vmware

Three Critical Digital Workspace Strategies for Government

Three Critical Workspace Strategies for Government

Technology is playing a key role in reshaping government activity. Government agencies at every level have been reimagining their workflows and processes in the digital age to achieve mission outcomes at optimal cost, protect information, improve employee engagement to attract and retain the best talent, and provide citizens a better experience. New requirements to support working from home on a broad scale and to enable workers to use personal as well as agency devices are forcing organizations to accelerate these projects and present opportunities to rethink how work gets done.

On the federal level, to reduce cybersecurity risks, FedRAMP mandates that technology solutions must comply with specific security standards. In addition, driven by the *President's Management Agenda*, government IT is executing a multiyear plan toward building and maintaining a modern, secure, and resilient technology foundation to improve agencies' ability to deliver mission outcomes, provide excellent service, and effectively steward taxpayer dollars.

If *research from the private sector* holds true in the public sector, there is a strong correlation between the digital employee experience and workers' performance and satisfaction with their job. Workers today expect access to technology that enhances their productivity and supports new ways of working, like bring-your-own-device (BYOD) programs.

This brief explores how a digital workspace strategy provides the foundation for improved government and a better and more secure digital employee experience. It addresses government-specific trends and issues to consider to help meet the goals of modernizing IT and improving productivity and cybersecurity.

Employee experience

Zero trust security

New ways of working

Elevate the Employee Experience

The government workforce encompasses a broad range of skillsets, including some of the worlds' most talented professionals in the sciences and business who have chosen the public sector over private enterprises. Across the board, attracting and retaining top talent boosts productivity, maintains consistency of services, and lowers training costs. To meet the goals set out in the President's Management Agenda, government agencies need to look closely at the employee environment and experiences and how technology plays in promoting engagement, productivity, and efficiencies.

Successful onboarding

How an agency onboards employees can directly affect their willingness to stay and could be a crucial element in hiring and retaining the best talent. The *Washington Post* recently reported that the House of Representatives' employee turnover rate is, on average, 18.5 percent, with state and local government services at 20.6 percent. A VMware survey done for the private sector revealed that as high as 73 percent of the participants strongly agree that the flexibility of work tools—technology, applications, and devices—influenced their decision to accept a job. Hard to imagine that it is any different for government employees. In a world where government agencies are now being directed to become more competitive with commercial enterprises, government agencies must match, or preferably exceed, the employee experience offered by alternative prospective employers.

Day one is a new hire's first impression of working life at an organization, offering a glimpse into its structure and culture. In fact, the U.S. Department of Agriculture has specifically highlighted employee engagement in its *2018 strategic plan*, stating that "Improved customer service and employee engagement will create a more effective and accessible USDA for all our stakeholders." Agencies can meet these goals, spur excitement, and build loyalty by providing both new and established employees seamless access to resources, teammates, and the required training and documentation.

Deliver exceptional experiences with mobility

Most federal agencies have agents, field inspectors, workers, and contractors who need to access data that often resides in multiple systems that are not connected or require different access methodologies. While some access hoops are intentional given the sensitive nature of the data, more often than not, the myriad requirements are due to IT silos that prevent the different systems from talking to one another. The resulting loss of productivity and efficiency breeds user dissatisfaction, disengagement, and eventual attrition.

Take for example a military recruiter who works both on and off site. Often, a recruiter visits communities and schools to explain employment and training opportunities. As part of the daily activities, a recruiter establishes contacts, advertises and markets the military, performs interviews, and evaluates and processes recruits. When an applicant agrees to enlist, the recruiter approves the application, collects important identification documents, and prepares the enlistment packet. Some branches of the military also require a biometric scan to capture a unique physical characteristic, such as a fingerprint or iris. Today, these tasks might be accomplished with a number of outdated devices housed in different locations. Rather than being burdened with maintaining extensive paperwork or saddled by a physical workstation, recruiters could accomplish these tasks with a single device configured with the right policies, applications, content, and collaboration tools to connect them with colleagues and other recruitment specialists. And it is not only recruiters who enjoy an improved level of efficiency and user experience with these streamlined processes but also the citizens with whom they are interacting.

Providing a better customer experience by improving digital services is another key goal of the President's Management Agenda. To do this, government agencies need to deliver experiences such as those being reimagined in branch banking. For example, as customers enter the bank, they are greeted by a digital ambassador equipped with a mobile device connected to all the information needed to take a customer through a variety of tasks, from withdrawing cash to completing a mortgage application.

Implement Zero Trust

Government data is among the most targeted for cyberattacks, coming under ever-increasing threat from nation-state actors. One of the highest profile breaches targeted the *Office for Personnel Management* in which an estimated 21.5 million records were stolen, including personal information and fingerprints. And a 2018 Associated Press investigation revealed that hackers targeted U.S. defense contractors working on advanced technologies with phishing attacks.

The security infrastructure in most agencies was developed in a perimeter-bound environment in which everything inside the network—users, devices, and applications—is treated as trustworthy.

However, in today's diverse IT environment, government workers are increasingly performing tasks outside of government buildings. Applications might reside in government or public clouds rather than on-premises data centers, and employees are using a wide variety of personal and agency-owned mobile devices. In this environment, the idea of implicitly trusting users, applications, and devices no longer applies.

A new security model called zero trust does away with the concept of implicit trust and considers all resources external. The zero trust security model relies on continuous verification of devices, users, and apps before granting access to data and resources. Two-factor authentication can be required for users accessing information from a smart device. Contractors can get application access through desktop and app virtualization to ensure that confidential information does not reside on the endpoint. Personal devices can be required to register with the agency to ensure basic security hygiene, such as maintaining patch levels and passcodes. BYOD policies could also require that the agency manage the device. With this new approach to security, government agencies can dramatically reduce the risk of a data breach as a result of hacked or phished credentials or through malware that exploits older or unpatched systems.

Adopt New Ways of Working

Today's employees expect their work digital experiences to mirror the seamless digital experiences in their personal lives. Increasingly, employees prefer to use their own tools for work, putting pressure on IT to enable different ways of working and better support remote employees and BYOD programs. For government agencies, the prospect of enabling workers to access agency information from a personal device could seem like an unnecessary risk, but modern mobile device management and digital workspace solutions make it possible to secure agency information on a device without encroaching on a user's personal information. And by deploying the correct type of solution, agencies can unlock new ways of working and communicating.

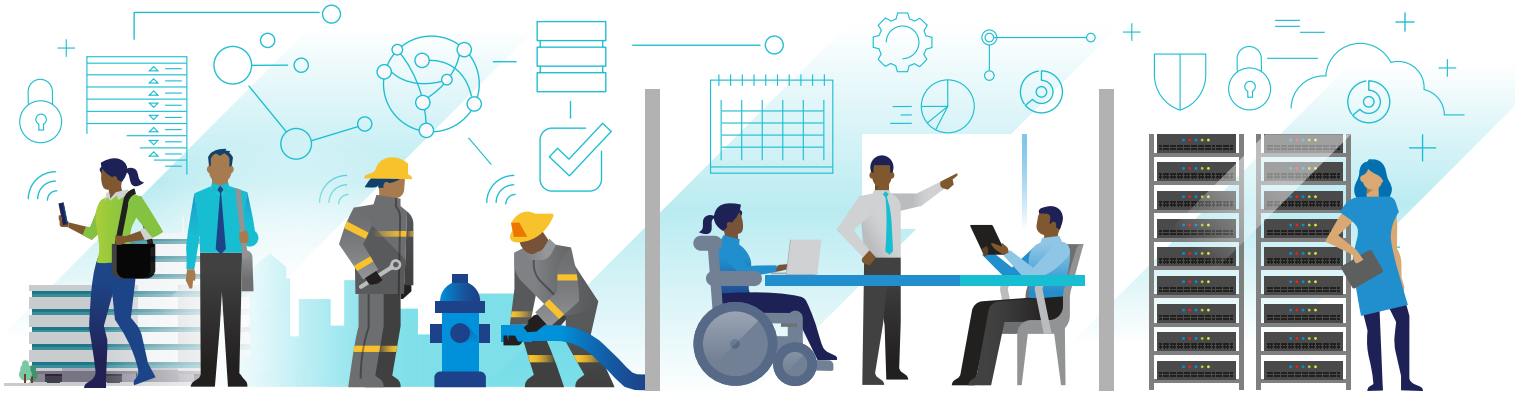
Embracing new and better ways of working with a software-defined digital infrastructure that gives government employees uninterrupted, secure access to internal applications and resources across any device or network is the first step toward modernizing the government workforce. Some benefits include:

- Increasing workforce agility and productivity with a consumer-like experience
- Making classified data securely and easily available in the field
- Working across data silos with streamlined single sign-on access across any device anywhere
- Meeting the demands of an increasingly digitally capable workforce and community

A great example of new possibilities gained from mobile technology is providing military pilots an electronic flight bag (EFB) on a secure mobile device. The EFB integrates with mission-critical applications and content to provide a display that simulates the look and feel of flight deck instrumentation. The EFB gives pilots faster and more secure access to information, thereby increasing efficiency, effectiveness, and safety during missions.

VMware Workspace ONE: The Digital Workspace for Government

VMware Workspace ONE® delivers the flexibility and security to meet the challenges of real-time connected government. Consistently ranked as a leader by industry analysts, Workspace ONE delivers best-in-class device management, access control, zero trust security, and application and desktop virtualization that enables government organizations to be productive and secure.



Workspace ONE combines device trust and multifactor authentication—including the use of smart cards, derived credentials, and biometrics—with features that ensure that only devices that comply with IT policies receive access to data and applications. A unique multitenant architecture further enables government IT to delegate policies and management across divisions, regions, and departments while modular and role-based dashboards deliver real-time analytics and updates. Built-in enterprise-grade security includes multifactor authentication across mobile devices while a privacy-by-design approach assures workers enrolled in a BYOD program that personal apps and data remain invisible to IT.

VMware's Digital Workspace for Government incorporates a framework of trust for operating in today's perimeterless world. By taking a better approach to delivering a better experience while not compromising on security, VMware Workspace ONE facilitates modernizing government IT to meet the challenges of the 21st century.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com VMW-WP-3CRITICALGOVL-USLET-20200513-WEB
5/20