EMPOWER THE DIGITAL WORKSPACE

Improve Citizen Service Delivery and Mission Outcomes with Secure Anytime, Anywhere Access to Government Data and Resources

Employ a Digital-First Government Workforce

Just as the Internet compounded the need for e-government services, mobile technologies have changed the way citizens and employees consume information—forcing federal agencies to innovate business processes and workflows in response. Microsoft applications and desktop PCs no longer dominate the government workplace; cloud, native, web, and SaaS applications are able to accomplish the same levels of productivity as legacy applications; and Apple iOS and Android devices are quickly emerging as primary mobile form factors.

Today, work is defined less by where someone goes each day and more by how he or she gets work done. Federal agencies continuously compete for talent against the private sector and, with the federal workforce expected to shrink in the coming years, flexible workspaces and consumer-simple remote access to data and resources are necessary to attract and retain a new generation of talent. As the foundation of a mobile workforce, the digital workspace represents a fundamental shift in the way that IT services are delivered and consumed—simplifying application delivery, unifying endpoint management, and modernizing Windows management and security.

AT A GLANCE

The consumerization of mobility forces federal agencies to reimagine how they deliver the apps and services that personnel need to be productive, efficient, and successful. Agencies can leverage the software-defined data center to transform application and desktop delivery, secure endpoints, and enable seamless access to data and applications across devices and locations. With VMware, federal agencies can securely deploy mobility to deliver peak levels of service and achieve mission success.

VMware Digital Workspace Solutions for Federal Government

As a platform, the digital workspace provides the necessary infrastructure to deliver the apps and data personnel need across any device. Based on an agile, software-defined infrastructure, VMware empowers the digital workspace with software-defined solutions designed to provision, manage, and secure any application on any device. VMware Workspace ONE™ is the unified platform based on a software-defined architecture that gives agencies a simple and secure way to manage identity and access to all application types, on premises or in the cloud.

The solution includes unified endpoint management, built on industry-leading VMware AirWatch®, enabling complete, over-the-air provisioning and lifecycle management, and real-time visibility for users, apps, and devices across any network, whether physical or virtual. VMware's digital workspace solutions also include application and desktop virtualization technology that enables any device to access a virtual application or desktop, regardless of OS.

KEY BENEFITS

- Enable new methods of citizen service delivery and mission support
- Reduce federal IT complexity, streamline management, and increase workforce agility and productivity
- Deliver secure access to cloud, mobile, web, and Windows apps—on premises, in the cloud, or offline—through a single catalog and single sign-on (SSO) experience across devices
- Ensure security and compliance with policy-based control over devices, data, applications, and identity
- Securely deliver and manage Windows and Linux resources within a unified platform
- Automate resource-intensive tasks to reduce OpEx, increase efficiency, and boost security

SUPPORTING PRODUCTS

SIMPLIFY APP AND ACCESS MANAGEMENT

- VMware Workspace ONE

UNIFY ENDPOINT MANAGEMENT

- VMware AirWatch

TRANSFORM WINDOWS AND APPLICATION DELIVERY

- VMware Horizon®
- VMware AirWatch

RESOURCES

Learn more about deploying and managing secure digital workspace programs within your agency with The Government Digital Workspace for Dummies, a guide to the brave new era of mobile-cloud computing in government. Download ebook now.

Figure 1. Digital workspace

Simplify App and Access Management

VMware Workspace ONE is an identity-defined app catalog that integrates identity, application, and mobility management to provide frictionless and secure access to all the apps and data employees need to work—anytime, anywhere, and on any device. Workspace ONE combines device trust and multi-factor authentication—including the use of smart cards, derived credentials, and biometrics—with contextual, policy-based access controls. Workspace ONE federates even the most complex on-premises Active Directory structures and protects against data leakage with an automated compliance engine that solves for rooted or jailbroken devices, restricts access based on the location of the device, restricts sharing of data between apps, prevents copy/paste of data within apps, and more. With Workspace ONE, federal agencies can securely deliver any app, from the latest mobile cloud apps to new and legacy Windows apps, to any device.

Unify Endpoint Management

Workspace ONE leverages the AirWatch mobility management system to unify endpoint management, and manage the full lifecycle of all endpoints from on-boarding to retirement. Gain full visibility and management of all endpoints—including macOS and Windows desktop and laptop devices—from a single admin console. Protect endpoints with device-level encryption, data encryption, and hardware security policies, and prevent data loss with granular DLP policies and automated compliance monitoring. Automate processes through dynamic and intelligent policy engines designed to alleviate manual tasks for IT. A unique multitenant architecture further enables IT to delegate policies and management across divisions, regions, and departments while modular and role-based dashboards deliver real-time analytics and updates.

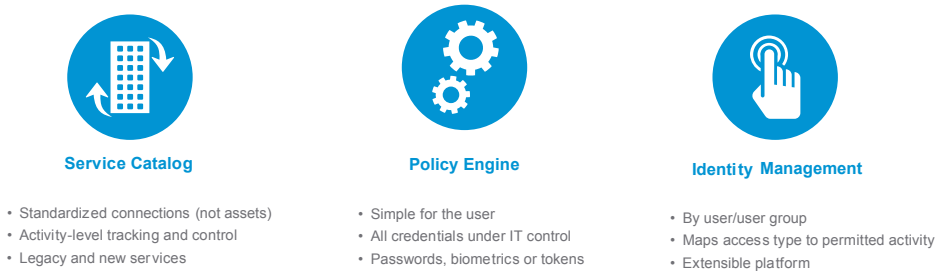

Figure 2. Workspace ONE architecture

Transform Windows and Application Delivery

VMware's digital workspace solutions enable agencies to quickly deliver Windows and Linux resources at scale across multiple data centers or clouds. VMware Horizon® virtual desktop infrastructure transforms static desktops into stateless, secure digital workspaces delivered on demand. Isolate apps from the operating system, enable real-time app delivery to virtual or physical desktops, enforce policy-based system management, and take advantage of tight integration with the software-defined data center to deliver and protect all the Windows or Linux and online resources users want, at the speed they expect, with the efficiency that missions demand.

Modernize Windows Management and Security

For today's federal agencies, it's not a question as to if they will migrate to Windows 10, but rather when they will migrate to Windows 10. From the department-wide push to Windows 10 issued by the Department of Defense to civilian agencies taking advantage of Office 365, Microsoft's groundbreaking approach to managing its OS both accelerates and supports federal digital workspace initiatives. VMware's digital workspace solutions enable IT teams to manage and secure Windows 10 PCs, with support for full application lifecycle management across modern Windows apps, legacy Windows apps, web-based apps, and SaaS apps.

Configure accounts, deploy security patches, install software, and distribute classic desktop and modern apps over-the-air. Establish automated workflows for product installation and remote distribution of apps, drivers, firmware updates, and other complex scripts, and consolidate operational processes across devices on or off the domain. Augment Microsoft security features—such as Windows Information Protection, Health Attestation, Secure Boot, BitLocker, Device Guard, Windows Hello, and Microsoft Passport for Work—with AirWatch security controls to maximize data protection and minimize risk. Ensure only authorized users can access enterprise resources, protect data with granular DLP policies and real-time compliance monitoring, enforce multi-factor authentication, and expose a limited set of data center resources to applications via app- and network-level micro-segmentation.

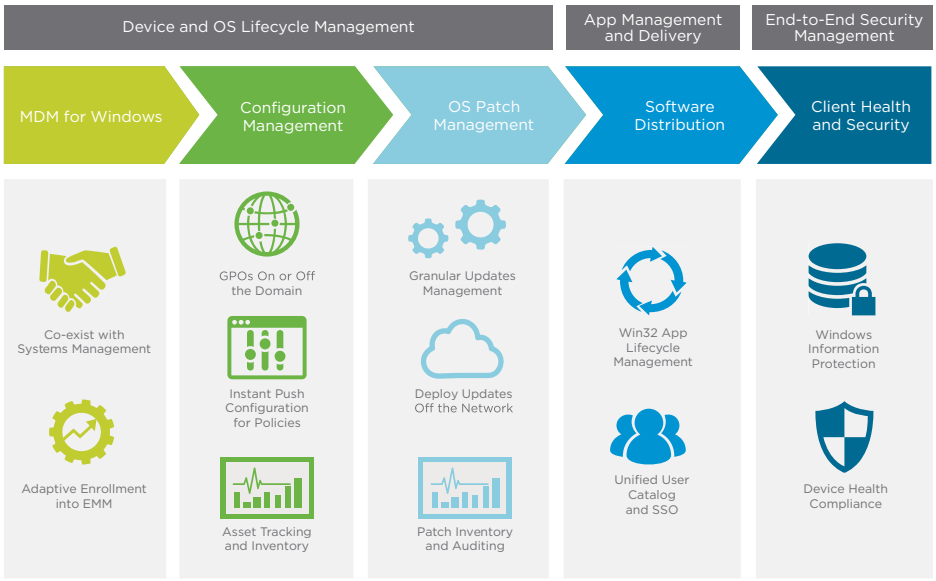

Figure 3. AirWatch Unified Endpoint Management technologies for more effective Windows 10 management

Learn More about VMware Solutions for Federal Government

As the number of devices and applications grow, federal IT must pivot from a device to a user-centric, identity-based approach to mobile management and data security. VMware empowers federal agencies to design digital workspaces that provide secure access to all application types, on premises or in the cloud. A unified platform built on an agile, software-defined infrastructure enables provisioning, management, and compliance of applications across operating systems, while a contextual policy framework enforces granular security controls across data and devices. With a transformational approach to delivering and securing applications, federal agencies can support secure digital workspaces and optimize agency performance and efficiency—without compromising security.

Realize the possibilities with VMware.

Visit www.vmware.com/solutions/industry/government/federal

vmware®

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