat Group focuses on placing information security professionals.
Secure Recruiting International – Tampa-based Secure Recruiting International has focused on cyber security industry recruiting since 1997.
SecurityHeadhunter – Florida search firm SecurityHeadhunter focuses on information security recruitment.
SecurityRecruiter – Colorado-based SecurityRecruiter provides recruiting, education, and career coaching for information security professionals.
Secur1ty – Secur1ty provides a social platform for connecting customers with security experts on demand.
Silverbull – Connecticut-based Silverbull specializes in cyber security, IT, and related technology search and recruiting.
Stanley Reid & Company – Stanley Reid & Company focuses on technical recruiting with inclusion of cyber and computer network operations (CNO).
Templar Shield – San Diego-based Cyber security consulting and staffing firm Templar Shield offers professional recruitment services.
Tiro Security – Tiro Security, located in Los Angeles, is a cyber security consulting firm with staffing and executive search services.

Tri-Secure – Tri-Secure, a division of Trinity Connected, offers cyber security, telecommunications, and data center recruitment services in London.
Via Resource – Via Resource offers search and recruitment services focusing on information security and risk management.
ZRG Partners, LLC – ZRG Partners offers a range of cyber security recruiting and related services from their resident cyber expert, Stephen Spagnuolo.

Additional Cyber Security Recruiters

BeecherMadden – BeecherMadden is a UK-based search and selection business providing corporate positions including cyber.
Glenmont Group – Glenmont Group offers executive search with emphasis on legal and litigation support positions
Robert Half – Robert Half offers professional staffing focused in accounting, technology & IT, administrative, creative, and legal. The company also owns Protiviti, a GRC-oriented security consulting firm.
Hammer Consulting – Hammer Consulting focuses on staffing positions related to sales teams for technology companies.
ExecRank – ExecRank provides an on-line marketplace for executive and board search and connections.
First Arrow Executive Search – First Arrow Executive Search focuses on the intelligence, DoD, and Federal marketplace.
Intelligent Executive Search – Intelligent Executive Search provides executive career development portal services.
Korn Ferry – Major executive search firm Korn Ferry has expertise in finance, industrial, technology, and life sciences.
Kreamer Search Partners – Kreamer Search Partners is a search firm located in Pennsylvania supporting placement in network and cyber security.
Ken Leiner Associates – Ken Leiner Associates is an executive search firm focused on VP, director, operations, marketing, and engineering positions.
Leathwaite – Global search firm Leathwaite is focused on executive positions within the financial services industry.
Nclav – Nclav is a platform from Jonathan Martinez for connecting hiring companies with security practitioners.
Nicholson Search – Nicholson Search focuses on business intelligence, CRM, IT management, and cloud computing positions.
121 Silicon Valley – 121 Silicon Valley provides executive search and recruiting services for software companies.
Potomac Recruiting – Potomac Recruiting is a Virginia-based firm that serves consulting, IT services, healthcare, and government sectors around the world.
Reflik – Reflik is a social recruiting platform for obtaining referrals of top talent in various industries.
Romack – Romack provides a range of professional staffing services in various areas of technology.

SSR Personnel – SSR Personnel focuses mostly on fire, safety, and physical security positions globally.
Syndicus – Syndicus places IT staffing and consulting service positions including emphasis in health and life sciences.
Software Placement Group – Software Placement Group provides search and recruiting services focused on software and sales positions.
Spencer Stuart – Spencer Stuart has emphasis on placing senior executive and board-level positions.
SRP Careers – SRP Careers is a Phoenix-based agency with a range of focus including technology jobs.
Top Dog Recruiting – Top Dog Recruiting provides mid and senior level recruiting services in IT, consulting, engineering, healthcare, and IT security.
Toptal – Toptal is a unique service that provides means for companies to hire expert free-lancers in various technology areas.

48. Security R&D

- ⇒ *Relative Focus* – CISO teams have much higher focus on security compliance, technology, and architecture than on innovative R&D in cyber defense.
- ⇒ *Creativity in Offense* – R&D innovation requires thinking differently about defense, including how the CISO team works, interacts, and manages.
- ⇒ *Prospects* – The trends in security R&D are mixed, with few CISO teams really understanding how to be creative and actually *innovate*.

To properly support cyber security in the enterprise, CISO teams must attend to four areas of protection: Compliance, technology, architecture, and innovation. The current level of emphasis is currently high for both compliance and technology. For example, enterprise cyber security teams must attend to dozens of different security compliance frameworks, and a plethora of governance, risk, and compliance (GRC) tools exists to support these goals.

Similarly, CISO teams must include the best available cyber security technologies to reduce the risk of malicious attack. The good news is that many hundreds of excellent cyber security technology vendors exist around the world to support these enterprise protection needs. Security technology solutions range from strong encryption, to identity and access management, to next-generation firewall platforms, and on and on. As a result, no CISO team would ever complain about a lack of available technology options.

Even in the area of architecture, CISO teams are now working more closely with IT and network staff to completely redesign the overall set-up for corporate applications, systems, and transport. This redesign is making use of powerful techniques such as virtualization in the data center and software defined network (SDN) technology in the mobile infrastructure to introduce more flexible means for delivering services. Even the manner in which software applications are provided to

enterprise users is shifting from familiar, on-premise hosting to more extensible mobile app delivery to the smart phone or tablet.

The level of emphasis, however, in driving a *deliberate program* of cyber security R&D and innovation across the enterprise is virtually zero. By innovation, we mean thinking, acting, and performing in a fundamentally different manner – and this can only be achieved through active programs of security research and development (R&D). Ask any CISO team if they are doing security R&D, and the response – after agreeing that proof of concept testing in a lab is not R&D – will be essentially zero.

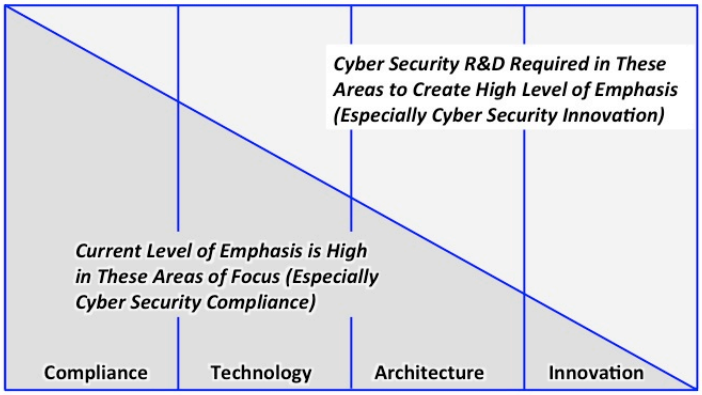

Figure 48-1. Relative Emphasis in Enterprise Cyber Security

It is worth mentioning that two types of innovation might be acknowledged in a given enterprise. First, *innovation-in-the-small* might involve incremental changes in existing approaches, such as changing how analysis is handled, or introducing a partnership with a separate organization. Most organizations do provide for some measure of innovation-in-the-small for cyber security, and this should continue to be encouraged. Larger teams might even have a couple of staff doing forward-looking work, perhaps investigating newer forms of cyber security technology.

But it is the *innovation-in-the-large* initiates that involve more substantive changes to existing strategy and tactics. These are the changes that require the type of deep insight, creative reflection, and thoughtful invention that are so missing from today's business environment. Sadly, in cyber security, the best innovation-in-the-large seems to be coming from the offensive community. Consider, for example, that botnets arose from attackers looking for better ways to control distributed systems in a resilient and secure manner. As further illustration, spend a day at the Black Hat or DefCon gatherings and you'll come away with a sense of exhilaration that is total missing from the vast majority of defensive programs.

Managing cyber security innovation in an enterprise is difficult because it will require investment in developing a security R&D community and atmosphere. Managing R&D of *any sort* is not easy, because it requires a free, non-prescriptive approach, which is usually associated in modern business with weak management.

Modern mangers are expected today to set goals, track progress, and incent behaviors that drive objectives. In contrast, the best R&D managers never determine a specific goal, but rather foster an environment where an eclectic group of diverse individuals is created and encouraged to think differently.

Even how people are arranged physically in the office workspace will affect the ability of the organization to think differently and innovate. Newer collaboration spaces with open physical arrangements might make a lot of sense for cyber security professionals who must exhibit high levels of information and idea sharing in order to be sufficiently creative to stop advanced attacks. CISO teams should seriously consider re-examining how the physical office is arranged for its employees.

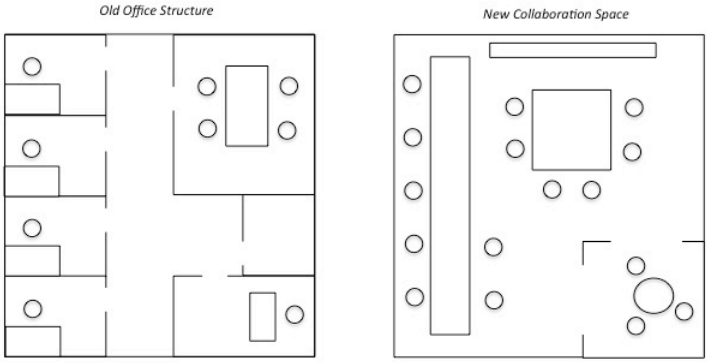

Figure 48-2. Physical Office Arrangement – Old and New

Since most CISO teams have never experienced true innovation in defense, let's look at a practical example: A US cable company several years ago noticed that their customers were modifying their set-top-boxes to steal pay-per-view content. Specifically, they were swapping out the CPU with a *test CPU* purchased on the Internet, because the test CPU could decrypt *everything*, including content that required payment. This created a challenge for the security team, because analog broadcast signals are not associated with any means for analyzing the endpoint; hence, this seemed the perfect crime.

The traditional solutions would have involved expensive home visits to inspect set-top-boxes for modification, or they might have involved stern warnings on Websites, doing little more than to perhaps help innocent customers understand how the bad guys were getting free content. Instead, the cable company achieved a more innovative solution after considerable reflection, thought, and innovative brainstorming. What was done involved creating an encrypted banner message during a popular pay-per-view event, and here is how it worked:

The banner message was sent to all subscribers, so that honest customer buying the event would see the message, but the banner was encrypted in a way that they'd only see garble. The dishonest customers, in contrast, would see everything in unencrypted form, including the banner. This allowed for a bogus

message to be delivered offering a "free tee shirt for the event, requiring just name, address, and phone number." Thousands of dishonest customers were identified using this novel means.

Note how this approach to cyber security is not a compliance project. It is also devoid of any reliance on a specific technology from a security vendor. It also has nothing to do with architecture. The approach instead represents true innovative defense of the form that can only come with creative individuals who are incented to try different approaches.

The modern CISO team desiring a program of innovative cyber security R&D has several options, each with its respective pros and cons:

- *Internal R&D Group* – Establishing a team that promotes, demonstrates, and guides innovation in cyber defense should be a priority – regardless of budget, headcount, capital, or operating expense pressures. This team should sponsor interesting speakers, run on-line social forums for creative suggestions, should fund and support active R&D projects, and should foster cross-fertilization with different parts of the organization – not to mention outside groups.
- *University Partnership* – By creating an alliance with a local university or college, the CISO team might have the opportunity to initiate R&D activities that would be of benefit to the enterprise. This has the great advantage of being quite inexpensive, but the corresponding disadvantage of creating intellectual property challenges. Nevertheless, every CISO team should be running a cyber security R&D program in concert with a local school.
- *Non-Profit Research Institution* – Many federally funded or university-affiliated groups exist across the United States and the world for performing advanced cyber security research and development. Government groups have long enjoyed the benefit of such groups, but commercial entities rarely do. The challenge here is the charter of most non-profit groups to avoid commercial gains.
- *Commercial R&D Services* – Professional service organizations are certainly willing to perform R&D, but they will have to be carefully vetted. The typical consulting engagement is goal-oriented with clear deliverables. The idea that a company might be hired to work on problems that might not even be solved is inconsistent with most management consulting approaches.

Perhaps the best available option – and this might be more for larger companies – is to create a locally managed, company-owned program of cyber security R&D toward innovative protections. The advantages in terms of intellectual property, staff development, and talent recruiting are obvious. Companies such as Google, Microsoft, and AT&T have recognized these advantages for many years, but they are the exceptions rather than the norm for the vast majority of CISO teams.

The outlook for cyber security R&D is somewhat mixed. On the one hand, university security R&D programs will continue to grow, but their attendance to

solutions that eventually drive better cyber defense is unknown. Clearly, universities enjoy developing good cyber offensive techniques, because that tends to be more politically acceptable to computer science professors. The federally funded programs of cyber security R&D will also continue to grow, especially for government-oriented applications including classified programs.

But the near-term future for commercially offered or internally managed programs of cyber security R&D is less certain. The need seems obvious, but the business pressures associated with allowing CISO teams to create programs for thinking differently may be too great to permit such luxury. The irony is that security R&D appears more a necessity than a luxury in the current threat environment.

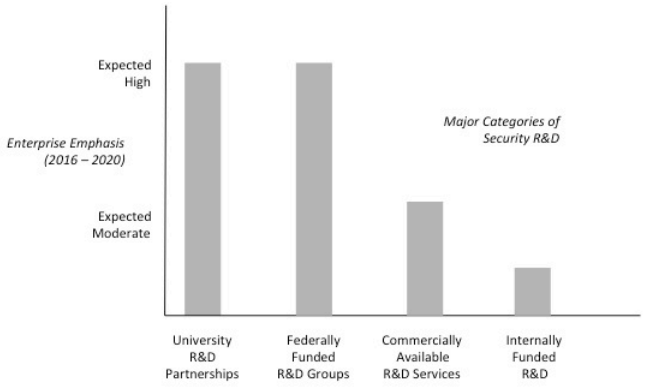

Figure 48-3. Growth Trends in Security R&D

The best advice for cyber security vendors and venture capital groups regarding security R&D opportunities would be to strongly consider the idea of deliberately creating, offering, and funding innovation programs for enterprise customers. This is different from incubator programs for start-ups, by the way, because the goal here is not to create companies that can sell new technologies, but rather to create ways for enterprise CISO teams to think, act, and perform differently.

Security R&D Providers

To ensure a better listing of security R&D providers, both for-profit and non-profit organizations are included. University programs of particular distinction are also included, although this is by no means a complete list of colleges and universities doing excellent work in cyber security. Organizations working in the area of offensive techniques including ethical hacking and vulnerability investigations are not included here since these tend to feed existing solutions and are no longer meaningful innovations. Companies listed below are included only if the R&D programs they support, have an externally focused innovation output for customers or other ecosystem participants.

2017 TAG Cyber Security Annual
Security R&D Providers

Adventium Labs – Adventium solves hard problems in cyber security research and development (R&D) with emphasis on automated reasoning.
AT&T – AT&T continues to maintain a group of security researchers focused on innovation and forward looking solutions for mobility and virtualization security. This work is often shared at public forums and conferences. AT&T also runs an annual cyber security conference that showcases innovation in cyber.
Blue Coat Systems – As part of its real time protection services, Blue Coat does extensive research on Website malware. The company has been very open about sharing the results of its research with the community.
BlueRISC – BlueRISC provides hardware-assisted endpoint security for anti-tamper and cyber protection.
ERNW – ERNW is an independent IT security services and consultation company specializing in knowledge transfer.
Galois – As part of its computer science and mathematics services, Galois provides R&D in several areas of computer security.
Google – Google includes a cyber security research team focused on innovation in various aspects of security and privacy. Google's R&D in cyber security is often directed at helping the overall Internet ecosystem.
HPE Security Research – HPE operates a major corporate cyber security research group. The company has a long-standing tradition in supporting R&D objectives sharable with the larger external community.
IBM – The Watson Research group at IBM continues to provide excellent R&D output in so many different areas including cyber security research and development.
IOActive – IOActive provides a range of security hardware and software assessments and research services.
Intel Security (McAfee) – Intel's McAfee division provides advanced research in malware techniques and structures.
Kyrus – Kyrus focuses on security research, reverse engineering, computer forensics, and secure software development.
Microsoft Research – Microsoft has one of the leading corporate-funded research teams. The group includes security R&D focus.
MITRE – MITRE is a US Federally-funded organization focused on a variety of research and development solutions including cyber security.
NSS Labs – NSS Labs provides expert cyber security research and analysis services for enterprise customers, with emphasis on practical, hands-on experience and test with security products.
RAND Corporation – RAND conducts research in cyber space and cyber security with emphasis on government-related issues.

Reservoir Labs – Reservoir Labs provides a range of scientific and technical research in areas such as network technology and security.
SecDev Group – SecDev Group is a cyber research think tank that provides open intelligence to improve awareness in cyber security and related areas.
Securosis – Securosis is an independent security research and advisory firm offering insights into Web 2.0, APT protection, and security investment.
Symantec – As part of its endpoint solutions, Symantec provides advanced research in malware techniques and structures.
Syndis – Syndis is a security think tank in Iceland offering a range of services including penetration testing.
Wapack Labs – Wapack Labs provides cyber threat analysis, security research, and intelligence services.

Additional Security R&D Providers

Applied Physics Laboratory (APL) – Part of Johns Hopkins University, APL includes a program of Asymmetric Operations focused on various aspects of cyber security, mostly for defense purposes.
Brookings Institute – Brookings is a think tank in Washington that offers forward-looking views on cyber security and related issues.
CSIS – CSIS is a DC-based organization that includes many major retired and former officials from government and industry with a unique insight into future trends in cyber security.
Lincoln Laboratory – Lincoln Laboratory is a Federally funded research institute connected with MIT.
Maryland Cybersecurity Center – Connected to the University of Maryland, the Maryland Cybersecurity Center supports research, education, and outreach.
Naval Research Laboratory – NRL is one of the original research laboratories in cyber security with capability in formal methods.
NYU Tandon Engineering – Several research activities are supported at NYU led by Nasir Memon.
Oxford University – Oxford provides cyber security and privacy research with focus on formal methods.
Sandia National Laboratories – Sandia is a Federally funded national laboratory includes cyber security program.
SRI International – SRI is a non-profit research institute that has pioneered many areas of cyber security including intrusion detection. Peter Neumann and Dorothy Denning are names that seem synonymous with some of the best work done at SRI over the years.
TechGuard – TechGuard provides a range of cyber security and information assurance solutions for commercial and government customers including security R&D.
Tel Aviv University – Tel Aviv University supports cyber security research and sponsors Cyber Week each year.

University College London – University College London includes an information security research group focused on cryptography, anonymity, authentication, and other areas.
US Army Research Laboratory – The US Army's research lab include programs in cyber security research and information assurance.

49. Security Training

⇒ *Training Options* – Enterprise cyber security training programs should be designed to support both experts and non-experts respectively.
⇒ *Security Awareness* – Security awareness training needs to evolve from bland on-line forms to social, video-based content developed professionally.
⇒ *Training Trends* – Training needs will grow at the greatest rate for the highest-end security experts and lowest-end technology novices.

In every organization and enterprise, the type of *security training* available to staff comes in two basic forms:

- *Expert Cyber Security Training* – This includes expert training for CISO team members to maintain their cyber security skills and professional certifications such as Certified Information System Security Professional (CISSP).
- *Security Awareness Training* – This includes basic awareness training and programs for all staff members – both expert and non-expert – to help them avoid making bad day-to-day decisions that can compromise the cyber protection posture of the organization.

Most of the cyber security training that is available today for expert CISO team members is quite good. Companies like SANS and IANS have been providing advanced education and training that is well taught, highly relevant, and arguably as good (or better) that comparable offerings at most universities and colleges. The only downside to these offerings is that they are not cheap, and they do require commitment of time away from the job. For virtually every CISO team in every sector and size, however, the decision to support staff members taking expert training will pay back the investment many fold. Team training should be a requirement, rather than a desire.

In stark contrast, the vast majority of cyber security awareness programs in the typical enterprise will involve dry, boring, or mediocre attempts to convey either trivial or confusing messages. Some companies do awareness training through bland, but stern email messages addressed to "all staff" from "IT security management." The messaging usually warns staff in lengthy wording to be careful of this or that piece of malware, or this or that type of download. It is usually unclear what people should be looking for, or even what their response should be if

something is suspicious, other than to follow instructions to "contact the security team." As a result, if you ask the employees of most organizations what they think of the corporate security training and awareness programs, you'll see eyes roll.

The good news is that several vendors have begun to provide much more creative and captivating awareness training services, including phish testing. These vendors tend to have more varied backgrounds, often with non-technical team members who understand how to create content that is fun, interesting, and even humorous. CISO teams who have limited resources for awareness training should take full advantage of these vendor offerings, some of which come in forms that are priced very reasonably.

All types of security training – including expert CISO team training and non-expert awareness training – come in many forms including instructor-led courses, on-line programs, conferences and symposia, videos and podcasts, and other specialized materials. Security training is generally more focused and immediate than related cyber security educational courses one might find in an academic program toward Bachelor's or Master's degrees. The purpose of good security training is always to provide compelling information that drives improvements in behavior, both for experts and non-experts.

As mentioned above, a welcome niche in the market exists to train expert CISO team members in more advanced aspects of cyber security. Let's examine this a bit more closely; the types of security training courses available to these cyber security professionals can be grouped as follows:

- *General Cyber Security Training* – Includes general coverage of cyber security basics such as security compliance, security policy awareness, and cyber threats. These are good options for new CISO team members, perhaps who are new to cyber security.
- *Task-Specific Cyber Security Training* – Addresses more specific day-to-day practical CISO team tasks such as incident response, PKI management, or secure coding. The local CISO team experts will know exactly which types of courses are required here, generally based on personal skills assessments.
- *Vendor-Specific Cyber Security Training* – Focuses on the usage or system administration of a specific tool or vendor product. This usually comes as part of a license deal, and is an excellent way to gain training without much additional expenditure.
- *Hacker Training* – Usually involves hands-on learning about break-in techniques for relevant technologies such as Android or Windows. Learning offensive techniques is less useful for managers (and arguably less useful than is generally presumed, for anyone doing cyber defense).
- *Cyber Security Team Boot Camps* – Involves group training, often scenario-driven, focused on improving readiness and team dynamics. This type of training is becoming more popular.

The presumed expertise level for most available CISO team training course and programs will range from novice background to advanced expert focus. Since the cyber security profession includes focus on compliance, technology, and architecture, it is perfectly reasonable for an expert in one area to require remedial training in another. Your best cloud security developer, for example, might know absolutely nothing about the basics of designing and operating a governance, risk, and compliance program. So novices in a specific area might actually have deep insights into another aspect of cyber security.

In addition, the threat level in a given organization might dictate a specific level of security attentiveness. Some smaller organizations with a clearly limited threat, for example, might dictate only casual demand for detailed security expertise. Most organizations, on the other hand, will view security as being clearly business-relevant, with a subset viewing their security obligation as having critical infrastructure consequences. The diagram below provides a two-dimensional grid that maps these progressions of CISO team member capability and emphasis into specific focus areas of cyber security training.

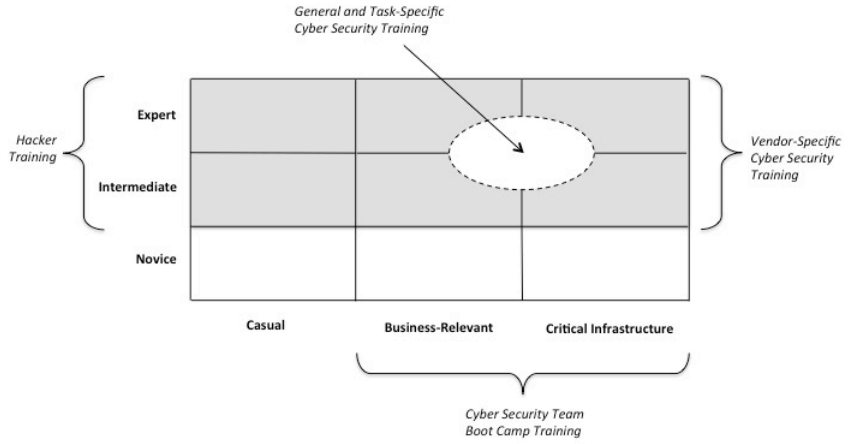

Figure 49-1. Cyber Security Training Focus Areas

Using the training focus area grid as a base, we can make trending predictions about the intensity of focus that should be expected for all forms of security training. First, it is clear that as more aspects of business and government recognize their critical infrastructure role, the need for detailed training of CISO teams members working in this segment will expand dramatically. This will be true more for experts and intermediate skilled staff than for novices, simply because critical infrastructure security should not be handled by newbies. Organizations like SANS and IANS will do well to grow their offerings for experts with huge responsibilities.

In contrast, as more consumers and individuals recognize the need for good cyber security practice in their day-to-day information handling, the market for basic cyber security awareness programs will expand. This market opportunity will be most intense for novice users with casual needs, since this demographic is often

either ignored or is handed the most trivial tips and training on the evening news or on popular Websites. Companies like PhishMe and Wombat should consider significantly expanding their security awareness focus in a manner consistent with the needs of the general public.

Phish testing, in particular, has been a vibrant area of growth in security awareness. In such cases, the cyber security team sends bogus messages to staff with links that convey hints about possible malware infections. The most obvious hint is usually a hyperlink whose actual value does not match the listed destination. Employees are taught to hover over the link to check for discrepancies. Other heuristics are also typically taught to staff such as being suspicious of emails that are too personal or that request information that does not seem relevant or reasonable.

In the coming years, there will be growth trending at the corners of the training focus area grid – namely, for experts with critical infrastructure obligations and for novices with casual needs in their day-to-day computing. Senior citizens are a good example of the type of user in this category that will need help. One could argue, sadly, that corporate board members are also novices requiring training assistance. This effect does not, however, imply reductions in the existing training and awareness market for the majority of users with business focus and intermediate skills. But this segment will certainly see more modest growth – if not a clear leveling off over time.

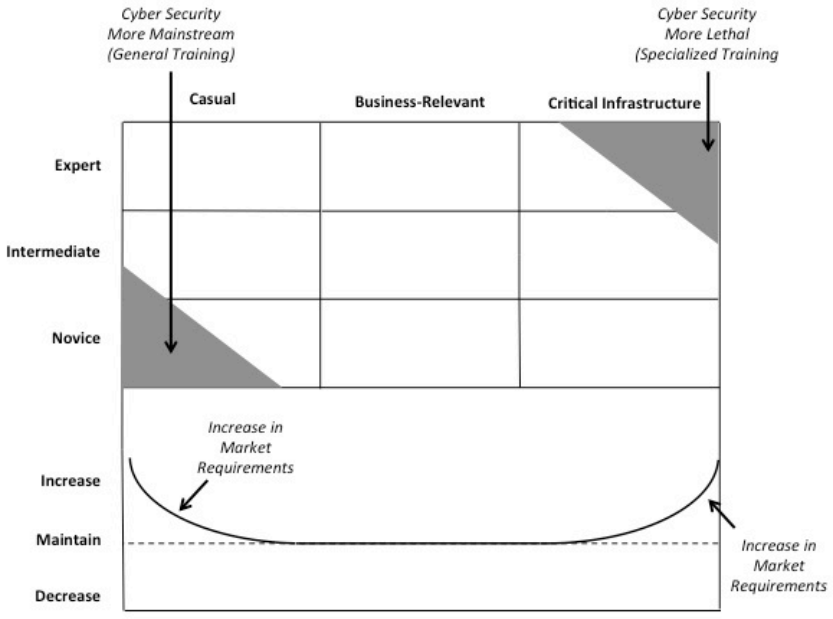

Figure 49-2. Trending in Cyber Security Training

A key practical consideration when one is planning a security training program is that all major technology vendors will offer focused product training. Even business

partners and consultants provide training, often for free, or embedded in the terms of existing contractual agreements. In addition, cyber security topics are covered in expert on-line videos, including academic courses posted on many university Websites. CISO teams can save money by reviewing on-line options before purchasing commercial cyber security education courses.

Regarding security awareness training, the trends will be toward increased use of multi-media, video, and social networks to improve understanding and participation. Companies specializing in these more creative security awareness approaches will be more successful than companies who continue to provide the traditional types of dull materials – posters, emails, documents.

Across the board, however, all forms of security awareness will continue to see increased demand, up to and including senior executives on Corporate Boards requiring more awareness of their cyber security-related fiduciary responsibilities as directors. Security consultants and training firms will see significant opportunities in the area of C-suite and board member training and awareness programs to assist security governance.

Even the major and minor security conferences focused on cyber security, such as the fine meetings set up by Tom Billington focused on government cyber security, or the huge conference run each year by RSA, will see continued increases in attendance as people realize the value in continuing to expand their cyber security knowledge. Smaller, more focused conferences that address topics ranging from IoT security to mobile security are also appearing, and CISO teams should expect a growing assortment of options during each year.

Security Training Providers

Cyber Security Training providers are listed below. The list has grown in the past few years, as this area has developed into a legitimate discipline. More and more conventional training companies are also offering cyber security and risk management as additions to their curriculum. Universities offering cyber security certificates or even degree are not included, because the material is generally not focused on the day-to-day needs of the practitioner (by design). Also, vendors offering training on the operation and use of their products are not included.

2017 TAG Cyber Security Annual
Security Training Providers

Above Security – Above Security includes training as part of a large portfolio of managed and consulting services.
Accumuli – Training is included as part of larger set of service offerings from Accumuli, which is part of the NCC Group.
Advent IM – Advent IM provides knowledge-based holistic information and physical security consulting and training services for enterprise customers in the UK.

AppSec Labs – AppSec Labs provides application security services including design, analysis, training, and assurance.
Aspect Security – Aspect Security includes training as part of its application security service suite.
Attack Research – Attack Research provides a range of security consulting, assessment, and training services.
BHC Laboratory – BHC Laboratory provides independent security consultation and advice for business customers.
Billington Cyber Security – Tom Billington provides world-class cyber security seminars with focus on relevant issues in Federal Government cyber policy and technology.
BitSec – BitSec Global Forensics consults with government and law enforcement agencies to help detect, prevent, and investigate cyber crime and terrorism.
Bitshield Security – Bitshield security provides IT security consulting services and professional training for customers in the Philippines.
BugSec – BugSec offers a range of information security services and products for enterprise customers.
CIS – The Center for Internet Security (CIS) includes a range of training and awareness resources in support of the CIS Controls.
CompliancePoint – CompliancePoint provides a range of compliance assessments, consulting, and managed IT.
CyberCrocodile – CyberCrocodile offers information technology education specializing in information security.
Cyber Diligence – Cyber Diligence is a forensics firm that provides a range of computer crime and investigative training.
Cyber Gym – Cyber Gym offers a unique real-world cyber defense-training arena for critical infrastructure organizations in Israel.
Denim Group – Denim Group provides secure software capabilities, including application development, assessment, training, and consulting.
Fortalice – Fortalice provides security consultation and training services for business and government.
Fox IT – Fox-IT combines human intelligence with technology to provide security solutions and training for customers.
Global Learning Systems – Global Learning Systems is a veteran-owned, Maryland-based company offering security awareness training.
The GRC Group – The GRC Group provides GRC training, certification, and resources for enterprise professionals.
GRC 20/20 Research – GRC 20/20 Research provides research, workshops, and consulting support in the area of GRC for enterprise.
Grid32 Security – Grid32 provides a range of security services including penetration testing and vulnerability assessment.
HackLabs – HackLabs provides a range of security consulting and training services including penetration testing.

H-Bar Cyber Solutions – H-Bar Cyber Solutions provides a rage of security consulting, compliance, and security training services.
IANS – IANS offers seminars with expert coordinators focused on a variety of practical cyber security topics.
Infinigate – Infinigate is a UK-based value added reseller that includes security training and consulting services.
InfoSec Institute – Information security training from InfoSec Institute includes hands-on and boot camp offerings.
InfoSec Skills – InfoSec Skills offers training courses in the UK and Australia to support professional cyber careers.
InfoSecure – Part of BeOne Development Group, InfoSecure provides awareness and security training.
Internetwork Defense – Internetwork Defense is a small training consultancy offering CISSP training boot camps.
IT Security Experts – IT Security Experts is a UK-based group offering security consulting and training.
justASC – justASC is a UK-based security consulting company includes training and awareness.
Kindus Security – Kindus Security is a UK security consulting company with on-line security training.
Lunarline – Lunarline offers a range of cyber security and vulnerability management products and services including SOC operation, penetration testing, and privacy services.
MAD Security – VAR security solutions and consulting firm MAD Security offers range of security training options.
Maven Security – Maven Security provides a suite of security consulting and training services including Web and network security assessments.
MediaPro – Pacific Northwest firm MediaPro provides awareness, security, and privacy training.
Metacompliance – Metacompliance provides policy management, GRC, compliance, and security awareness products and services for customers in the UK.
Meta Intelligence – Meta Intelligence provides intelligence-based services, cyber risk management, security training, and penetration testing.
MIS Institute – MIS Institute offers courses in internal audit, IT audit, and information security.
Navixia – Swiss information security consulting firm Navixia offers security awareness training.
Offensive Security – Offensive Security provides information security training, certifications, and services.
Optiv – Value added reseller Optiv offers information security solutions and training services.
PA Consulting Group – PA Consulting Group is a large consultancy that offers information security training for customers.

Palo Alto Networks – PAN offers a range of security training services including a Certified Professional Services Provider (CPSP) program.
Parameter Security – Parameter Security is a technical security audit and ethical hacking firm specializing in financial services. The company operates a Hacker University training program.
Phish Labs – Phish Labs provides a range of security and training services focused on detecting and preventing phishing-related threats.
PhishMe – Phishme provides a service for using simulated phishing scenarios to train employees about the threat.
RavenEye – RavenEye provides a range of security consulting services including ethical hacking, PCI DSS QSA services, and penetration testing.
Red Tiger Security – Red Tiger Security is a SCADA consulting services firm offering courses in securing ICS/SCADA systems.
Root9b – root9b provides advanced cyber security training and consulting along with regulatory risk mitigation services.
Safelight – Part of Security Innovation since 2014, Safelight offers a range of security training options.
SANS – SANS offers a full curriculum of cyber security courses, education, and training from expert instructors.
SCADAhacker – SCADAhacker offers expert training services and resources for securing ICS/SCADA systems.
Secure Ninja – Secure Ninja offers a specialized range of cyber security training and IT security services.
The Security Awareness Company – The Security Awareness Company is Winn Schwartau's information security training and resources organization.
Security Awareness, Inc. – Security Awareness Inc. is a Tampa-based company offering security awareness courses for government and commercial customers.
Security Innovation – Security Innovation offers software security services and application security training.
Security Mentor – Security Mentor is a California-based training and security awareness services firm.
SecurityOrb – SecurityOrb is an information security and privacy Website with training and awareness resources
Security University – Security University specializes in CISSP, CompTIA, and Q/ISP security training.
Skillbridge Security – Skillbridge Security provides a range of cyber security training services including tailored courses.
Symantec – Now part of Symantec, The Hacker Academy provides access to modules and instructor-led sessions in information security.
Symosis – Symosis helps customers manage risk on emerging application, mobile, and cloud platforms through assessments, gap analysis, and due diligence.
TeachPrivacy – TeachPrivacy offers privacy and information security training including HIPAA.

Trail of Bits – Trail of Bits provides expert cyber security research and training services.
Varutra – Varutra is a security consulting firm located in India that offers information security training.
VigiTrust – VigiTrust provides security training, compliance readiness, GRC, and related security professional services.
Visible Statement – Visible Statement provides 24/7 information security awareness solutions in multiple languages.
Wombat – Wombat offers a range of interactive security training and phish simulation services. Wombat acquired ThreatSIM in 2015.

Additional Security Training Providers

Interskill – Interskill provides mainframe training with catalog of IBM mainframe and security courses.
Learning Tree – Learning Tree offers a range of networking, data, application, business and cyber security training.
Pentester Academy – Pentester Academy offers a range of technical course including Javascript, Linux Forensics, Shellcoding, and penetration testing.
Phoenix TS – Phoenix TS provides various vendor certifications, learning resources, and instructor-led course in IT, cloud, and security.
RedVector – RedVector provides online education and training course for various industries including some cyber security offerings.
See Security – See Security is an information security and cyber warfare college located in Israel.
Syntrio – Syntrio is a compliance and training organization that includes cyber security training courses.

50. Value Added Security Solution Providers

- ⇒ *Custom Solutions* – Value added resellers offer customized solutions for enterprise teams desiring streamlined, integrated support.
- ⇒ *Decision Process* – Enterprise teams should follow a deliberate decision process in the selection of a suitable VAR for security solutions.
- ⇒ *Virtualization Implications* – As enterprise security virtualizes to on-demand provisioning, VAR solutions will shift toward cloud-based infrastructure.

The primary mission of the *value added reseller (VAR)* of cyber security solutions is to provide a convenient, helpful, and streamlined interface to security technology vendors. Many value added security solution providers differentiate their value proposition on their ability to provide bundled solutions from multiple vendors in ways that incorporate advise, guidance, and assistance to the CISO team. Such bundled solutions also typically include both pretested interfaces between selected

products as well as integrated contractual and billing services to simplify business operations for the enterprise buyer.

Some providers, such as Alliant Technologies, go so far as to create a truly integrated experience, sometimes referred to as a utility service, where the security functionality is embedded in the underlying infrastructure solution. In such an arrangement, different partner security technologies can be swapped into and out of the utility service without need for the client to worry much about the implementation details. These value additions separate the VAR solution provider from pure product resellers or direct purchases from vendors.

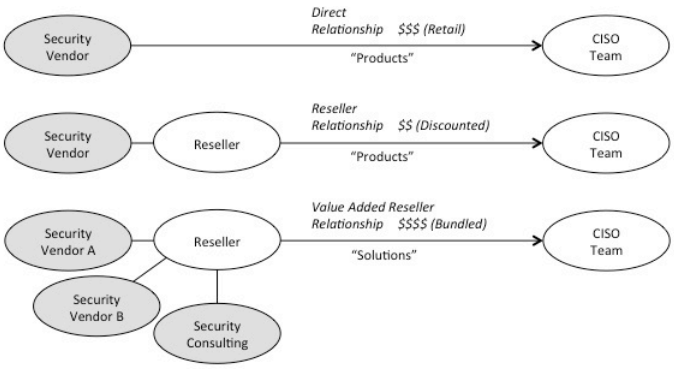

Figure 50-1. Value Proposition for Security Solution Providers

The selection of a value added security solution provider should be based on a number of practical business factors that will help ensure a good experience. These factors include the following:

- *Location* – The region in which a solution provider operates is a key success factor with any customer, particularly if language or cultural issues are a consideration. Many security technology firms partner with solution providers in remote parts of the globe for this reason.
- *Specialty* – The selected solution provider might have an area of specialty, such as network security, SMB security solutions, or the provision of an integrated utility service. Other providers specialize in simplifying the schedule of payments to vendors so that CISO teams can focus on technology. The selection of a specialized solution provider is an especially important consideration if a CISO team belongs to a unique demographic (e.g., Federal Government).
- *Relationships* – Since value added security solution providers will market their value propositions around customized, intimate solutions based on the real needs of a customer, any previously positive relationships with VAR principals should be an important consideration.

- *Size* – Security solution providers tend to target different market size demographics, with some providing services to massive organizations and others focused on boutique services to smaller companies.

The decision-flow chart below provides a high-level depiction of the type of management thinking CISO teams should follow in the selection of a value added security solution provider. It is entirely possible, as should be evident from the decision flow, that some enterprise security teams would be advised to not work with a security solution provider.

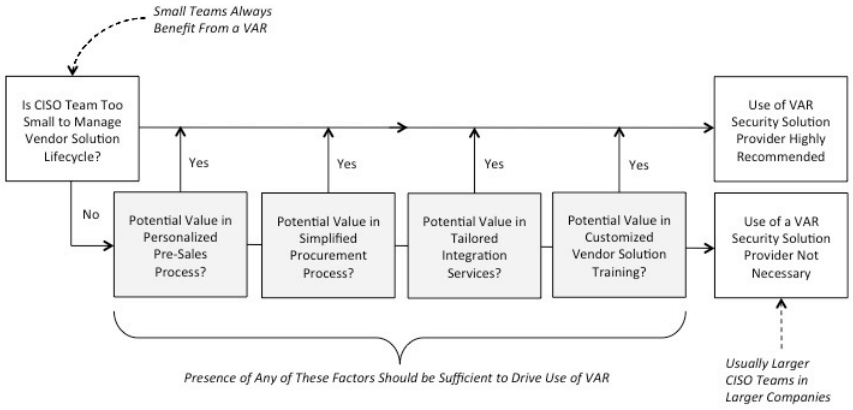

Figure 50-2. Decision Flow Chart for Selecting a Security Solution Provider

The advantages of a security solution provider are often inversely proportional to the size of the company and CISO team. Smaller teams will benefit from the pre-sales support, procurement and billing assistance, consulting and integration services, and training that a solution provider can provide. Larger teams might find these services tedious and in many cases, impeding of the team's ability to build close relationships with the vendor and its principals. This does not preclude larger companies from using resellers, but the motivation is often more around the procurement convenience a given vendor might offer through a VAR, rather than the sets of consulting services offered over the top.

One interesting development from the value added solution provider community, alluded to above, is the establishment of value added network services offered as a bundled utility-based solution. The idea is that utility IT and network services can be offered to a business as a bundled infrastructure solution with interfaces into and out of the utility capability. Security services can conveniently be embedded into utility IT and network solutions providing layer 3 and below security alarms and data to the SIEM, and also accepting task requests from application-level security tools through a defined interface.

The outlook for value added providers in the security solutions business is mostly healthy. As more and more companies realize how important cyber security is to their present and future success, the need for security solution services will

grow steadily for the foreseeable future. This is particularly true for providers that have the ability to assist with mobility and cloud integration of the enterprise.

A major caveat for pure resellers, however, is that as cyber security services move to a more virtual, on-demand, point-and-click provisioning experience, the role of the VAR will shift from procurement interface to trusted consultant and advisor as services shift to the cloud. This is good news, however, because the nature of the value added solutions provider is to focus on the most challenging aspects of a client's business. If this challenge becomes the progression to cloud, then the attendant solutions are more upscale than performing resale, and move the solution provider higher up in the value proposition.

Value Added Security Solution Providers

Value Added Security Solution Providers tend to be located all across the world since one of their obvious benefits is the ability to service remote geographic locations with unique cultural and language needs. This can really come in handy for CISO teams with massive global presence. Working with a VAR can help a team deal with technical issues in some remote area, where language and cultural barriers exist. So larger companies might consider discussing this type of support with their prospective VAR.

Many solution providers deliver a range of IT and network solutions, with only a minor security offering through one or two partners. A judgment call had to be made here as to whether they look like a value added security solution provider. CISO teams might therefore encounter in the marketplace value-added provider selling a particular solution, but who is not on the list below.

2017 TAG Cyber Security Annual
Distinguished Value Added Security Solution Providers

Alliant Technologies – My longtime colleague Phil Towle first introduced me to the really fine work on-going at Alliant Technologies under CEO Bruce Flitcroft. I had been casually aware of Alliant's wonderful offerings through its alliance as an AT&T partner, but it was not until I heard Bruce vividly describe the promise of utility IT infrastructure services at a CIO event in New Jersey that I fully realized how this might be useful for security. I thus made several visits to the offices of Alliant, learning more from Bruce and his team about how utility services work in general, and I'm confident that such value added support for security teams will become even more relevant with virtualization.

Optiv – I've known Jason Clark, Chief Strategy and Security Officer at Optiv, for some time now, and I consider him one of the great experts in the field. Jason and I had several conversations during my research that helped me understand the interplay between providing bundled value added services for clients, and the need to tailor these services to modern architectures. I'm also in debt to Optiv CEO Dan Burns for his support and personal guidance to me throughout this entire research project.

ABR-PROM – ABR-PROM has been providing IT and information security solutions such as SecPoint to customers in Poland since 2000.
AccessIT – AccessIT provides IT security and infrastructure solutions for customers through VAR partnerships with major technology providers.
Accunet – Accunet provides storage, data center, security, network, and virtualization solutions since 1997 with locations across the United States.
Aggeios – Aggeios is a value added reseller of managed IT services, information security, and data center located in Kuwait City.
Alliant Technologies – Alliant is a New Jersey-based solution provider offering utility IT security, unified communications, LAN/WAN services, and data center solutions. The integration of security into utility IT services is an innovative way for organizations to buy security as part of an underlying infrastructure offering.
Alpine Cyber Solutions – Alpine focuses on value added security solutions for customers in the Baltimore-Philadelphia market.
Alvea Services – ALVEA Services provides aggregated managed IT security and business continuity solutions through channel partners.
Alus Outsourcing – Alus Outsourcing provides information security and related services to customers in Brazil.
Aman Information Security – Aman Information Security is a Qatari-owned consulting and VAR security solution firm.
ARAMA TECH – ARAMA TECH offers VAR security solutions including GRC in the Netherlands and Denmark.
Arcon – Arcon is a managed security services provider serving enterprise customers in Latin America.
Asgent – Asgent provides network security and value added reseller (VAR) solutions for small and medium sized businesses, primarily in Japan.
Assuria – Assuria provides security solutions, security software, and managed SIEM services supporting security operations and enterprise security needs.
Axxum Technologies – Axxum is an IT security solution provider offering value added services in cyber security and information assurance.
Bridgeway Security Solutions – Bridgeway Security Solutions is a consultative information security reseller offering support and guidance for businesses, especially in the UK.
Carahsoft – IT solutions provider Carahsoft focuses on trusted government offerings including cyber security.
Cirosec – Cirosec is a German information security consulting firm with value added solutions through partners.
Comda – Comda is an integrator of IT and security solutions in Israel with focus on biometrics, access control, and digital signing.

Conquest Security – Conquest Security provides security services and solutions in conjunction with a set of security technology partners.
CriticalStart – CriticalStart is a security consulting firm located in Texas area with penetration testing, risk, and VAR solutions.
CyberDefenses – CyberDefenses provides a range of security professional services for business and government customers.
Denver Cyber Security – Denver Cyber Security provides IT security services for customers based on partnerships with Solutionary and Wombat.
DigitalScepter – Services firm DigitalScepter offers a range of value added reseller security solutions.
Digivera – Digivera provides information security, managed services, and technology consulting services.
eMazzanti Technologies – eMazzanti technologies provides IT technology consultation services for business including various IT security services.
eSecurityToGo – eSecurityToGo provides value added security and networking solutions including IT security consultation.
GigaNetworks – Florida-based firm GigaNetworks offers network security solutions including VAR services.
GuidePoint Security – GuidePoint Security provides customized, innovative information security solutions for its customers using a range of technology partners.
HardSecure – HardSecure provides values added resale (VAR) security solutions including consulting.
Infinigate – Infinigate is a value added distributor in the UK for a set of security services from companies such as Corero, Dell, and Trustwave.
Infogressive – Lincoln, Nebraska firm Infogressive offers cyber security VAR services and training.
InfoGuard – InfoGuard provides ICT security products, professional services, and managed security for business customers.
InfoLock – infoLock provides information security consulting, integration, and value added resale (VAR) services.
Intellect Security – Intellect Security provides value added data security and encryption solutions for enterprise and cloud using a network of partners.
Intrinium – Cloud and managed IT consulting firm Intrinium offers a range of VAR solutions including security.
IPS – IPS is a Canadian value added reseller (VAR) of cyber security products and services.
ITC Secure Networking – ITC Secure Networking is a UK-based network and security integrator including management services from the company's SOC.
IT2Trust – IT2Trust is a Scandinavian value added distributor of IT and network security solutions.
Lumenate – Lumenate provides a range of value added solutions including security and compliance through partners.

MAD Security – MAD Security provides value added resale (VAR) of security products and services, in addition to a range of security training services.
MindPoint Security – MindPoint Group provides a range of managed, compliance, and cloud security services.
Mission Critical Systems – Mission Critical Systems is an IT security reseller and integrator providing solutions across the Southeast United States and Caribbean.
M.TECH – M.TECH is a regional IT security VAR focused on end-to-end security solutions offered through security technology partners.
NCC Group – Accumuli Security, part of NCC Group, provides value added security professional, managed, and training services.
Netbox Blue – Netbox Blue, now CyberHound Pty. Ltd, provides a range of security solutions including next generation firewall and secure Web gateway through technology partnerships.
Netpolean Solutions – Netpolean is a network and security solutions value added reseller (VAR) focused on the Southeast Asia region.
Network Security Group – Network Security Group provides network security solutions through a series of security technology partnerships.
Nexum – Nexum is a security solutions provider offering services through a range of technology partners supported from Nexum SOC centers.
NH&A – NH&A provides security solutions for enterprise customer through partnerships with security technology providers.
Nuspire – Nuspire provides a range of managed security and network solutions through a variety of technology partners.
OneSecure – OneSecure Technology provides a range of IT and enterprise security solutions including email, network, data, and Web security.
Optiv – Optiv is the industry-leading VAR cyber security solutions provider built from the recent merger of Fishnet Security and Accuvant. Optiv has begun to offer security advisory solutions for enterprise organizations shifting their operations to cloud.
Performanta – Performanta provides a range of security VAR, technical, and consulting services to business customers.
ProactiveRisk – ProactiveRisk is a New Jersey-based VAR with security, software, and supply chain focus.
Proficio – Proficio is a VAR solutions provider emphasizing managed security services including SOC and SIEM.
Referentia – Referentia is a VAR solutions provider located in Honolulu that includes cyber security offering.
ReliaQuest – ReliaQuest is a security consulting firm located in Florida that includes VAR security solutions.
SecureNation – VAR security solutions provider SecureNation is located in Baton Rouge, Louisiana.
Securicon – Information security consulting firm Securicon is located in Northern Virginia offering VAR security solutions.

Security in Motion – Security in Motion provides IT security solutions included value added resale of security technology products.
Sengex – Sengex provides a range of security solutions for mobile and data protection through partner integration.
Starlink – Starlink is a security advisory and value added solutions provider located in the Middle East.
Syntegrity – Syntegrity provides a range of security products and professional services including support for identity and access management.
Techlab – TechLab provides a range of managed and value added data security products and services including mobile device security.
Templewood Homeland Security Solutions – Templewood Homeland Security Solutions offers cyber security solutions through partnerships.
Torus Technologies – Torus Technologies provides valued added resale security solutions along with a range of security consulting offerings.
Towerwall – Towerwall is a security consulting and VAR security solutions provider located in Massachusetts.
2B Secure – 2B Secure is a security consulting firm that provides a range of value added reseller solutions in the area of information security.
2Keys – Canadian firm 2Keys provides design, integration, and operating security solutions with VAR capability.
VILSOL – Managed security services and VAR security solutions provider VILSOL offers next-generation firewalls in Latin America.
Westcon – Westcon Group is a value added reseller (VAR) and distributor of network, unified communications, data center, and security solutions.
Wontok – Wontok provides value added services (VAS) and endpoint security solutions to protect business and government from malware and theft of data.

Additional Value Added Security Solution Providers

AVP Sistemas – AVP Systems is a VAR solution provider located in Ecuador and serving Latin America.
Baicom Networks – Baicom Networks is a Latin American value added security solution provider in Argentina.
Br-secure – Brazilian value added security solution provider Br-secure offers a range of technology partners.
Colvista – Colvista is a Latin American IT provider in Bogota offering consulting and integration services.
Dimension Data – NTT parent owned IT services firm Dimension Data offers VAR security solutions.
E-Data Teknoloji – Value added reseller security solution provider E-Data Teknoloji is located in Turkey.
Empowered Networks – Canadian firm Empowered Networks offers technology services and solutions including security.

Enterprise Technology Partners – Government-focused solution provider Enterprise Technology Parters includes information assurance and VAR offerings.
E-SPIN – Part of a group of companies in Malaysia, Hong Kong, and China, E-SPIN offers VAR services.
ETEK – Bogota-based value added reseller ETEK offers cyber security and related services.
Fortress – Singapore-based value added reseller Fortress provides IT security with an office in Malaysia.
iSecure – Woman-owned IT security provider located in Rochester and offering VAR security solutions.
ISnSC – ISnSC is a Middle Eastern penetration testing and IT security solutions vendor with VAR capabilities.
Italtel – Italian telecommunications and IT solutions firm Italtel offers a range of managed and VAR services including security.
MSPStream – Managed IT services and solutions provider MSPStream is located in North America and offers cyber security solutions.
Namtek – Namtek is a New Hampshire-based security controls and services provider with VAR capabilities.
Norseman Defense Technologies – Norseman is a small VAR provider serving Federal Government customers in the DC area.
RRC – Ukrainian VAR solutions provider RRC includes resale offerings for data security.
SaaS Security – VAR security solutions provider SaaS Security located in Norway offers a range of technology partners including Proofpoint.
Secure Commerce Systems – Secure Commerce Systems is a VAR solutions provider in Texas that offers a range of security products and services.
Seguridad IT – Seguridad IT is a VAR security solutions provider in Spain with extensive Cisco product offerings.
Sharper Technology – Sharper Technology is a veteran owned IT infrastructure and data security VAR solutions provider.
Simet Teknoloji – Simet is a Turkey-based VAR solutions provider focused on computer and network security.
SNB Group – SNB Group is a VAR solutions provider in the Middle East focused on data storage, security, and IT.
STEBRI – STEBRI is an IT Solutions provider located in Slovenia with cyber security offerings.
Supya Security – Supya Security is a Turkish VAR solutions provider that includes resale offerings for data security.
X-mart Solutions – X-mart Solutions is a VAR solution provider located in Sao Paulo, Brazil serving Latin America.