Secure Remote Access for Government Teleworkers

WHITE PAPER
VMware View™ helps federal agencies implement teleworking as a cloud-based service to meet new requirements, keep employees productive, and contain costs.

The North American blizzard of 2010 included snowfall totals of 20–36 inches throughout the Washington D.C. region and closed the government for four days. It cost millions of dollars, and served as the ideal use case to support the newly enacted Telework Enhancement Act of 2010, H.R.1722.

Nearly every federal IT organization today is working to embrace mobile computing for a number of reasons, including:

- Lowering its carbon footprint and energy costs by reducing employee commutes.
- Improving employee satisfaction and work/life balance, especially for younger workers who expect more flexible, mobile work arrangements.
- Striving for an “always-on” and agile eGovernment infrastructure that gives employees immediate access to information.
- Supporting continuity of operations (COOP) in the event of emergencies by helping employees do their jobs effectively from home or remote locations.

The Telework Enhancement Act and initiatives around disaster recovery and COOP pose both an opportunity and a challenge for federal IT leaders. Users expect and require access to applications and data on a variety of devices to maximize productivity, but IT is pressured to secure information and control critical processes and data.

VMware View™ helps federal IT leaders comply with the Telework Enhancement Act, meet COOP initiatives, and solve the access-control dilemma by helping IT personnel manage desktops centrally and effectively. The VMware View solution, based on the VMware vSphere™ platform, provides all of the resiliency, security, and operational advantages of VMware’s robust infrastructure solution, while removing dependencies on physical machines. It provides anytime, anywhere access to applications and data that reside not on individual devices, but rather in the data center, enhancing security and information availability.

The Case for Telework

Telework creates benefits for the triple bottom line of profit, people, and planet, as shown in Table 1.

<table>
<thead>
<tr>
<th>BUSINESS BENEFITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Reduced real estate costs</td>
</tr>
<tr>
<td>• Reduced IT capital expenditures (CapEx) and operating expenditures (OpEx)</td>
</tr>
<tr>
<td>• Improved flexibility to expand the business</td>
</tr>
<tr>
<td>• Increased employee productivity</td>
</tr>
<tr>
<td>• Simplified business continuity planning</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EMPLOYEE BENEFITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Increased flexibility with personal/family life</td>
</tr>
<tr>
<td>• Increased job satisfaction</td>
</tr>
<tr>
<td>• Reduced or eliminated commute time and costs</td>
</tr>
<tr>
<td>• Simplified work anytime from anywhere</td>
</tr>
<tr>
<td>• Improved performance</td>
</tr>
<tr>
<td>• Simplified management by results</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ENVIRONMENTAL BENEFITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Decreased fuel consumption</td>
</tr>
<tr>
<td>• Decreased greenhouse gas emissions</td>
</tr>
<tr>
<td>• Decreased traffic congestion</td>
</tr>
<tr>
<td>• Decreased road maintenance costs</td>
</tr>
</tbody>
</table>

Table 1: Telework benefits
How VMware View Enables Telework
VMware View, the most widely deployed and trusted desktop virtualization solution, enables government workers to access their desktops and applications at any time from a variety of devices, such as government-furnished laptops, personal computers, thin clients, and tablet computers. Sensitive data stays safe and protected behind the corporate firewall, with security policies in place for managing access. With VMware View, IT staff can deploy large volumes of virtual desktops for teleworkers as easily as they could deploy a single desktop, improving security and lowering operating costs.

Deliver Secure Desktops for Teleworkers
With built-in Secure Sockets Layer (SSL) encryption, the VMware View solution offers federal IT strong network security to protect sensitive data. SSL tunneling ensures all connections are completely encrypted. VMware View Security Server enables secure access to virtual desktops without the need for a traditional virtual private network (VPN) solution. Alternatively, it can also be integrated with an agency’s existing VPN solution. VMware View fully supports the federal Personal Identity Verification (PIV) access cards, Department of Defense (DOD) Common Access Cards (CAC), and RSA SecurID®, providing the added security of two-factor authentication for tightened access control.

Enable a Superior Telework Experience Over Any Network
VMware View, with PC over IP (PCoIP) protocol technology, allows federal IT to deliver a high performance desktop experience for teleworkers, even over most high-latency and low-bandwidth connections. PCoIP is an adaptive technology that is optimized for the delivery of virtual desktops to users over both local and wide area networks. VMware View gives teleworkers access to their desktops through a wide variety of devices, from Windows® and Linux® desktops to the Apple Mac®, and iPad® systems, and other mobile devices. Users can access their critical applications and choose from any number of monitor configurations, while strict policies can be set for locally attached USB peripheral devices such as printers and mass storage.

Optimize Management of Telework Environment
Desktop and application virtualization breaks the bonds between applications, data, and operating systems, eliminating the need to actually install or manage desktop environments on end-user devices. From a central location, IT teams can provision, manage, and update Windows desktops and applications in minutes.

Automated Provisioning
VMware View provides a single management tool to provision new desktops or groups of desktops, and an easy interface for setting desktop policies. IT administrators can use a template to customize specific groups of desktop pools, provision and manage applications, and set policies to govern the number of virtual machines in a pool, the login and logoff parameters, and so on. This feature enables greater IT efficiency through automated and centralized desktop provisioning activities.

Advanced Virtual Desktop Image Management
VMware View allows federal IT administrators to rapidly create desktop images from a single parent image. Updates implemented on the parent image can be pushed out to any number of virtual desktops in minutes, greatly simplifying deployment of operating system (OS) and application patches. This update process can run in the background so users can remain productive—then, the next time a user logs on to their desktop, they connect to the updated image and user settings, and application settings and user data can be preserved to ensure continued user productivity.

Control Costs of a Telework Solution
A VMware View solution streamlines CapEx costs by allowing federal IT to invest in low-cost “zero” or thin clients as an alternative to traditional desktops, and to extend the life cycle of existing hardware by converting legacy equipment into thin clients. The real benefit of VMware View, however, results from the potential OpEx savings. This is important because, according to an IDC study conducted in 2009, for every dollar spent on hardware in a traditional desktop environment, roughly three dollars are spent on managing that environment.

By decoupling the operating system, applications, and data from the end device, and by pushing those components into the data center where they can be more effectively managed, federal IT can dramatically save on the time and resources needed to fulfill help desk tickets, push out updates and patches, and provision new images to pools of teleworkers.

Technical Considerations
Several technical considerations must be addressed in order to provide an optimal experience for government teleworkers while ensuring that the solution encompasses adequate security and control measures. These considerations include network bandwidth, end-user experience, security, and endpoint hardware.

Network Bandwidth and End-User Experience
You can easily optimize VMware View with PCoIP for desktop delivery over wide area network (WAN), 3G, wireless WAN, direct, or over VPN. The PCoIP protocol provides real-time delivery of a rich user desktop experience using user datagram protocol (UDP), and it can be simply optimized and tuned to meet WAN bandwidth concerns while addressing other quality of service issues, such as latency, jitter, and packet loss.

You might require increased bandwidth based on the type of work performed by teleworkers. Creating profiles for typical
Secure Remote Access for
Government Teleworkers

Secure Remote Access for Teleworkers

You can achieve secure remote access through a VMware View solution in several ways, including the following:

• Integrate VMware View with an existing VPN solution to maximize technology investments.
• Deploy VMware View with the built-in VMware View Security Server.

With built-in SSL encryption, VMware View can be integrated with your existing VPN solution to establish a secure connection between the remote device and the virtual desktop in the data center. VMware View Connection Server manages SSL VPN connections and can provide secure access to specific desktop resources. Also, vendors such as Juniper, F5, Cisco, and OpenVPN have completed preliminary PCoIP validation for their access gateways to ensure there is no service degradation while using SSL VPN solutions with PCoIP.

The VMware View Security Server provides PCoIP with a full-duplex end-to-end network link. Configuring the Security Server in gateway mode for the Connection Server and locating it in a DMZ isolates the internal network from Internet requests coming from the VMware View Client. With a DMZ configuration, the following ports must be opened for a PCoIP connection between the View Client and the virtual desktop:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>EXTERNAL FIREWALL</th>
<th>INTERNAL FIREWALL</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 4172</td>
<td>Inbound</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Outbound</td>
<td>Inbound</td>
</tr>
<tr>
<td>UDP 4172</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Table 2: Open ports for a PCoIP connection

As shown in Figure 1, VMware View 4.6 uses PCoIP to establish the connection between the View Client and the Security Server. If the user successfully authenticates through the View Connection Server, the user can select a virtual desktop. If the user has rights to access the requested virtual desktop, a secure PCoIP connection is established directly between the Security Server and the requested virtual desktop.

Security

The VMware View solution helps protect mission-critical data in a telework environment by centralizing desktop images and data in the data center. This helps eliminate security breaches due to data corruption, loss, or theft. VMware View supports smart card single sign-on with CAC/PIV cards, RSA SecurID, biometric sensor, and USB eToken two factor authentication devices. The following security considerations should be addressed for a telework environment.

teleworkers can make managing the end-user experience easier. When creating teleworker profiles, take the following factors into consideration for network planning:

• Graphical intensity of the user (for example, forms, pages, or a 3D viewer)
• Importance of image quality to the user (for example, administration or designer)
• Amount of interactivity versus static viewing

Once you identify teleworker profiles, you can optimize performance for remote telework access by:

• Tuning the Windows operating systems
• Ensuring sufficient minimum bandwidth for PCoIP packets
• Minimizing packet buffering for PCoIP packets through the network
• Ensuring an appropriate queuing/priority configuration in the switch/router
• Adjusting VMware View settings based on user profile, to optimize for:
  – Image quality
  – Maximum display frame rate
  – Maximum bandwidth


Table: Open ports for a PCoIP connection

As shown in Figure 1, VMware View 4.6 uses PCoIP to establish the connection between the View Client and the Security Server. If the user successfully authenticates through the View Connection Server, the user can select a virtual desktop. If the user has rights to access the requested virtual desktop, a secure PCoIP connection is established directly between the Security Server and the requested virtual desktop.
Secure Remote Access for Government Teleworkers

If your environment does not have an existing VPN solution, using VMware View Security Server can provide secure remote access for teleworkers.

Telework Policy Enforcement
To comply with the new Telework Enhancement Act you must ensure that all levels of policies can be implemented when needed. VMware View provides the intuitive policy management needed to address telework policy requirements for civilian personnel and service members.

- Telework eligibility, denial, and termination. You can grant or deny access to desktops using your native Microsoft Active Directory users and groups. VMware View supports Online Certificate Status Protocol (OCSP), Certificate Revocation List (CRL) update, and centralized Active Directory policy management and control. This instantaneous support to update or revoke teleworker access to network resources is a critical component of enforcing telework access policies.
- Auditing and information control. VMware View provides centralized management, with one-click allow or deny USB peripheral access. You can also set Active Directory policies to disable copy and paste. VMware View centrally logs all desktop session entries by date, time, and endpoint system information, which makes it easier to comply with auditing policies.

- Emergency situations. VMware View allows a federal IT administrator to provision a desktop pool, control access, and entitle users on-demand. In the event of a natural or man-made disaster, a properly configured Active/Active or Active/Passive virtualization platform can be deployed to achieve a minimal recovery time objective (RTO).

Endpoint Hardware
The VMware View solution runs on a number of different endpoint devices, including:

- Traditional or thick clients, like desktop and laptop computers
- Thin client and zero client devices running little to no OS
- Tablet computers and mobile devices, like the iPad

When providing secure remote access for teleworkers, federal IT administrators need to consider how a user will access the desktop in the data center. This will guide IT to the best choices for security and configuration of users and desktops. You can use these general device categories to determine how to provide secure remote access with a VMware View solution:

Connection Sequence
- User connects to View Connection Server and authenticates via Https
- When a PCoIP desktop is selected, the PCoIP protocol goes to the Security Server
- If the PCoIP session is on behalf of an authenticated user it is forwarded to the correct desktop
- Support for RSA SecurID and SmartCards

Figure 1: View Security Server access with PCoIP support in VMware View 4.6
Secure Remote Access for Government Teleworkers

The following sections provide general technical guidelines for these endpoint device categories. Please consult with your hardware vendor and/or your VMware account manager for the best configuration for your situation.

**Personal Device: Desktop or Laptop**

Some government agencies are not comfortable with allowing workers to use their own personal desktop or laptop for work. This reticence arises from several concerns, including:

- Policies that prohibit the agency from asking employees to use their own equipment
- Increased security risks, including data leakage and malware infection
- Questions around who has responsibility to manage the device
- Concerns about increased support costs

For agencies that allow their workers to use personal devices for telework, a VMware View solution provides secure remote access to virtual desktops. VMware View with VMware ThinApp™ also provides a secure remote access solution that addresses agency concerns around security, management, and liability. Table 3 summarizes each of these solutions.

<table>
<thead>
<tr>
<th>Solution</th>
<th>ALLOW PERSONAL DEVICES</th>
<th>CONCERNED ABOUT PERSONAL DEVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>How Does It Work?</td>
<td>The VMware View Client is installed on the personal device to provide secure access to the worker’s virtual desktop. Suggested best practice: configure the View Client executable with appropriate Security Server settings so the worker doesn’t have to make configuration changes.</td>
<td>ThinApp is used to encapsulate the View Client, completely decoupling it from the OS on the personal device. This ensures ultimate security and separation from the personal device. ThinApp is included as part of the VMware View Premiere Bundle and Premium Package.</td>
</tr>
<tr>
<td>Install Client on Personal Device?</td>
<td>Yes—The worker downloads and installs the VMware View Client on the personal device.</td>
<td>No—The worker downloads a ThinApp executable that runs independently of the OS on the personal device.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Single sign-on with two-factor authentication including CAC/PIV smart card, RSA SecureID, eToken, and biometric finger print sensors</td>
<td>Single sign-on with RSA SecurID or Windows authentication</td>
</tr>
<tr>
<td>Device OS, Access Protocol, and View Client</td>
<td>Windows: PCoIP, View Client for Windows; Mac: RDP, View Client for Mac; Linux: RDP, open View Client for Linux</td>
<td>Windows: PCoIP or RDP, View Client for Windows wrapped in ThinApp</td>
</tr>
<tr>
<td>USB Support</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Limitations</td>
<td>N/A</td>
<td>No USB access for smart card readers, biometric devices, or location-based printing</td>
</tr>
</tbody>
</table>

**Table 3: Personal device solutions**
Using a VMware View solution to facilitate teleworkers’ use of their personal devices provides several benefits, including:

- Workers use their personal devices, reducing hardware costs for a telework initiative.
- Workers enjoy increased flexibility, and a better quality of life.
- Secure remote access is easy to set up and use.
- ThinApp minimizes concerns around device management, support, and security.

This type of remote access solution is ideal for a casual teleworker—someone who works away from the office less than 50 percent of the time—because the agency doesn’t have to supply an endpoint device. It is also an inexpensive way to implement a disaster recovery or COOP solution, with workers using personal devices during emergencies.

**Government-Furnished Device: Laptop or Thin/Zero Client**

Using government-furnished devices for federal employees removes the concerns associated with using personal devices for telework. In this scenario, teleworkers generally use VMware View on a laptop or a thin or zero client device to access their virtual desktops.

**Laptop:** A laptop with VMware View is an excellent choice for a highly-mobile worker. Using a government-furnished laptop for telework reduces hardware costs because the worker can use the same device inside or outside of the office. Laptops also allow single sign-on with two-factor authentication using CAC/PIV smart card, RSA SecureID, eToken, and biometric finger print sensors.

As with a desktop, a laptop with the VMware View Client installed can easily connect to a virtual desktop pool and access an authorized virtual desktop. However, laptops can also take advantage of VMware View Local Mode, which lets the worker download (or check out) an image of their virtual desktop, disconnect from the network, and continue using the virtual desktop locally. The first time the worker checks out their desktop, the entire desktop is downloaded to the laptop. For each subsequent time, only block-level changes to the virtual desktop image are synchronized to the data center for faster backup of the virtual desktop. Security policies and authentication are configured on the View Connection Server, and AES 128-bit or 256-bit encryption can be implemented for the copy of the virtual desktop that resides on the user’s local hard disk.

Because the original desktop image is always housed in the data center, workers can always revert to the original copy if the checked-out image is damaged or lost. Local Mode gives workers access to all resources available on the laptop (for example, the video card, CPU, memory, and so on), and the virtual desktop is encrypted for additional security. Workers can also establish a VPN connection to access other network resources as needed.

Most importantly, even while the laptop is in Local Mode, IT staff still maintain full control of backups, access and revocation, maintenance, and network communication.

**Thin or Zero Client:** A VMware View solution running on a thin or zero client offers the ideal in security for devices that sit at the edge of the network. Thin clients have a very small footprint of a base OS, such as Windows XP Embedded or Linux distribution. Zero clients take this one step further, with no embedded OS on the endpoint device, which means there are no local OS patches or updates to maintain. Teleworkers simply access their virtual desktop using the thin or zero client, which also provides support for peripherals like monitors, printers, and smart card readers. This solution supports effective telework without the need for a complex client device and its accompanying OS, specialized drivers, and other potentially disruptive features.

Reducing or completely removing the OS with a thin or zero client offers 80 to 90 percent of the features found in a desktop or laptop, while providing the following benefits:

- Optimal endpoint security: no data storage, small (or no) attack surface for virus or malware attacks, USB redirection and single sign-on two-factor authentication through internal or external smart card readers
- Simplified management, with no patching requirement, and reduced OpEx associated with managing endpoint devices
- Well-performing plug and play devices for non-technical teleworkers
- Lower energy use than desktops or laptops

Several vendors offer a solution to repurpose PCs by removing the OS on the endpoint device and replacing it with a very thin OS purpose-built to only run the View Client. This approach helps reduce OpEx associated with managing the endpoint OS while helping to keep down CapEx by enabling the reuse of existing PCs.

VMware View on a laptop or a thin or zero client device is ideal for a semi-permanent teleworker—someone who works away from the office two to three days a week. This solution provides all the tools the worker expects and needs, including location-based printing and USB access for smart cards and other authentication devices. With a laptop in Local Mode, workers can access their virtual desktop and use local resources wherever they are, regardless of whether they have a network connection.

**Mobile Device: iPad or Tablet**

Mobile devices like the iPad and other tablets are becoming increasingly popular, especially among highly-mobile workers. VMware View fully supports the iPad with the View Client for iPad. If a federal employee does not require CAC/PIV smart card support, and if their agency is willing to include the iPad as a supported telework endpoint, an iPad running VMware View Client for iPad can be configured to access a virtual...
Secure Remote Access for Government Teleworkers

desktop using a direct connection through View Security Server or an existing VPN solution. Such a configuration offers the same connection security as any other endpoint device using the View Client.

The View Client for iPad offers the following features:

• Fully supported over WiFi or 3G connections
• PCoIP protocol for a great user experience
• Tight integration with VMware View 4.6 for easy virtual desktop access and reconnection by selecting from a list of previously connected desktops
• Support for Bluetooth or dock connected keyboards
• Support for the iPad video graphics array (VGA) connector to connect your VMware View desktop to an external monitor or projector

The View Client for the iPad supports a subset of the features available on other VMware View clients. For more information on the View Client for the iPad, visit http://www.vmware.com/ipad.

Offering secure remote access to teleworkers through VMware View on an iPad or other tablet device might not be a short-term goal for federal agencies, but the option exists today for those workers that need to access their Windows desktop for a particular application or data set.

Conclusion

VMware View helps federal IT leaders provide teleworkers with secure remote access to their virtual desktops. A virtual desktop offers several inherent security and manageability benefits because data and applications do not reside on the endpoint device. While each type of endpoint device might require some configuration to obtain optimal security, teleworkers can enjoy a “follow me” desktop experience, with all of the resilience, security, and operational advantages of the robust VMware infrastructure solution.

Additional Resources


• Security Server in View 4.6 Video http://vimeo.com/20365429
• Certificate Revocation Checking Using OCSP and CRL in View 4.5 http://communities.vmware.com/docs/DOC-15291
• For more information about zero clients, see: http://www.clearcube.com/zero-clients.html
• VMware Hardware Compatibility List http://partnerweb.vmware.com/comp_guide2/search.php
• For more information about the VMware View Client for iPad, see http://www.vmware.com/ipad
• Demo of VMware View Client for iPad http://www.youtube.com/watch?v=ldECHtfDyjs

Meet Your Telework Goals with a VMware View Solution

VMware View helps federal agencies achieve telework compliance while reducing time and resource demands on IT administrators. A telework solution built on VMware View:

• Delivers a familiar desktop to personnel at any location, helping keep end-user productivity high
• Provides a flexible and uncompromised user experience, enabling teleworkers to interact seamlessly with their desktops from remote locations
• Supports sustainability programs by reducing commuting
• Simplifies desktop management with quick provisioning, configuration, and automated updates from a central console, reducing complexity and OpEx
• Reduces support calls from remote users, making it easier for a small IT staff to serve many workers
• Accelerates time to deploy applications and new operating systems, further reducing OpEx, while increasing the agility of the IT organization
• Increases security for sensitive information by keeping data in the data center where it is easier to protect
Use Advanced Virtualization Technology to Implement Secure Telework Solutions

A VMware View solution can ease the security and compliance concerns that can accompany telework initiatives. Consider the following concerns and the VMware View features that alleviate them:

Control access to agency information and information systems, including personally identifiable information:

- VMware View Security Server provides simple and secure access
- With built-in SSL encryption, you can also integrate VMware View with your existing VPN solution
- Workers can use smart card (CAC/PIV) or RSA two-factor authentication to securely access their virtual desktops

Limit the introduction of vulnerabilities:

- The client endpoint device is secured from the work environment
- The solution uses limited port openings and simple firewall rules, reducing the number of penetration points
- The client endpoint device is limited to accessing virtual desktop

Protect information systems used for telework that are not under the control of the agency:

- Zero clients have no OS, eliminating the attack surface and the need for patch management
- Client protection tools are kept inside the agency

Safeguard wireless and other telecommunications capabilities used for telework:

- Communication between the endpoint device and the virtual desktop is encrypted

Prevent viewing, downloading, or exchanging inappropriate content:

- Zero clients have no built-in web browser, eliminating access to the web
- The client endpoint device is limited to accessing virtual desktop
- The solution can use existing egress rules
- The solution uses limited port openings and simple firewall rules, reducing the number of penetration points

Provide a consistent high-performance desktop experience across the LAN and WAN:

- VMware View with PCoIP adaptive display protocol ensures a high performance desktop experience over any network connection—even high latency and low bandwidth
- Remote worker data is protected by storing it in the data center rather than on the local device
- SSL encryption secures communication over the network