LEARNING MADE EASY

Anywhere Workspace

for dummies®
A Wiley Brand

VMware Special Edition

Supporting a distributed workforce — including frontline, hybrid, and remote workers — has become a global imperative, essential to business continuity and success. More and more employees want to have the flexibility of working from anywhere, and employers are finding that providing that option simplifies recruiting, reduces their overhead costs, and increases innovation, inclusion, and empowerment. Many traditional organizations have had some fears about loss of productivity, but studies are showing that remote work actually *increases* productivity in many cases. Employees report less stress, better work–life balance, and higher overall satisfaction, which leads to higher retention rates. So, it's turning out to be a win-win.

But even though an "anywhere" environment has the potential to be a huge win-win for employees and employers alike, it doesn't just happen automatically. A company can't just send its workers home with laptops and virtual private network (VPN) credentials and expect business to continue as usual. It needs much more than that, in order to deliver that user experience and ensure that the employees are productive and at the same time ensure that the IT departments can support them. Remote and hybrid workers — and the IT departments that support them — need some specific tools and procedures.

Some companies don't have the systems and processes needed to support employees working remotely, and instead of making the investment, they try to get by on legacy technologies and point solutions. That's a big mistake. Traditional IT environments and software management solutions are not designed to support a distributed workforce; they're built around corporate networks and data centers. Traditional remote worker support structures such as VPNs worked fine when a limited number of people were using them, but they aren't practical for enterprise-wide use because they aren't scalable. Without an integrated IT management system that offers features like rapid device setup and onboarding, solution scaling, remote support, and robust security, supporting a distributed workforce can be complex and chaotic.

In many organizations, there are three critical technology issues that prevent distributed workforce success:

- **Operational complexity:** Trying to juggle all the different devices, connections, and apps that a diverse workforce needs can be so complicated that both your IT staff and the systems they support can suffer.
- **Fragmented security:** Maintaining separate security systems for multiple silos makes it difficult to deliver security that protects effectively without getting in the way of productivity.
- **Poor user experience:** Often, the employee experience provided by existing tools is not satisfactory. This wastes people's time, causes them frustration, and often drives them to attempt a workaround that compromises security.

On top of those challenges, organizations must have the flexibility to support a distributed workforce. They are categorized into three use cases:

- **Frontline workers:** Workers who are doing physical things, like taking care of people, making deliveries, and repairing equipment, make up the majority of the global workforce. They can be found across essential and nonessential industries, including retail, health care, and supply chain sectors. Frontline workers have different technology requirements than desk-based employees do, and they need solutions that are optimized to support the mission-critical devices and apps they rely on.

Anywhere Workspace is designed to optimize frontline worker efficiency and enable them to access corporate data securely and easily. From delivery drivers to warehouse workers, store associates, and nurses, frontline workers need an intelligence-driven platform built to support complex, mission-critical device deployments at scale.

- **Hybrid workers:** Today's "office workers" are not necessarily in an office building every workday. Often, they get the job done from remote locations that can include private homes, local coffee shops, and even travel destinations. With today's fast, reliable Internet connections, "on the job" can be anywhere, on any device.

  Anywhere Workspace empowers these hybrid workers to get access to the applications securely, wherever they might be hosted, on-premises or in the cloud. It delivers the end-to-end Zero Trust security that a hybrid worker needs — endpoint security, secure access and protecting the apps from any security threats.

- **Remote workers:** Many organizations are moving to at-home call centers and deploying seasonal workers and consultants to scale up the workforce. These workers need a modern platform for secure delivery of virtual desktops and applications across public and private clouds.

With a modern multi-cloud approach, Anywhere Workspace delivers a secure virtual desktop infrastructure (VDI) solution that prevents data loss and isolates device issues by utilizing best-in-class virtual desktops and apps.

In this paper, you'll learn about the key capabilities required across all types of user profiles (frontline, hybrid, and remote) to build into your IT strategy and make your organization more resilient, flexible, and better prepared for future challenges.

Delivering Exceptional User Experiences
Let's face it: If lines of business, teams, and individuals believe that IT gets in the way and isn't efficient, employees will avoid adopting the tools and services designed to protect them.

IT must design and deliver an engaging employee experience to improve productivity and security in the distributed workforce. This experience must account for the different devices and form factors employees use throughout the day and the locations from which they need to work. It must also provide a level of flexibility and choice that will keep up with the demands of employees and departments.

For example, when it comes to retaining frontline workers, some industries experience 50 percent to 100 percent turnover. Employee disengagement is the number-one cause of turnover, and the biggest culprit of employee disengagement is technology. You need to deliver seamless, consumer-like end-user experiences across shared devices by giving workers access to only the apps, content, and settings they need to stay productive and engaged. With frontline workers, having easily customizable multiuser device user interfaces (UIs), configuring devices in single or multi-app mode, and enabling multiuser devices with check-in and check-out exponentially improve user experience.

Here are some make-or-break facets of user experience:

- **Remotely onboarding new employees**: To make the onboarding experience a positive one, you need a touchless and seamless remote onboarding experience. Unified endpoint management (UEM) enables your IT organization to introduce rapid, automatic, self-service, and on-demand capabilities for first-time setup. Instead of going through an expensive onboarding process, you can do a simpler and cheaper provisioning that minimizes a lot of pre-employee-handover steps. You can push out all the necessary configurations and software via a secure connection to any Wi-Fi network, wherever the employee happens to be.

- **Providing seamless access to apps:** Software distribution is an ever-growing challenge for your IT organization. Every year, you need to distribute more software and more updates to more endpoints and more types of devices. And you need to do it all quickly to keep operating systems and apps up to date. A UEM solution helps you streamline the process of getting the right software on your end-user devices.
- **Supporting flexible user choices:** Supporting your employees' preferred devices is increasingly important. The keys to delivering an exceptional user performance on a choice of devices includes supporting both bring-your-own-device (BYOD) and corporate devices on a single platform and eliminating back and forth between multiple apps by providing personalized workflows.
- **Enabling self-service support:** The distributed workforce must be more self-reliant because employees working from home are more physically isolated from their peers. Organizations can enable robust self-service support capabilities that include virtual assistants, remote support, and self-service password reset.
- **Reducing password proliferation:** From the user's perspective, reducing the burden of managing multiple accounts and passwords is critical to employee experience. From an IT support perspective, you reduce the burden of unlocking user accounts and resetting forgotten passwords. By implementing technologies and capabilities such as password-free authentication, single sign-on (SSO), multifactor authentication (MFA), and conditional access, organizations not only reduce user friction but also improve their IT service management.

These are all make or break employee experience (EX) requirements for all types of users.

Equipping IT for Success

To provide those exceptional user experiences, you must equip your IT department for success. They need a unified system for managing all the endpoints (that is, the end-user devices), no matter what kind of devices they are and where they're located. A UEM system is a key part of any digital workspace strategy. It provides a digital workspace platform that combines the efficiency of mobile device management (MDM) and the full breadth of desktop management capabilities.

With a digital workspace approach, your IT organization can securely deliver and manage any app on any device by integrating access control, application management, and multi-platform endpoint management. The digital workspace platform collapses the silos between desktop management, MDM, and application management to enable all devices and applications to be managed holistically from a single pane of glass. It enables you to take a consistent approach to managing and securing all your user endpoints and all the apps and data associated with them in a single, unified management platform.

Some key capabilities of an effective UEM include the following:

- **Unified control point management and governance:** UEM eliminates the need to use a hodgepodge of point solutions to manage mobile, desktop, and Internet of Things (IoT) devices. With a comprehensive UEM solution, you can use a single platform to manage every device and every operating system, across any use case, with a consistent set of policies.

- **Performance and experience management:** UEM can help address the issues of top importance to users: easy access to applications and data, device choice, collaborative and meaningful work, and flexible work options.

- **Cloud-native management:** Digital infrastructures are central to driving successful business outcomes, and cloud adoption is how organizations standardize platforms and reduce time to market. By taking a modern, cloud-based approach to the unified management of endpoints and business processes, organizations can standardize and automate operations across multiple platforms, as well as improve efficiency and innovation.

- **Analytics:** The core power of UEM can be extended with a consolidated pool of data and analytics tools that enable smarter endpoint management. This next-generation approach gives your IT team the ability to leverage data captured from across the digital workspace environment — from the device to the apps to the identity of each user — to gain deep insights into what's really going on across your distributed workforce.

- **Automation:** With visibility and analytics, you can build automation and orchestration. You need a platform that will allow you to collect contextual information from across the entire environment. This contextual awareness feeds intelligence, allowing you to make just-in-time decisions and use automation for threat remediation.

- **Compliance:** Conventional approaches to asset management and reporting don't usually provide on-demand visibility into the installed updates on end-user systems. A modern management platform, on the other hand, provides patch intelligence and reporting that helps you stay on top of your information security requirements.

Anywhere Access to Virtual Desktops and Apps

Today's distributed workforce technologies are often characterized by diverse and untrusted devices, multiple operating systems, and a wide array of consumer-oriented applications. All of that creates a chaotic end-user computing environment that's difficult to support and secure. To regain some order and control, organizations must change the way they deliver, manage, provision, and enable desktops and applications.

Modern web and cloud delivery models avoid these distributed issues by pushing application execution and integration back to the data center or cloud, where applications and data are centrally managed and maintained. Dependencies on device and operating system (OS) type are removed from the management equation.

The most common approach to centralizing a full desktop environment is virtual desktop infrastructure (VDI). VDI leverages server virtualization so that instances of client operating systems (such as Windows 10 or 11) can be launched and run in their own virtual machines and then remotely delivered to users. In contrast, with Remote Desktop Services (RDS), applications are installed and configured on a Windows Server OS (instead of a client OS) in a multiuser environment, so that multiple users can simultaneously access the application remotely. Like VDI, RDS is a remote solution that alleviates the need for local execution of applications on an end-user device. It's not uncommon for organizations to use both VDI and RDS, depending on user needs and application requirements.

Especially for remote workers, VDI capabilities are critical to maintaining business continuity. Take call center agents or remote contractors, for instance: organizations need to ensure these remote users leverage existing on-premises and cloud information to securely deliver remote desktops and applications. When each virtual PC is entirely autonomous, the agents' work environment will remain consistent and connected. Plus, each agent's system will be customized based on the role, group, or campaign wherever they're located.

Ensuring Effective Identity and Access Management

Users today access enterprise and productivity applications through a variety of mobile devices, laptops, and desktop PCs. These applications may be installed on the devices themselves or in the data center, or cloud. IT doesn't necessarily manage all these applications; they may be installed and maintained by the users themselves or managed by line-of-business or non-IT operational teams.

To support every possible environment, most organizations have embraced a multimodal style of end-user computing that enables any user to potentially work with any application, on any device, and any infrastructure. Although this approach is beneficial in terms of productivity and user engagement, it introduces other challenges, including gaps in employee experience, complexity in access procedures, and exposure to new risks and issues.

Identity and access management (IAM) technology is a key means of supporting this “any-to-any” approach. IAM simplifies the employee experience and enables users to access the applications they need in a way that is secure, reliable, and easy to use. IAM is the system that an organization uses to manage access to its applications and content.

With modern management, organizations can ensure cloud-native, simplified IT operations, secure their endpoints, and enhance the employee experience from all devices. IT can easily access preconfigured lists of identities and roles, and hybrid users can save time with remote support, user self-service options, and zero-touch recovery to protect sensitive data.

IAM includes the policies and technologies that enable an organization to manage the digital identity and access permissions of its users. IAM provides the following functions:

- **Identity management:** The creation, management, and deletion of identities associated with users
- **User credentials**: User ID and password or credentialed access to applications, devices, and services
- **Unified access:** A system that allows a user to authenticate once to a range of applications and services without necessarily knowing their login credentials for each application or service, similar to SSO

Implementing Zero Trust Security

Traditional approaches to endpoint security are typically based on reactive tools, such as antivirus and malware detection. VPNs, encryption, and group policies provide additional layers of protection for users and devices.

Under modern management, there’s a new shift toward security. The solution now has the ability to proactively prevent, detect, remediate, and react to new and existing threats faster. With the inclusion of the latest AI/ML technologies, the device is able to sync with the latest threat databases to prevent attacks in real time. To achieve this, security teams need to embrace a holistic security approach that links to all the components in use — user, device, operating system, network, application, and context — at any given time.

Zero Trust is a key to modern endpoint security in a distributed environment where network perimeters have all but disappeared. It mandates a data- and identity-centric model based on the concept of "never trust, always verify."

The Zero Trust approach ensures that the users and devices are verified, authenticated, and authorized before giving remote access to the applications in the corporate network. The security posture of the user and devices are continuously verified, the network is secured and optimized, and finally the user is provided access to the applications wherever they may be hosted — on-premises or in the cloud.

Hybrid and remote employees in the distributed workforce are accessing applications from practically anywhere — in the office, at home, or in a coffee shop. Zero Trust means not inherently trusting your users, devices, or applications simply because they're "on the corporate network."

Bringing It All Together

The key to successfully managing a distributed workforce is having the right IT tools and technologies in place to ensure scalability, automation, robust security, and a great user experience for all frontline, hybrid, and remote workers.

Instead of a patchwork solution to support hybrid work, you need one that's integrated and unified. The VMware Anywhere Workspace Platform addresses end-user, IT, and security challenges by providing exceptional multi-modal employee experiences, enabling automated workspace management, and securing the distributed edge. The solution takes a holistic approach combining industry-leading digital workspace and security technologies, working harmoniously across any application on any cloud to any device by any user. From frontline workers to hybrid workers to remote workers, Anywhere Workspace Platform provides seamless experiences at any place, at any time.

VMware Anywhere Workspace Platform extends UEM, VDI, and a single app catalog experience with new capabilities around ZTNA, mobile threat detection, endpoint detection and response, SaaS app management, and enhanced digital employee experience. By integrating these industry-leading technologies into a single platform, Anywhere Workspace Platform enables a comprehensive view, avoids the management complexities and blind spots created by fragmented offerings, and enables security that doesn't come at the expense of experience and productivity.

For more information about VMware Anywhere Workspace Platform, check out the following:

- **Modern Management ROI Calculator Tool**: https://pathfinder.vmware.com/activity/save_with_work-space_one
- **Anywhere Workspace Solutions:** https://www.vmware.com/solutions/anywhere-workspace.html

For Dummies is a trademark of John Wiley & Sons, Inc. ISBN: 978-1-394-15387-9