



# 5 Signs Your Windows Management Strategy Isn't Working

How Modern Management Can Get You Back on Track

GET STARTED





## Traditional Windows Management Is Holding IT Back

Windows 10 management is a core part of IT's work, as it makes a direct impact on how effective and productive people are in their jobs. It's also become increasingly complicated in the age of distributed devices and growing security risks.

A successful Windows 10 management strategy helps IT improve desktop management processes, reduce complexity and costs, close security gaps, and empower employees to do their best work.

But many IT organizations take a traditional approach to Windows management, or employ a hybrid approach that involves juggling multiple tools. Unfortunately, those approaches require lots of manual labor, and can lead to frustrating employee experiences, inconsistent policies, and security gaps.

### Ready to troubleshoot your approach?

Take a look at five common pain points of Windows 10 management and learn how modern management can help you fix them.

## 1

## Your IT department looks more like shipping and receiving

In a traditional management approach, IT “owns” a unique image for each device and must load and manage it directly. Provisioning devices and keeping them updated is a physical, time-consuming job. IT departments often turn into a hive of activity, where laptops and desktops are received, unboxed, imaged, and shipped out again.

Even if an organization maintains inventory of new or used devices to provision, and places orders for each device required from a contracted supplier, they still need to unbox, power up, and reimage laptops and desktops. Once completed, they must re-package and ship devices to employees. When a device gets damaged or requires a fix that can’t be administered remotely, the employee must ship the device back to IT, who then might need to send them a loaner.

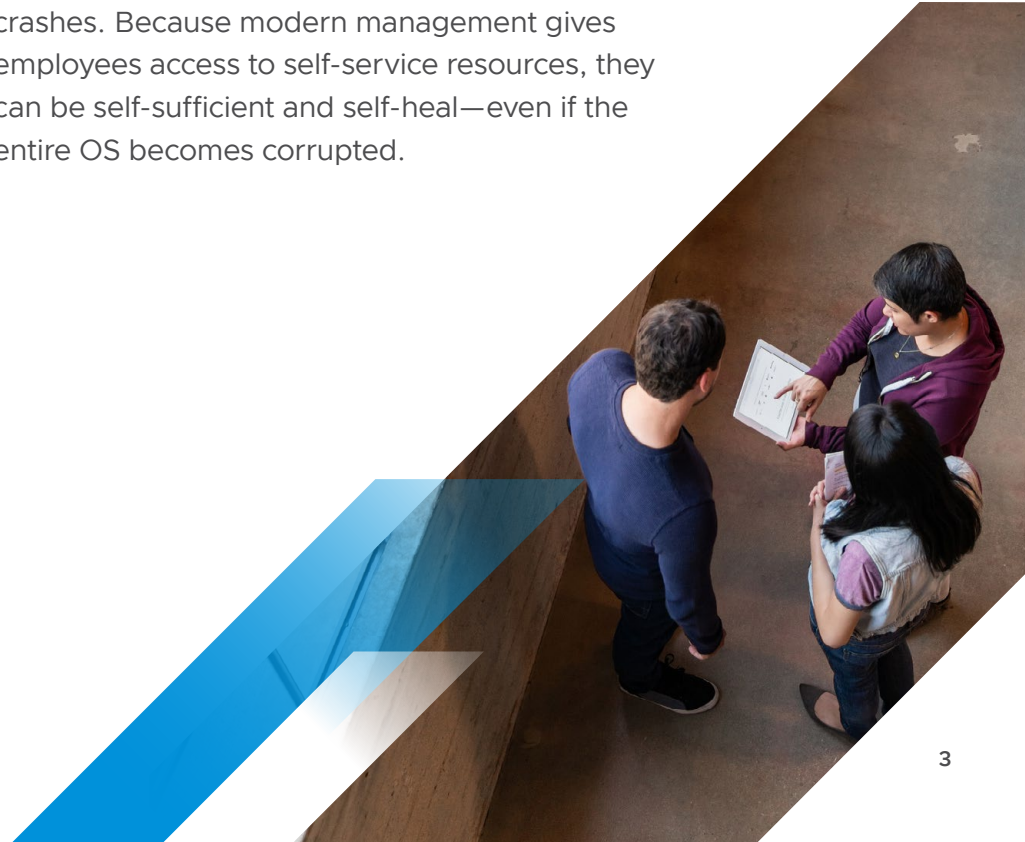
Ultimately, it’s a costly, complex, and time-consuming approach.

### What’s different with modern management?

Modern management makes it possible for IT to take the complexity out of managing official Microsoft Windows images by working directly with their favorite OEM provider.

Fully configured devices may be shipped directly to employees from the OEM; there is no reason for IT to ever physically touch the assets. That eliminates the resource-intensive steps of receiving, unboxing, provisioning, repackaging, and shipping out.

It also requires fewer IT tickets and resources, for everything from requesting new apps to restoring desktops from crashes. Because modern management gives employees access to self-service resources, they can be self-sufficient and self-heal—even if the entire OS becomes corrupted.



## 2

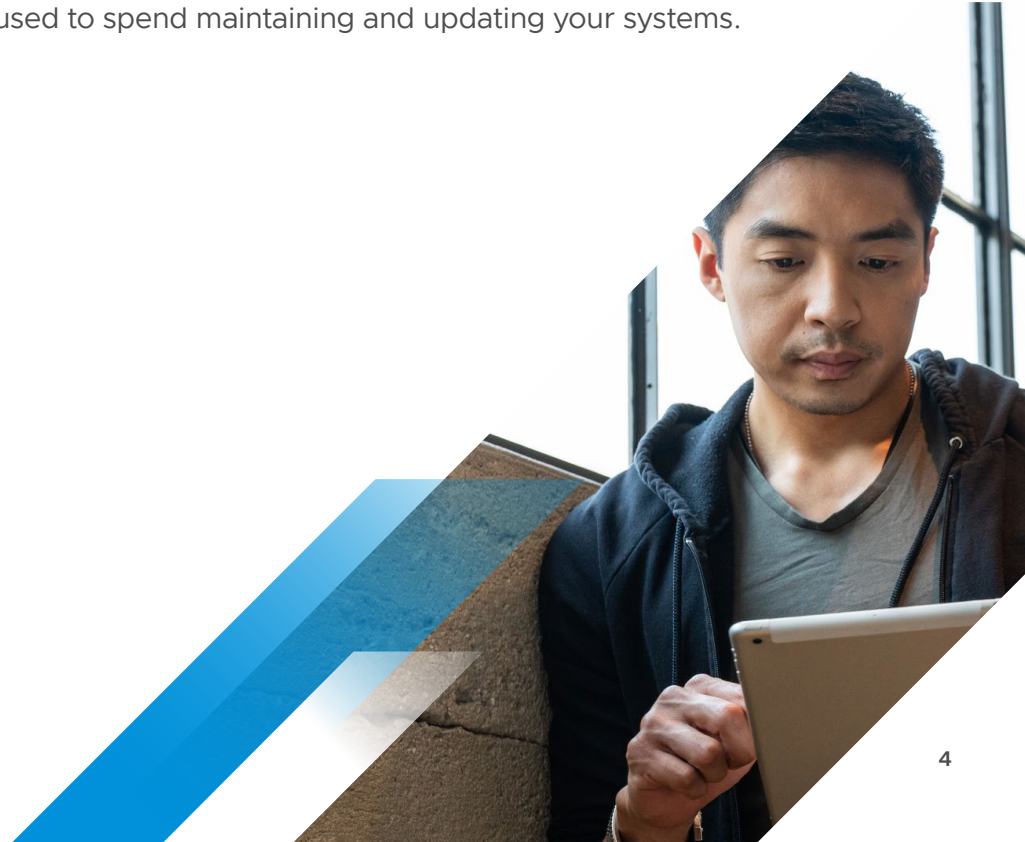
## You spend as much time updating your management infrastructure as you do managing desktops

Maintaining traditional, on-premises management tools in a distributed environment is highly complex. The system allows IT to provide support, deploy software, review and manage alerts, and enforce compliance across devices. But to do those things, you must build and maintain an on-premises database and push out images to remote offices—while continually working to keep the infrastructure up to date and maintain the health of the environment.

The list of tasks required to maintain these traditional management tools on a daily and weekly basis is long and continues to grow. Even for desktop pros, it's a massive undertaking that requires ongoing oversight, management, and communication to get it right.

### What's different with modern management?

Modern management provides a cloud-based solution that eliminates reliance on IT for system maintenance. It gives IT access to the latest features and security updates on a monthly SaaS release cadence. Many routine tasks are automated—freeing up time you used to spend maintaining and updating your systems.



## 3

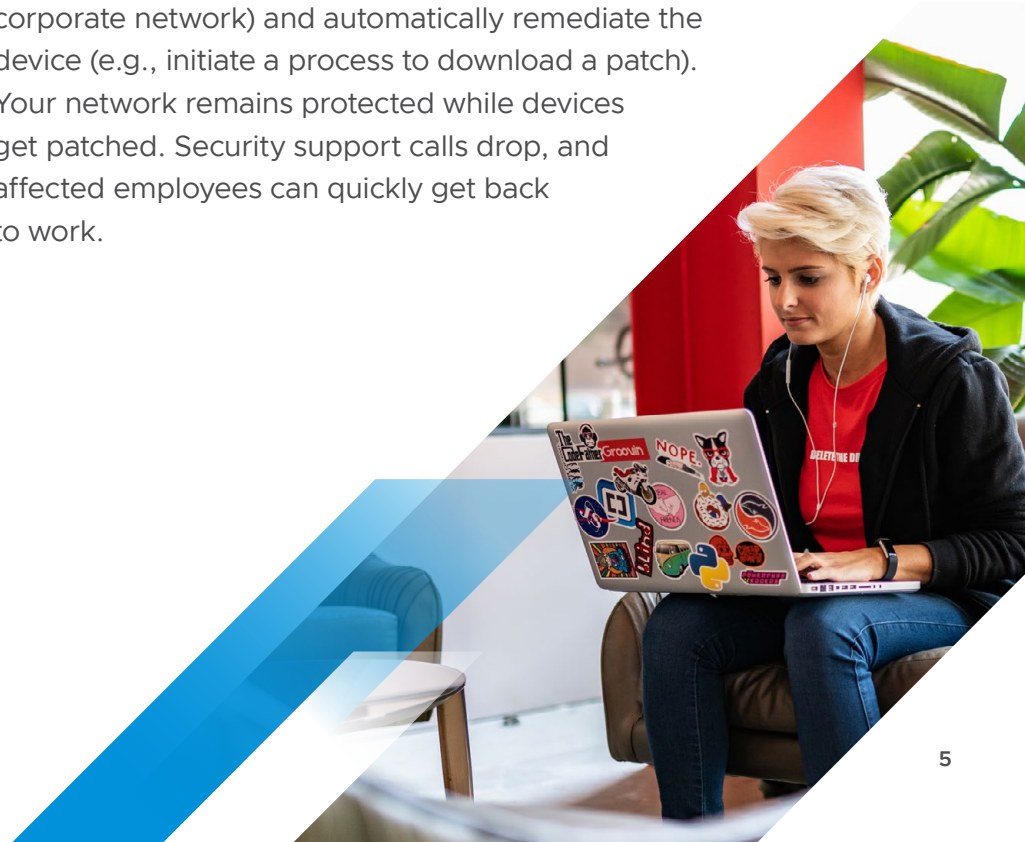
## You have to let unpatched laptops onto your network because you have no other way to update them

In a traditional management approach devices must be on the corporate network for IT to manage them—which can create security gaps. For example, if Microsoft released a critical patch to protect devices, you would have to first allow the device onto the network to then discover that it needs patching and include it in the patching process. Meanwhile, a vulnerability on that same device could already be impacting the network.

Even if you had a way to detect and prevent an unpatched device from connecting to the network, you would essentially be keeping the employee from doing work, because there would be no way to remediate the device.

### What's different with modern management?

In the same scenario described earlier, modern management can to detect a vulnerability or out-of-compliance patch level for devices that are both on *and* off the corporate network. When it makes that determination, a policy could quarantine the device (e.g., prevent the employee from accessing the corporate network) and automatically remediate the device (e.g., initiate a process to download a patch). Your network remains protected while devices get patched. Security support calls drop, and affected employees can quickly get back to work.



## 4

## Employees can get all the apps they want, as long as they already know where to get them

Traditional management assumes that applications are either baked into an image or packaged applications are published onto the PC by the admins. Employees have little or no choice in the matter; applications are typically selected for them, through their membership in an organizational group. The process is entirely push-based—there's no way for employees to pull or self-install other applications.

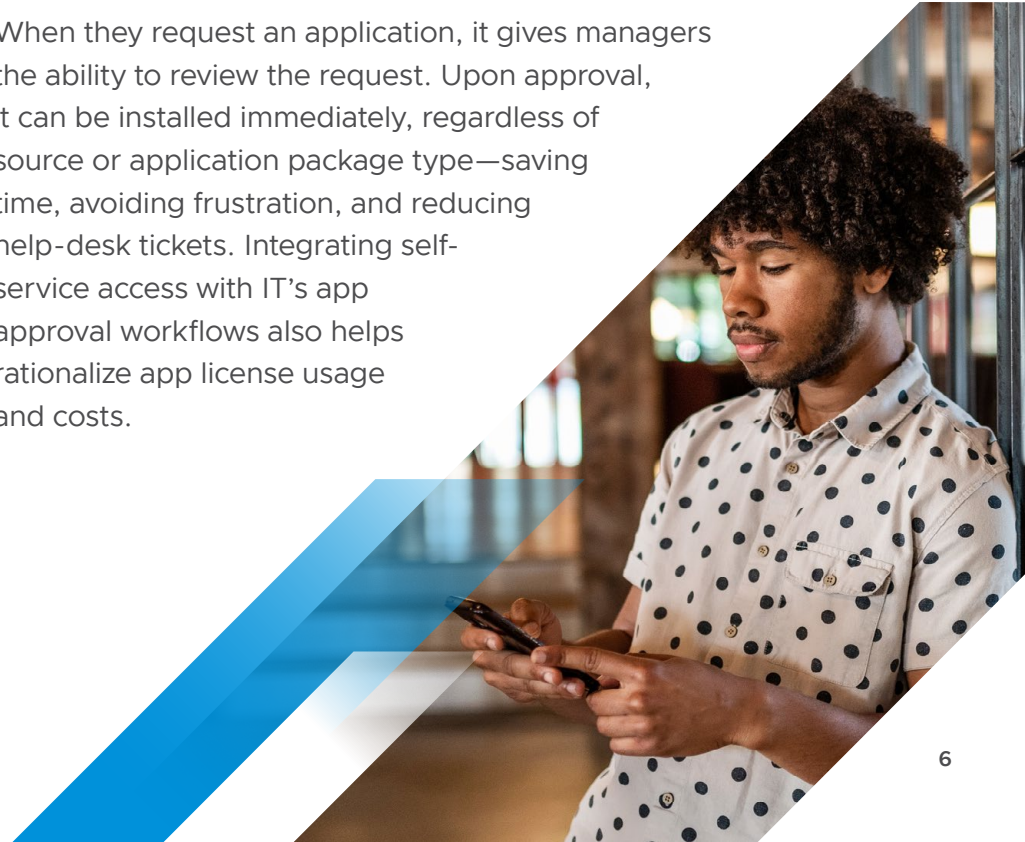
But not all employees within an organizational group have the same needs, and traditional management makes it hard to fulfill diverse requests.

If an employee wants something different, they must request it and wait for delivery. That involves submitting a ticket for a new application and waiting for the ticket to get processed. There are some exceptions with modern apps available on the new Windows Store for Business, but only a small portion of applications are available.

### What's different with modern management?

Modern management makes a fundamental transition from push to pull—instead of an “IT down” approach, it lets employees choose what they want and when. IT can still pre-provision popular applications, but employees are free to browse and choose the apps they want.

When they request an application, it gives managers the ability to review the request. Upon approval, it can be installed immediately, regardless of source or application package type—saving time, avoiding frustration, and reducing help-desk tickets. Integrating self-service access with IT's app approval workflows also helps rationalize app license usage and costs.



## 5

## You have policies for everything, but can't remember whether they are all applied

The robust nature of legacy solutions can be a weakness. For instance, traditional management tools allow you to allow you to build an infinite number of policies—but managing them is tremendously challenging. You need people who have a deep understanding of how to set policies up the right way; what policies are needed for your device, OS, and app versions; what policies are critical to keep your infosec team happy—all of which requires a level of expertise that many IT organizations don't have. Not surprisingly, these experts are in high demand. Even if you know which policies you want to implement, not all policies are pushed out consistently to devices if they aren't "on the network" or domain-joined.

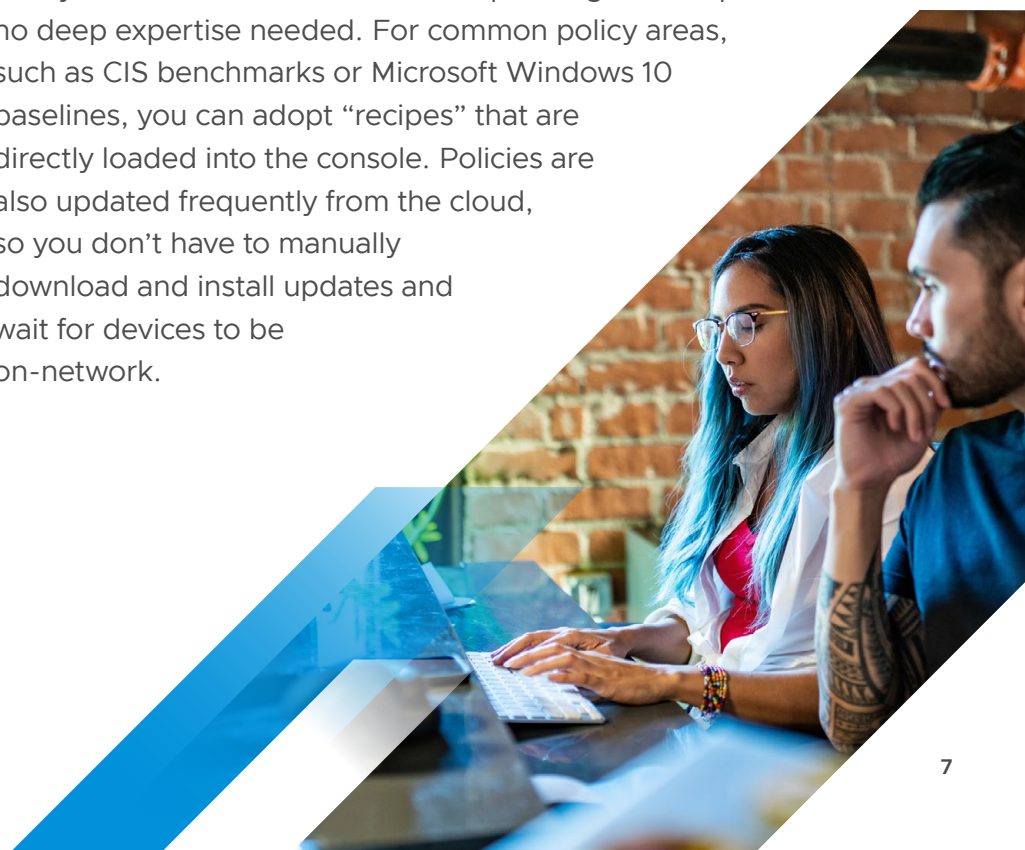
Once the policies are in place, your team needs to know that they exist, and when and how to apply them. It's not a process that can be solved all at once; it requires continual oversight, organization, and frequent communication.

### What's different with modern management?

A modern management approach creates one common record of policies that are both recommended and applicable for the OS you are supporting. Some solutions come pre-loaded with

Microsoft-recommended baseline policies, making it far easier to tap into your compliance requirements. You no longer have to wait for an expert or scavenge through thousands of policies; you can start using policies right away.

If you need to edit a policy, WYSIWYG tools provide the ability to tweak and refine with a simple drag and drop—no deep expertise needed. For common policy areas, such as CIS benchmarks or Microsoft Windows 10 baselines, you can adopt "recipes" that are directly loaded into the console. Policies are also updated frequently from the cloud, so you don't have to manually download and install updates and wait for devices to be on-network.



# A Successful Strategy Starts with VMware Workspace ONE

VMware Workspace ONE™ is an intelligent digital workspace platform that helps IT organizations put employees first while securing apps and data in a perimeter-free world.

VMware commissioned Forrester Research to conduct a study on the economic impact of Workspace ONE for Windows 10. They interviewed three organizations that transitioned from a traditional management approach to modern management with Workspace ONE. These organizations used Workspace ONE for enterprise-managed devices, including laptops and desktops running Windows 10, along with devices for highly mobile users that may not connect to the office network for periods of weeks or months.

Forrester found that a modern unified management approach enabled by Workspace ONE delivered a significant return on investment and helped organizations save millions of dollars in operational expenses.

Workspace ONE benefits by the numbers<sup>1</sup>

IT ADMINISTRATIVE SAVINGS ADDED UP TO:

**\$2.1 million**

REDUCED PC SETUP COST SAVINGS OF NEARLY:

**\$452,000**

REDUCED ENTERPRISE SECURITY RISKS ADDED UP TO A SAVINGS OF:

**\$318,000**

1. Forrester Research, *The Total Economic Impact™ of VMware Workspace ONE for Windows 10*, September 2018





# Windows Management Made Simple

VMware Workspace ONE is the modern digital workspace platform that offers a high degree of flexibility, choice, and security. It helps you meet the diverse and changing needs of employees and the business, which frees up your IT teams to be more innovative and strategic.

Workspace ONE provides multiple benefits that traditional management can't match:

- Reduces management complexity and automates common tasks
- Strengthens security to reduce the risk of a breach
- Delivers a superior user experience that facilitates employee self-service
- Equips organizations to build privacy-first policies to ensure that personal employee data and information stays private

Modern management delivers cost savings and time savings—but most importantly, it lets you deliver better digital experiences that help support business goals.

Take the next step

[Read the Forrester Report >](#)

Join us online:



**vmware**<sup>®</sup>

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 [www.vmware.com](http://www.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 <http://www.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. Item No: 14320\_VMW\_1904 Modern Management Additional Materials\_Ebook5Signs\_R3\_01062020\_ms 1/2020