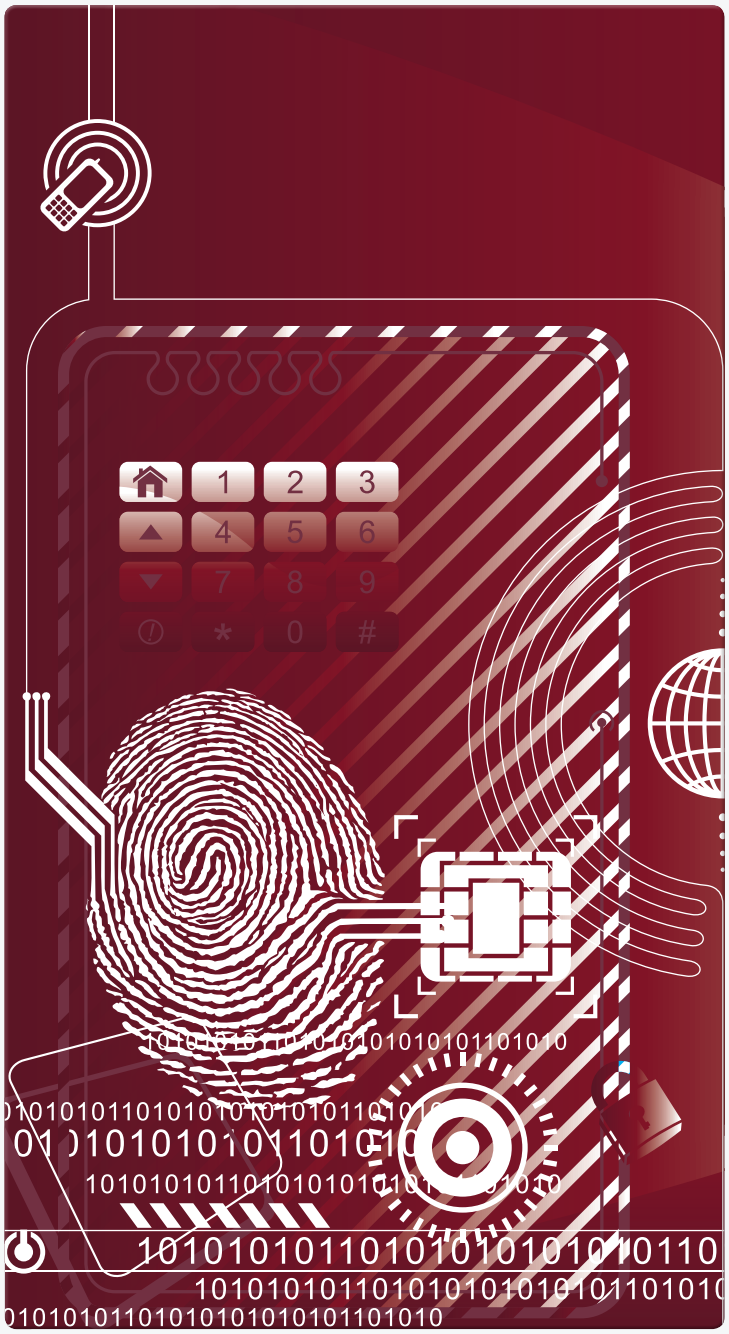
UBM Tech

E-PAPER

DECEMBER 2014

Overcoming Security Woes to Expand Mobile Adoption

By recasting mobile devices as simple points of access to applications and data, agencies can reduce risks and control costs.



vmware®

Federal and defense organizations have made progress toward empowering their personnel with a variety of productivity tools that enable them to complete work when and where they choose. Chief among these tools are mobile devices and applications, which deliver many benefits, including greater productivity, enhanced collaboration, faster service delivery, and stronger employee recruitment and retention.

Mobility has taken off across many sectors of government. According to IDC, smartphone spending accounts for more than 90% of hardware investments in government. Yet that's just part of the equation: The Mobile Work Exchange found that 90% of government employees use at least one mobile device for work purposes.

However, security concerns are still preventing agencies from achieving the benefits that mobility can deliver. But there is a solution. By recasting the device – whether desktop, laptop, tablet, or smartphone – as a simple point of access to applications and data that reside in the datacenter, agencies can reduce risks, manage a dynamic device environment, and control costs.

Challenges of Broader Mobile Adoption

The challenges around mobile data, application, and device security are very real. The study from the Mobile Work Exchange indicates that 41% of government employees are putting themselves and their agencies at risk due to insecure mobile device practices. According to the study, the biggest challenges to broader mobile adoption are:

- Security of sensitive data and applications
- Lack of defined telework policies, training, and governance
- Concern over supporting multiple device platforms

To solve these issues, agencies must find a way to secure and easily manage devices, applications, and data from a central location, while still allowing employees to use the devices of their choice. That means preparing the infrastructure to securely handle properly credentialed devices to access data and other necessary resources.

The optimum solution addresses security head-on, while transforming the way data and applications are managed and delivered to agency personnel. Using zero clients or thin clients, no government applications or data actually reside on the devices themselves; instead, they remain securely behind an appropriate government firewall, hosted in a datacenter along with the desktop operating system. This dramatically reduces the risks associated with having data and applications reside on endpoint devices and also allows agencies to save money by extending the useful life of the devices.

Another option is for agencies to allow specific applications and data to be downloaded to user devices with proper authentication and permission, but only with specific technology applied. This option requires that agency applications and data be kept completely separate from personal device use, generally through isolation capabilities or containerization on the devices.

With both approaches, all components of end-user access – mobile devices, desktops, applications, and connections to applications – are secured across agency infrastructure. At the same time, important features such as automated policy enforcement and configuration management can be leveraged.

This strategy allows federal and defense organizations to enact strong security policies and architectures that seamlessly coexist in a multi-device, multi-platform environment. It also gives personnel the flexibility to be productive anywhere, anytime, from any device.

VMware Mobile Secure Workplace

VMware Horizon is the underlying technology of VMware's Mobile Secure Workplace solution. It addresses the challenges of mobile adoption by government agencies in one comprehensive solution, providing secure, mobile access to applications and data across devices and locations.

VMware Horizon:

- Improves data security and compliance by centralizing all data and applications in the datacenter. It delivers applications as a managed service from the cloud, and allows IT departments to grant or restrict access to data and applications based on endpoint device configuration, network location, and user identity.
- Allows IT managers to centrally manage user images and automate policy enforcement, configuration management, and isolation capabilities on a range of devices. IT staff also can prevent unauthorized users from accessing certain data or applications based on their classification. Mobile devices are synchronized with the datacenter image and automatically receive updates and changes.
- Supports an array of operating systems, allowing users access to their entire desktops or specific applications through an HTML5-compatible browser or by downloading a specific client that works with their mobile operating systems.
- Helps agencies get more out of the devices they already own. Because the hardware itself is just a portal, refresh cycles can be lengthened.
- Reduces operating expenditures by more than half by not only keeping devices longer, but by optimizing labor around hardware, software, and user support, and automating policy and configuration management.

Conclusion

Organizations that embrace mobility have realized significant benefits of stronger IT security, increases in employee productivity, and improved employee recruitment and retention. By transforming devices into secure points of access to applications and data, establishing a formal telework policy, and delivering mandatory training to qualify personnel for telework, government can do much more with less, increase security, and recruit tomorrow's organizational leaders while empowering today's.

VMware is the leader in virtualization and cloud infrastructure solutions that enable businesses to thrive in the cloud era. Customers rely on VMware to help them transform the way they build, deliver, and consume Information technology resources in a manner that is evolutionary and based on their specific needs. With 2013 revenues of $5.21 billion, VMware has more than 500,000 customers and 75,000 partners. The company is headquartered in Silicon Valley with offices throughout the world and can be found online at ***www.vmware.com***.