The Secure Digital Workspace for Government

Securely Mobilizing and Modernizing Government IT to Advance Missions

vmware®

Secure Digital Workspace for Government

The consumerization of mobile devices continues to transform the government IT landscape, bringing with it a host of opportunities to radically improve mission effectiveness, service delivery and agency productivity. Both citizens and employees expect a more responsive, flexible and innovative government, yet agencies grasp with balancing the benefits of a mobile workforce with the risk of compromising intelligence.

Key Information Technology Drivers in Federal Government

Employee Mobility

Agencies are challenged with enabling secure mobile workflows to improve service delivery.

Data Protection and Security

Sensitive information must be protected across users, devices, applications, and locations.

Continuity of Operations

It is critical that agencies maintain operations through inclement weather, cyber attacks or any event that would cause a shutdown.

Modernizing IT Infrastructure

Agencies are seeking ways to augment legacy IT infrastructure to enable mobility and increase efficiencies.

Hiring and Retaining IT Professionals

Lack of widespread mobile workflow adoption and competition from private sector affect the government talent pool.

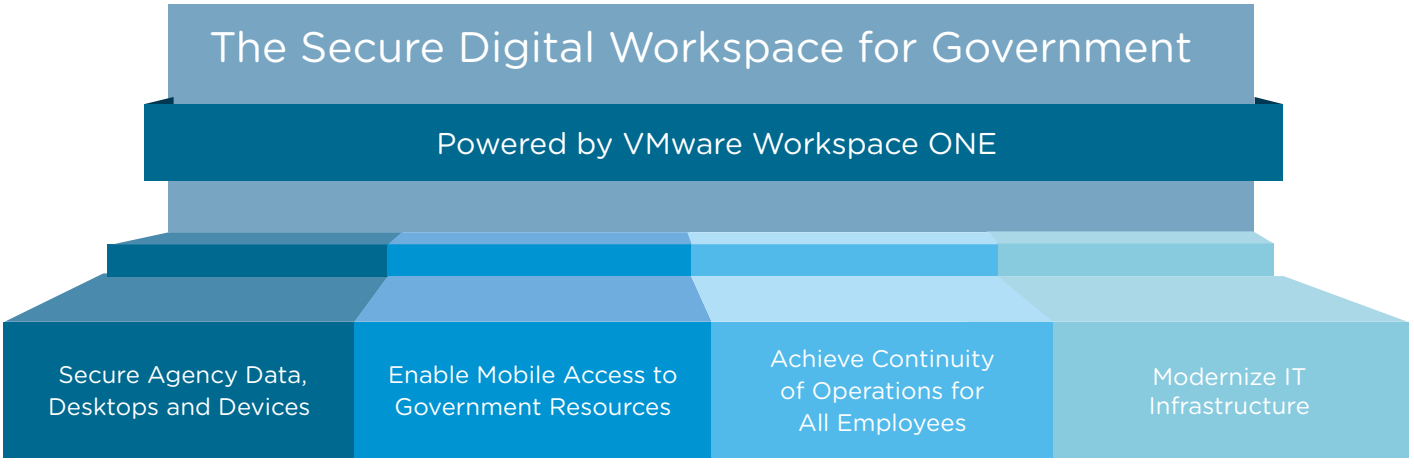
Securely Mobilizing and Modernizing Government

VMware addresses the speed at which government employees are adopting mobility and revolutionizes service delivery by integrating identity, application and enterprise mobility management to deliver a consistent, unified workspace available across any computing environment.

The Secure Digital Workspace for Government, powered by VMware® Workspace™ ONE™, enables federal employees to securely access government resources, data and applications anytime, anywhere, and on any device—transforming workflows and advancing missions.

Enabling Federal Government to:

- Increase cyber security posture
- Reduce the risk of a data breach across any device or platform
- Enable secure remote access to desktops and applications from any mobile device
- Maintain an agile, highly available infrastructure
- Bridge legacy systems with cloud-based technologies



Secure Agency Data, Desktops and Devices

Secure Desktops, Applications and Mobile Devices across the Software-Defined Data Center

- Policy-driven access to data and apps on any device
- Support for Federal CAC/PIV cards, derived credentials and biometric authentication
- Automated OS security patches and updates
- Advanced data loss prevention tools including file editing and sharing restrictions and remote device wipe
- Store data in the data center—not on endpoint devices—and protect data at rest and in transit
- Segregate desktop and application traffic to specific workloads in the data center

Enable Mobile Access to Government Resources

Transform Service Delivery and Missions through Secure Field Mobility

- Access full desktops and apps across any mobile environment or device
- Support for Windows 10 with streamlined deployment
- Secure access to file sharing, collaboration tools and email on any mobile device
- Managed access to Windows, web and mobile apps within unified app store
- Same-day support for OS updates

Achieve Continuity of Operations for All Employees

Support COOP, Teleworking and Disaster Response Goals

- Remove dependency on physical systems and enable on-demand remote access to resources, even in the case of a disaster
- Access information across any device type or operating system
- Support teleworking and increase employee morale

Modernize IT Infrastructure

Bridge Legacy Investments with Mobile Cloud Technology

- Deliver virtual or published desktops and applications through a single platform
- Transform app delivery and lifecycle management
- Save on IT support, hardware, capital and data center storage
- Deliver immersive 3D graphics from the cloud
- Deliver a consistent user experience across device types

How Mobility is Transforming Federal and National Government

CENTCOM: Centralized Desktop Management and Improved Data Security

Through VMware® Horizon, CENTCOM was able to replace a cumbersome legacy environment with a centralized and standardized virtual desktop infrastructure.

- Avoided $160M in storage costs
- Enabled superior application compatibility of 3D graphics
- Reduced user login times from 3-5 minutes to 30-45 seconds
- Cut provisioning times for new images from one week to eight hours
- Achieved 100% uptime

"Our desktop systems are as critical to CENTCOM's mission as our F-18 fighters. We have to have 100 percent uptime, and with our VMware Horizon environment, we do."

Tony Emery
Senior Systems Engineer, Contract Lead, CCJ6-EL,
CENTCOM Integration Lab (CIL)

U.S. Department of Defense: High Availability For Mission-Critical User Community

Agency within U.S. Department of Defense replaced unmanaged legacy desktops and apps with Horizon VDI.

- Enabled high availability, load balancing and disaster recovery of entire service stack
- Centralized desktop and application configuration and authentication
- Met rigorous U.S. Federal security compliances, including CAC-enabled Active Directory

"Cost containment, agile service delivery and high availability are now a reality for this mission critical organization."

Don Wiggins
President, DHDW Consulting, LLC

US Army Corps of Engineers.

U.S. Army Corps of Engineers: Improved Service Delivery Through Mobility

With VMware AirWatch®, the U.S. Army Corps of Engineers drastically improved service delivery to victims of natural disasters.

- Replaced inefficient, paper-based emergency response process with centrally managed smartphone and tablet-based reporting application
- Reduced claim processing time
- Enabled mission leaders to remotely locate and communicate with deployed response personnel

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Item No: VMAW_5468_FED_NAT_BRO