

# Blueprint for a Future-Ready Healthcare Workforce

A 3-Stage Approach for Adopting  
Modern Management and Security



Table of contents

How IT adapts in times of change.....3

Journey to a Future-Ready workspace on your Windows 10 PCs .....3

Modern management enables faster adaptation..... 4

**Phase 1: Respond**

Focus on the immediate needs of employees..... 5

With modern management, you can: ..... 5

- 1. Onboard employees faster by drop-shipping devices
- 2. Give employees fast, simple access to apps they need for work

**Phase 2: Adapt**

Manage and secure your device fleet more effectively ..... 6

Modern management helps you create a solid foundation for Windows Anywhere with the ability to: ..... 6

- 1. Quickly apply policies over-the-air without any network dependencies
- 2. Provide remote support for uninterrupted productivity
- 3. Achieve best-in-class modern management for Windows 10
- 4. Optimize security across endpoints and applications

Integrate management and security .....7

**Phase 3: Accelerate**

Achieve ongoing transformation ..... 8

- 1. Develop a long-term initiative to cultivate employee experience
- 2. Seize opportunities to accelerate security initiatives

What does a Future-Ready Workforce mean for IT? ..... 9

A digital workspace platform that grows with you ..... 9

### How IT adapts in times of change

When global events caused healthcare organizations to make a rapid pivot to more remote work, IT had no choice but to act fast. No matter where they were on the path to digital transformation, IT organizations across the healthcare industry were responsible for onboarding a large number of employees onto new devices, managing a bigger population of distributed users, and keeping them all connected and secure.

For teams still using traditional PC lifecycle management methods on their Windows devices, these new demands quickly became a massive headache—making it clear that a legacy approach is no longer adequate. IT teams taking a modern, cloud-native approach for managing their Windows 10 PCs find themselves in a better position to meet changing workspace demands.

### Journey to a Future-Ready workspace on your Windows 10 PCs

The transition to modern management often happens in stages. This diagram provides a snapshot of three phases that are common across healthcare IT teams moving toward digital transformation. Your journey can be a gradual one, from addressing urgent needs to making progress toward longer-term goals.

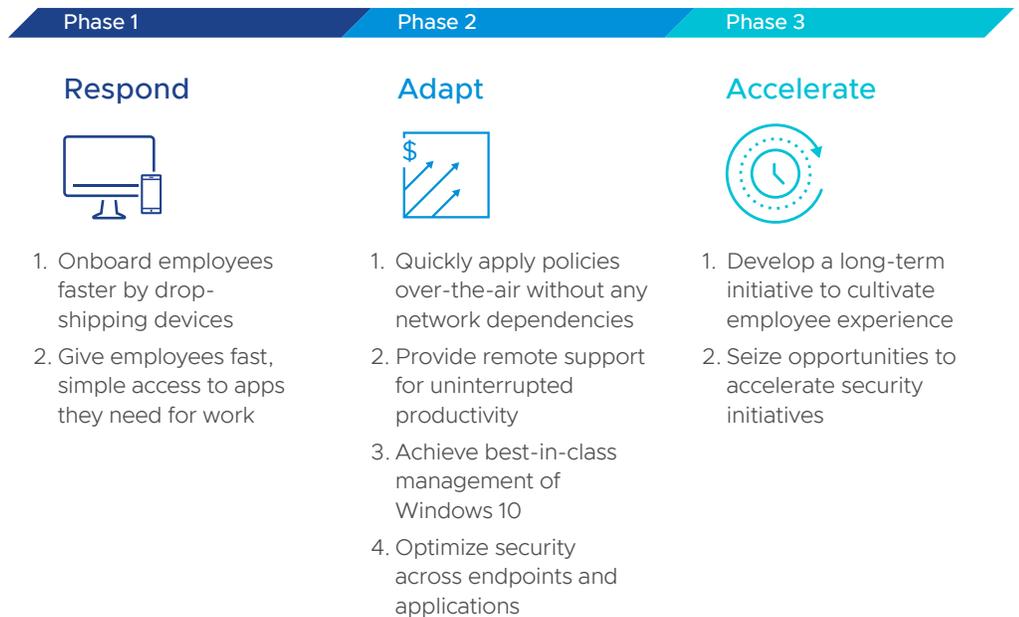


### Modern management enables faster adaptation

When remote work was limited to a fraction of the employee population, most healthcare IT teams treated it as an exception. But instantly widened adoption quickly revealed inadequacies and gaps in infrastructure, support, and security—along with rapidly escalating costs. It also revealed how much employee experience can fluctuate amid changing workplace conditions, and how critical good experiences are to keeping the organization moving forward.

Windows 10 modern management gives IT the ability to better meet the needs of end users no matter where they are located, making it easier to adapt as your distributed workforce grows or changes.

Whether you're already familiar with modern management, or just getting started, this sample journey illustrates how you can build value at every step. For instance, you can gain immediate value in the Respond phase, grow your use of it through Adapt, and continue to evolve and grow in Accelerate. These phases can be taken concurrently, in parallel, or out of order; this is just one example of how healthcare organizations are navigating the transformation.





## Phase 1: Respond

### VMWARE WORKSPACE ONE

Workspace ONE delivers complete, cloud-based Windows 10 modern management and security, with intelligent automation to empower users and simplify IT. It integrates access control, application management, and multi-platform endpoint management into a single platform, and is available as a cloud service or on-premises deployment.

### Focus on the immediate needs of employees

For many healthcare organizations, the rapid shift to remote work for some employees spurred an investment in PCs and peripherals for employees to use at home. But supply chain disruptions caused delays, creating a surge of interest in Bring-Your-Own-Device programs.

IT teams were faced with managing a mix of new devices and aging hardware, both company- and employee-owned. When PCs did arrive, the need to image devices—a time-intensive and manual process—and onboard a large number of remote employees created an additional cost and resource burden.

A digital workspace platform that includes VMware Future-Ready™ Workforce Solutions such as VMware Workspace ONE® provides the most efficient way to onboard employees and improve the way they access apps—whether they're working at home, in the office, or a mix of both.

### With modern management, you can:

#### 1. Onboard employees faster by drop-shipping devices

The days of manually provisioning employee devices are over. With Workspace ONE, you can drop-ship pre-configured PCs from the OEM directly to your end users, eliminating the need for IT to manually provision these devices. Devices arrive with apps pre-loaded and additional configurations completed over-the-air on first boot. Not only is it fast and efficient, but it's also a smart move—employees will be ready to work on Day One. The same is true for device restoration; it's fast, simple, and entirely remote—for truly “hands-off” IT.

#### 2. Give employees fast, simple access to apps they need for work

In addition to the core apps that are pre-loaded on the device, Workspace ONE also offers a self-service app catalog. The catalog can live in the cloud or be installed as an app on the PC. Wherever they access it, employees can use the catalog to view, launch, and install pre-approved or request new applications, whether these applications are web-based, SaaS, virtual, or native. With one place to go for any app and single sign-on (SSO), employees can be productive right away—without waiting for IT and losing valuable time, or having to remember passwords across each app.



## Phase 2: Adapt

### WORKSPACE ONE ASSIST

Workspace ONE Assist is a comprehensive, fully integrated remote support solution that enables healthcare organizations to deliver quality IT support and maximize their end-user computing investments, while mitigating lost revenue, productivity, and decreased employee satisfaction. Workspace ONE Assist empowers IT and help desk staff to remote-view or control Android, iOS, macOS, and Windows devices, directly from the Workspace ONE console, while maintaining employee privacy and trust.

### Manage and secure your device fleet more effectively

Once you've met the most urgent needs, you can move onto the next step: simplifying the complexities involved in managing and securing a distributed workforce. An increasing number of apps and devices outside the organization "perimeter" only adds to the off-network management pains, growing security risks, and end-user support requirements. A modern management approach simplifies these critical requirements by providing IT a line of sight across every device, located anywhere—remotely, from the cloud. You maintain complete management control and security, while providing users a productive experience on an "always up-to-date" PC.

### Modern management helps you create a solid foundation for Windows Anywhere with the ability to:

#### 1. Quickly apply policies over-the-air without any network dependencies

With Workspace ONE baseline templates, quickly apply industry-standard security policies—whether modern mobile device management (MDM) or traditional Group Policy Objects (GPO)—in real-time from the cloud. These turnkey templates allow you to rapidly achieve 100% policy compliance in a matter of minutes, instead of manually sifting through thousands of configuration policies. Templates are customizable to meet the specific needs of your organization. Also, Workspace ONE provides the option to easily export your existing policy set from the domain to the cloud for over-the-air configuration management—without domain or network dependencies.

#### 2. Provide remote support for uninterrupted productivity

Keep work in motion with Workspace ONE Assist, a remote employee support solution that enables IT to remotely view or control any device, directly from the Workspace ONE console. This capability makes it easy to support employees who have issues related to devices or app tasks. Workspace ONE Assist gives you the ability to remotely support a broad range of devices, including Android, Windows CE, Windows 10, macOS, and iOS devices—so that people can get back to work faster.

#### 3. Achieve best-in-class modern management for Windows 10

Experience all the benefits of the latest Windows 10—with additional controls beyond what Windows 10 alone can provide. Meet requirements for security, control, and usability on a single platform, without having to juggle multiple tools.

#### 4. Optimize security across endpoints and applications

Deploying the most recent Windows patches across endpoints is a time-consuming effort. Many IT organizations delay patching for weeks or months, leaving security exposures that make you more vulnerable to a breach. Patching gets even more complex in a remote-first environment, where not all users are connected to the organization's network or a VPN. Workspace ONE takes a cloud-native approach that automates and streamlines patching, continually reducing risk while allowing you to focus on bigger priorities. It combines industry-leading modern management and threat detection and response, for an intrinsic approach to endpoint security that ensures secure application access.

You will also need the flexibility and automation to activate key updates. Integration with third-party vulnerability feeds (e.g., CVE by NIST) allows you to identify "at risk" devices in real-time and automate patch rollout to keep your organization protected at all times.

### WORKSPACE SECURITY

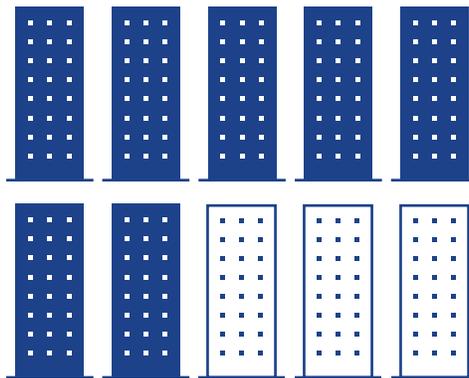
Workspace Security provides the most advanced endpoint security combined with integrated insights, and app analytics. This solution integration leverages the deep endpoint telemetry and alerts of suspicious or malicious behavior from Carbon Black, and correlates that data with Workspace ONE's other native and third-party data sources. By working hand-in-hand, Workspace Security provides unified visibility, rich visualization, and custom reports that offer a single view into your digital workspace to gain deep insights that enable data-driven decisions across your environment.

### Integrate management and security

A built-in zero-trust approach to endpoint security is also key to helping IT proactively secure the digital workspace of users, apps, and endpoints. Workspace Security combines Workspace ONE and Carbon Black to provide compliance and threat data to drive intelligence-based actions either through its automation engine or by working with real-time querying products to effectively remediate any threat present. The Carbon Black Cloud delivers the entire protection cycle of harden, prevent, detect, and respond for endpoints and workloads spread across the globe.

### As a result, you are able to:

- Leverage intrinsic zero-trust architecture to secure users, endpoints, apps, and networks, across any cloud or device.
- Secure the organization and gain the visibility needed to detect, identify, and prevent threats.
- Benefit from industry-leading modern management and threat detection and response, for an intrinsic approach to endpoint security that ensures secure application access.
- Keep endpoints protected with intelligence and automation; activate auto approval for key updates or granularly target updates to specific users or groups.



7/10

of healthcare organizations are riddled with devices running legacy Windows operating systems.<sup>1</sup>

<sup>1</sup> "Forescout Device Cloud Report", May, 2019. [Web](#).



## Phase 3: Accelerate

### Achieve ongoing transformation

With a secure foundation, you can now focus on the ultimate promise of modern management: the ability to continually improve digital employee experiences, strengthen protections, and seize new opportunities for transformation.

#### 1. Develop a long-term initiative to cultivate employee experience

Outside the familiar office environment, PCs are the biggest link to colleagues, projects, and workflows—making it imperative that these interactions be simple and seamless. When people can easily get access to the apps and information they need, they can get more done. Without the obstacles and frustration caused by slow, outdated systems, they feel empowered to do their best work.

#### Happier employees lead to better outcomes

Employees' experiences with technology play a key role in both productivity and workplace satisfaction—and are even linked to greater patient care.

#### 2. Seize opportunities to accelerate security initiatives

This final phase is a great time to evaluate where you are and address bigger security risks that will impact the organization in the long term. In many IT organizations, endpoint management and security tools operate in silos. How can you close this gap moving forward?

#### Use these questions to start an internal analysis:

- Do you have a clearly articulated public cloud strategy? Which applications have you already migrated to the cloud—and which ones should come next?
- Are you having difficulty managing and updating endpoint protection on remote devices?
- Is growth in virtual desktop infrastructure (VDI) and VPN making a downstream impact on your network load?
- Is your remote workforce being impacted by sluggish consumer broadband when accessing mission-critical applications?

Technology is responsible for an array of positive emotions and responses in the workplace.<sup>2</sup>

# 53%

of US employees say that digital tools make them more successful

# 28%

of US employees say that technology actually makes them happier

<sup>2</sup> "The Undeniable Link Between Technology and Employee Happiness", HR Technologist, February, 2020. [Web](#).

### What does a Future-Ready Workforce mean for IT?

From onboarding to everyday workflows, modern management helps IT improve employee experiences for everyone, whether they're working at home, in the field, or in the office. With intelligent insights and automation, you can improve device health while identifying opportunities to reduce IT costs, improve security, and optimize experiences.

Expand your ability to:

- **Proactively identify workspace issues.** Leverage intelligence to find problems linked to the OS, apps, devices, and more—and remediate automatically.
- **Get in-depth insights on user experience metrics.** Timely data on devices, apps, and users can help shape what proactive steps you take to improve scores and experiences.
- **Troubleshoot and contain experience hurdles.** Quickly assist employees by identifying and fixing issues before they spread across the organization.
- **Evolve toward a unified response to security threats.** Combine management and security of endpoints with deeper insights into device compliance and security risks.

### A digital workspace platform that grows with you

As your IT organization adapts to a changing world, VMware Future-Ready Workforce Solutions help you quickly achieve the benefits of a digital workspace and seamlessly support the organization.

- VMware Workspace Security provides the most advanced endpoint security combined with integrated insights and app analytics. It not only protects data and endpoints, but also provides the visibility and compliance that keep the organization in motion.
- VMware Workspace ONE allows you to provide a consistent, unified workspace across any computing environment—mobile, desktop, special purpose, or virtual—for work-from-home employees and everyone else.

Whatever the future holds, VMware solutions help you to stay nimble and prepared to meet the next challenge. With the right balance of automation and control, you are equipped to meet rapid changes and evolving demands while helping employees stay secure, connected, and productive.

[Learn More through our Pathfinder Trial Experience page >](#)



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 [vmware.com](http://vmware.com) Copyright © 2020 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at [vmware.com/go/patents](http://vmware.com/go/patents). VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. 9/20