TERADATA

GOVERNMENT
10.12 | EB 7369

NARUSINSIGHT™ CYBERANALYTICS POWERED BY TERADATA

DYNAMIC NETWORK VISIBILITY

What started out as a low-level DDoS alert on the network of a government agency, turned out to be a systematic DNS enumeration originating from a botnet. Another government body discovered multiple infrastructure policy violations, including unauthorized equipment and applications connected to and running on their networks.

These are the types of well-hidden security breaches that Narus and Teradata help clients detect and neutralize.

Networks continue to increase in complexity and capacity, challenging organizations to keep their systems fully operational and secure. The shift to laptops and mobile devices has blurred the borders of networks, rapid proliferation of polymorphic malware has tested the effectiveness of signature-based protection, and the continuing swell in network traffic has slowed forensic analysis while driving storage costs skyward.

While traditional network security tools are critical to cyber security strategies, the continuing rise in attacks and the increasing time it takes to discover a breach demonstrate that these tools alone no longer suffice to maintain acceptable levels of security and operational effectiveness.

NARUS®

NarusInsight CyberAnalytics powered by Teradata is a real-time, network-based traffic intelligence and security solution that delivers dynamic, organization-wide network visibility and enables timely discovery and analysis of anomalous, suspicious, and malicious network traffic. NarusInsight passively collects network traffic and delivers Layer 2 through rich Layer 7 metadata known as Narus Vectors. A library of Narus real-time analytics tools analyze this traffic, identifying suspicious behavior as vectors stream by. You can create your own behavior-based real-time analytics and run them continuously to deliver wire-speed protection based on the unique characteristics of your network.

When combined with NarusInsight CyberAnalytics, Teradata data warehouse's petabytes of scalable storage capacity and parallel processing power quickly sifts through hundreds of millions or billions of rows of network data. This industry leading capability allows you to access the information you need to gain visibility into network activity.

In addition, NarusInsight CyberAnalytics powered by Teradata contains SQL-based tools for on-demand visualization and analysis of network traffic. With just a few clicks, operators can visualize, drill in, pivot, and report on nearly any aspect of your external, internal, and transient network traffic.

PROCESS FLOW

1. TRAFFIC COLLECTION AND VECTOR GENERATION

Intelligent Traffic Analyzer

- Uses passive tap interface (up to 10GbE) to collect bi-directional network traffic
- Identifies and collects traffic elements as defined by the analytical engines
- Creates sessionalized metadata collections of network traffic – called Narus Vectors
- Uniquely supports consumption of packet capture files for ad-hoc forensic analysis

Data Collection Agent

- Collects structured traffic data from other network sources such as routers, log files, etc. and loads the data into the Teradata data warehouse for access, querying and visualization

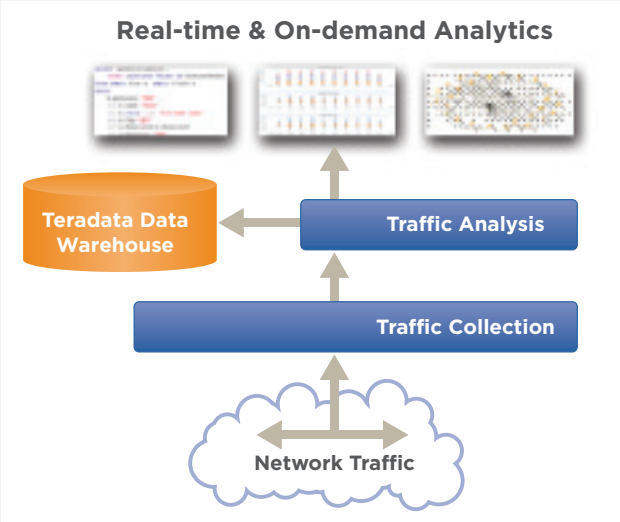

Figure 1. Process Flow

2. NARUS REAL-TIME ANALYTICS

Narus real-time analytics tools analyze network traffic and are applied to the metadata (Narus Vectors) collected, including Layer 7 elements.

- Run real-time and continuously in streaming mode
- Are stateful and session-aware
- Can be cascaded for complex functionality
- Deliver results captured to the Teradata data warehouse

3. ON-DEMAND VISUALIZATION AND ANALYTICS

The NarusInsight CyberAnalytics powered by Teradata delivers unparalleled on-demand visualization of network traffic that provides a deep understanding of network behavior. The solution's modules are SQL-based to simplify implementation and reduce the learning curve of the client's personnel. In addition, existing SQL-based tools, such as in-house visualization and reporting mechanisms, can be connected to the NarusInsight Cyber Analytics powered by Teradata to leverage existing technology investments. The on-demand modules access the Teradata data warehouse which contains Layer 2 through rich Layer 7 network traffic information. The major on-demand modules are:

SQL Query/Display – Creates SQL queries to access and display any data stored in the data warehouse in tabular form. This includes rich Layer 7-data elements. Queries can be grouped and stored for reuse as needed.

Visualization Dashboards – Displays network traffic data in graphical and tabular form. Minutes, days, weeks or even months of network traffic by port, protocol, application, and more can be easily visualized. Narus provides a standard group of user-customizable dashboards; new dashboards can be created as needed.

KEY FEATURES

UNPRECEDENTED VISIBILITY INTO THE NETWORK

- Collect internal, external, and transient network traffic
- Provide network-wide, behavior-based anomaly detection
- Identify unauthorized or suspicious traffic as well as surface changes in traffic patterns
- Support analysts in making educated decisions based on actionable knowledge
- Enable easy addition of secondary data such as past events, registry information, IP geolocation, blacklists, whitelists, and more

RICH READILY AVAILABLE LAYER 2 THROUGH LAYER 7 METADATA (NARUS VECTORS)

- Sessionalize and normalize packets into conversations that are ready for analysis
- Use storage that is typically 5% of the volume of PCAP files
- Accurately determine ports, protocols, and applications via observed Layer 7 behavior analysis
- Organize metadata from multiple sources into one data warehouse

DASHBOARD-DRIVEN ON-DEMAND ANALYTICS FOR TRAFFIC-AT-REST

- Visualize and analyze days, weeks, or even months of network traffic
- Work with user-customizable dashboards that enhance third party analytics
- Support analysts in investigation and making educated decisions based on institutional knowledge
- Enable additional toolsets for data exploration through its open SQL interfaces
- Easily convert ad-hoc queries into automated streaming analytics

POWERFUL REAL-TIME ANALYTICS

- Run analytics in real-time and streaming mode
- Provides stateful and session-aware operation
- Cascade analytics for complex functionality
- Plug into Narus Analytics Server
- Capture results in central data warehouse

READY FOR BIG DATA ANALYTICS

- Rely on scalable carrier-grade architecture with high availability and reliability
- Save storage with proven metadata design
- Allow data to reside where it is most convenient
- Integrate effectively with third-party tools such as SIEM and reporting

KEY DIFFERENTIATORS

UNPRECEDENTED VISIBILITY INTO THE NETWORK

- Real-time comprehensive view of the network
- Identification of unauthorized traffic
- Enhanced situational awareness

FULL RANGE OF EXPLORATION AND ON-DEMAND AND REAL-TIME ANALYTICS TOOLS

- On-demand tools for SQL-based query and display
- Customizable visualization and graphical drill-down via dashboards
- Relationship analytics
- Streaming live analytics can be processed against network traffic without slowing down the network

POWERFUL DATA WAREHOUSE

- In-database processing allows data to remain on storage appliance, reducing query access and execution time
- Big data hardware-accelerated datastore handles queries into hundreds of billions of records, in seconds
- Optimize data management, access and storage with industry leading database technology
- Secondary data (e.g. past events, registry info, IP geolocation, blacklists, custom-user analytics) seamlessly incorporates into the database

ACCELERATED INVESTIGATION

- Near real-time visualization of traffic anomalies
- Full application data improves decision making
- Optimized ability to search within forensic data
- Staff enabled to look for things “that shouldn’t be”

KEY BENEFITS

Narus and Teradata deliver Big Security by applying big data analytics to network security and risk management.

- Enhance cyber situational awareness
- Reduce risk
- Improve security
- Maximize operational efficiency

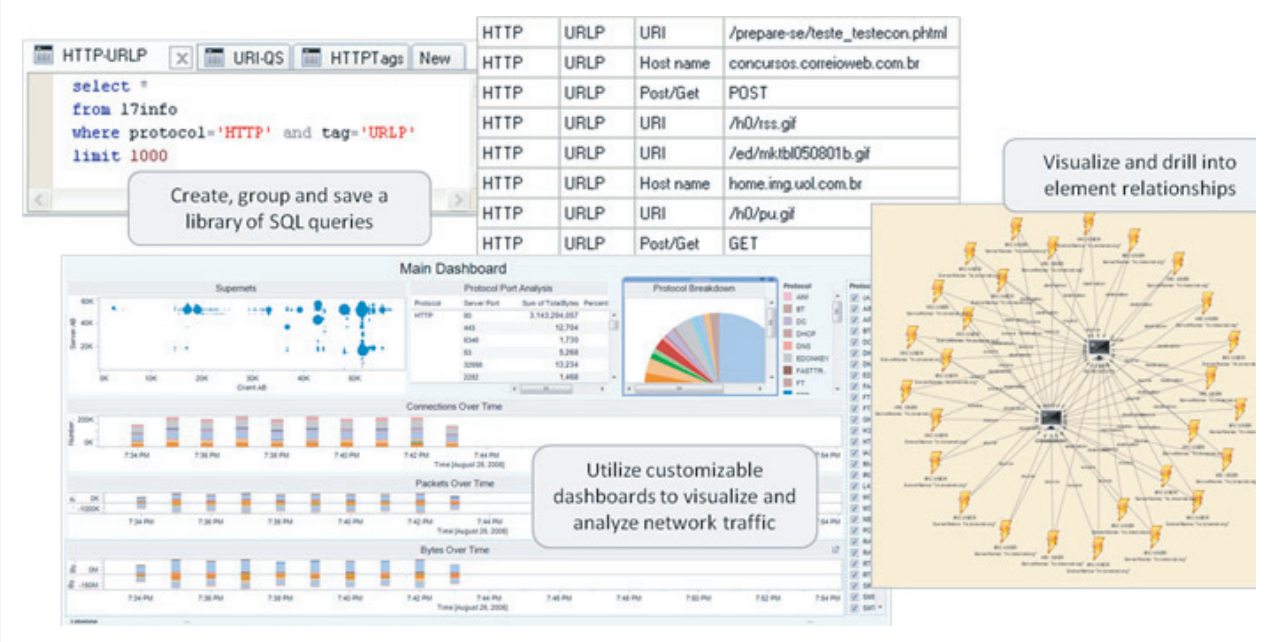

Figure 2. Rich cyber analytics and visuals to easily identify anomalous activity

GOVERNMENT
10.12 | EB 7369

ABOUT NARUS, INC.

Narus is a leader in cyber analytics and risk management technologies, enabling customers to identify and act on anomalous traffic in its network. Narus helps organizations manage and protect their large IP networks against cyber threats and the risks of doing business in cyberspace. Narus is a wholly owned subsidiary of The Boeing Company. Narus is headquartered in Sunnyvale, Calif., with regional offices around the world. **Narus.com**

ABOUT TERADATA

Teradata is the world's largest company focused on analytic data solutions through integrated data warehousing, big data analytics, and business applications. Only Teradata gives organizations the advantage to transform data across the organization into actionable insights empowering leaders to think boldly and act decisively for the best decisions possible. For more information about this solution, contact your Teradata representative or visit **Teradata.com**

10000 Innovation Drive Dayton, OH 45342 teradata.com

TERADATA. THE BEST DECISION POSSIBLE™