The Value of a Centralized and Virtualized Desktop Infrastructure

Q2_2014

CORPORATE HEADQUARTERS

3700 West Parmer Lane

Austin, Texas 78727

512.652.6500

www.clearcube.com

The Value of a Centralized and Virtualized Desktop Infrastructure

At many enterprises and agencies across the globe, mission-critical information technology works because it HAS to. Failure at any level is never an option due to the incredible high costs associated with it. At many of ClearCube's customers, costs of a technology failure to support mission requirements 100 percent may even put lives at risk. Moreover, the job continues to get done from one technology generation change to the next. From an Information Technology (IT) perspective change happens because there are always improvement opportunities and critical requirements to make work environments more secure, better managed, and less expensive to deliver on satisfying the mission.

…change happens because there are always improvement opportunities and critical requirements to make work environments more secure, better managed, and less expensive to deliver on satisfying the mission.

However, stakeholders are naturally resistant to change. They do not want work disruption or productivity loss. They want to mitigate risk. Stakeholders need compelling reasons to make change, justification for their decisions to embrace something new and different, and assurances of gains in meeting their objectives.

Technology change is coming. Buzzwords abound: "centralized computing," "virtualized desktops," "Zero Clients", "cyber secure," "move to the cloud," and many more. All of them imply big change.

Centralization and desktop virtualization initiatives are being adopted at a phenomenal pace. The tantalizing results of reducing overall total cost of operation, energy savings, space savings, decreasing desktop management overhead, and improving worker efficiencies are driving technology adoptions away from distributed desktop PCs toward putting centralized computing resources and virtualization into practice.

CVDI for smooth iterative change

Change can be abrupt, painful and a shock to the system. Or it can be iterative, smooth, and non-disruptive. The latter is where ClearCube's Centralized and Virtualized Desktop Infrastructure (CVDI) fits for agencies that have a variety of users with very unique computing needs. CVDI is not a one size fits all approach. CVDI is tailored to the needs of the organization to meet task, knowledge, and power user requirements most efficiently in moving desktops to the datacenter.

CVDI is not a one size fits all approach. CVDI is tailored to the needs of the organization to meet task, knowledge, and power user requirements most efficiently in moving desktops to the datacenter.

Figure 1 - Many Zero Client Options

The starting point for CVDI is at the desktop, represented by a PCoIP-enabled Zero Client, which is a connection point for all the user peripheral devices such as displays, mouse and keyboard, and the Ethernet network. The "zero" in Zero Client means that it has no operating system, no hard drive, and no addressable memory. Since it has no operating system, a Zero Client does not have to be patched, managed, or STIG'd because the PCoIP protocol is host rendered and only sends incremental pixel changes secured in a UDP-based 256bit encrypted compression algorithm. The stateless Zero Client does not store any data locally. Because PCoIP Zero Clients address the necessary security requirements at the end points, the devices do not need to be locked up at night and they can reside in an Open/Non-Open Storage environment. So the immediate benefits greatly appeal to the cyber security and information assurance officers that worry about cyber threats and data leaks.

At the core of CVDI is the highly efficient AES 256bit encrypted PCoIP protocol that factors into the performance equation and is therefore critical to creating a video-rich user experience. With UDP, data is not transmitted to the end point; only pixel changes are sent, along with USB signaling. The PCoIP protocol also "throttles" the users' sessions based on the performance needed thus limiting the bandwidth needed for the user session at the desktop. This results in a great user experience over distance from the host resources to the end point.

CVDI centralizes computing resources

Zero Clients use host-side rendering. Once the image is rendered on the host (virtual or physical), PCoIP protocol sends just the incremental pixel changes in a UDP-based AES 256 bit encrypted algorithm. Host rendering also improves latency insensitivity. With PCoIP protocol, the one-way delivery of only pixels (no data) to the Zero Clients mitigates network latency and bandwidth limitations and enables a rich user experience-- even on high latency wide area networks. The critical point of this capability is that migrating to CVDI, when architected correctly, does not compromise the user experience in terms of responsive performance. Satisfied User Experience means there is one less worry for the stakeholder justifying the CVDI migration.

Another advantage to host rendering is that organizations do not have to upgrade user devices based on industry developments from Microsoft, Intel, and ISV applications that require graphics enhancements

Another advantage to host rendering is that organizations do not have to upgrade user devices based on industry developments from Microsoft, Intel, and ISV applications that require graphics enhancements. The upgrades are instead addressed at the datacenter, thus alleviating unnecessary product upgrades as well as the continued desktop "touch" maintenance and life-cycle replacements.

PCoIP Zero Clients provide investment protection with an average long life cycle of seven years. This is important cost-reduction justification for the stakeholder.

Plus, CVDI enables agencies and organizations to address a high percentage of their user communities with a common desktop platform. All of the user devices have the same look and feel. For the stakeholder this means within the user community no one appears to be favored over another (although the real behind-the-scenes determinant is based on the resources that are made available to each Zero Client).

Brokering capabilities mean that the host resources can stay put in the datacenter, while people move from office location to office location to work. They are not bound to their cubicle as they would be with a distributed PC.

This ability to dynamically route a desktop to compute resources is called "brokering". Brokering allows users using Zero Clients to connect to their designated desktop computing resources from any Zero Client that has a network route to the designated resources. A Zero Client can broker a connection to different host resources, such as a physical Blade PC and a virtual VMware desktop machine, from the same end point location. Brokering capabilities mean that the host resources can stay put in the datacenter, while people move from office location to office location to work. They are not bound to their cubicle as they would be with a distributed PC.

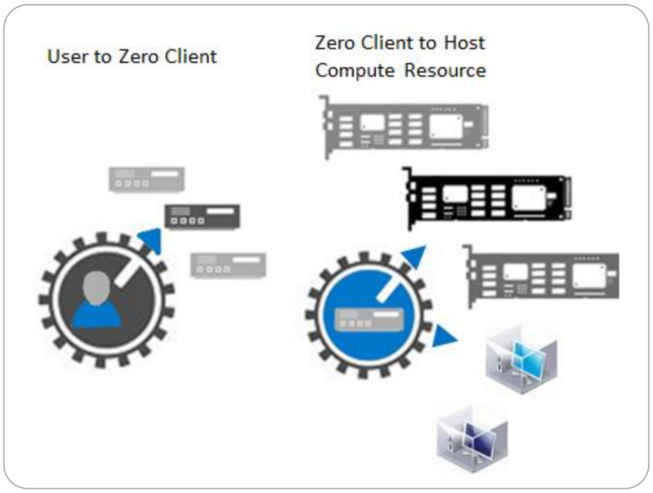

Figure 2 - Brokering User to Zero Client and Zero Client to Host Resource

To summarize the desktop portion of the CVDI equation, migrating to Zero Clients is compelling for increasing security, lowering energy costs, reducing desktop footprints, enabling collaboration through brokering and reducing management costs. All those benefits help justify changing the desktop paradigm. What the Zero Clients connect to is the next part of the CVDI equation.

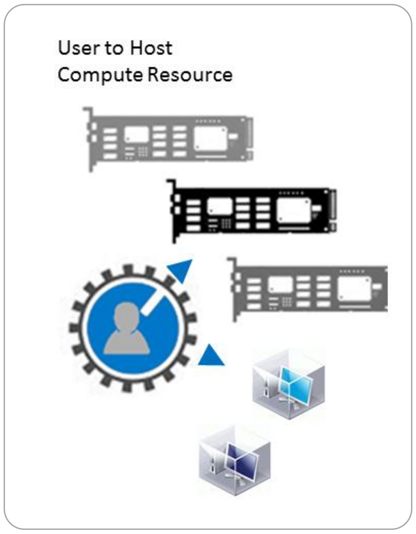

Figure 3 - Brokering User to Host Resource (any Device)

Agency intelligence mission is graphical

One example customer has a mission that provides a heavily graphical data product to several different federal agencies. The common denominator among the agency's different customers is this heavily graphical data product, which has copious demands for graphics processing and dissemination, statistical analysis and data crunching. To address those needs, a portion of the CVDI equation uses Zero Clients connected to Blade PCs. PCoIP host adapters with protocol accelerators in the Blade PCs deliver frame rates to the Zero Clients at twice the speed of those from virtual PC sources, so 60 frames per second are achievable. This is a valuable metric for those analysts maneuvering through satellite imagery and it eliminates stakeholder worry about performance.

Often though, only a small percentage of people need to access that specialized software concurrently. This approach, leveraging ClearCube CVDI technologies, can save thousands of dollars ($300,000 in this example).

From a migration and compatibility perspective, PCs still exist in the CVDI architecture. If the agency analysts had PC configurations that were defined with specific processor, memory, storage, and Graphics Processing Unit (GPU) elements, those still exist with CVDI – but instead of being located near the analysts, they are located in ClearCube designed Blade PC rack mount form factors in the secure, climate-controlled data center. What is extremely valuable for the stakeholder in justifying the CVDI migration is that all the Zero Client desktop benefits are realized without having to alter the core tested and validated computing environments that already exist on their networks. No special training, unique management tools, complicated metrics or burdensome support learning curves are introduced. From a migration viewpoint, risk is extremely low. For the stakeholder, migration is easier to justify.

When brokering is combined with centralized Blade PC resources, as is the case with CVDI, economies of scale can be reached. For example, specialized software applications that reside on workstations that control RPA's and UAV's can cost as much as $20,000 per system. The software applications that reside on the workstation often cost more than the workstation itself. Loading the application on 20 workstations would cost about $400,000. Often though, only a small percentage of people need to access that specialized software concurrently. If there are 20 users in a SCIF, and only five of them need to run the software at the same time, rather than license the application on all 20 workstations, a pool of five dedicated Blade PCs in the datacenter can be brokered to by users with Zero Clients that need the application. This approach, leveraging ClearCube CVDI technologies, can save thousands of dollars ($300,000 in this example). The same benefits apply to users who are TDY or out of the office/ in meetings. In contrast to distributed workstations that sit idle and unused, Zero Client brokering allows Blade PCs to be reassigned to users that need to use them.

Much of the example agency's content is delivered to and sent from multiple classified sources

The benefits of the CVDI architecture are most obvious in multiple domain settings found ubiquitously across the agency's IT infrastructure. Instead of four bulky, noisy PCs at the analysts' desks connected to four independent classified and unclassified network domains, with CVDI there are four small, low-energy, noiseless, completely secure Zero Clients, (often packaged in a ClearCube ClientCube desktop solution) connected to four Blade PCs or virtual machines. Yes, virtual machines are supported too.

As part of the elegance of ClearCube CVDI architecture, when pure VDI best suits the user need, depending on the user profiles, processing needs, and software application requirements, CVDI embraces it.

In addition to Zero Clients and physical Blade PCs, CVDI has pure VDI, Virtual Desktop Infrastructure, elements that include VMware core components. For the stakeholder, this VMware based VDI platform has a wider migration chasm to cross because virtualization has complexities that are not found in implementing ClearCube Blade PCs. As part of the elegance of ClearCube CVDI architecture, when pure VDI best suits the user need, depending on the user profiles, processing needs, and software application requirements, CVDI embraces it. We believe a large portion of the agecny population may benefit from running on virtual machines.

Figure 4 - Multiple Security Levels Supported ClientCube 2

...this flexibility within CVDI can deliver the best solution for each type of user – task, knowledge, and power user – or for each type of resource dictated by the application.

For many similar agencies, this flexibility within CVDI can deliver the best solution for each type of user – task, knowledge, and power user – or for each type of resource dictated by the application. Take, for example, a SCIF environment with three analysts/ users that are stationed next to each other. Analyst #1 may need to connect to a virtual machine on Network1 NIPR to access standard applications from the Army Gold master, and a different virtual machine on Network2 SIPR to access classified email, and a Blade PC on Network 3 JWICS to run satellite development content. Analyst #2 may have heavy computational loads and geospatial content running on all three networks and may need to connect to Blade PCs on each. Analyst #3 may use lightweight applications on all three networks and may connect to ClearCube SmartVDI virtual machines. All of this flexibility and versatility can be delivered from a common CVDI. From the stakeholder's perspective, all users have the same Zero Client look and feel on their desktops which removes the "user envy" of why one analyst has more powerful resource provision than another. It also removes the insider threat of users "need to know" since now these developers and engineers are not "targeted" based on their processing profile. To observers, they all look alike.

In training environments, cost savings can also be realized by using CVDI by avoiding the need to pay for the most powerful common denominator. Often times distributed "more-powerful than most commonly needed" box PCs are specified-in for worst case processing scenarios since the classrooms need to accommodate performance ranges of high-end graphics course work to light text based content. In addition, PCs in classrooms are left unattended which often leads to undetected theft of memory and local storage devices. Often many classrooms sit idle and unoccupied, yet each is filled with PCs. This approach is inflexible and inefficient. Instead, by implementing CVDI, IT can replace the PCs in all classrooms with zero clients. Course content is then delivered only as needed to certain IP ranges (classrooms) based on the course work and training schedule. IT can now reap significant savings by delivering performance based systems from Blade PC's (CDI) and basic course content from server based computing (VDI) all through brokered connections from Zero Clients in the classrooms. And a smaller number of host resources may serve the larger community of active and inactive classrooms. If re-imaging has to be performed after every class, which is often the case, then re-imaging distributed PCs adds layers of complexity, inconvenience, and labor. The alternatives using linked clones to spin up and destroy a few VM images for the various coursework after each class session and/or the close proximity of centralized Blade PCs for "easy touch" maintenance make for a much easier management environment.

Security Threat Vulnerabilities Force Change

The news is full of increased data breaches and cyber threats that cannot be ignored. No responsible manager wants to increase his or her agency's exposure to data security breaches. Burdened with traditional networked desktop computers, IT administrators are severely limited in terms of manageability, reliability, and security. As a result, IT support personnel are tasked with fighting the fight to provide tight security, longer uptime, and quicker return-to-service on the most hostile and fragmented battlefield – at the desktop. The objective-is, or should be, to move the battle to controlled friendly terrain – the datacenter. That is where ClearCube CVDI comes in.

Data security has been one of the driving forces in the adoption of ClearCube's CVDI solutions at the most secure facilities in the world. What differentiates ClearCube is that security is addressed and embraced at every layer of the CVDI solution equation.

Data security has been one of the driving forces in the adoption of ClearCube's CVDI solutions at the most secure facilities in the world. What differentiates ClearCube is that security is addressed and embraced at every layer of the CVDI solution equation. Zero Clients are known throughout the industry as the most secure IP-based desk top platform available. By their very nature, zero means zero. At the desktop, there is no operating system, no memory, and no local storage.

The next secure layer is the PCoIP protocol itself that is based on host-rendered processing. Data does not leave the data center and no processing is done at the desktop. In addition, PCoIP uses AES256/128 bit algorithms to encrypt the pixels. Where multiple Zero Clients need connections to independent and physically separated networks, ClearCube's ClientCube integrates a NIAP EAL 2, Protection Profile v2.1-approved secure KVM switch to share the common set of peripherals on the desktop with the ClearCube Zero Clients within. Across the entire Zero Client product line, secure authentication is enabled using integrated card readers to support the NIPR CAC as well as the SIPR token. PCoIP has extensive authentication and single sign-on (SSO) capabilities for use with smart cards. Even with all those layers of security, additional prevention to ensure data does not leave the network takes place on ClearCube Zero Client products on two more levels, software and hardware. PortAuthority policy-based software prevents mass storage access (such as USB drives, CDs) on the Zero Clients. Mass Storage Lockout, a ClearCube patented technology, is designed into each ClearCube Blade PC and host cards to disable USB access completely at the Zero Client end point.

For the stakeholder who must protect the integrity of his or her agency, the benefits of CVDI are easily identified.

Some aspects of distributed PCs carry a price tag harder to quantify. What is the true cost of losing classified information to our enemies from someone downloading files to a USB device on a desktop PC or laptop? The ripples felt when the protection and well-being of our citizens is compromised because a mission critical PC failed and could not be restored quickly may cost many times more than a small premium upfront. Devastating losses far exceeding the monetary damage of someone stealing a laptop that contains the trusted identities of our intelligence agents may be unrecoverable. At many agencies security compromise could be devastating to national security, people's safety, and people's careers. For the stakeholder who must protect the integrity of his or her agency, the benefits of CVDI are easily identified.

Change to CVDI can be iterative and smooth

It is extremely important to note that the benefits offered by CVDI will not require drastic changes to existing infrastructure. No forklift overhauls will be necessary.

It is extremely important to note that the benefits offered by CVDI will not require drastic changes to existing infrastructure. No forklift overhauls will be necessary. If distributed PCs are at network end points, an Ethernet infrastructure is already in place from the data center to the users. If multiple security levels are delivered to the desktop today, then dedicated Ethernet cabling for each domain or discrete network path from desktop to datacenter to guarantee separation of classified and non-classified data already exist. Ethernet switches are in place to connect users to servers and storage devices. Anti-virus and malware prevention programs are already in place. Active Directory, profile management, and user application program assignments already exist. In moving to CVDI, all of that remains in place to protect existing infrastructure investments. What changes with CVDI is where data resides – CVDI moves all of the data to the data center to storage devices integrated on Blade PCs or SmartVDI virtual machines.

CVDI is often implemented during technology refresh cycles when the existing PCs are typically out of date and are underperforming. Therefore, current ClearCube Blade PC technology performs better than the PC being replaced. In place of bulky, noisy, heat-producing, power consumptive, un-secured desktop PCs are small, noiseless, Zero Clients connected via existing Ethernet accredited infrastructure. As Blade PCs are replacements for existing distributed PCs, asset management and inventory processes are simplified but mostly unchanged.

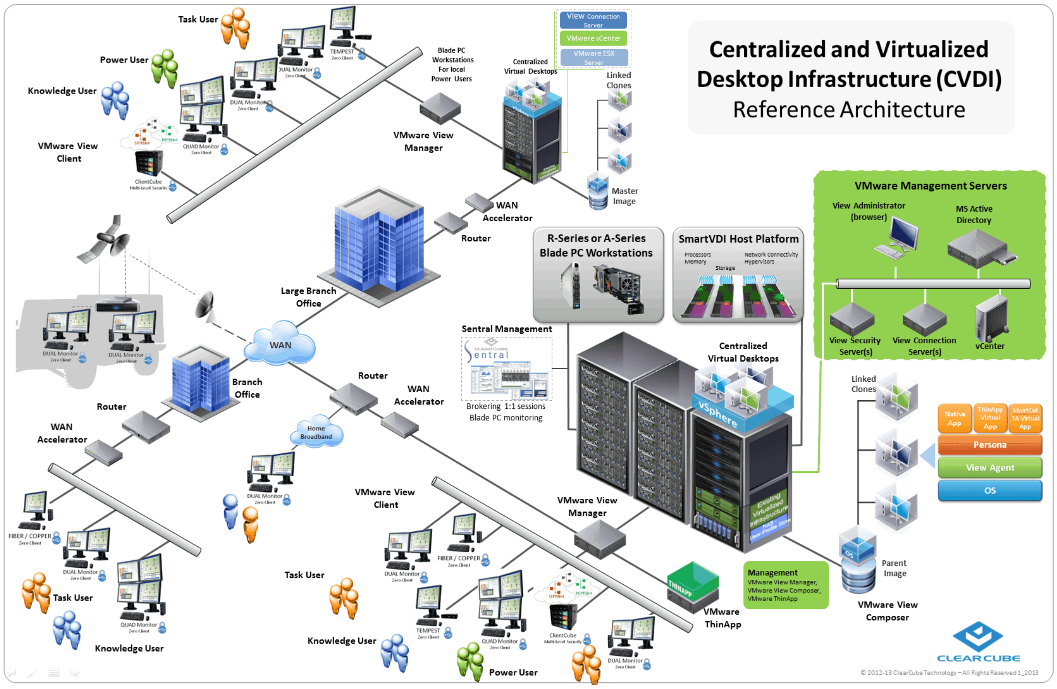

Figure 5 - CVDI - The Big Picture

From an operational perspective, Blade PCs provide tangible cost savings in comparison to the distributed PCs they replace. This savings is attributed to many factors including reductions in technical support labor, maintenance costs, training needs, help desk support, administration, licensing, equipment moves and changes, and energy consumption. ClearCube's solution reduces operating costs by at least 30% (Source: IDC, US Air Force) across each of the above hard cost areas.

From an operational perspective, Blade PCs provide tangible cost savings in comparison to the distributed PCs they replace. This savings is attributed to many factors including reductions in technical support labor, maintenance costs, training needs, help desk support, administration, licensing, equipment moves and changes, and energy consumption.

Many of these cost-savings are easy to quantify. Power-savings are obvious in human habitant areas where HVAC costs are high. A Zero Client consumes 6 watts of power. A PC consumes 200 watts of power. Labor to support distributed PCs runs three times that of centralized Blade PCs. Downtime and loss of productivity can be extremely costly. Return-to-service on a desktop PC can take hours, as compared to minutes for swapping in a Blade PC in the datacenter, or milliseconds with automatic failover designed by allocating an active spare pool of Blade PCs, or implementing a high availability SmartVDI cluster.

CVDI's Pathway to the Private Cloud

Cloud Computing and CVDI have much in common from the end point perspective since they both use slimmed down end point devices to access remote datacenter resources. Cloud computing is generally defined as providing desktop, network and storage services from a common set of datacenters. CVDI can be thought of as a "private cloud." Currently applications are being delivered via the Cloud from DISA to the Army for enterprise email. As time goes by, more and more applications will be delivered via this method until the complete desktop image can be supported for remote delivery. This transformation process will not be overnight, and will take some time as the necessary bandwidth becomes available and additional funding is released to fulfill the infrastructure requirements to ensure a smooth transition. The benefits of a CVDI private cloud parallel many of the benefits proposed by public cloud adoption. The big difference is that CVDI is implemented on premise, under the control and management of the stakeholders.

The benefits of a CVDI private cloud parallel many of the benefits proposed by public cloud adoption. The big difference is that CVDI is implemented on premise, under the control and management of the stakeholders..

Technology change does not have to be daunting, challenging, disruptive and filled with risk and anxiety. There must be compelling reasons for stakeholders to make change. This CVDI White Paper presents a few of them: increased desktop security, reduced operational costs, improved desktop ergonomics, better managed resources, increased productivity from reduced downtime, and more. Viewed in total, all help justify stakeholder decisions to embrace something new and different, and with assurances of gains in meeting organizational objectives.

About ClearCube Technology

ClearCube Technology CVDI adoption is prevalent throughout the US Intelligence Community. ClearCube maintains a Secret level secure facility through the US Department of Security Service in its Austin, Texas headquarters and thus can provide engineers and technicians with secret clearances for installations, break-fix, troubleshooting and architectural analysis/ consulting.

To better serve our intelligence community customers, ClearCube:

1. manufactures its Zero Clients in the United States and all products are TAA compliant.
2. provides the industry's only advanced replacement warranty for Blade PCs and Zero Clients.
3. offers a Windows 7 licensing solution that provides customers with a Microsoft Windows 7 Diskless COA license that enables agencies to include Zero Clients under their existing Microsoft Enterprise agreements which include software assurance just like a desktop. COA licensing provides significant savings over Volume Licensing/ subscriptions and helps accelerate the return on investment. Considering the average lifecycle of Zero Clients at over five years, ClearCube Microsoft COA licensing returns a payback after two years.
4. was the first manufacturer to develop PCoIP Zero Clients and Blade PCs. ClearCube Technology has invested in building an experienced PCoIP engineering support staff that understands the performance variables with differing network topologies and how to optimize the environment to deliver maximum performance. ClearCube's professional services team can help you get the most performance out of your available bandwidth.
5. has experienced ClearCube sales engineers and account executives to help you define a CVDI architecture to meet your needs. Products are quoted by hundreds of government resellers and prime contractors through Carahsoft's federal distribution team.

Appendix Solution Component Images

Zero Clients Solutions

Copper, Fiber, Dual Display, Quad Display, Integrated SmartCard Reader, Small Form Factor, Multiple Security Levels, 7 USB ports, PortAuthority Endpoint Device Control Management Software (Policy-based USB Access Enable/Disablement)

Centralized Desktop Infrastructure Solutions

Zero Clients (Copper, Fiber, Dual Display, Quad Display, Integrated SmartCard Reader, Small Form Factor, Multiple Security Levels, 7 USB ports, PortAuthority Endpoint Device Control Management Software (Policy-based USB Access Enable/Disablement))

Blade PCs (Series A High Performance Graphics , Series R Rack Dense) Sentral Management Software

Virtualized Desktop Infrastructure Solutions

Zero Clients (Copper, Fiber, Dual Display, Quad Display, Integrated SmartCard Reader, Small Form Factor, Multiple Security Levels, 7 USB ports, PortAuthority Endpoint Device Control Management Software (Policy-based USB Access Enable/Disablement))

SmartVDI Host Platform Series 100, SmartStor

Centralized and Virtualized Desktop Infrastructure Solutions

Zero Clients (Copper, Fiber, Dual Display, Quad Display, Integrated SmartCard Reader, Small Form Factor, Multiple Security Levels, 7 USB ports, PortAuthority Endpoint Device Control Management Software (Policy-based USB Access Enable/Disablement))

Blade PCs (Series A High Performance Graphics , Series R Rack Dense) Sentral Management Software

SmartVDI Host Platform Series 100, SmartStor

Centralized High Performance Engineering Workstation Solutions

Zero Clients (as listed above) Blade PCs (Series A High Performance Graphics, M Series 1022W, 1024W Engieering Workstations) Sentral Management Software

Zero Client Solutions

Centralized Desktop Infrastructure Solutions

Virtualized Desktop Infrastructure Solutions

Centralized and Virtualized Desktop Infrastructure Solutions

Centralized High Performance Engineering Workstation Solutions