VMware® Federal Secure Desktop™ and BYOD

Straight Talk About Security

WHITE PAPER
Introduction

Cyber security is on everybody’s mind these days, nowhere more than in the defense community, where IT managers and security officials are subjected to a daily barrage of promotional material from device manufacturers and providers of application and device management solutions. As threats increase in number and sophistication, security policy becomes ever more important—that’s clear. Yet policy enforcement is expensive and time-consuming, and even with appropriate staff and spending decisions, oversight is often lax. For instance, a recent NASA audit found that security policies were not implemented on half a dozen servers that host critical data and IT assets associated with control of spacecraft, leaving the door wide open to intruders.

In the office and in the field, there are always individuals who find strict security measures constraining and look for personal shortcuts. There are also sloppy habits, such as failing to remove a smart card when taking a break. What’s more, the increasing popularity of BYOD smart phones and tablets—whether managed or not—can create additional vulnerabilities, especially when they are used to access restricted material. Their very size and capabilities make it tempting to cut corners in unauthorized settings. That’s one reason why the endpoint is a weak point and perhaps why BYOD is often defined as Bring Your Own Disaster.

Once sensitive data is stored on any device, rather than simply displayed, a careless person can enable leakage between public and private zones or between secret and top-secret data. Even a well-meaning person can also be careless enough to lose a device containing sensitive data—a database of social security numbers, weapons plans, compromising personal or other sensitive information—at an airport or other public place. A malevolent person can do even more harm, of course. The mention of Bradley Manning or Edward Snowden, not to mention Stuxnet, should be enough to remind any security official of the wisdom of blocking—rather than merely advising against the use of—USB device access to sensitive material.

In an environment where increasing demand for secure access is accompanied by threats of increasing number and sophistication, what solutions should agency management and IT security officials consider for the near and middle term?
Multiple Physical Desktops for Multi-Network Access

Today, a DoD analyst typically requires two or, for top-secret work, three complete workstations, each with an isolated physical connection to a public or secret or top-secret network, with appropriate authentication and encryption at each level.

Figure 1: Segmented Model for Multi-Network Access with Isolated Physical Connections
This solution has been in place for many years and has been fairly effective in keeping classified data in its proper place while making appropriate access available. In the field, though, it is neither practical nor convenient to carry too many dedicated hardware devices, regardless of form factor, to perform essentially parallel tasks. The ability to access multiple, secure networks remotely from a single device remains the hope and desire of many who travel on assignment.

Of course, the quest for convenience and timeliness must be balanced by realistic security concerns and individual responsibility. For instance, regardless of technical feasibility, it would make no more sense to read classified documents in public, whether on an iPad or hardened PC, than to flaunt hardcopy documents in a cafe. And, as many people have asked, “How can you trust your iPad once it’s been to Starbucks?” That’s why architectures, equipment combinations, and procedures must be vetted. On the other hand, cumbersome procedures and delays can prevent critical decisions from being made within a given window of opportunity, and a “good enough” on-time decision is better than a perfect one made too late.

**Multi-Network Access from a Single Device**

The suggestion that an analyst might like to have wireless access to secret documents on a portable device is one of the ideas that prompted VMware® to address this question. A viable implementation may not be far off, since the technology and ciphers that can enable secure wireless access are available today. However, even with the best authentication and encryption available now or on the near-term horizon, endpoint devices such as smart phones, tablets, and even traditional laptops, which store data or enable storage devices, increase the potential attack surface by exposing data at rest. That’s why device access to the most secure environments still needs to be restricted. Agency policies should prevent access to secret networks from public hot spots, hotel rooms, or other venues that are clearly vulnerable to attack and should scrutinize device types and form factors carefully.

The best and perhaps most elegant current approach to the hardware device problem is to use a thin client, such as a Teradaci PCoIP zero client, instead of the usual Windows PC, in the office and a portable zero client, such as a ClearCube PZC, in the field to connect to VMware Horizon View™ desktops on multiple networks. This is a No Data at Rest (NDAR) solution that reduces the attack surface at the network and device levels.
Less desirable solutions include the use of repurposed laptops, which proffer initial savings at the price of security, and tablets and smart phones, which are convenient but not secure. Recent studies show that repurposing hardware seldom produces a net cost reduction because of the continued, often increased, cost of administration, maintenance, and upgrades of older equipment. As a rule, every CapEx dollar spent on traditional desktop hardware requires three dollars in OpEx. This is not the case with zero clients, which have a much longer shelf life and typically require no maintenance.
Server, storage, and desktop virtualization and cloud conversion projects are already implemented or in process at many government sites, where Horizon View desktops and zero clients offer performance advantages and better management solutions as well as cost effectiveness. By centralizing IT management in the datacenter, Horizon View and VMware Horizon Workspace™ provide at least one additional layer of protection, reducing the attack surface and eliminating the need for additional edge or endpoint management software. Information can be displayed on endpoint devices but not stored or replicated. Instead of data files, which are often the targets of focused attacks, this solution exposes only key strokes and mouse events from the client and pixel data from a server, enclosed in FIPS 140-2 validated encryption packets.

At the discretion of the IT administrator or policy makers, potentially compromising functionality—such as the ability to use USB storage devices to copy files or download executables—can be restricted with global or role-based settings. Even with best-of-breed VDI offerings, however, the most popular endpoint devices may not be optimal choices for secret and top-secret deployments, where security has to trump convenience and user experience.
Untrusted Network, Trusted Connection

Suite B ciphers and portable zero client form factors make it possible to combine mobility with stringent security, but requirements for secure connections place certain limits on the Secure Wireless Access Anywhere on the Go (SWAAG) model.

![Diagram of secure connection over insecure network using Suite B ciphers](image)

Even with the best current technology and the latest regulations, wireless networks can be used securely only under limited circumstances, requiring both vetting and common sense. So, although it is possible to establish trusted connections over untrusted networks, agencies and regulators still have to determine exactly what these limits should be. The tendency, in 2013 at least, is still to recognize the possibility but to favor security over convenience.
Authentication and Encryption

It is not necessary to review the history of modern encryption from the Enigma machine to RSA to make the case that multifactor authentication and sophisticated encryption are important technologies that enhance the level of protection wherever they are deployed. Everybody who cares about security should use them.

Smart Cards and Multifactor Authentication

Although smart cards are not ordinarily compatible with smart phones or tablets, they can be used easily with some thin or zero clients and, of course, smart card readers. VMware currently supports Common Access Card (CAC), Secret Internet Protocol Router (SIPR) Token, and Personal Identity Verification (PIV) smart cards as well as a broad range of compatible smart card readers.

Smart cards offer another layer of authentication and encryption, depending on the type of card and contents of the smart card token. There is also a convenience factor. If a site or agency is fitted with zero clients wired to appropriate networks, there is no need to carry a laptop or tablet because the smart card can provide access to the owner’s Horizon View session (or sessions, if separate devices are connected to different networks) from any available zero client device. Although it may not be everybody’s first choice, this is one way to effectively circumvent the BYOD problem. IT administration also has the option of allowing wireless access for zero client laptops, preferably equipped with smart card readers.

For commercial sites with less stringent security requirements, IT administrators can choose to enable wireless access for Horizon View Clients on iOS or Android endpoints. In these cases, proper security policies and workforce education can mitigate risk to some degree.

Using the Right Ciphers

Until now, NSA has allowed only Suite A ciphers to protect secret and top-secret information. Devices and keys are tracked closely, and anybody accessing them must undergo a strict background check.

Suite B ciphers are NSA-approved ciphers that rely on the strength of AES 128-256 to allow communication between two nodes to pass secret up to top-secret information. Looking toward the future, some vendors already have National Information Assurance Partnership (NIAP) approval for devices that use Suite B ciphers. Again, agencies need to evaluate new devices carefully in the light of new capabilities, such as ciphers, and other considerations, such as durability, reliability, and risk of intrusion or data loss if a device is lost or captured.

Horizon View Security Gateway

Navy/Marine Corps Intranet (NMCI) Webmail access for Windows 7 has been possible for several years and should work from a Horizon View Windows 7 desktop. Precedent has been set, and the solution should be viable. Individual commands should seek the appropriate approvals, including Authority to Operate (ATO), Certification and Accreditation (C&A), and Certificate of Networthiness (CoN).
Product Differentiation

Desktop products, such as Parallels and VMware Fusion®, are designed for individual users and run a second operating system on a single end-user computer. Many people who carry a MacBook Pro also need to run Windows 7. These products leverage the power of the personal computer to enable that solution and similar ones, but they do not scale up effectively, and they do not provide the enhanced levels of security needed for military or other sensitive work.

VMware Horizon Workspace provides secure access to applications hosted behind a corporate or agency firewall. These applications can be used with relative safety on iOS and Android devices as well as on conventional computing platforms.

VMware Horizon View desktops are designed for large-scale enterprises, private or public. Hosted Horizon View desktops leverage the power of the datacenter. With zero-client access and other measures described in this paper, they offer a high-security solution for mobile government workers.

Reduced Cost, Improved Mobility

Replacing hardened desktops or laptops is an expensive proposition when scaled out, even if the replacement cycle is extended beyond the customary three years. Zero client devices have a much longer life span and much lower initial cost in addition to being intrinsically more secure than workstations, laptops, tablets, or smart phones. In addition, diskless clients have no state and no operating system in the traditional sense, so the devices themselves carry no licensing fees. More important than acquisition and licensing costs, though, are device security concerns. When a BYOD laptop, iPad, or BlackBerry is lost, all the data it contains is not only lost but compromised. When a zero client is lost, the device has no practical use to a thief or foreign agent except as a paperweight, and total loss is limited to the replacement cost of the device. There are no security consequences.

Although Horizon View desktops are not cost-free—there are still acquisition and maintenance costs and Microsoft license fees—acquisition, maintenance, update, and administration are significantly less expensive than they are for dedicated hardware. Perhaps most important, Horizon View desktops accessed from zero client devices over a succession of secure gateways, using multifactor authentication and Suite B ciphers, offer a viable, affordable, and relatively secure solution to the problem of mobility in an age of increasing risk and continual attack.
About the Author

David G. Young, Jr. is an End-User Computing Solutions Architect representing the VMware Federal Solutions Engineering Team. Dave has over 24 years of experience in the IT industry, including the US Navy, where he served in the Submarine Communications arena. His background includes expertise in datacenter and cloud architectures, systems engineering, desktop management, and mobile device management.

References

BYOD at the NSA? Maybe someday with mobile hardware root of trust
CAC Use on Mobile Devices
ClearCube White Paper: Best Practices Pairing Virtualization and Centralization
Desktop Virtualization with VMware View 5 Compared to Citrix XenDesktop 5.5
DOD Policy on Commercial Mobile Devices (CMD)
Future DoD SIPRNET VMware View
Inadequate Security Practices Expose Key NASA Network To Cyber Attack
Network Insecurity
Network Virtualization in the Software-Defined Data Center – Office of the CTO blog post
NIAP and COTS Product Evaluations
PCoIP Cryptographic Module for VMware View
Protecting virtual desktops: Nine ways to ensure VMware View security
Quantifying the Business Value of VMware View – IDC white paper
Secure Remote Access for Government Teleworkers
Security Advisories, Certifications & Guides
Suite B Product Overview
Tablets and Smartphones in the Enterprise
Teradici PCoIP Zero Clients
Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules
VMware View for Government-Agency Multilevel Secure (MLS) Desktops
Virtual Desktop Implementation and Maintenance: VMware View 4.6 Premier vs. Citrix XenDesktop 5 Platinum
VMware Federal Secure Desktop Validated Design Guide