WHITE PAPER–MARCH 2020

What's the Next Wave of Workspace Mobility in Your Organization?

Foundational digital workspace journey milestones

vmware®

Table of Contents

Executive Summary

For the past decade, enterprise mobility has been a critical component of any IT strategy, impacting both users and organizations, but the results have focused more on the organizational experience rather than the user experience. The first wave of workspace mobility enabled mobile email, along with some device and application management. In the second wave, organizations focused on employee productivity, bring-your-own-device (BYOD) policies, and promoting a "mobile-first" approach to developing and delivering applications to all devices.

Mobility introduces a more efficient device management model with significantly less operational overhead, but it also demands new forms of authentication and security. Most importantly, going forward, mobility will support the redesign of many existing business processes and the creation of new ones for workers who have never been equipped with any form of endpoint computing, including many frontline workers.

Although in many organizations, the second-wave initiatives are still underway, forces such as contextual awareness, virtual assistants, and immersive technologies are already driving a third wave of workspace mobility. This third wave will transform user identification, device management, business processes, and the breadth of user engagement.

So, if you think you are done with your mobile workspace strategy, think again.

Recommendations

To move forward in your digital workspace journey, assess what your organization has achieved through the first and second waves of mobility. To venture to the third wave requires

- Consistent enterprise mobility management processes and tools that embrace device and platform diversity. These processes and tools set the basis for unified endpoint management and ensure that you are ready to employ the next generation of devices, including those yet to come.
- A mobile-first approach to sourcing and developing applications.
- A holistic deployment approach for new and legacy applications to simplify your move to lighter-touch endpoint management and to shift from device provisioning to enrollment.

Next, plan how your organization can take advantage of the new wave of mobility, prioritizing the initiatives that are likely to deliver the most valuable business outcomes.

- Redesign and mobilize critical workflows to expand productivity.
- Transform and introduce work processes with wearables and immersive experiences.
- Ensure that your endpoint management and security support existing and emerging mobile work styles.

Ready to get started and learn more to bring the future of mobility closer?

Riding the Mobility Waves: What's Next

Workspace mobility has delivered value to enterprises in several ways. Employees can be productive at times and in places where they couldn't be productive before. Mobility promotes faster interactions and turnarounds. And it enables organizations to set increasingly consistent levels of management and security for their data.

The advent of mobility caught many IT departments unprepared. But then, organizations began to incorporate the mobile technology developments offered by the first two waves in an incremental fashion.

Figure 1: Catching the Workspace Mobility Waves.

The first wave of workspace mobility began with the broad adoption of mobile phones that had few capabilities beyond voice. Expensive personal digital assistants followed with a broader set of features, but they did not offer affordable and ubiquitous access to Wi-Fi or cellular networks. The appearance of business-class smartphones combined these features, but they were initially made available only to executives and VIPs. Mass-market adoption really began with the arrival of consumer-grade smartphones and their compelling user experience. Smartphones quickly became a standard tool for all workers, both as company-provided assets or, in many cases, as personal tools also used for work.

Mobile devices enabled users to access applications and data unconstrained by network, device, or location. The resulting flexibilities created a new expectation: access to corporate resources anywhere, anytime, and on any device. During this second wave of workspace mobility, enterprises realized the business value of mobility and began focusing on productivity "on the move." But at the same time, they confronted challenges that were completely new to IT: how to manage and secure enterprise data on mobile devices, understand and control mobile costs, and govern the blurring line between personal and work use of mobile devices.

Enterprises face at least four areas of growing maturity and ongoing evolution in workspace mobility.

Endpoint management

Initially, mobile management tools were weak and incomplete, but over time they evolved to provide sophisticated features, such as policies, configuration management, and a management overlay for mobile applications and content. Mobile management tools quickly advanced to support new platforms and mobile devices, such as smart watches, headsets, other wearables, and IoT devices. At the same time, the operating systems used on traditional computing devices evolved to embrace the lightweight management approaches of smartphones and tablets. Since the arrival of Windows 10, all mainstream operating systems, including macOS and Chrome OS, support this "modern management."

Bring your own device

By 2015, every company was eager to demonstrate that culturally and technically it could accommodate users' preferences and choices for devices and platforms through different ownership models. Some BYOD programs failed due to conflicting objectives, such as lowering TCO while attempting to increase user satisfaction. In other cases, BYOD led to skepticism and loss of trust because of intrusive tools that were perceived as undermining user privacy. The emphasis on alternative ownership of devices has since decreased, and many enterprises have shifted their focus toward tools and technologies that allow them to govern programs that respect the balance of corporate data security and user privacy. Examples of this include the ability to maintain separate work and personal profiles and letting employees protect their privacy by having full visibility of the data that organizations can see and access.

Management consistency

The proliferation of mobile devices and the launch of BYOD programs exposed inconsistencies in the way organizations secured data on different device types and with different ownership models. While applications and data are typically well managed and protected on corporate-owned computers, many enterprises initially adopted looser approaches for mobile devices. Some organizations did not adopt an official BYOD governance policy, jeopardizing efforts to protect corporate data. Other organizations pushed back on all types of BYOD programs. As a result, a "shadow IT" emerged to circumvent the restrictive policies, causing mainstream users to have a negative perception of IT.

The adoption of enterprise mobility management (EMM) stemmed the loss of enterprise control by enabling organizations to increase the level of consistency applied to different device types, although issues often resurface as new device categories enter the organization or new user groups access mobility. EMM led to a new corporate IT objective: establishing a unified endpoint management approach across all device categories, including those yet to arrive, through a common set of tools and skills.

Mobile-first approach

The explosion of mobile devices and apps made it clear that the workspace needed to be redesigned around a new access paradigm: any application from any device and any platform. This paradigm is the core of a mobile-first approach. New applications, including most productivity and communication tools, are now designed to be accessed from anywhere and through any device, often relying on only the most limited computing capabilities. Application design and development first focus on the lowest common denominator, that is, the performance and display constraints of mobile devices. Only then does development cater to devices with larger screens and more extensive processing and graphic capabilities.

For existing and legacy applications, many enterprises have adopted a holistic deployment approach that allows for remote delivery to any device through a virtual desktop infrastructure, remote hosts, or cloud-based services.

Workspace Mobility: The Third Wave

Although many of the first- and second-wave initiatives are still in progress, recent and upcoming developments are about to enable a third wave of workspace mobility. This wave will impact four areas: user identification, device management, business process transformation, and the breadth of user engagement. These areas have strong interdependencies with other key digital workspace journey milestones.

Mobile transforms security needs

With mobility, workspaces are no longer constrained by the enterprise's physical network, so new approaches to endpoint management and security are required. Employees now use many different device types, which are not always company owned, to run a variety of apps from different locations. The concept of zero trust has already emerged as work styles have evolved. Zero trust isn't a single technology or product but an IT approach that considers every user and every device to be untrusted until a number of factors have been verified. Only after verification is complete is access to corporate apps and data granted. Moreover, the requirement of verification is ongoing, rather than one time.

A number of technology developments are moving the zero trust architecture and designs to the fore, including biometrics, multifactor authentication, identity and access management, and strong conditional access engines. Modern platforms and operating systems also support more sophisticated approaches to verifying the integrity of a device. As a result, we expect zero trust to become a foundational component of digital workspace strategies, enabling new work styles through highly mobile workspaces while also improving the employee experience.

Zero trust does introduce complexities to workspace design and technology selection, requiring an even more coordinated effort across the IT teams responsible for networking, security, devices, and access. It also requires strong governance, because success depends on a consistent approach to both existing and new applications.

Mobility drives unified endpoint management

Establishing a unified endpoint management approach across all device categories brings about organizational and cultural changes, not just technological ones. After technological changes have been implemented, existing mobile and desktop computing teams start to merge, bringing together different levels of management overhead and asset lifecycles.

Computer management typically requires one full-time equivalent (FTE) to support every 250 users, and equipment replacement cycles are relatively slow, usually between 3 and 5 years. In contrast, when managing mobile devices, one FTE can support 2,000–5,000 users, even with much faster refresh cycles of 18–24 months. Because most existing processes used with desktop devices will need to be replaced with more lightweight processes, some IT professionals will see their job functions and responsibilities change, which could require careful change management. This transition must be carefully managed to avoid the risk of compromising costs and TCO—by extending old computer management principles to mobile and new enterprise devices—or functionality by reducing the set of capabilities available to employees. In the longer term, the newly formed endpoint team will need to at least partially integrate with the teams managing applications and access, bringing more change management challenges.

Mobility requires redesigning workflows into mobile flows

Unleashing productivity has been and continues to be the greatest promise of workspace mobility projects. It is already possible to pack a miniature workspace with services, data, and applications onto a mobile device. However, many business applications were designed for larger screens, presenting a much-compromised user experience for employees on the go. This impediment relegates the completion of some tasks to fixed and often specific locations, such as the office. It also often obliges employees to postpone tasks until they get back to their computers, resulting in batch-mode rather than real-time activity.

A truly mobile and contextual workspace delivers key workflows and business application functions wherever the user is. With minimal code development, organizations can look for opportunities to reuse and recombine existing business processes and present them through a new mobile front end. The ability to present notifications and to enable progress or completion of simple tasks, such as approvals, on mobile devices can reduce latency for many workflows. Most current-generation business applications expose APIs and the data required to enable selected user actions, so they are already well suited to mobile use. Identifying and prioritizing workflows that can benefit from being mobilized usually requires the collaborative effort of employees, line of business leaders, and HR.

Mobility expands opportunities for immersive experiences

While most think of wearables as entertainment devices, they are becoming workplace tools for many non-office workers. The intersection between wearables, immersive technologies, and IoT creates the potential to serve new user constituencies. These tools can increase safety in the workspace, accelerate task completion, decrease error rates, and reduce onboarding time for new hires.

In collaboration with HR and business units, IT and the digital team should assess and prioritize opportunities for new and improved workflows. Projects centered on wearables and immersive technologies should start small, with a minimum viable product approach, because technology is still in flux. Broadly available platforms and SDKs are currently the most viable choices. They reduce the risk of vendor lock in and leverage management tools and skills that are most likely already available to the organization. It is also important to carefully assess the ramifications of embracing these approaches, including legal, health, and security.

Riding the Waves

The outcomes gained from the first and second waves of mobility have been to some extent linear, delivering incremental features and capabilities to employees across all types of organizations. Many projects are still ongoing, and mobile and endpoint computing leaders must identify the dependencies that these projects create in the digital workspace. An effective mobile-first approach requires strong governance and a consistent implementation of the mobility vision and these management principles:

- Extend EMM deployments to all relevant use cases across existing and emerging categories of mobile devices to avoid inconsistencies in data and app management across device types and ownership models.
- Clearly define employees' and IT's responsibilities for managing and securing corporate information when using personal devices for work.
- Drive consensus for adopting a mobile-first vision when sourcing and developing end-user software across the organization.
- Implement a consistent approach to deliver legacy, computer-based applications via the data center or cloud to achieve ubiquitous access.

In contrast, the upcoming third wave of mobility will deliver transformational business value, but these changes will not be incremental, impacting organizations in different ways. Success hinges on both technical and on nontechnical factors, including how established processes and organizational changes are managed:

- Pursuing a zero trust strategy and implementing new identity access management principles require cross-collaboration between security, application, and device management teams. Clear and firm governance is also needed to achieve adherence from the entire organization.
- Moving from separate mobility management suites and client management tools to a unified endpoint management model requires redesigning processes for managing devices and application provisioning to not compromise end-user capabilities and productivity. Do not underestimate cultural and organizational challenges, and carefully manage changes to IT personnel's roles, responsibilities, and objectives.
- Redesigning work processes into mobile flows requires collaboration between IT, business units, and HR to identify opportunities for workflow adaptation and understand the value and feasibility of the proposed changes.
- The deployment of wearables and immersive technologies to address new use cases within the organization is likely to require technical and nontechnical skills that organizations might not have in-house. When evaluating these projects, consider all ramifications, including legal, health, security, and privacy.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Item No: FY20-5770-WORKSPACE-NEXT-WAVE-MOBILITY-WP-USLET-WEB-20200310 3/20