WHITE PAPER

KEY CONSIDERATIONS FOR MOVING TO A DIGITAL WORKSPACE

vmware®

Table of Contents

Introduction: IT Needs a New Approach in a Changing World

It's clear that IT organizations are at a crossroads in today's world of digital transformation. Cloud technology and mobility are changing the way people work, and redefining priorities for the technology teams that support them. Changes outside the workplace are impacting businesses as well. As people become more comfortable with new consumer apps, digital devices, and a more mobile lifestyle, their expectations for IT service and personal productivity are also evolving.

And yet, while perhaps an obvious trend, surveys indicate that there is still a significant disconnect between CIOs and end users. According to a recent Forbes Insights survey, a less-than-ideal 39 percent of CIOs agreed that their IT team makes it easy for employees to request and obtain new apps, tools, and services. But only a dismal 21 percent of end-users agreed.[1]

The fact is that today's business users expect the same level of flexibility, choice, convenience, and self-service that they enjoy in their personal lives. Individuals and teams are always exploring alternative services to innovate or simply work more effectively. They're more than willing to try out unsanctioned cloud services and other shadow IT initiatives, especially if their existing IT tools and processes can't deliver the new tools and applications they want or require.

This consumerization is creating new application demands, and driving business processes in new directions. In this dynamic environment, IT can no longer sustain the status quo of rigid, time-consuming PC management, asset management focus, siloed teams for mobility, and overlay security that encumbers employee productivity and slows business agility. But IT may not always be aligned to quickly-evolving mobile opportunities. People are accustomed to the freedom to work and collaborate from anywhere, on their favorite device. For many, office-bound approaches to IT are no longer viable, and technology teams understand that they need to reimagine their delivery models for emerging mobile and cloud technologies.

It's Time for a Digital Workspace Strategy

To deliver the agility and user-centric experience their businesses demand, IT organizations are aggressively defining digital workspace strategies. A fundamental change in the way end-user services are delivered, the digital workspace enables IT to securely and reliably deliver the apps and data employees need to work across any device, from personal devices like smart phones and laptops, to less personal devices like point-of-sale tablets, warehouse scanners, or fixed desktop PCs.

The digital workspace is based on a software-defined architecture that makes it simpler to manage user services and app access policy across all types of applications, on premises or in the cloud. It liberates users to work on any app they wish, using any device they choose, at any location so long as the compliance requirements defined by the application or service owners are met. Requiring a secure, extensible platform helps take the friction out of application delivery, and enables IT to focus on improving usability and providing the personalized, intuitive experience that employees expect when they access the mission critical apps and data they need.

[1] "THE IMPACT OF THE DIGITAL WORKFORCE," FORBES INSIGHTS, 2017.

WHAT IS A DIGITAL WORKSPACE?

A digital workspace is a unified and persistent end user experience that enables users to simply and securely gain access to the applications, services, data, and experiences across devices, networks, locations, or operating systems.

Businesses are also adopting digital workspace strategies to streamline processes and boost business agility. The agile delivery model makes it easier for IT and LOB teams to collaborate and innovate together as partners, so they can respond with the right technology solutions to new business challenges more quickly and effectively. And when requirements change, IT can adapt and adjust, to make their processes more efficient and less costly.

A digital workspace is more than initiatives based solely on technology, tools, or operations. It's a transformational effort that requires a new way of thinking. To make the most of it, and to be responsive with business needs, IT teams need to examine their user engagement models, and align them to take advantage of this innovative approach.

More than a technology, however, a digital workspace strategy requires a cultural shift by IT, away from standardization and a focus on asset management. Instead, the digital workspace focuses on enabling all employees to take advantage of self-service engagement, improve choice, offer consumer-friendly and rugged device experiences, and access to modern cloud-based applications.

A key component to this strategy is shifting IT services away from device-dependent services (i.e., PC images, asset management) and instead focusing on the needs of users.

VMware believes that a platform is required to effectively deliver on a digital workspace strategy. This platform includes a core set of technologies that leverage modern cloud-based identity techniques and open operating system management API's. The platform also includes built-in privacy safeguards to establish trust between devices, users, and the company as a way to better deliver services and secure company data.

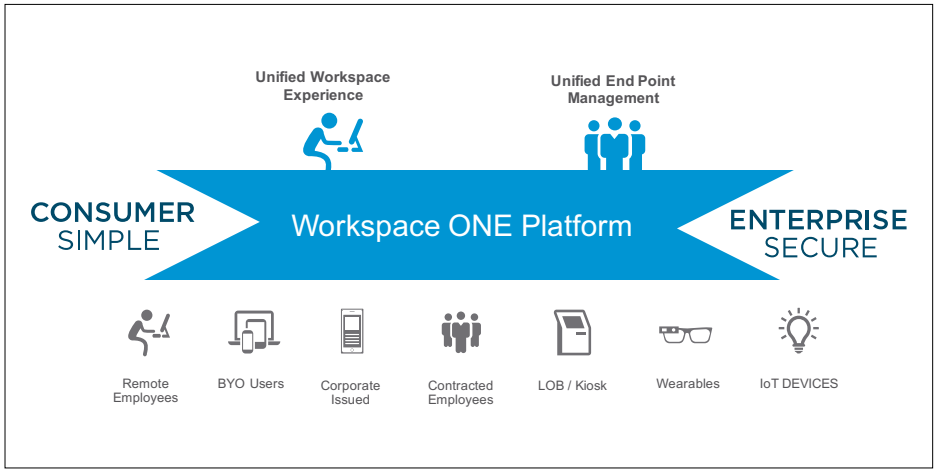

Figure 1: A platform approach is required to deliver on a digital workspace strategy.

Taking IT Engagement to the Next Level

Every organization needs their own digital workspace strategy unique to their mission, employees, and industry requirements. Digital workspaces are built upon the fundamental concept that users should be empowered and enabled instead of being restricted. Unlike traditional IT models that focus on top-down mandates, restrictions, and managing assets, a digital workspace strategy is about providing lines of business and individual users with choice and flexibility. An effective IT engagement model will consider not only corporate priorities like compliance and security, but the best way to empower users with self-service, business workflow innovation, and a superior experience. By first managing users and application policy with an identity-centric approach, then understanding the state of any given device, the stage is set to use context to make intelligent decisions that simplify user experience—while reducing risk of data loss. Let's take a closer look at three key planning considerations for organizations implementing a digital workspace.

Leverage Self-Service as the Engagement Model for Employees

Users are comfortable identifying and accessing the applications they need, and an enterprise application catalog plays a fundamental role in the digital workspace, providing a single source for every employee to find applications and onboard new devices for use for work. This centralized resource can support any type of app required, ranging from Web and native apps, to virtual apps—inside or outside a VPN. Employees can simply bookmark their desired web or virtual apps, and easily install native apps directly onto their device of choice. Some users may check the app catalog every day as a convenient way to launch apps. Others may prefer to simply set a bookmark, or visit the catalog only when they are looking for a new application or service.

An enterprise app catalog puts simple, self-service access to applications in reach for all users that need them, and covers all application types (i.e., cloud, SaaS, Windows, published, locally installed), both existing and new. Deploying an enterprise app catalog simplifies the way people work with their apps and services, providing a single, pre-integrated resource that's friction-free. One of the main benefits of the application catalog is its use of a "pull" delivery model, rather than traditional models where all apps were "pushed" directly to users from IT. Enabling users to request applications from the application catalog instead of waiting for IT to take the initiative, users become more actively involved, fundamentally changing the dynamics of how apps are consumed.

Another strength of an app catalog is that it represents a user-centric approach to IT engagement that is device-agnostic, rather than a strictly-defined "top-down" approach. Instead of imposing a pre-defined mandate, it lets employees choose the application option that works best for their own needs. When it's time for IT to make changes to the catalog, those changes will be reflected instantly across all devices.

Easing Experimentation Helps Drive Faster Innovation

Innovation can't happen without experimentation. A digital workspace strategy is a great way to encourage innovation by allowing for more experimentation and freedom of choice for departments in the apps, devices, and platforms they're using.

For example, consider a business unit that's trying out a new file sharing app. Under a traditional approach, IT might spend months comparing products, surveying users, choosing the right vendor, beta testing, and advocating for the product. But a wide variety of file sharing apps are available, optimized for different tasks and business processes. Why should an organization limit itself?

A digital workspace approach gives teams in an organization the freedom to choose the app that's best for them, and puts IT in a position to support and deliver any of them. IT doesn't have to pay for it, but simply enable it. Departments can adopt the file sharing tool that's best for them, and IT can charge them back for support. Charging applications to the business units that have initiated them is not only a good way to control IT costs, but can also help give key stakeholders better insight and visibility into their use.

Making it faster and easier to add new options to an enterprise application catalog is another important way to embrace new apps. As the catalog's acceptance builds, employees will automatically look to it as the resource of choice for every new app, and its use will grow. The catalog is the common denominator of access, making its use and adoption de facto. A catalog creates momentum and uniformity for app delivery, and creates a multiplier effect, driving faster growth in adoption.

A more user-centric digital workspace strategy also helps IT position itself to be part of conversations about new technologies and apps, encourage adoption and innovation, and play a more strategic role. Instead of acting as an obstacle, IT acts as a supportive enabler.

Deliver an Outstanding Consumer Experience

Effective engagement requires a relentless focus on the employee experience. To help every employee make their best start, IT can collaborate with HR organizations to make the digital workspace integral to onboarding. For example, they can populate their enterprise app catalog with essential tools and resources, to enable employees to work productively from day one.

A digital workspace can also fast-track onboarding by giving employees additional device flexibility. Traditionally, IT might set up a company laptop, provision it, and deliver it to an employee. However, with a digital workspace, employees can access the apps and services they need on the enterprise catalog, from their own device, and start productive work immediately.

Surveys show that as employees become more empowered, they become more productive. Putting the right business apps and productivity solutions in reach helps them make faster, better decisions, boost productivity, improve collaboration, and enjoy higher job satisfaction. Digital workspace employees report a significantly greater impact on personal productivity (63 percent) than on accomplishing more in a typical workday (38 percent), with the help of business apps.[2]

[2] "THE IMPACT OF THE DIGITAL WORKFORCE," FORBES INSIGHTS, 2017.

The benefits extend not only to users, but to IT. Traditional, asset-based IT approaches are based on managing complexity by reducing variables. For example, image management for employee laptops and desktops includes drivers and utilities that are tied specifically to manufacturer, product line, and model.

A digital workspace gives IT an opportunity to dissolve these restrictions. IT should embrace any device with an out-of-box experience that lets users start working right away, without sending the device to IT for imaging and other configuration requirements. With public cloud-accessible APIs instead of restrictive, proprietary tools, organizations can manage devices they either own or support from anywhere, no longer needing to wait for a device to be "on the domain" to ensure that critical patches, updates, or new applications are delivered. IT can employ Device Enrollment Program (DEP)-style device onboarding, made popular by Apple, and now extending to Dell, HP, Samsung and many other ChromeOS, Windows 10 and Android-based devices, that pre-provision devices and enable them to automatically self-register to the company without touching them. Providing this freedom of choice for employees leads to faster time to productivity, without introducing additional IT complexity.

For example, instead of dictating that users must employ a specific smart phone model and OS, IT can employ a device-agnostic approach that lets employees choose their favorite communication device, without compromising company requirements. Whether the company is paying for the device or not, the same management principles apply, allowing each organization to design appropriate policies or restrictions.

Beyond IT: Cultural Shifts Are Required

Today's IT professionals appreciate the challenges of operational optimization and troubleshooting. While these skills are important, they are no longer the principle abilities required for a business built around the digital workspace. Instead, as organizations become more user-centric, they will want to emphasize user experiences first; everything else is of lesser priority.

Users today are more sophisticated, and bring new demands to the workplace. They're familiar with a wide variety of technologies, and most have developed strong preferences about which technologies works best for them. After enjoying individual empowerment and freedom of choice in the consumer world, they are resourceful and proactive. They're also less likely to have their technology delivered in a strict, prescribed fashion. They're less interested in the requirements of past IT operations, and more interested in freedom of choice, self-service, and having their requirements met based on user needs. However, according to Forbes Insights, only 10 percent of end-users agreed that employees are currently free to choose business apps that were not sourced by the company.[3]

The most successful IT professionals will be those that can leverage empathy skills in designing employee experiences. While IT may not always be designing the apps themselves, they play a critical role in how those apps are deployed, managed, secured, and experienced by the employees on their chosen devices. In a digital workspace culture, IT gains a more strategic role in business transformation. IT also moves from reactive to proactive in assisting the organization and its users to more effectively deliver what matters most to both.

[3] "THE IMPACT OF THE DIGITAL WORKFORCE," FORBES INSIGHTS, 2017.

For example, an IT team might observe that many of its users are actively using a cloud-based set of team collaboration tools like Slack. A traditional IT organization might simply shut the initiative down if it had not been authorized. But in a more user-centric culture, IT can step back and examine what's driving users to the new application. They can collaborate with proponents to deploy it more widely across the organization in a safe, compliant way.

In an increasingly crowd-sourced world, the best ideas no longer need to be restricted or come directly from IT. According to Forbes Insights, nearly one in four business apps are already brought to the company by employees themselves.[4] Corporate culture is already shifting toward a more open-minded approach, emphasizing learning and discovery to drive a better, more productive employee experience.

Security is Always Critical

Security considerations will always be important for technology teams that are adopting a digital workspace. Traditionally, most companies managed information risk at the network perimeter. They:

- Safeguarded assets and communication behind firewalls
- Employed standardized hardware and approved images and patches
- Mitigated risk with antivirus and malware apps that required frequent updates

Anything outside the firewall required brute force security and cumbersome measures like clumsy VPNs, two-factor authentication or token requirements, which could hamper productivity and degrade the user experience. However, these perimeter-based approaches are no longer effective within the framework of a digital workspace.

A better approach to enhancing security is by delivering a better user experience with policy-driven application access controls enabled by the digital workspace and identity management capabilities. Identity management helps organizations remove the friction of access so employees can get work done in real time from any device or location, without jeopardizing security. It provides users with a single repository to access all business apps, optimized by device type. One-touch mobile and simple self-service onboarding make the solution convenient and easy to use. Single sign-on (SSO) minimize friction and makes the user experience convenient and intuitive. An intuitive, frictionless approach means users will be less motivated to sidestep security and reduce the overall integrity of the network and its data.

A digital workspace lets IT, users, HR, business units, and other key stakeholders work together to define security levels and safeguard assets and data. Security can be based on the sensitivity of data, user roles, and other factors, instead of employing a one-size-fits-all approach. Organizations can tailor granular access policies based on network location, geographic location, or specific users and applications. They can keep highly sensitive data and information off limits using policies based on device type or type of network connection. With a digital workspace, organizations can establish the control they need to ensure consistent compliance, without compromising the user experience.

[4] "THE IMPACT OF THE DIGITAL WORKFORCE," FORBES INSIGHTS, 2017.

For example, when the WannaCry ransomware attack emerged in Spring 2017, Microsoft quickly discovered the vulnerability, issued bulletins, and released software patches for Windows OS to mitigate the issue. However, distributing these patches to users depended on devices logged in at the correct domain or at least connecting via VPN. Blocking devices that did not yet have the patch would be ineffective, because it would prevent most users from connecting. Even communicating mitigation instructions to users would be difficult. Under a digital workspace environment, any user connecting to the Internet could receive an automatic patch via cloud-based tools, whether they logged into the correct domain or not. Their device would remain compliant, and their entire organization more secure. No device could be allowed to have access to any corporate resources unless it complied with policy, a policy that employees could easily comply with and get back to work.

Maintaining Both Employee Privacy and IT Control: No Longer an Oxymoron

A final consideration for deploying the digital workspace is the balancing act between employee privacy, and IT control. These questions aren't limited to bring-your-own-device (BYOD) initiatives. In our consumerized world, people increasingly do work on their personal devices, and handle personal business on their employee devices. Establishing ownership and control of data and equipment becomes difficult, especially if an employee is employing consumer cloud products and storing data in a variety of locations.

Instead of focusing on ownership of equipment, IT teams can do better by carefully defining compliance requirements for "trusted devices"—whether they are company-owned or employee-owned. Under a digital workspace, a company doesn't need to own a device in order to establish trust with the device. Establishing trust can be as simple as ensuring that each device has a strong unlock PIN or that it hasn't been jailbroken or hacked. What is most essential is that the device is deemed to be unique, commonly through a certificate, and is established to belong to a specific user.

Effective privacy control requires more than a static policy, but a digital "social contract" with employees, outlining the boundaries and ownership of data, applications, and their acceptable use. This contract, enabled through technology gives employees the best guarantee that their personal applications, data, and information will not be available to their company. And conversely, the company will always maintain control over their own intellectual property and information that resides on the device. Technology is merely a tool to enforce the contract, rather than the center of the privacy policy.

Digital privacy is an emerging, complex topic, so education plays a critical role in maintaining employee privacy. It's essential for organizations to continuously inform users about measures they can take to protect their own data, as well as company assets. This also helps strengthen transparency and mutual trust between companies and employees. It engages and enlists employees in a collaborative way to help improve security, rather than relying on traditional top-down directives from IT.

Taking the Next Step

The digital workspace has come of age, and organizations are rapidly embracing this strategy to keep pace with today's rapid changes.

The time is now to move toward a more user-centric approach to IT. As businesses consider the tremendous potential of the digital workspace, it's important to step back and reflect on the success of current implementations in terms of user adoption. A transformation of this scope is not only about technology, but should consider processes and culture as well.

The technology behind a digital workspace is impressive, but it's important not to lose sight that this approach is a dramatic transformation. Like any major transformation, it requires careful consideration and a well-planned strategy. For IT organizations that consider the impact on their engagement and company culture, the digital workspace holds limitless potential.

Like any journey, the path toward this new level of IT engagement begins with a first step.

GET STARTED

Learn more about developing a digital workspace strategy

Join Us Online:

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