The Time is now for the Digital Workplace

Virtualization and mobility technologies have truly enabled this digital transformation.

The federal government is clearly encouraging agencies to become more digitally savvy. The emergence of the U.S. Digital Service and the 18F office within the GSA are good indications of those increasing digital priorities. And agencies are doing just that by embracing digital technologies like cloud, collaboration tools, Internet of Things (IoT) and pervasive mobility.

According to last year's Federal Leaders Digital Insight Study, 87 percent of federal leaders want greater access to digital technology. The vast majority strongly agreed if the agency improved access to information through digital technology, employees would be more productive at achieving agency goals. Using digital technology helps federal employees better serve their agency stakeholders.

The true goal of digital transformation is to create a fully digital workplace, and help government employees be productive anywhere, with any device, at any time. While the digital workplace is based on pervasive mobility, it also requires communications technology, collaborative tools, social platforms, self-service applications and tools, and secure connectivity. It's a more dynamic, user-focused approach to getting work done that promotes greater levels of flexibility and collaboration. And it's an important issue—Gartner found it to be a top priority for government.

Moving toward the digital workplace is an effective way to stem the tide of qualified employees leaving federal agencies. Retaining qualified employees is a long-time challenge. Employees today value flexible work hours, the ability to telework, and they want to use cutting-edge technology. The digital workplace addresses all of these issues.

Providing access to the resources necessary to do a job are empowering, which directly impacts employee satisfaction. Millennials particularly prefer flexible environments and access to new communications methods, such as social media. A Deloitte study found a 20 percent increase in employee satisfaction when organizations installed social media tools—often part of a digital workplace solution.

There are many reasons beyond employee satisfaction to embrace the digital workplace. For example, it can greatly enhance productivity by providing users with secure access to all of the data and applications they need on demand, even on mobile devices. Pervasive and secure connectivity helps team members communicate and collaborate in real time, reduces downtime and improves overall productivity.

The digital workplace can also make employees more responsive to team members and citizens by helping them quickly find the information they need. Nearly three-quarters of federal leaders say their agency's productivity has increased significantly as a result of digital technology, according to the Federal Leaders Digital Insight Study.

The digital workplace can also reduce operational costs. For example, meetings can take place virtually, waiting for access to data or applications is eliminated, and travel time to attend meetings is drastically reduced. Having more employees working remotely also reduces the need for real estate. Some agencies are actually using that to reduce their office footprints. Finally, the fully automated nature and central repositories of the digital workplace can help reduce redundant work.

A fully digital workplace ensures higher operational and business continuity. Some organizations are even beginning to rely on the digital workplace as a legitimate backup in case of disaster. Finally, embracing the digital workplace can remove some of the user-related hassles employees have traditionally had to deal with—challenges like performance issues, platform support and interoperability.

Mrmohock/Shutterstock.com

Digitize the Workplace

Assembling the tools and technology is just part of the equation. Those must also be supported by the right processes and policies.

Everything's Possible/Shutterstock.com

Increasing productivity, improving employee satisfaction and saving money are a few of the many reasons federal agencies are working so hard to embrace the digital workplace. Agencies have made progress toward the goal of providing all the technologies employees need to get work done anywhere, anytime, and from any device. In most cases though, they have not yet assembled the full arsenal of digital-ready tools and processes they need to create a fully digital workplace.

Finishing the job requires a comprehensive strategy that includes a host of tools and technologies, along with effective policy and governance. The first step is developing a list of technologies and tools Deloitte calls the "Digital Workplace Toolbox." The specific tools and technologies may vary depending on user base, budget and mission, but generally include:

Full mobility: The core of any digital workplace initiative is policy-driven approval for employees to use smartphones, tablets and other mobile devices to get work done, along with management and security to keep things under control.

Communications tools: This includes fully integrated and secure e-mail, IM, chat and social networking environments.

Productivity tools: At the minimum, this includes a comprehensive office productivity suite (probably cloud-based), project management software and big data analytics.

Collaboration tools: Efficiency will suffer without the ability to collaborate with team members at any time. The digital workplace demands an enterprise collaboration tool that supports both online and offline meetings and can integrate data and services. The most popular collaboration tools today tend to have a social media feel to them.

Business applications: These are the applications agencies need to deliver on their missions. Some can be written as apps, while others may require users to access them via a virtual desktop on a mobile device.

Connectivity: Strong, secure connectivity is another must-have for the digital workplace. An enterprise-grade network to support voice, video and data communications simultaneously and can scale to meet any need is critical. The network also should be fully redundant to ensure smooth and seamless communication at all times, and meet all federal security requirements. To ensure secure communications with employees using their own devices, the set-up also should include Virtual Private Network (VPN) capabilities.

Security: Security is a constant. And it runs through the entire technology stack that makes up the digital workplace. It's especially important since many of the tools employees use in the digital workplace, such as cloud computing, social media and mobile devices, can invite risk. There are many ways to approach security, depending on agency requirements. Agencies are doing what they can by employing enterprise mobility management (EMM) software, along with containerized applications, network segmentation and VPNs.

These methods work well to secure applications and data, but don't fully address user authentication. For many, the best solution for authentication is embedding identity management in the digital workplace experience. This helps an agency set acceptable parameters and accepts or rejects users' access based on their role, location, and device type. And because so many employees now work via mobile devices, the federal government is moving toward derived credentials—a cryptographic key derived from a Common Access Card (CAC) or personal identity verification (PIV) card and stored as a soft token on a mobile device.

Achieving a full digital workplace won't happen overnight, but it's more than possible. And it is definitely a worthwhile endeavor. With the right approach to both process and technology, agencies can create the kind of collaborative and productive workplace that generates true results.

Power the Digital Workplace

The critical components to drive the digital workforce are finally all readily available.

Mobility is the foundation of the modern digital workplace. Without a fully mobile-enabled workforce, the “work anywhere, on any device, at any time” promise could never truly become a reality. Encouraging mobility through telework and BYOD initiatives is a great start, but it only sets the foundation. Truly effective mobility—mobility that powers the digital workplace—requires more. It demands secure end-to-end connectivity as well as identity, device, application, and data management.

While government agencies have made great strides in many of these areas, progress has come in bits and pieces—a VPN from one vendor, virtualization from another, device management from a third, and so on. Crafting a fully functional digital workplace requires higher levels of integration and connectivity. That goal is fully achievable today. With the right integrated infrastructure that’s secure and easy to manage while at the same time easy to use by the end users, agencies can truly provide the tools employees need to work securely from anywhere, at any time, at any place.

Providing ubiquitous access to data and applications, especially back office and older applications, has always been challenging on mobile devices. Thanks to virtualization and VDI a mobile worker could for example simply launch a VDI instance on a smartphone or tablet quickly to access an older .NET-based application.

One of the most important advances that make this possible for government was when NIST updated FIPS 201-2 to include additional form factors as an alternative to smartcards (i.e. CAC or PIV). In 2014, NIST also published Special Publication 800-157 (Guidelines for Derived Personal Identification Verification (PIV) Credentials). This enabled federal agencies to use Derived Credentials as part of their overall single sign-on strategy.

Single sign-on is what lets users access multiple applications, devices and other resources with one single set of login credentials. It’s a critical piece of the digital workplace puzzle, especially since smartcards don’t work with the native operating systems on mobile devices and the majority of the mobile apps that run on those devices. It’s also a productivity enhancement. It simplifies access to resources and helps users securely move between applications and services without interruption—even containerized and cloud-based resources.

Another important piece is endpoint management. This includes several critical capabilities:

- quickly configuring and enabling remote management of devices which includes locking down and/or remote wiping in the case of theft or loss
- enabling automated compliance and remediation actions
- deploying, managing, and configuring web, native, containerized, and VDI applications
- recognizing which specific applications need network segmented secure connectivity and applying it when needed
- enforcing rules for wiping data from a device when it is compromised

When all of those parts of the equation—virtualization, single sign-on, endpoint management and secure connectivity—are integrated into one solution, agencies can experience the benefits of a true digital workplace. Workspace ONE, a secure digital workspace from VMware, combines all of these features and more to create what Eugene Liderman, a director in VMware’s Mobility division, calls “a Swiss Army knife for the digital workplace.” This integrated solution includes a customizable, self-service app catalog to deliver agency-approved apps and data access to credentialed users, single sign-on through identity and access management, user, device, app, content provisioning and management, policy enforcement, remote configuration management, and virtual apps and desktops all with secure connectivity and through network segmentation.

“Think of it like a contextual start menu of all of the tools IT has provided for you,” says Liderman. “If its an application that isn’t compatible with the operating system on your device, you can run it as a virtualized application and get your work done. If it’s a app that stores data on the device, you can deploy it containerized or enable full disk encryption and per-app VPN to allow secure connectivity so it can synchronize with your backend resources. It’s fully flexible, depending on where you are accessing from and what you’re trying to access. It’s ever-changing and adaptive.”

Access to this technology will drive change for federal agency mobile workers. “Leveraging the full set of capabilities of Workspace One will allow government IT departments to deliver the same end user experience in the workplace that their users experience in ther personal lives, with the added protection, security, and compliance that are required by the respective agency,” says Michael Wilkerson, Sr. Director of Federal End User Computing at VMware.

With today’s fully integrated approach to mobility, agencies can fulfill the promise of the digital workplace—truly secure and always available access to the resources necessary to be productive in any location, on any device.