GET STARTED

THE 5 CRITICAL REQUIREMENTS FOR THE DIGITAL WORKSPACE IN STATE AND LOCAL GOVERNMENT

vmware®

Challenges of a Digital Workspace

As the digital workspace becomes a more pressing need, state and local government agencies are adapting to new ways of connecting staff, stakeholders, and information. Now the digital workspace is expanding to include new technologies like artificial intelligence (AI), which is emerging as the next best way to secure information, handle growing complex threats, and evolve productivity tools.

Despite all of the conversations about the digital workspace, it remains challenging for agency IT leaders to plan for the changes required to make it a reality. Many of the skills, tools, and processes used today are based on 20-year-old, PC-centric technology. A new approach is needed to make the digital workspace strategy a successful one for state and local agencies.

From Device Management to Staff Empowerment

The requirements for a digital workspace solution start with agency staff. This is the most fundamental shift in IT planning and, though simple in concept, requires a different way of thinking and the development of new skills. While yesterday's tools and processes revolved around devices, they missed the critical connection of how an individual staff member moves between devices throughout their workday.

To capture the complete experience, IT must consider:

- How do staff members learn about new applications?
- How intuitive is the process when using the app for the first time?
- Is the process different depending on the device or location?
- Does the app require access to other apps or services, like cameras, sensors, or local files?

- When changes are made to the app, does it improve or hurt its usage and adoption?
- Is the application or its data stored in a public cloud or on-premises?

In a consumer context, app developers are constantly sweating over these design details because adoption is their primary goal. Now IT can partner with their agency stakeholders to make tool and service adoption their top goal as well.

5 Critical Requirements for a Digital Workspace

The increased use of government-owned and personally owned devices to access information and execute work has led to the development of a set of requirements that will help state and local agencies plan and implement their digital workspaces. The details underlying each requirement will be unique to your agency, but each requirement must be met.

The 5 critical requirements identified are:

1. Putting Staff Experience First
2. Delivery of Applications — Anytime, Anywhere
3. Device Management
4. Manage Experience and Security
5. Automate to Succeed at Any Scale

Let's take a closer look.

1 Putting Staff Experience First

Addressing the staff experience as the first requirement for a digital workspace is not a simple nod to keeping agency employees in mind as you go about the process of delivering IT. Instead, building a strong design culture around the human experience is critical to meet the demands of the agency, as well as the ability to secure government data. If agencies, teams, and individuals believe that IT gets in the way and slows them down, staff members will avoid adopting the tools and services designed to protect them and improve their workday.

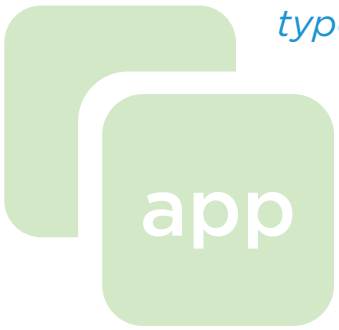
IT must put themselves in a position to design and deliver the productivity experiences agency staff will use. This takes into account the devices and form factors staff members use throughout the day, and the locations from which they need to work, as well as providing a level of flexibility and choice that will keep up with the demands of both individuals and teams. In many cases, this takes a shift in skills and culture, but it represents growth opportunities across IT.

2 Delivery of Applications — Anytime, Anywhere

The next critical requirement is the ability to deliver any application through the digital workspace experience. “Any application, anytime, anywhere” is a tall order. It doesn’t just mean the latest mobile app on an Android or Apple device, but the 12-year-old Windows app, internally developed Java-based apps that no longer have an internal owner, or the old Excel app with macros that don’t work in recent versions of the program. It also means web apps delivered internally through complex and ever-changing VPN tools, or SaaS apps accessible from anywhere, but with passwords no one can remember.

The bottom line is: you can’t deliver a positive user experience if you can’t deliver all of the applications agency employees need to get their jobs done. As soon as you begin to have caveats about what works some of the time, depending on how you are trying to connect, staff members will go back to fending for themselves, and avoiding IT for new apps.

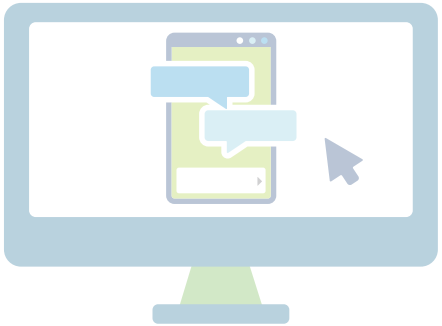
Applications must be portable across device types, locations, and ownership models.



3 Device Management

Device management is based on the now-universal trend that modern operating systems need to be updated on demand, anywhere, from the cloud, in an effort to manage billions of devices at scale and ensure application compatibility for developers. To allow state and local agencies to effectively manage the experience and security policies of devices, device management APIs that potentially disclose hundreds of policy options and context data for each operating system have been exposed through device management tools. Device management has been extended to every device operating system: Windows, Mac, Chrome, Android, iOS, and flavors of embedded Linux. There is no question that, in the near future, every agency-managed or personally owned device accessing government data will be connected to a management platform.

The question is, when? Many agencies have heavily invested in years of tools, skills, and processes revolving around domain and image-based management of PCs and Macs. We believe device management is a necessary requirement for the digital workspace; it's the only way to deliver consistent experiences in a perimeter-less work environment by having real-time context of the devices used to access the apps and data agency staff need to do their best work. Device management helps secure access management so there is only one app and one place to go. It also ensures unified endpoint management for a consistently great user experience that is also highly secure.



In the near future, every agency-managed or personal device accessing government data will be connected to a management platform.

4 Manage Experience and Security

You might have noticed a pattern here: each of these requirements builds on the one before. Start with agency staff and the ability to design a complete experience that extends across all their devices and locations. Then ensure that all their apps are accounted for, and leverage modern device management to make sure you have the ability to deliver and protect those apps across all endpoints and locations.

However, IT can't proactively drive successful experiences if they can't measure the adoption of these experiences. This is where insights come in. IT has never been in an ideal position to track the adoption and usage of applications across devices. Sure, you can run reports and try to look back through historical data, but these tend to be one-off efforts that look at the past with a hit-or-miss approach based on what information is available across disparate platforms. True insights from data are gained from the ability to spot patterns and trends, identify potential gaps in experience or security, and make recommendations for change.

5 Automate to Succeed at Any Scale

In the end, having visibility and even control of this new digital workspace environment is fantastic, but with more devices, more apps, and more threats, the digital workspace becomes increasingly complex.

To handle the scale of a digital workspace, in the agency environment, automation is critical, whether onboarding a new staff member or device, deploying apps, serving up patches and updates, or automating remediation steps to assure an agency employee's device is compliant with policy. These all must be achieved without generating tickets that require administrators or application owners to take manual actions. Automation assures that operational costs are minimized, and removes gaps that could result from inconsistently applying security policies or leaving devices in noncompliant states for too long.

The Digital Workspace Is Here to Stay

Implementing and maintaining a digital workspace that puts agency staff needs first is critical to supporting state and local government initiatives and fostering better ways to connect people with data. IT leaders need to lead the charge toward a more efficient, user-friendly, and secure digital environment. Taking the right steps now — examining and incorporating the five requirements discussed here — will help to ensure the likelihood that staff members will adopt new apps and adhere to new IT policies that are put in place now and in the future.

GET STARTED TODAY

Learn more about empowering your digital workspace

Join Us Online:

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2020 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. 12/20