Foster telework through secure remote access

Federal and state agencies have worked hard to implement telework, and it's paying off. According to official reports at both levels of government, it has resulted in lower costs, higher employee satisfaction, improved productivity and better preparation for continuity of operations plans.

Agencies understand that teleworking conveys many advantages, but also introduces increased security concerns. Remote PCs or mobile devices—whether owned by the agency or the employees themselves—can't be consistently protected.

To mitigate these threats, almost all agencies have implemented secure remote access in the form of a virtual private network (VPN). This includes identification, authentication and authorization at the firewall level, as well as encryption technology. Government agencies have learned the hard way though that not all VPNs are created equally. VPNs don't all provide the same level of security. Some only require a username and password for access, despite the OMB's requirement for two-factor authentication in all cases of remote access. Two-factor authentication requires any two of the following:

- something you know (like a password)
- something you are (biometrics, like a fingerprint)
- something you have (a smartcard or Common Access Card)

Besides ensuring a VPN uses two-factor authentication, agencies can improve their remote access security by implementing network monitoring, Security Information and Event Management (SIEM), network access control, advanced malware protection and data loss prevention (DLP).

Then there's always the human element. All the technology in the world isn't worth much if employees don't know what's acceptable and what's risky. At the very least, any remote access security policy should include:

- List of specific equipment, operating systems and software acceptable for use outside the agency's offices
- Requirements to keep the operating system, anti-virus and anti-malware software up to date by applying patches as soon as they become available
- Rules for how to connect to the VPN
- A "whitelist" of acceptable apps and/or "blacklist" of unacceptable apps
- Teleworkers responsibilities when it comes to protecting the security and integrity of agency data
- Applications and data workers can't access remotely
- Teleworker accountability and responsibility for data integrity and confidentiality
- Specific repercussions if guidelines are not followed

PROTECT THE MOBILE ENDPOINT

PROTECTING mobile endpoints like smartphones and tablets has never been easy. The sheer explosion in the number of mobile devices in use at all levels of government agencies, many of them owned by employees themselves, is part of the issue. The way employees use those devices is another issue.

According to a recent report from the Ponemon Institute, employees who don't comply with security policies are the greatest source of endpoint risk. All this means traditional methods of protecting mobile endpoints—anti-virus software, host-based firewalls and so on—aren't enough anymore. These solutions and strategies can complement and integrate with existing enterprise mobility management solutions:

- Identify the threats your users face today, and rewrite your endpoint security governance and control processes to reflect those realities. Without this, you won't have the right information to choose the right tools.
- Upgrade to more advanced anti-malware detection that can analyze multiple file types, detect different forms of evasions and block bad files.
- Invest in a solution that enforces continuous endpoint monitoring. These solutions offer real-time visibility and monitoring of all endpoints, policy enforcement, threat remediation and other security capabilities.
- Include a threat intelligence component that analyzes real-time user and network data for potential threats.
- Implement a real-time endpoint forensics data capture and analysis tool that can monitor all processes running on endpoints at all times, along with processes that aren't considered normal behavior.

What is Virtual Mobile Infrastructure and why do we need it?

When it comes to protecting mobile data and securely accessing mobile apps, government agencies have increasingly turned to solutions like Mobile Device Management (MDM) and Mobile Application Management (MAM). These solutions are effective to a point, but with the increasing adoption of Bring-Your-Own-Device (BYOD) throughout government, the stakes are higher—and protection more elusive. Enter Virtual Mobile Infrastructure (VMI).

WHAT IS VMI?

Think of this as Virtual Desktop Infrastructure (VDI) for mobile devices. The purpose of VMI is to provide secure access to mobile applications, data and secure networks from mobile devices. Like VDI, users are assigned a profile. This profile is centrally managed and stored on agency servers. Applications and data are delivered to the device via a secure remote protocol. To access applications, users must log in securely on the device. No agency data is stored on the device. Because nothing sensitive is stored on the device, there is no risk of data loss due to device theft. It's more efficient because installation, upgrading and patching are automated.

HOW DOES VMI HELP WITH SECURITY WHEN MANY EMPLOYEES USE THEIR OWN DEVICES?

Agencies can be confident there's no cross-over between agency data and apps, and personal data and apps. This means the chance of confidential data getting into the wrong hands is slim to none.

WHY DO WE NEED VMI IF WE ALREADY USE ENTERPRISE MOBILITY MANAGEMENT SOLUTIONS LIKE MDM AND MAM?

MDM focuses on distributing data, applications and security configuration settings to mobile devices. MAM provides more controls specific to applications and often manages an organization's app store. MAM solutions can also store fully encrypted data without fully encrypting the device and remotely enforce policies. However, both have limitations. MDM doesn't do much to secure applications and isn't ironclad when it comes to protecting against attacks or data leaks. Also, both MDM and MAM solutions require multiple protocols, which means more potentially weak links. And enforcing policies on these solutions is time-consuming.

DOES THIS MEAN OUR INVESTMENT IN MDM AND/OR MAM WAS A WASTE OF TIME AND MONEY?

Not at all—these solutions are an important step in managing mobile devices. Layering a VMI solution over your existing infrastructure will strengthen security. Existing solutions are still useful in securely delivering some mobile apps, while VMI can take care of more sensitive, complex apps and provide access to more sensitive data.

BY THE NUMBERS: THE MOBILE SECURITY THREAT

29%	The percentage of mobile devices connected to the network of a major U.S federal agency that has encountered a mobile threat during the past year.
33%	The percentage of organizations that never test their apps.
40%	The percentage of organizations that aren't scanning the code in their apps for security vulnerabilities.
75%	The percentage mobile malware in the U.S. has grown over past year.
85%	The percentage of commercial mobile apps that track when WiFi and data networks are used, if the device is turned on, or the device's current and last location.
188%	The percentage by which Android vulnerabilities have increased compared to 2011.
262%	The percentage by which iOS vulnerabilities have increased compared to 2011.
More than 20,000	The number of mobile applications that fail to properly validate SSL certificates.
16 million	The number of mobile devices worldwide that have been infected with malware.
1,432,660,467	The number of attacks launched from online resources located throughout the world.

Secure Mobility Across the Board

There's a lot riding on mobility at all levels of government. It can improve productivity, increase employee satisfaction and even play a key role in agencies' disaster recovery plans. Yet despite significant progress in providing at least some degree of mobility to government employees, security concerns have hampered progress.

To manage security concerns, government has largely turned to solutions like Mobile Device Management (MDM) and Mobile Application Management (MAM), which help secure data on devices through encryption and containerization. While these measures are helpful, they're far from foolproof. For example, if a device is lost or stolen, there's a risk of sensitive data falling into the wrong hands.

There's a better way—by not storing data on mobile devices in the first place. That way, first responders, field workers and office workers who need mobile devices can access sensitive or classified data securely without the risk. The data is never stored on the devices. Instead, users see the data redisplayed on their screens.

Government agencies have been using virtual desktop infrastructure (VDI) technology for years on laptops. VDI runs a user's applications and desktop, storing their data on a server and displaying that information on the endpoint. For example, a federal law enforcement agency uses Raytheon|Websense's Trusted Thin Client® solution for employee laptops. That way, agents in the field can access multiple sensitive networks without having to bring multiple laptops and encryption devices. And if they need to leave the unit behind during an unexpected evacuation, there's no risk of data loss.

Today, agencies can use the same type of technology for smartphones and

tablets. "We knew this was something government needed to solve security concerns, especially in the case of sensitive and classified information on mobile devices," says George Kamis, CTO of Raytheon|Websense, Federal Sector. "Trusted Access Mobile uses an encrypted network connection, a secure mobile gateway and virtual mobile infrastructure to ensure that when users need to access sensitive information on mobile devices, what they are really seeing is only a display of the information on a screen."

The Trusted Access Mobile solution runs on both Android and iOS devices. It uses Defense-grade security with Suite B encryption algorithms and nested TLS encrypted tunnels. Its hardened mobile gateway uses an SE Linux® foundation, and the mobile gateway blocks all other traffic between the device and the agency.

With this technology, mobility becomes more secure across the board. Agencies allowing BYOD no longer have to worry about sensitive information falling into the wrong hands. Employees appreciate the flexibility it gives them to use the device for their personal needs as well as work.

There are other benefits as well. In situations when the office is inaccessible, such as a weather or threat event, employees can remain productive. And when traveling abroad, employees can securely access email, calendar and data on mobile devices. The data isn't stored on the device, which greatly reduces data loss or exposure.

At the other end of the spectrum, agencies that require solutions with top-level security can equip their employees with mobile devices for use in the office without raising undue concern if a device mistakenly leaves the building. "For a long time, thin clients have been considered more secure than PCs," says Kamis. "Now mobile devices can be just as secure."

Raytheon | websense

http://www.raytheoncyber.com/capabilities/products/trusted-thinclient/
http://www.raytheoncyber.com/capabilities/products/trusted-mobile/
http://www.raytheoncyber.com/resources/