SOLUTION OVERVIEW

OVERVIEW
Government agencies are leveraging VMware end-user computing solutions to securely manage their Windows 10 deployment across any application or device.

SIMPLIFY YOUR MIGRATION TO WINDOWS 10 FOR GOVERNMENT WITH VMWARE

Derive Additional User Benefits Beyond a New Operating System
Initiatives that modernize the U.S. Department of Defense (DoD) IT infrastructure can help Combatant Commands, Services, Agencies, and Field Activities achieve the missions of today and support the strategic requirements of tomorrow. A rapid transition to Microsoft Windows 10®, according to the DoD CIO, will improve the DoD’s cybersecurity posture, lower the cost of IT, and streamline the operating environment.

The DoD’s objective is to complete the Windows 10 migration by January 2017 for IT systems currently running Microsoft operating systems (OS). It’s a tall order to quickly upgrade millions of laptops, desktops, and mobile devices; yet closer to achievable when complemented by VMware solutions that streamline and simplify application delivery, enhance compatibility, and ease desktop and device management. VMware Workspace™ ONE™—featuring desktop and application virtualization powered by VMware Horizon®, advanced identity management, data, device, and threat protection; and enterprise mobility management (EMM) solutions powered by VMware AirWatch®—includes benefits ranging from cost savings to security enhancements to increases in productivity and efficiency. With Workspace ONE, the DoD can improve the way user services are securely provisioned, delivered, and managed across the enterprise.
SIMPLIFY YOUR MIGRATION TO WINDOWS 10

REDUCE COST AND COMPLEXITY OF MANAGEMENT:
• Streamline deployment
• Simplify onboarding
• Manage devices and applications from a central console
• Simplify product provisioning and remotely deliver apps, files and commands
• Deploy a unified app catalog that supports universal, web, and desktop applications
• Manage Office 365
• Automate tasks for complex workflows

ENSURE SECURITY AND CONTROL OF DATA AND DEVICES AT ALL TIMES
• Enable device and app-level restrictions, including per-app VPN
• Enforce conditional access based on user identity
• Apply granular data loss prevention capabilities
• Monitor compliance against policies in real time
• Support multi-factor authentication, including smart cards, Windows Hello, and Passport for Work
• Manage and build policies for the native Windows Defender antivirus

Speed Deployment with Out-of-the-Box Windows 10 Features

With Windows 10, Microsoft embraces the mobile-cloud era and promises the best Windows experience ever. Consumers are adopting the new release at record rates, and large enterprises taking a considered approach are discovering a Windows 10 migration is the ideal opportunity to not only deploy a new OS, but to significantly improve end-user computing services.

PCs containing individual OSs, applications, data, and user information are costly to deploy, challenging to maintain, and operationally exposed. This has made traditional PC upgrade processes (for example, from Windows XP to Windows 7) painful. Moreover, IT teams have had to manage mobile devices and desktops separately using on-premises management tools. Windows 10 is a catalyst for DoD change because of its significant impact on end users and IT management. The transition to Windows 10 is reported to be enterprise friendlier, and VMware solutions and services can do more to help reduce costs, drive operational excellence, and improve security.

New Windows 10 capabilities are designed to speed and ease enterprise deployment. For agencies already running Windows 7, Windows 8, or Windows 8.1, Microsoft enables IT to build Windows 10 upgrades into deployment task sequences and avoid the traditional, lengthy, and time-consuming rip and replace imaging process. A new dynamic configurable option in Windows 10 also streamlines Windows image customizations, eliminating the need for IT to rip and replace PC images (even new PCs) for configuration changes. IT teams can instead execute a runtime provisioning package on images to make devices comply with enterprise standards. Although Windows 10 will still support rip and replace imaging, runtime provisioning can ensure the process is faster and less dependent on existing (PXE/Boot CD) methods. Windows 10, which includes more lightweight EMM-managed policies and support for new methods of device enrollment, finally enables enterprises to embrace EMM management for Windows 10 devices rather than relying on traditional tools.
Further Reduce Time, Costs, and Risks with Advanced VMware Solutions

VMware end-user computing solutions enable the DoD and other government entities to securely deploy and manage Windows 10 across endpoints while simultaneously embracing new mobile cloud workflows and enterprise mobility management functionality.

Desktop Transformation in the Federal Government

DoD staff still rely more on physical desktops than smartphones and tablets to work remotely, making VDI a modernization opportunity to improve the manageability and security of the entire desktop environment while extending the lifecycle of existing desktops and laptops that would otherwise need upgrades to support Windows 10. While shifting to a more agile, mobile-ready infrastructure built on virtualization, IT can now treat physical desktops as agnostic endpoint devices that are capable of delivering secure access to information across OSs and locations.

Virtual Desktop Infrastructure (VDI)—along with complementary delivery technologies like application publishing—offers a proven means by which a complete Windows 10 desktop image can be delivered to any device. Although many applications are increasingly offered as native to mobile OSs, such as Android and iOS, VDI fulfills the need to deliver an intact Windows OS workspace, complete with a predefined suite of applications and a customizable environment that closely replicates the physical desktop experience so many workers are accustomed to using. For use cases that require the delivery of Windows applications to non-Windows devices, application virtualization techniques such as Remote Desktop Session Host (RDSH), support Windows 10 environments across the device landscape.

Built on the software-defined data center (SDDC) that integrates compute, networking, and storage into a centrally deployed and managed virtual platform, VDI is unlike the traditional desktop management model that groups the physical device, OS, and applications into a bundled architecture requiring considerable IT involvement. VDI replicates the physical desktop environment by running applications in the data center, and enables multiple user desktops to run as separate virtual machines (VMs) that are then remotely presented to end-user devices. In contrast to traditional desktop architecture, the DoD can quickly begin to realize lower TCO through decreased operational expenses, which will continue to pay annual dividends.

During an upgrade to Windows 10, VDI helps to improve agency operations and efficiency:

• **Centrally deploy standardized desktops** – VMware Horizon supports Windows 10 as a guest OS running on a virtualized server. Virtual desktops and applications can be instantly published to any desktop or device—anytime, from anywhere. While users enjoy a consistent, high-performance, highly available, and highly reliable computing environment on thin clients and desktop PCs, IT maintains centralized control over access to data and applications. Centralized management increases data security and IT efficiency by improving consistency of operations. VDI also inherently strengthens data loss prevention and security because information—regardless of sensitivity and classification—resides in the data center rather than on the endpoint device.
• **Enhance security and control** – While desktop and application virtualization centralizes mission-critical information, protects “data-at-rest,” and prevents scenarios where information is lost on local devices and storage, VDI cannot be the sum total of a security architecture. With VDI, IT has to consider hundreds or thousands of virtual users now residing on the trusted side of the data center firewall. These users have continuous access to email and Web, and are susceptible to traditional browser/email-borne threats including ransomware and other malware. These users are also now in much closer proximity to other mission-critical assets, such as databases, file-servers, and backend storage.

With a centralized VDI deployment running Windows 10, combined with the VMware network virtualization platform, VMware NSX®, IT can restrict the unmitigated lateral movement a threat might have behind the firewall, and dramatically reduce or contain the attack surface of such exposures. Agencies can bring security inside the data center with automated, fine-grained policies tied to the VMs by enabling micro-segmentation—a technique that involves placing a distributed virtual firewall around every desktop VM. This significantly reduces the lateral spread of threats inside the data center, inherently improving the data center security model. This technology is unavailable in traditional physical networking environments or hardware-defined data center architectures.

• **Reduce hardware refresh costs** – Organizations have experienced longer refresh cycles of 5-7 years with VDI versus 3-5 years with traditional PCs. VDI can be deployed on thick, thin, and zero clients, reducing hardware costs during the upgrade to Windows 10. Moreover, hardware refreshes are simpler with virtualization.

• **Unify the application experience** – Using identity management, VMware enables IT to deliver a consumer-like application experience that dynamically adjusts to end-user roles, locations, devices, and privileges through a contextual, risk-based security model.

• **Transform application delivery and management for any user and device** – Windows 10 migration has all IT teams fundamentally rethinking how they deliver applications. With a just-in-time application delivery and lifecycle management model that disaggregates IT-managed applications and user-installed applications from the OS, VMware Horizon with VMware App Volumes™ enables IT to dynamically deliver managed application containers in seconds. IT can cost-effectively and efficiently manage, deliver, upgrade, and maintain applications throughout their lifecycles—from inception, to testing, to delivery, and finally to retirement. The solution’s capabilities are especially beneficial to budget-conscious organizations.

• **Easily manage remote features and application compatibility issues** – VMware Horizon offers a wide array of remote experience features, including location-based printing, optimized performance for scanning and imaging devices, smart card authentication for faster access, and user access to local files on USB storage devices. With VMware ThinApp®, enterprises can better manage Windows 10 application compatibility issues. Although Windows 10 will present fewer application compatibility issues compared to past Windows releases, some applications will be incompatible on Windows 10. By placing incompatible applications onto ThinApp packages that isolate applications from the underlying OS, enterprises can move problematic applications to the data center and simultaneously support multiple versions of applications that would otherwise compromise performance.
To learn more about how VMware supports and complements Windows 10 management, download “A Definitive Guide to Windows 10 Management.”

- **Successfully support disconnected users** – Enterprises can more successfully support disconnected Windows 10 users with VMware’s policy-based, containerized desktop solution, VMware Horizon® FLEX™. The solution enables IT administrators to create, secure, and manage local desktops to meet the needs of warfighters, field-based employees, and Mac users in the enterprise. End users work within a restricted VM on their endpoints and can be either connected or disconnected from the enterprise network. To better address application compatibility challenges, IT can use the solution to deliver a fully managed Windows 7 instance onto an upgraded Windows 10 host machine. This will enable the migration of applications to a Windows 10 environment over time while still maintaining the ability to run applications under Windows 7 until IT can complete the migration.

- **Support next-generation guest OSs** – Agencies running Windows 10 across physical domain-joined devices must support a hardware-based Trusted Platform Module (TPM) cryptography chip to take advantage of specific security features, such as Credential Guard. Agencies managing Windows 10 on virtual domain-joined machines, however, are exempt from the hard TPM requirement as long as the virtual machines are non-persistent. Non-persistent virtual desktops are built from a master image that is centrally managed, patched, and deployed across all end users. When users log off, the machine reverts to its original state devoid of any end-user settings and data. VMware vSphere® will fully support virtual TPM 2.0 requirements and will be able to run Windows 10 in a virtual environment securely. With VDI, agencies can avoid additional capital expenses to support hard TPM requirements while taking advantage of advanced Windows 10 security features.

Enterprise Mobility Management in the Federal Government

Windows 10 provides a promising opportunity for the DoD to manage devices, applications, and OS environments using an EMM solution. As a mobile-first, cloud-first platform, Windows 10 is redefining how organizations treat desktop and device management by allowing IT to take full advantage of EMM capabilities. VMware AirWatch meets government deployment complexities, security requirements, and work styles, providing the most comprehensive EMM solution to get commands Windows 10 ready.
During an upgrade to Windows 10, EMM enables enterprises to standardize processes and reduce risk:

- **Streamline deployment to get users up and running quickly** – Devices can be joined to the domain, configured over-the-air, and set up for management with AirWatch in one streamlined workflow. IT administrators can enroll devices on any public or private network thanks to native single sign-on (SSO) and integration to cloud-based identity management solutions. They can also bulk enroll devices via policy and deliver a complete provisioning package that can be installed by the end user with just one click.

- **Create a more unified application experience** – VMware solutions enable enterprises to provide the same user experience to all application types and distribute applications through online or offline channels and with or without a Microsoft or directory services account. Enterprises can also provision classic Win32/Win64 desktop applications with AirWatch, without relying on traditional systems management or PCLM tools. IT administrators can establish automated workflows for product installation and remote distribution of applications, drivers, firmware updates, and other complex scripts, as well as create compliance policies with custom allowlist and denylist inventories that allow only applications from trusted sources.

- **Take endpoint and data protection to a new level** – IT staff can monitor device health and detect compromised devices through the AirWatch compliance engine and the health attestation capabilities in Windows 10. IT can define automated escalation policies in the AirWatch management console to notify users and/or perform actions on compromised devices. IT can prevent sensitive data leakage by defining granular controls such as conditional access rules, per-application VPN, and encryption policies. IT can also test advanced data loss prevention (DLP) capabilities with early access to Enterprise Data Protection (EDP) features for Windows Insiders customers, as well as set policies for user verification, including biometric gesture, by leveraging AirWatch integration with Windows Hello and Passport for Work.

- **Streamline update management and delivery** – With AirWatch, IT teams can choose whether users can control OS updates on their own or enforce OS updates via subscription to Windows update sources; decide to integrate with an existing Windows Server Update Services (WSUS) solution or the new Windows Update for Business service; control the deployment schedule based on the organization’s preferred approach or sensitivity to feature and security updates; and define maintenance windows, such as the preferred day and time for installation, so updates don’t interfere with user productivity. IT can also support the new Windows Update Delivery Optimization feature for peer-to-peer delivery, so users receive updates and applications more quickly.

**Deploy the Digital Workspace Purpose-Built for Government**

Because the DoD must adhere to specific security standards and mandates, the VMware digital workspace aligns with the following federal requirements:

- 256-bit, FIPS 140-2 encryption
- Smart card support
- Common Criteria/NIAP framework
- Criminal Justice Information Services (CJIS) compliance
- IPv6
- National Institute of Standards and Technology (NIST) 800-53, Security and Privacy Controls for Federal Information Systems and Organization
To learn how to leverage EMM to manage a Windows 10 environment, download "Redefine Windows 10 Management: Embrace True Business Mobility" by VMware AirWatch.

- Public Key Infrastructure (PKI)
- Third-party antimalware software
- Federal Risk and Authorization Management Program (FedRAMP) Authority to Operate

Confidently Move to Windows 10 and Enhance User Experiences

By embracing mobile and cloud, the Windows 10 platform offers new opportunities as a stand-alone OS. However, when deployed together with VMware end-user computing solutions, agencies can optimize desktop and device management within a heterogeneous environment and transform application delivery. Agencies can also better protect data while delivering a unified application experience that dynamically adjusts to user locations, devices, and privileges—all of which positively impact Windows 10 adoption in the enterprise.

By managing data, applications and devices from the software-defined data center, DoD IT teams can also support continuity of operations (COOP) planning and secure telework initiatives. Moreover, through Horizon and VMware vCloud® Government Service provided by Carpathia™, DoD personnel can experience high-quality simulated training solutions that don’t require expensive on-site hardware. Organizations can use both computers and mobile devices to access simulation programs, increasing training availability and resources to more personnel worldwide.

To learn more about how to simplify your Windows 10 deployment, visit http://www.vmware.com/industry/government/federal-euc.html.

About VMware

VMware, a global leader in cloud infrastructure and business mobility, accelerates our customers’ digital transformation journey. We enable enterprises to master a software-defined approach to business and IT with solutions for mobility, hybrid cloud, application and infrastructure delivery, and security architecture. Based in Palo Alto, CA, VMware has over 500,000 customers and 75,000 partners worldwide and can be found online at www.vmware.com.