Secure mobile workspaces for government enterprises

Empowering new levels of mobility and productivity for federal, state and local agencies

CITRIX®

citrix.com/USgovernment

"We must enable citizens and an increasingly mobile federal workforce to securely access high-quality digital government information, data and services – 'anywhere, anytime, on any device'."

-Digital Government Strategy

Introduction

Increasingly, federal, state, and local government workers are moving out from behind the desk—whether it be to go across the street or across the country—making mobile workstyles a necessity instead of a luxury. Agencies that act to meet the growing demand for mobile workspaces and architect around services-based computing best position their workforce for the future. For an optimal computing experience, a mobile and services-based design philosophy must balance user experience, total value of ownership (TVO) and governance for protection of valuable information assets.

"Mobile workspace" solutions is an emerging category of technologies predicated on the Gartner definition, "A set of virtual and cloud solutions that present a user's applications, data and services to any device over different types of networks to provide work-style flexibility and improved employee engagement."

This white paper from Citrix Public Sector describes options for a mobile workspace-focused computing architecture that empowers government productivity through mobility, telework, consumerization and collaboration.

Mobile workspaces for government telework and BYOD

Mobility plays an increasingly important role in today's government agency. For many types of workers, "always-on and connected" is now a core requirement. E-mail is no longer enough; full productivity depends upon real-time access to applications and files and the ability to share resources, collaborate or meet from anywhere at any time. Wherever and however they work—in the office, at home or on the road—agency workers depend upon reliable access to a consistent,

high-performance computing experience. At the enterprise level, agencies and processes are being transformed by a move toward mobile workspaces and telework that shifts work to the optimal location, time and resource.

"Bring your own device" (BYOD) computing adds another nuance to this changing landscape. As the push toward mobile workspaces gains steam, many government employees and contractors are now using consumer devices such as smartphones, tablets and laptops to support business productivity—a trend called consumerization. Consumerization often involves the use of the same mobile device for personal and business purposes.

Increasing use of mobile workspaces has presented its challenges to IT departments, forcing them to rethink traditional methods of providing computing services, ensuring information security and controlling the use of enterprise technologies. The need to manage risk must be balanced with the demand by highly mobile workers for freedom of choice and personal control over their computing experience. An optimized mobile computing experience, defined through an innovative and evolutionary approach to mobility, can enable IT to meet the requirements of both telework and BYOD.

Citrix mobile workspace technology securely delivers apps, desktops, files and services seamlessly to any user, on any device, over any network. Citrix mobile workspace solutions are:

- Common Criteria / NIAP Certified
- FIPS 140-2 Compliant for Encryption
- FIPS 201 Compliant for Authentication
- Section 508 Compliant for Accessibility

Challenges and opportunity of mobility

The need for mobile workspaces challenges enterprise architectures

Is the iPad® tablet the enemy? To many IT departments, iPad tablets and other consumer-grade mobile devices present an untenable threat to network security and control, one that unfortunately exists by design. Traditional enterprise networks and security measures were designed around a core assumption: IT maintains full, end-to-end ownership.

These traditional architectures required IT to know and approve every device, network, application and usage of computing. In the face of these constraints, though, many workers responded by acquiring their own alternative computing resources, such as personally owned devices, mobile networks and rich SaaS applications, all of which bypass IT inflexibility.

Recipe for a failed mobility workspaces initiative

- Using the same stale practices and tools from the past
- Treating all apps and data equally
- Relying on users to accept risks and create policies
- Attempting to manage what you don't own
- Ignoring user experience—especially for security

Agency IT departments that see iOS or Android tablets as the enemy need to realize that the problem isn't the device itself; it's the outdated enterprise computing architecture that fails to support these devices effectively. The forces of

consumerization, mobility and telework need to be seen as core design tenets to enable the next era of computing in government.

Mobile workspaces bring freedom

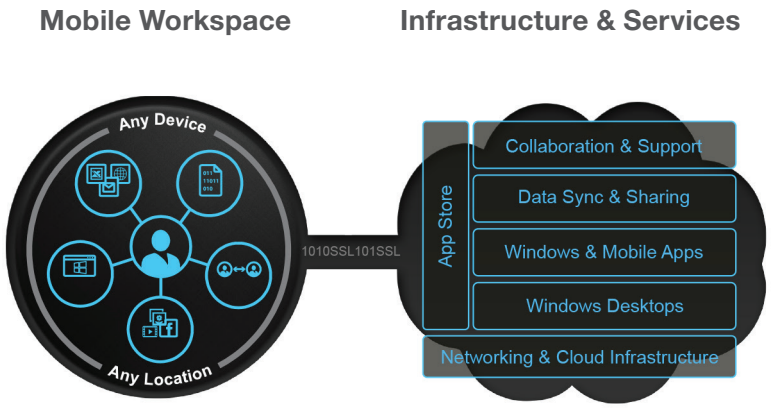
Mobility frees government staff to work from anywhere, frees their agencies to leverage the full value of telework and frees the enterprise from the constraints of inflexible computing. Through consumerization, mobility brings freedom to personalize the computing experience, while empowering agency agility, productivity, innovation and work satisfaction. However, some still see the freedoms of mobility as a potential threat opportunity to be exploited by outside parties.

Optimizing for mobile workspaces: recommendations for federal, state, and local government IT

1. Enable mobility for workers, apps and data
2. Keep highly sensitive data in the datacenter whenever possible
3. Protect distributed mobile data in an encrypted secure container
4. Enforce policies specifying what should happen under specific contextual circumstances – not just at logon
5. Control data distribution and usage through policy
6. Personalize the worker experience for optimal productivity
7. Automate both the desired worker experience and data protection needs
8. Enhance ease of use by unifying the management of accounts, passwords and access for all apps, both internal and external

According to federal IT workers, a mobile workforce is more productive, helps to form successful telework programs and enhances staff satisfaction and retention.

Citrix: Mobile workspaces for government agencies



Using Enterprise Mobility Management (EMM) to secure mobile workspaces

Enterprise Mobility Management (EMM) is comprised of technology solutions that manage the increasing array of mobile devices, applications, data, secure access to enterprise infrastructure, and related services to enable use of mobile computing in a business context. EMM goes beyond traditional Mobile Device Management (MDM) solutions and expands to all mobile use cases including BYOD, government-furnished equipment (GFE) and government-owned, personal-enabled (GOPE).

As Microsoft Windows still provides the majority of all agency line of business (LOB) applications, enabling mobile access to these Windows apps will help enable the transition from a legacy PC workspace to a mobile workspace. EMM is an evolving trend within the federal enterprise that will only increase in importance as more agency workers adopt smartphone, tablet and laptop devices, and seek IT support for them while in the office and working remotely.

	GFE	BYOD / GOPE
Laptop / MacBooks	Encrypted local VM deployment and device management	Windows desktop/apps with no data at rest
Tablets	• Mobile Device Management • Container-based productivity apps	• FIPS encrypted container-based productivity apps • Windows desktop/app with no data at rest
Smartphones	• Mobile Device Management • Container-based productivity apps	• FIPS encrypted container-based productivity apps • Windows apps with no data at rest

EMM addresses key government initiatives including enterprise mobility, telework and BYOD by empowering agency employees to work from anywhere, at any time using the device of their choice. Further, as the emergence of consumerization has outpaced the ability of agency enterprise systems to deliver IT services to mobile devices, EMM solutions offer secure access to enterprise resources from any device, while ensuring security, compliance and governance.

Making IT mobile: EMM benefits security

Successful agencies can achieve greater flexibility and agility by taking advantage of the security benefits of EMM to optimize mobility, embrace consumerization and broaden teleworking programs. While key security concerns for federal, state, and local agencies regarding enterprise-wide mobility adoption are many, although EMM can help in each case:

Protecting sensitive data at rest. Agencies can keep extremely sensitive data in the datacenter, while users can leverage a thin-client approach to access applications and data on their mobile devices. This averts all data-at-rest concerns as only the presentation layer user interface is displayed on the mobile device.

The federal government recently announced a game-changing shift in IT operations, mandating a concerted effort to better mesh agency systems with mobile workspaces.

For disconnected use, local mobile apps can be deployed and isolated into an encrypted container to ensure separation from personal apps and data. Agencies will require a solution that enables FIPS 140-2 encryption for any data at rest on the mobile device. Remote wiping for all government data at rest is also a key benefit to ensure that data can be remotely managed if the device is lost or stolen.

Protect sensitive data in transit. Agencies should enforce FIPS 140-2 encryption for all data in transit as the majority of mobile data will be transmitted over unsecured mobile and Wi-Fi networks.

Protect sensitive data in use. Sensitive applications and data should be isolated into a secure encrypted container, thereby keeping government and personal apps separate on the device. The ability to "sandbox" applications that would otherwise present greater risk and/or security vulnerabilities, such as being able to open in/send to any native app on the device is also critical.

Local security policies. Every mobile device has a set of local security policies that agencies are seeking to enforce. Ensuring a complex passcode and denying access due to jailbroken or rooted devices is top of mind.

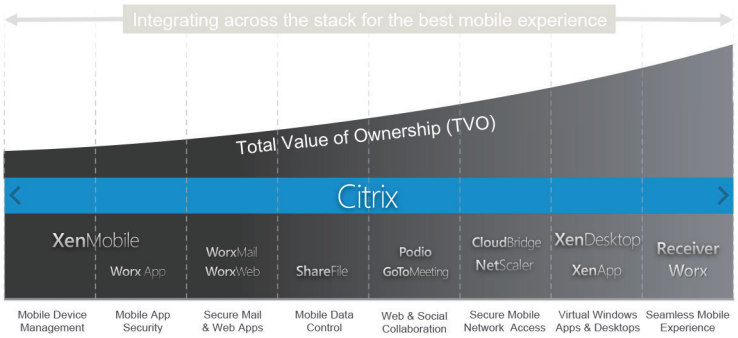
Authentication and access. Agencies are evaluating options for authenticating mobile devices into secure networks using FIPS-201-compliant methods. Several solutions are emerging including sled-based smartcard readers along with NFC, SD-card and derived credentials. As new federal requirements emerge for mobile-based strong authentication, ensuring mobile devices can be deployed enterprise-wide with a cost-effective strong authentication method will be key.

Granular access should be enabled based on multiple access factors, including user credentials, role, device characteristics, location, thresholds, approvals and workflow. Eliminate the risk of a single actor exceeding his access or authority, thereby protecting sensitive transactions and administrative actions.

The Citrix Secure Mobile Workspace

Citrix is focused on delivering mobile workspace solutions through a comprehensive set of EMM capabilities. As more and more of these mobile capabilities are adopted, there is an increasing Employee Productivity "ROI" that is generated from the mobile infrastructure. This leads to increased IT agility, flexibility and employee satisfaction.

Citrix Secure Mobile Workspaces



Citrix provides a multi-tiered, secure-by-design approach for Enterprise Mobility Management products spanning the cloud-based SaaS, network and datacenter.

This solutions suite enables agencies to adopt mobility along a whole spectrum of products focused on delivering a true mobile workspace solution. Each of the following components of EMM can be deployed together as a comprehensive solution or piecemeal based on agency requirements.

The individual components of the Citrix secure mobile workspace solution are detailed below:

Capability	Benefit to government agencies	Citrix solution
Mobile Device Management (MDM)	MDM can be the basis of an Enterprise Mobility Management solution as it is a way to enforce device-based policies and provide tracking as required by contracts, regulations and governance. Agencies are generally drawn to MDM as a first step toward managing mobile GFE devices. This includes iOS, Android, Blackberry and Win 8.1 platforms.	XenMobile
Sandboxed e-mail and browser	Native applications for iOS and Android devices are seen as inherently insecure due to their open interactions with other applications on the device. Additionally, for mobile enterprise e-mail, agencies may choose not to expose OWA servers publicly for security reasons. Agencies will require a secure mobile e-mail client that encrypts all messages and attachments locally, while ensuring that all network access is secured. Agencies that also wish to grant mobile access to intranet portals or websites are shying away from using standard OS browsers since they do not encrypt cookie, history or cache information. A secure encrypted browser that can be controlled only for enterprise browsing is an alternative to using built-in mobile browsers.	Worx Apps for XenMobile: WorxMail and WorxWeb
Secure mobile network access	Several agencies leverage their existing network infrastructure to provide device level VPNs enabling enterprise access for mobile devices. This presents a security risk, as all applications on the device would potentially have access to the agency intranet using this solution. Agencies have also leveraged third-party NOC architectures to prevent direct access to their secure network. Ensuring all data in transit is encrypted using FIPS-validated modules is also vital, as mobile devices will often be accessing services over unsecure Wi-Fi or wireless carrier networks.	NetScaler Gateway
Laptop/MacBook management	Client virtualization simplifies management and security for laptops and MacBooks. It extends the benefits of desktop virtualization to agency laptops so that staff can work from anywhere, at any time—whether they have slow, intermittent or no network access—for exceptional flexibility and productivity. Government IT gains new levels of security, reliability and control as well as simplified desktop management.	Desktop Player
Mobile virtual desktop	Federal, state and local agencies with highly sensitive data are looking to mobilize their enterprise. Windows desktop and app virtualization will allow these agencies to mobilize Windows resources in a thin-client type model with mobile devices ensuring no data at rest. As desktop virtualization can be used for thin clients, thick clients and laptops as well, having mobile-specific technologies which help "mobilize" existing UIs can help further drive adoption of existing virtualization infrastructures for mobile.	XenDesktop

Through the power of EMM, Citrix provides a multi-faceted, secure-by-design approach to optimizing mobile workspaces.

Mobile data control	Just as applications are important to mobile, controlling mobile document access is another imperative for enabling staff. Several agencies are grappling with what they call the "dropbox problem" where sensitive agency data is being placed into cloud storage environments without any IT control. Additionally, several initiatives are investigating how to deploy "home-drive as service" within federal service provider organizations. This can open the door to several compliance and regulatory issues if not controlled. By enabling these workers with a controlled capability, this can prevent the circumvention of enterprise compliance when using cloud-hosted storage offerings.	ShareFile
Mobile virtual apps	Virtual application delivery provides Windows apps as secure mobile services. IT can thus mobilize an agency while reducing costs by centralizing control and security. With HDX technologies, XenApp gives users a native touch-enabled look-and-feel that is optimized for the type of device, as well as the network.	XenApp
Mobile collaboration	Web conferencing software makes it simple and cost-effective to meet online with agency colleagues and contractors. Participants can also share their webcams in high definition for more personal interactions without needing a complicated setup. Workers can attend an online meeting from anywhere, using their Mac, PC, iPad, iPhone or Android tablet.	GoToMeeting

Citrix's Enterprise Mobility Management platform is focused on delivering applications and data to mobile devices using several different methods. All of these components work in concert to deliver a holistic, enterprise-scale solution to ensure both administrators and users get a seamless simplified experience.

Citrix EMM solutions support mobile workspace initiatives for government agencies

Government agencies have been challenged to make enterprise mobility, telework and BYOD a priority to better serve taxpayers and improve department agility and productivity. The key in this effort is to securely provide mobile government workers with apps and resources that are available anywhere, anytime and on any device—an on-the-go workstyle that Citrix can help agencies deliver today.

When federal, state and local agencies embrace mobile workspaces, BYOD and telework programs are made easier and they unlock new forms of business value. IT gains assurance that traditional obstacles and risk factors posed by mobility can be addressed, and develops new mobile strategies and best practices for supporting agency goals. Far more than an incremental change in enterprise computing, mobile workspaces have the potential to transform the way government business is done and open the door to all-new opportunities for productivity, staff retention and cost savings. Helping government realize this potential is central to IT's mission—and a core focus for Citrix Public Sector.

For more information on mobile workspace solutions for federal, state and local government, visit **www.citrix.com/USgovernment.**

Citrix Public Sector
Bethesda, MD, USA

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

About Citrix
Citrix (NASDAQ:CTXS) is the cloud company that enables mobile workstyles—empowering people to work and collaborate from anywhere, easily and securely. With market-leading solutions for mobility, desktop virtualization, cloud networking, cloud platforms, collaboration and data sharing, Citrix helps organizations achieve the speed and agility necessary to succeed in a mobile and dynamic world. Citrix products are in use at more than 260,000 organizations and by over 100 million users globally. Annual revenue in 2012 was $2.59 billion. Learn more at www.citrix.com.

Copyright © 2014 Citrix Systems, Inc. All rights reserved. Citrix, XenApp, XenMobile and XenDesktop are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.

0314