VMware® View™ for Government-Agency Multilevel Secure (MLS) Desktops

Integrating market-leading technologies into a single, easy-to-deploy solution

WHITE PAPER

vmware®

Table of Contents

Executive Summary

Human lives depend on the multilevel secure (MLS) desktops used in government agencies. From fighter pilots and emergency responders who need clear communication based on real-time data, to homeland security professionals gathering and interpreting intelligence, to state department staff preparing sensitive briefings, the people who use MLS systems rely on them to get their jobs done at peak efficiency.

Yet today's government MLS systems are not always as efficient as they could be. They typically consist of complex webs of networks and devices running multiple operating systems and applications over a host of network connections. They often require end users to interact via multiple incompatible devices—so workers end up with a diverse array of computers and monitors crowding their workspace. MLS systems can also be difficult to deploy and manage, and in some cases they don't scale easily.

Virtual desktop infrastructure (VDI) provides a compelling solution to many of these challenges. VDI has evolved and matured to the point where it now delivers superior security, access control, and efficiency compared with traditional MLS desktop environments. Specifically, VMware View, combined with products from VMware partners such as ClearCube and Raytheon Trusted Computer Solutions (RTCS), delivers security and isolation of government networks at the desktop workstation, while providing a level of simplicity, agility, and cost efficiency that makes VDI an attractive solution for federal government agencies.

This paper summarizes the challenges of traditional MLS desktop solutions, recaps the technologies that make VDI a viable option, and highlights the capabilities of VMware View and the added value of products from ClearCube and RTCS.

Challenges with Traditional MLS Desktops

The complexities of delivering simultaneous access by users with different security clearances and needs-to-know, and preventing users from obtaining access to information for which they lack authorization, are almost overwhelming. Recurring security problems such as covert channels (where highly classified data is transmitted inappropriately to lower-classification users), bypassing (where unsecured data paths are opened maliciously or mistakenly), and an assortment of other issues have plagued MLS systems. And today, the accelerating pace of technological change creates additional challenges for government-agency MLS systems. To cite just a few examples:

Increased Security Risks

MLS systems are designed to increase the security of sensitive information, but often they end up creating additional security risks. For example, the incompatibilities among the multiple systems on a desktop may lead a user to write down information from one screen so that they can transfer it to another desktop; or the user may physically move data on floppies from one network to another (via the "sneakernet") and forget to log it or neglect to wipe data from the disk later. The data that resides on physical desktop systems is also vulnerable to theft from the user's desktop, and the need to physically move and lock away systems overnight is extremely inefficient.

Device Proliferation

Many government tasks now involve collaboration and cooperation among workers and contractors, government agencies, and international or coalition agencies. While this higher level of interaction can lead to higher productivity and better results, it also creates a proliferation of networks, operating systems, applications, and devices, many of which are incompatible.

From an end user perspective, the result is a cramped workspace loaded with hardware: multiple computers, monitors, radios, and other devices on and around the desk. This "desktop sprawl" also introduces new challenges for the IT department; management becomes more complex, time consuming, and error prone, resulting in higher costs and sometimes leading to "spillage" of sensitive data.

Figure 1: Collaboration is more important than ever—but more interaction leads to more networks, computers, monitors, and other devices on the desktop, resulting in higher costs and risks.

Inefficient Communication

Perhaps the most serious problem created by device proliferation is that it can actually get in the way of timely and effective communication. In a combat operation, for example, a cyber war fighter may need to share information in real time with a physical fighter in the field. He or she may see something on one monitor that needs to be communicated quickly via a second monitor. If there are compatibility issues, complex log-on processes, or delays in access authorization procedures, missions and human lives can be jeopardized.

MLS Desktop Virtualization: A Real Solution

The virtualized MLS desktop is not simply a concept. It is real; it is proven; and it is working in real-world federal government installations around the world. This section provides an overview of desktop virtualization, the technological underpinnings provided by VMware, and the added value of partner solutions.

Overview: What is Desktop Virtualization?

Desktop virtualization refers to hosting a desktop operating system within a virtual machine (VM) running on a hosted, centralized or remote server. Simply put, it brings centralized management to decentralized users. All of the data, applications, and state information that was once stored on each individual device is now housed, managed, and protected centrally. This makes desktops easier to manage and provision, and at the same time brings greater control and flexibility to IT—without requiring users to give up any of the functionality of their familiar desktops.

MLS desktop virtualization enables government workers—field-based, office-based, remote, deployed, and contractor personnel—to access their desktops and applications at any time from a variety of devices, such as government-furnished PCs or laptops, personal computers, thin clients, and tablet computers. Essentially, their desktop comes to them when they log on. Even their "persona" or user profile and personal preference information is maintained and managed centrally. Through this model, all of the user's desktop computing resources are better protected from theft, corruption, hacking, or loss, because they are maintained and managed centrally.

How Does VMware View Work?

Traditional desktop environments link together desktop components—hardware, operating system, applications, user profile and data. As a result, a problem at one layer often causes a chain reaction that can destroy the entire desktop and make recovery of locally stored user data and settings very difficult and costly. VMware View breaks the bonds between the desktop and associated OS, applications and hardware, and dynamically assembles and delivers desktops and applications to users with a personalized view of their individual desktops.

By encapsulating the desktop OS, applications and user data into isolated layers, VMware View enables IT staff to change, update and deploy each component independently for greater agility and improved response time. The result is a more flexible access model that improves security, lowers operating costs and simplifies desktop administration and management. VMware View provides the following key benefits and capabilities:

Continuity of Operations (COOP) and Service Availability
VMware View is built on the VMware vSphere™ platform—the leading industry-standard platform for virtualization, which is EAL4 certified for the NIAP/Common Criteria Certification. With VMware View, virtual desktops are always on; no time is lost waiting for machines to boot up; and desktops are accessible anytime, anywhere. Once users' credentials are validated, their desktop sessions appear immediately on the chosen access device regardless of location.

Secure, Manageable Desktops
VMware View enables federal IT departments to manage desktops, applications and data centrally through a single administrative console. This provides greater control and flexibility in provisioning, updates and delivery.

A Better Desktop Experience
Unlike traditional PCs, VMware View desktops are not tied to the physical computer. Instead, they reside in the cloud and authorized users can access their desktop when needed. VMware View with PCoIP delivers the richest, most flexible and adaptive experience for end-users around the world in a variety of network conditions. Business happens everywhere and whether online or offline, basic or 3D applications, LAN or WAN, VMware View delivers maximum workplace productivity.

VMware View is not a single product but rather a tightly integrated solution that brings together multiple products and technologies:

- **VMware® vSphere™ for Desktops**—A highly scalable, reliable and robust platform for running virtual desktops and applications.
- **VMware vCenter™ Server for Desktops**—Unified management for VMware vSphere providing control and visibility.
- **VMware vShield Endpoint**—A virtualization-aware security solution that enables offloaded and centralized antivirus and anti-malware solutions.
- **VMware View™ Manager**—Enables IT administrators to centrally manage thousands of virtual desktops from a single image to streamline the management, provisioning and deployment of virtual desktops.
- **VMware® ThinApp™**—An agentless application virtualization solution that streamlines application delivery while eliminating conflicts.
- **VMware View™ Composer**—For rapid creation of desktop images that share virtual disks with a parent image so they can be managed independently.
- **VMware View Client with Local Mode**—Runs on Windows PCs, Macs and thin clients, enabling end users to access their virtual desktop environments with or without a network connection.
- **VMware View with PCoIP Display Protocol**—A high-performance display protocol—specifically built for delivering virtual desktops over the WAN or LAN for a superior end-user experience from the task worker to the designer.

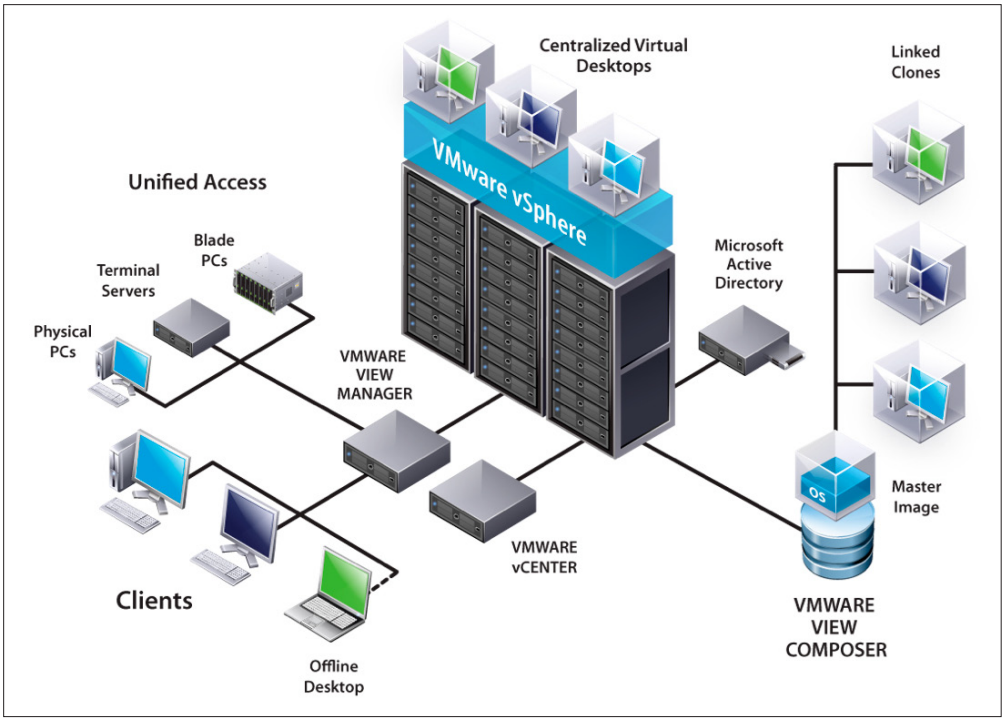

Figure 2: VMware View enables federal government organizations to create a private desktop cloud for delivering dynamic virtual desktops on demand over any network to end users on any device.

Evolved MLS: Added Value of VMware Partner Solutions

Tightly integrated with the value-added products of partners, VMware VDI solutions for MLS deliver the security and isolation government networks require at the desktop workstation while providing a higher level of simplicity, agility, and cost efficiency to government agencies. Of particular interest to government-agency MLS system users are ClearCube and Raytheon Trusted Computer Solutions (RTCS).

ClearCube ClientCube: Line of Sight Isolation from the Datacenter to the Desktop
ClearCube's ClientCube is the first endpoint that consolidates multiple networks into one device at the desktop, while maintaining physical network separation to centralized computing resources in the datacenter. VMware View and BladePC workstations can be isolated and secured in the datacenter without compromising the user experience or network security at the desktop.

Figure 3: ClearCube Client Cube

Co-developed by ClearCube and Belkin, this sleek all-in-one unit integrates ClearCube's secure stateless Zero Client devices with Belkin's NIAP-approved secure KVM (keyboard-video-mouse) switch to create a multi-network workstation. The results are zero PCs on the desktop, physical isolation of networks, and secure high-performance access to any configured virtual desktop using VMware View.

ClearCube is a leader in centralized computing and desktop virtualization, and has maintained a technology partnership with VMware for many years, resulting in the creation of fully integrated VDI solutions combined with best practices in high-performance computing and security. ClearCube also has a long history of deployments within the federal government due to the many benefits of ClearCube's PCoIP blades and Zero Client solutions. These benefits include:

- Full-performance computing solutions with PCoIP to VMware View or blade desktops.
- Extended, tightly controlled security profiles from end to end, providing line-of-sight isolation from the data center to the ClearCube Zero Client, increasing security of both physical and data assets.
- Full integration and optimization for network environments, saving space, power, and configuration management, including quick deployment or redeployment.
- Tamper-resistant, with no hard drive or OS, eliminating vulnerabilities that storage and operating systems may introduce.

ClearCube's ClientCube connects monitors, keyboard, mouse, and USB devices to up to four dual monitor PCoIP Zero Client devices over fiber or copper networks using the Belkin advanced secure keyboard-video-mouse (SKVM) switch. The SKVM switch, provided by Belkin International, Inc., allows users to securely switch from Zero Client to Zero Client, completely isolating network segments in a switched environment with the following features:

- Support for legacy and and/or the latest CAC, smart card, high-definition monitors, and keyboards and mice
- Intelligent Smart Card switching to minimize multiple logins
- Complete reset and data clear of USB channels whenever switched to another computer, preventing data leakage from network to network or computer to computer
- Secure audio channel support
- Uni-directional, light-diode USB port circuitry, impervious to data sniffing or signaling attacks
- Tamper-proof and isolated on-board circuitry and case

By replacing box PCs with ClearCube Zero Clients, over 94% of the heat and noise is eliminated from the work environment. In addition, ClearCube Zero Clients utilize less than 15 watts of power or less, which significantly improves the ability to sustain command and control operations and reduce costs.

ClearCube ClientCube seamlessly connects to high-performance workstations or VMware View virtual machines to deliver a lossless image for the demands of high-performance, high-definition multi network user. The entire system is tamper resistant, contains no programmable ROMS, drives, or operating systems, and does not require upgrades or patches, making them immune from worm or virus attacks. Designed, manufactured, and shipped from secure U.S. facilities, ClearCube ClientCube and its SKVM are among the most trusted computing devices in the industry.

Raytheon Trusted Computer Solutions Trusted Thin Client: Multi-Network Access via a Single Wire
With the increasing need to access disparate sensitive or classified networks, desktop environments must maintain a physically separate connection to each required network, resulting in multiple workstations and network connections per user. Often the user can view only one network at a time; there is no toggling back and forth between views; and extraneous hardware, software, and administration is required.

RTCS offers its Trusted Thin Client (TTC) solution to address these challenges. An accredited Commercial-Off-The-Shelf (COTS) solution proven in large-scale, mission-critical enterprise and command and control environments, TTC provides secure simultaneous VMware View (PCoIP) connections to information on any number of different networks through a single connection point. TTC maintains secure data separation while allowing users appropriate access to networks at different classification levels, or to networks that hold the same security level in a government organization.

This reduction in desktop hardware is achieved through the use of the Distribution Console (DC). The DC securely maintains all network separation within the software, which then allows a single wire to the desktop. Because TTC is a software-based solution, it provides the ability to repurpose existing devices, thus reducing many infrastructure costs including hardware, wiring, and energy consumption. Additional benefits are environmental and aesthetic improvements of reduced workplace noise and heat, and more streamlined and spacious working environments for the end user.

TTC utilizes commercially available, non-proprietary, x86-based thin client devices, including ClearCube's TC8900. The client software is flash loaded, unclassified, and is used to connect the thin client to the DC. At rest, the thin client is stateless, with no writable persistent resident memory or storage for added security. If a thin client is lost or stolen no data exists on the device, thereby protecting the data from unauthorized access.

TTC utilizes VMware solutions in a variety of ways from access to virtual desktops with VMware View to PCoIP for enhanced graphics support to the use of VMware Player to present and secure a virtual thin client. Additionally, the VMware View client (PCoIP implementation) has FIPS140-2 Level 2 certification providing assurance of the encrypted PCoIP connection between the View client and View back-end.

RTCS has been an industry leader for over 18 years supplying secure MLS solutions to government, civilian agencies, 5 Eyes nations, and NATO member countries. RTCS solutions appear on the Unified Cross Domain Management Office (UCDMO) Baseline List and have successfully completed formal evaluation with other 5 Eyes technical authorities. Products listed on the UCDMO Baseline List are pre-approved for operational use, which expedites procuring and implementing these solutions.

Five Reasons to Make the Move to VDI for MLS

The combination of VMware View and partner products not only creates powerful incentives to initiate the transition to VDI for MLS deployments, but also to make this transition a top priority. Just a few of the key reasons government agencies are making the move to VDI for MLS today include:

1. Strengthen Security of Data, Networks, and Desktops

Joint MLS solutions from VMware and its partners are properly certified to run in highly sensitive MLS environments and are simply more secure. For example, viruses, spyware, malware, and other threats can be handled centrally by security specialists through updates, patches and desktop refreshes, and specific security policies and practices can be centrally set and consistently enforced and monitored across users and devices.

With VMware and partner solutions for MLS, administrators also have more control over the desktops with a management platform that allows them to set group/individual desktop policies—for example they can turn off USB access and turn on/off cut and paste capability—or if policies dictate that users should power off at 5pm every day administrators can enforce that policy. Equally important, data is removed from the endpoint and stored in secure datacenter, providing another dimension of security. In addition, VMware View supports single sign-on (SSO) with Common Access Cards (CAC) and prevents data leakage and network intrusions with SSL encryption, multifactor authentication and access control policies for USB devices.

Moreover, the VDI model protects against the risks associated with lost or stolen hardware, such as laptops, through centralization of the desktop and data within the datacenter. With the desktop running centrally, sensitive data can remain safe and secure in the datacenter, and there is no need to physically move and lock away sensitive systems overnight. All users' desktops can be backed up quickly and easily from a central location.

2. Consolidate: Cut Clutter and CAPEX

At a certain point, all of those devices cluttering the desktops of government workers begin to hinder productivity rather than add to it. They also represent large—and largely unnecessary—capital expenditures. Beyond the acquisition and installation costs of the hardware itself, each device consumes power and takes up space that could have been used for other purposes. Many of these devices have short useful lives and are quickly replaced with other devices, and the original devices can rarely be repurposed.

An MLS solution based on VMware View, in conjunction with one of our partners such as RTCS or ClearCube, delivers immediate CAPEX savings because many of these devices can now be consolidated. It can also cut CAPEX by giving agencies the ability to delay hardware refreshes—you can also repurpose PCs and laptops by hardening them down and essentially turning them into thin clients. When the existing hardware does need to be replaced, it can be replaced with less expensive, easier-to-maintain thin clients or zero clients.

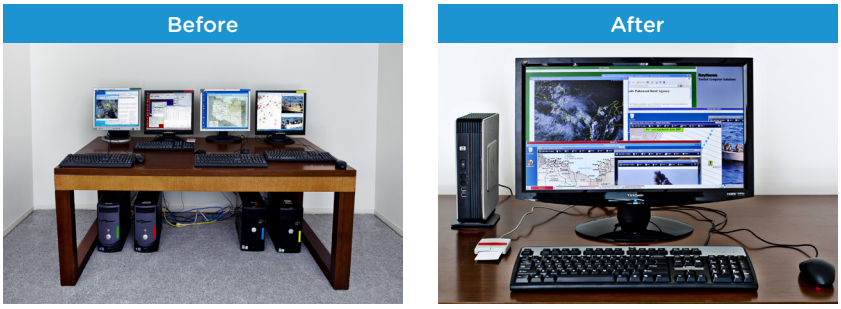

Figure 3: Consolidation of devices cuts clutter and CAPEX.

3. Unburden Administrators and Slash OPEX

In the traditional desktop model each device must be supported individually, and that is enormously expensive, particularly as the sheer number of devices continues to grow. Each supported device requires OS, application, and network upgrades; compatibility testing; end-user permissions management; security updates; help desk and technical support; and more. This support is very labor intensive, and according to Gartner, while the cost of hardware has declined since 2005, people costs continue to rise significantly.[1] The result is that for every $1 of CAPEX (the cost of the devices themselves), an additional $3 of OPEX is spent on device management.[2]

MLS solutions based on VMware and partner products replace this expensive one-off support with cost-efficient, centralized management. Now administrators can:

- **Manage desktop components from a single console** and apply policies, entitle applications, patch and upgrade the OS and applications while deploying desktops quickly and easily
- **Monitor and troubleshoot** with a unified view of MLS desktop infrastructure to quickly and easily identify key information and events
- **Accelerate provisioning and migrations**, such as adoption of Windows 7, by minimizing application incompatibilities and regression testing requirements while enabling the rapid deployment of desktops to new end users
- **Customize applications and desktops** quickly, efficiently, and independently of the endpoint device

4. Improve Communications and Preparedness

VMware View enables field-based, office-based, remote, deployed, and contractor personnel to stay connected and productive using their familiar desktop environments—with all data and applications instantly available, from anywhere. Vital information can be more quickly shared with the appropriate, authorized personnel, resulting in faster emergency response times, faster and more accurate in-field combat intelligence, better preparedness, and more timely information sharing in dozens of other vital government services.

Equally important, the VDI model can deliver MLS desktops as a continuously available service to any access device in case of a catastrophic or disruptive event. With VMware View, virtual desktops are always on, so no time is lost waiting for machines to boot up. The desktops run off powerful servers in the data center that are accessible anytime, anywhere. Once the user's credentials are validated, their desktop session appears immediately on the chosen device regardless of location.

1. "IT Key Metrics Data 2010: Key Infrastructure Measures: Client and Peripherals Analysis: Multi Year," by Gartner, April 2010.
2. IDC study, 2009

5. Provide the Best End User Experience

Together with products from VMware partners such as ClearCube and RTCS, VMware View delivers a superior end-user experience for MLS users in LAN/WAN environments, even those working with 3D and rich graphical, multimedia applications. VMware View with PCoIP (adaptive protocol) delivers the richest, most flexible and adaptive experience for end users in a variety of network conditions, with support for unified communications. VMware View also works with Adobe Connect for users who use Defense Connect Online, and it works seamlessly with CAC cards, so all users are more productive. Whether online or offline, basic or 3D applications, LAN or WAN, VMware View delivers maximum workplace productivity.

Conclusion

VMware, together with strategic partners such as RTCS and ClearCube, are delivering on the promise of efficient, effective MLS systems. With VMware View at the core of the VDI solution, government agencies can provide more immediate, flexible, secure access to vital information; enhance COOP preparedness for desktops and applications; simplify IT management and costs; and quickly provision new desktops and manage the entire desktop population, including advanced SKVM for enhanced security among shared peripherals.

In short, desktop virtualization presents a unique opportunity to transform MLS desktops from a source of inefficiency and waste into a source of agility, higher productivity, and better communication among government workers.

Additional Resources

For more information or to purchase VMware products, call 1-877-4VMWARE (outside of North America dial +1-650-427-5000), or visit www.vmware.com/products, or search online for an authorized reseller. For detailed product specifications and system requirements, please refer to the VMware View documentation.

VMware also encourages government agencies to contact VMware directly to request an assessment. Our experts will help you determine the opportunity for your organization—and chart your course to consolidated, efficient MLS desktop access.

About VMware, ClearCube and Raytheon Trusted Computer Solutions

VMware, the global leader in virtualization and cloud infrastructure, delivers customer-proven solutions that accelerate IT by reducing complexity and enabling more flexible, agile service delivery. VMware enables enterprises to adopt a cloud model that addresses their unique business challenges. VMware's approach accelerates the transition to cloud computing while preserving existing investments and improving security and control. With more than 250,000 customers and 25,000 partners, VMware solutions help organizations of all sizes lower costs, increase business agility and ensure freedom of choice.

ClearCube was founded in Austin, Texas in 1997 and is a recognized leader in centralized computing and desktop virtualization markets. These growth markets are a result of global organizations seeking to reduce IT management costs by consolidating resources, improving manageability and enhancing security while efficiently delivering the best computing capabilities for each user. The company also engages with a variety of value added reseller and integrator partners who represent ClearCube solutions throughout the world.

Raytheon Trusted Computer Solutions has over 18 years of proven leadership providing multilevel security and cybersecurity solutions to US and International governments, 5 Eyes nations, NATO, and commercial organizations. RTCS' MLS products are certified and accredited by some of the most stringent security organizations in the world. These MLS solutions help protect sensitive, classified, and mission-critical information while ensuring that the right data gets to the right people at the right time. All RTCS products are backed by the company's Professional Services group, which consists of nationally and internationally recognized experts in security policy, architecture, planning, and implementation.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com