WHITE PAPER

READ BEFORE OPENING!

Four Design Considerations Before Embarking on a Digital Workspace Project

vmware®

Table of Contents

Introduction

Mobile apps represent 60 percent of total digital time spent. [1]

Digital transformation is happening all around us, and technologies like cloud and mobility are rapidly changing the way people work and live. People are increasingly comfortable with consumer applications and services delivered in new ways, and these trends are crossing over into the business world.

Cloud application services (software as a service [SaaS]), one of the largest segments in the global cloud services market, is expected to grow 21.7 percent in 2016, according to Gartner's 2015 cloud adoption survey." [2]

More than ever, employees are working primarily from mobile sources, both in terms of devices as well as networks, and they expect a smooth, consistent experience using the device they choose. Their organizations are turning to mobile solutions as well, seeking to transform processes to boost efficiency, improve workflows for end users, and drive better employee to customer engagement — while driving productivity to the next level. To drive these new outcomes, many are exploring digital workspace initiatives.

[1] Enterprise Mobility Exchange: Engaging Customers with Mobility

[2] "Gartner Says Worldwide Public Cloud Services Market to Grow 17% in 2016," Gartner, September 15, 2016, http://www.gartner.com/newsroom/id/3443517

49 percent of U.S. IT managers "strongly agree that BYOD improves worker productivity." [3]

Supporting a Dynamic Workforce with a Digital Workspace

A digital workspace strategy lets IT harness the rapid changes that consumerization is bringing to their businesses. It's a holistic change in the way end-user services are delivered by IT, enabling organizations to deliver the apps and data employees need to work across any device.

VMware empowers a digital workspace strategy by delivering a consumer simple experience, together with enterprise-class security. VMware Workspace ONE™ is a unified platform for the provisioning, management, and policy enforcement of applications and data to devices across all major operating systems, including iOS, Android, and Windows. The solution is based on a software-defined architecture that makes it simpler to manage identity and access to all application types, on premises or in the cloud.

The digital workspace has tremendous potential to streamline processes and boost business agility. But before you move forward, it's important to think about some key design considerations.

1. Start with a People-Centric Approach

Every business is ultimately about people, so a digital workspace initiative should start with a people-centric approach. Not long ago, IT defined employees and their departments only by the applications they used, and maybe what class of PC (portable vs. power) they were authorized to receive. Finance departments used financial services tools and apps; while marketing teams might use personal productivity apps.

Now, in the era of the digital workspace, it makes more sense to think about employees not just in terms of the type of work they do, but how and where they are doing it. Today's financial services professionals not only have specific applications, but they may be extended across global environments, with location-specific requirements. An organization may have people on the finance team who are working from home, rather than coming into the office every day. Some may require access to sensitive or heavily regulated data. Consider how employees are working, and set up groups that align with them.

Traditional ways of thinking about infrastructure requirements also centered around employee devices. Engineers would require dedicated workstations with lots of processing power, while finance employees might require large screens for spreadsheet applications, and so on.

Today, new initiatives like BYOD are forcing IT to rethink the way it considers devices. Instead of standardizing on a few approved devices and limiting employee choices, IT groups are exploring better ways to make as many options available to employees as possible. That means developing an infrastructure that can support the device that's best for a particular job. In the past, the key to controlling costs was standardization.

[3] "The New BYOD: Best Practices for a Productive BYOD Program," VMware.

Whether you offer employees support for their personal device of choice, or a department or line of business has particular requirements and developed preferences, you want to be in the business of supporting any device that's needed.

2. Who Owns the Device?

Consumers in mature markets will use and own between three and four devices by 2018.[4]

Digital transformation is changing the old rules of device ownership as well. Ideally, in a digital workspace, it shouldn't matter whether the company purchases an employee's device or not, since it will be managed the same way. But if an employee owns the device—and often, even if they don't—they'll want to know what IT is doing with it, and whether their privacy or personal data is at risk of being lost or compromised.

When designing a digital workspace, IT should consider whether they truly need to own an employee's device. Security will play a key role in that decision. If the company believes that they need the option to wipe the entire device, then they will need to own it, to avoid liability for erasing employees' personal information.

In a recent survey, 50 percent of IT managers, CIOs and CTOs surveyed said managing mobile users and devices was a medium or major priority.[5]

However, it's not always a given that IT needs to own an employee's device. If IT has the ability to wipe any corporate information that will ever touch that device, and they have all the right management capabilities and policies in place to ensure that corporate information can't escape their control, then device ownership often isn't necessary. Modern native containerization controls across all major platforms, such as iOS, Android, and Windows 10, are built for native containerization that protects personal data and apps.

Even with today's BYOD initiatives gaining momentum, most employees still have an expectation that when they show up for work, their employer will provide a device. But with the right infrastructure approach, an organization could simply pay for the device and allow the employee to choose the one they prefer, without sacrificing security or compliance concerns.

Balancing Choice and Compliance During Onboarding

Determining device ownership standards is an important step, and IT needs to address the question as part of the employee onboarding process. In the past, IT would set up a company laptop, provision it, and ship it to the employee. With a digital workspace strategy that offers an enterprise app catalog, employees can access the apps and services they need from any device, regardless of form factor or OS. Some applications might require a higher level of protection, and stricter compliance in the device.

The global BYOD and enterprise mobility market is expected to grow at a CAGR rate of 24.12% from 2017-2021. [6]

As part of the onboarding process, IT can install a profile on the device to enforce compliance. It can be as minimal as installing certificates to verify uniqueness and device ownership, or ensuring basic passcode requirements that are regularly changed. On the other hand, if the company owns the device, compliance is easier to enforce.

---

[4] "Gartner Says Consumers in Mature Markets Will Use and Own Three to Four Devices by 2018," Gartner, Inc., December 8, 2015.

[5] "IT Budgets: Drivers, trends, and concerns in 2016," Tech Pro Research, August 2015.

[6] "Global BYOD and Enterprise Mobility Market 2017-2021," Infiniti Research, July, 2017.

The ownership approach you choose will need to balance employee choice and compliance. The flexibility of a digital workspace means you'll have fewer tradeoffs than with traditional approaches.

3. Consider the Employee Work Style

The employee work style is another important design consideration when developing a digital workspace. A field service technician using a mobile tablet might need a ruggedized device provided by their employer, equipped with a camera or scanner. But they might also want to stay productive on the weekends or after hours using their personal smart phone to access enterprise apps or HR resources.

When developing a digital workspace strategy, consider what users might wish to accomplish at different times, and whether they require different devices, different experiences, and different ownership policies.

Different devices also have different purposes. Portable, always-connected devices can do things that a standard desktop PC can't. The real opportunity in making employees more mobile is the potential to take advantage of this small form factor to make them more productive and agile. It's an opportunity to change the way people get the job done, or accomplish things that weren't possible before.

The average mobile session of 72 seconds[7] is considered the "mobile moment."

It's important not to sacrifice this advantage when developing a digital workspace. Access management needs to be fast and intuitive, and take advantage of the "mobile moment."

One-third of support centers reported that more than 30 percent of their tickets were related to password resets, even though 69 percent allow customers to reset at least some of their passwords without contacting the support center.[8] The average cost of a password reset is $18 per support call.[9]

If a mobile employee can't perform a task on their device in a few seconds, such as forwarding information to a customer, it simply winds up as yet another item on a "to-do" list when the employee returns to the office.

Accommodating employee work styles requires minimizing friction wherever you can. For example, single sign-on (SSO) or "no sign in" with certificate-based authentication can streamline workflows, and enable employees to take advantage of mobile opportunities, without introducing security risks. Ideally, users shouldn't need to retype passwords and configure or enter information to get to a corporate app. These processes should be automated ahead of time.

4. Employ Smart Security and Access Policies

Security and access play a major role in design considerations for a digital workspace. Although employees are already comfortable using mobile devices and downloading their favorite apps, IT still has to think about security, compliance, and protecting its intellectual property, employees, and customers.

According to the Ponemon Institute, mobile devices such as smartphones were cited as the greatest rise in potential IT security risk.[10]

The threat landscape is becoming more complex, security issues are multiplying, and the traditional approach to protecting the network periphery no longer works. In an increasingly mobile, cloud-connected world, the rule of the day is to trust nothing.

---

[7] "Mobile User Experience: Limitations and Strengths", Nielsen Norman Group, April, 2015.

[8] "Password-Reset Practices in Support," HDI Research, May, 2012.

[9] http://blogs.forrester.com/stephen_mann/12-06-21-it_service_management_and_automation_now_thats_a_double_whammy_of_business_enabling_goodness.

[10] "2016 State of Endpoint Report," Ponemon Institute, April 2016.

However, a zero-trust approach need not require a restrictive, one-size-fits-all security model. Excessive or repeated authentication requests, token requirements, and other processes can introduce more friction, and reduce usability and adoption.

Consider what you really need to protect, and take the time to carefully design security and access policies. You can tailor granular access policies based on:

- Network location
- GPS location
- Specific users
- Strength of authentication
- Authentication challenge timing preferences
- Reauthentication only when context changes

You can also apply highly granular security policies to access devices. For example, you may wish to require cryptographic modules for encrypted data as a compliance check for sensitive applications. You can specify that the latest security updates are installed on the device OS to run an application. Or, if a device has been compromised or modified by a jailbreak or root kit app, you could block access to corporate apps. An effective digital workspace solution will deliver the pinpoint control you need to ensure consistent compliance.

How Secure Are Your Apps?

Securing enterprise applications is an essential consideration for planning a digital workspace. A self-service enterprise app catalog enables you to define which applications employees can access, and control how they're used and where they reside.

For example, you can define which apps are pushed out to specific employees by default, and which ones require a self-service request.

Some applications should simply never reside on a device. If a device containing customer records or important financial or proprietary information is stolen, it's only a matter of time before the thief can decrypt its contents. Virtualizing critical applications and hosting them on the data center can provide superior security, because no trace of the data remains on the individual device. Not every digital workspace or employee needs virtual applications or a virtual desktop, but many of them will.

Conclusion

The promise of a digital workspace strategy is based upon its ability to help IT teams ensure smooth, policy-based access, using the device their employees choose. With careful planning and the VMware Workspace ONE solution, you can deliver an experience that is consumer simple, yet enterprise secure. After considering the needs of the people in your organization, your policies for device ownership, and your organization's security requirements, you'll be ready to move forward with your digital workspace initiative.

The Workspace ONE solution makes it fast and easy to adopt new services and workflows, while optimizing security with rich contextual access policies.

Workspace ONE gives you a simple way to manage access to all your application types, on premises or in the cloud. You can also take advantage of the unified platform for the provisioning, management, and compliance enforcement of devices across iOS, Android, and Windows. Its contextual policy framework lets you set granular policies, and deliver transformative mobile workflows through a suite of productivity apps and mobile services.

By partnering with VMware, you can take advantage of digital transformation while speeding time to integrate, securing data, and controlling the risks and costs of shadow IT.

LEARN MORE

Take the first steps toward simplifying app and access management

Join Us Online:

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