WHITE PAPER–MARCH 2020

Key Considerations to Supporting Work-at-Home Directives for Business Continuity

vmware®

Table of contents

Extraordinary events have the potential to change company culture faster than any other action. A natural disaster or pandemic, for example, prompts organizations to quickly review or put in place new, out-of-office work processes and technologies to reduce employee productivity losses when self-, executive-, or government-mandated employee isolation is necessary.

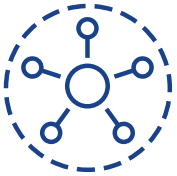
There's no silver bullet for changing employee experience when a disruption occurs. Yet organizations can make progress today that will improve how their employees work from home while accelerating enterprise-wide, remote-first goals with a digital workspace strategy.

Five IT Principles Driving Employee Experience

The steps leadership takes now to boost digital employee experience can quickly become the foundation for digital business or mission advantage later. That's if IT and executive teams understand and agree on some basic, not necessarily new, principles:

What applications employees need

Where key applications and data reside



How employees currently (and will be expected to) access work resources

How leadership and employees currently (and will be expected to) communicate and collaborate

What help employees will have available if and when issues arise

Knowing what applications employees need

Applications drive modern business—from customer experience to supply chain operations. While many knowledge workers—those primarily working regular hours, from traditional office locations—may be well positioned for remote work because they primarily use popular productivity applications, others are not.

Desk-less employee populations, those in case work or hospitality, clinicians and technicians, for example, may report somewhere before moving throughout their days to accomplish tasks. If employees are mandated to work from home beyond a week or two, will the critical applications other than email that they require be accessible from everywhere without incurring risk to the business? Making a list and understanding the impact of each application's use beyond the corporate network is imperative for both business and IT leaders.

Knowing where key applications and data reside

With a list of applications that each department or group considers mission critical in hand, IT staff can begin to assess where each application and its data reside—on premises in a corporate data center or in a private or public cloud—and all of the dependencies. For example, traditional client-server, .NET, and Java applications are often tethered to corporate networks for data and are highly dependent on client configurations. In contrast, internal, browser-based applications have client-device portability, yet still rely on corporate network app servers for delivery. Most flexible, SaaS applications simplify delivery because there's no dependency on the corporate network—unless IT has already-established access controls that require devices to be on the corporate network to access them.

Knowing which devices will connect (corporate-owned, personal, or both)

Only after knowing what applications employees need and where data resides can IT and business leaders effectively strategize about what devices can and should be permitted to connect into the enterprise, and how. Corporate-owned laptops are often pre-provisioned with VPN connections to allow for mobility and application portability.

Yet if those devices leave the corporate network for extended periods of time, how will IT support management updates, patching, and policies that reduce enterprise risk? And how should IT think about scenarios where it's too late to provision new laptops and employees are forced to connect with personal devices—from smartphones and iPads, workstations and PCs—running a variety of operating systems and unsupported software? Knowing that devices might be exposed to malicious Internet attacks and then reintroduced to the corporate network is a headache that IT teams can prepare to prevent.

Understanding organizational collaboration and communication

In industries like information technology and increasingly financial services where an organization's executives and knowledge-workers may already be accustomed to engaging with staff, colleagues, customers, and partners through online channels—from video conferencing to email and instant messaging—interruptions may be minimal. However, when the need arises for the organization and all of its employees (e.g., sales, tellers, maintenance, etc.) to collaborate and communicate more extensively or all the time through software, downtime can occur as executive staff, department heads, and individuals take time to become familiar with new ways of working.

To minimize disruption, IT and executive leaders must come together quickly when a workforce is suddenly more distributed than ever to document the many ways day-to-day communications happen at jobsites, in banks, clinics, and elsewhere before being able to introduce new virtual workflows and processes to support working remotely.

Recognizing support will be an issue

Among the biggest work-from-home unknowns is what level of support employees will need, with which apps and from what devices, at what places and what times. IT and business leaders or teams can map current processes to discover the biggest gaps and work to close them before further disruption. This includes reviewing remote support ticketing options, self-service opportunities, staffing, and more.

In tight talent markets, employees have options and providing a powerful work-at-home experience is a differentiator. *Recent survey results* reveal 73 percent of employees and HR decision-makers agree flexibility of tools (e.g., technology, apps, and devices) that they might need to use for work would influence their decision to apply or accept a position at a company.[1]

Empower Your Employees to Work from Home with VMware Solutions

In today's application-centric businesses, solving for each device, application, compliance rule, identity, and authorization is too difficult in the best of times, let alone in a crisis. IT teams have never been staffed, budgeted, nor incented to sort through the various combinations of clients, connections, compliance issues, application types, and authentications to ensure they all work. This situation has been acceptable until now because most employees working within the corporate network—with a domain login to a trusted computer and working email onsite and off-site—were satisfied. When every employee has to work remotely, that assumption may no longer be valid.

"This is an opportunity to take a good look at what you and your company are and aren't good at when it comes to communication and productivity."[2]

— TECHCRUNCH

The current workforce realizes enterprise IT environments are complex. Yet as disruptive periods occur with more regularity, talented employees will begin inquiring about employee experience more often. That's why organizations seeking to successfully deliver optimal employee experience—with less risk when staff is mandated to work from home—are choosing the VMware digital workspace.

The end-to-end platform, powered by VMware Workspace ONE® integrates access control, application management, and multiplatform endpoint management to deliver a consistent, unified workspace across any computing environment.

Bridge access to all apps across devices and networks

Enterprise business and IT leaders can count on the Workspace ONE platform to bridge access to all applications, across devices and networks, boosting three key initiatives:

- IT modernization
- Employee engagement
- Zero-trust security

Device management

Through Workspace ONE, enterprise IT staff can register any device—laptop, tablet, smartphone, desktop PC or Mac—requiring access to corporate resources and continuously monitor it with intelligent insights and automation. The solution enables device health by aggregating and correlating device, app, and user data while identifying opportunities to reduce IT cost, improve security, and optimize experience.

For organizations with corporate-managed devices for employees working from home, the solution saves IT administration time by quickly understanding the complete state of each device and managing it from the cloud anywhere the device connects to the Internet. For employees working from home using personal devices, such as smartphones and tablets, Workspace ONE simplifies IT management, enabling IT to isolate corporate information from personal apps while applying minimal conditional access rules to keep corporate resources protected.

1 Vanson Bourne. "The Digital Employee Experience." May 2019.

2 TechCrunch. *"How to work during a pandemic."* Devin Coldeway, March 2020.

Enterprises using the VMware digital workspace can drive consistent processes and policies across iOS, Android, Windows 10, macOS, Chrome OS, and more—wherever workers use their devices. It features a real-time, cloud-based approach to complement or replace legacy product cost and lifecycle management.

The comprehensive VMware platform has multiple zero-touch options for mobile, macOS, and Windows 10 PCs so IT teams can simply onboard new devices and users. It supports over-the-air configuration, policies, patches, and updates through automated policies. IT teams can easily entitle, provision, and deploy apps across devices and prevent data loss. They can distribute apps—even large Win32 apps—efficiently over the air or with peer-to-peer distribution. And with Workspace ONE® Assist, IT and help desk staff can troubleshoot and resolve Android, iOS, macOS, and Windows device issues in real time through both remote management and remote takeover capabilities.

Hiring doesn't have to stop during mandated work-from-home periods. A unique feature of the VMware digital workspace is the capability IT staff has to drop-ship cloud-provisioned laptops directly to new hires working remotely, enabling compliance.

Employee engagement services

Workspace ONE improves employee experience for prospects, new hires, and long-time talent mandated to work from home. The single-destination Workspace ONE® Intelligent Hub provides workers with unified and automated onboarding workflows, an updated application catalog, and access to Hub services. The Intelligent Hub app also delivers native apps for installation.

The following Hub services promote an intrinsically secure, consistent, cross-platform experience for individuals and the company to communicate and collaborate:

- **VMware Workspace ONE® Notifications** – Provides IT-administered push and in-app notifications with custom data or connections to third-party business systems with VMware Workspace ONE® Mobile Flows.™
- **VMware Workspace ONE® Catalog** – Empowers employees to view, launch, and install all application types (e.g., web, SaaS, virtual, and cloud-native) with single sign-on (SSO), no matter what device they use for work.
- **VMware Workspace ONE® People** – Enables workers to quickly look up colleagues via an employee directory; includes organization chart with name, email, phone, and search.
- **VMware Workspace ONE® Home** – Gives employees access to company resources by embedding an intranet or company portal.
- **VMware Workspace ONE® Assist** – Providers workers with access to frequently asked questions (FAQs) and knowledgebase (KB) articles to solve issues independently, so they can continue to be productive. A virtual digital assistant, or chatbot, embedded in the Intelligent Hub app also provides rapid answers, helping IT teams speed resolution when employees working away from the office have questions.

Virtual desktop and app delivery

Vital to any digital workspace solution driving a remote-first strategy is support for cross dependencies between local Windows applications still residing on many enterprise systems. Workspace ONE with VMware Horizon® Service can resolve conflicts when applications require specific configurations, browsers, plug-ins, and more, particularly where there are known issues with application interactions.

Workspace ONE with Horizon Service also supports the mission-critical networking requirements of highly regulated industries, such as healthcare and government. Virtual desktop infrastructure (VDI) using virtual desktops as proxies enables complete isolation of client endpoints—preventing devices and their applications from ever touching the corporate network.

If an organization typically provides workers with laptops, VDI permits remote access from any bring-your-own device with a browser. It spans on-premises data centers and cloud environments, providing these integrations and turnkey benefits:

- **On premises** – IT teams using the VMware digital workspace platform with existing virtual infrastructure and capacity can simply add existing VDI resources through VMware cloud orchestration and hyperconverged infrastructure such as VMware Cloud Foundation,™ powered by Dell EMC VxRail.
- **Hybrid and multi-cloud** – IT teams using the VMware digital workspace platform without capacity can quickly stand up new virtual desktops via VMware Horizon® Cloud on Azure, or VMware Horizon® 7 on VMware Cloud™ on AWS, even taking advantage of a free trial to quickly assess capabilities.
- **Remote access to physical PCs** – IT teams using the VMware digital workspace platform can set up remote access to physical Windows 10 PCs that must stay within the corporate office or perimeter, enabling remote work to continue from anywhere.

Access services

Security threats are always top-of-mind for IT and business leaders, and can add to the uncertainty of confidently asking employees to work from home. Even with reliable VPN technology, IT staff is concerned about sorting out access and authentication complexity.

Workspace ONE simplifies embracing zero-trust access control. Cloud-based VMware Access Services provide SSO authentication with built-in or support for existing multi-factor authentication (MFA). The platform also seamlessly integrates with existing cloud identity technologies such as Okta.

Enterprise IT teams can remain confident that their applications and data are protected using a single appliance to bridge on-premises resources through conditional access policies for everything from Microsoft SharePoint and file shares to intranet sites and internal APIs to virtual desktops and applications (e.g., Horizon and Citrix).

Endpoint security

All-employee work-from-home directives are less intimidating to IT teams managing devices with the VMware digital workspace because the platform continuously tracks device state, user details, and authentication context to determine user and device risk. It also automatically allows or denies access, and requires MFA or a remediation for access.

Moreover, IT staff can enforce a desired state for all corporate-issued devices, or assert a minimal state of compliance for each application or connection to sensitive resources. As part of conditional access capabilities, Workspace ONE establishes and maintains policies across identity, device, and application scenarios. Advanced risk analytics detects anomalies that might indicate malicious intent.

The platform is ideal for threat response, too; for example, remediating should employees working from home get caught in a phishing expedition identified through VMware Carbon Black EDR. The platform's automated threat response quarantines users or devices that present heightened risk. And to further protect applications and data, the VMware platform secures data transport, providing a per-app VPN that limits exposure to internal resources by reducing access to specific internal resources.

Build an Intentionally Remote-First Work Strategy

Because there's no stopping Mother Nature and most disruptions are unexpected, enterprises must start preparing now for the next worst-case scenario by intentionally building a remote-first work strategy and digital workspace environment that seamlessly supports their employees, the business, and IT.

No matter where and when they happen, work-from-home directives are shocking to corporate cultures. Organizations already in the process of shifting greater accountability to employees and evolving to outcome-based results may encounter less friction as teams are forced to adapt.

For any organization not yet fully prepared, now is the time to take advantage of shifting mindsets and budget allocations to meet work-from-home expectations today and tomorrow. For teams to rethink security from the inside out and to ensure distributed employees have easy, on-demand access to all the apps and data they need for greater collaboration and productivity—from wherever, whenever they're mandated to work.

To learn more about how VMware supports work-at-home directives impacting business continuity, visit *our Business Continuity site*.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Item No: FY20-5807-BC-GUIDE-WP-WEB-USLET-20200316 3/20