WHITE PAPER – FEBRUARY 2017

# FIVE CRITICAL STEPS TO MODERNIZE YOUR WINDOWS ENVIRONMENT

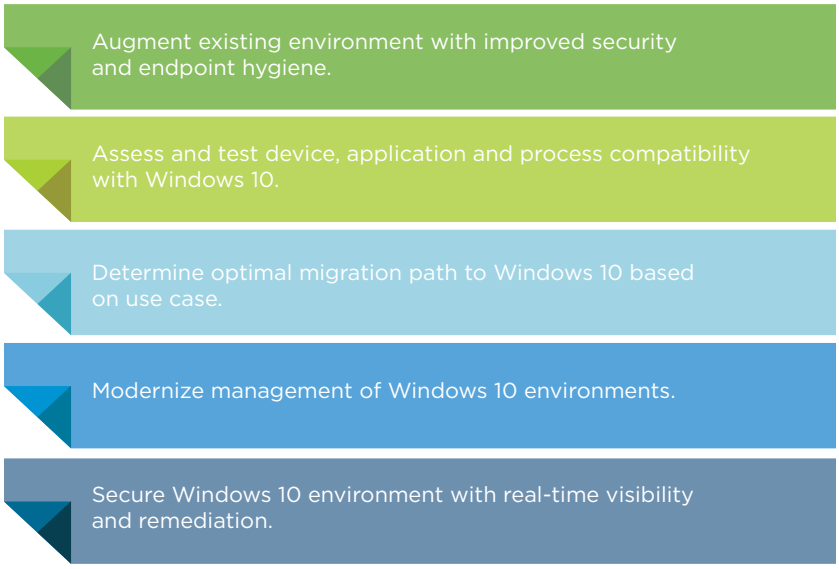
A guide to getting the most out of your existing investments in Windows and provide light on your path to Windows 10 for virtual and physical deployments.

vmware®

## The World Runs on Windows

There are more than 1.5 billion devices that run Windows*. Over the past 30 years, most organizations around the world have standardized on Windows with significant investments in their Microsoft environments, including licensing, configuration, professional services and infrastructure for Active Directory, Microsoft Exchange, PC lifecycle management and more. Microsoft also continues to develop solutions to help organizations transition to the cloud with products like Microsoft Office 365 and Azure Active Directory, and with the creation of a modern, mobile-cloud management framework in Windows 10.

At the same time, IT departments across the board receive constant pressure to cut costs while somehow simultaneously hardening security and boosting employee productivity with the latest technology. Windows 10 introduces a better experience for users and opportunities for IT to adopt a fundamentally different management and security approach that eases their burdens. However, to truly optimize and get the most out of their Windows environment, organizations need to:

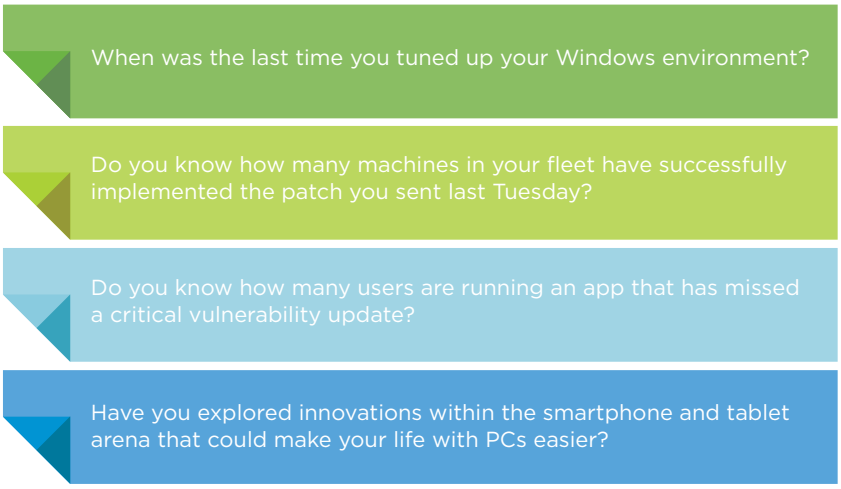



This paper will explore how organizations can take five steps to both optimize their existing investments in Windows and outline how organizations can embrace modern management and security on their path to Windows 10.

## Step 1: Tune Up Your Windows Environment for Extra Mileage

Responsible car owners perform tune-ups to inspect, repair or replace spark plugs, air filters and other parts that are not functioning at peak performance. Sometimes complementary solutions are used like switching to high mileage oil or using a fuel additive to remove carbon build-up in the fuel line. The result is a more fuel efficient, longer lasting vehicle.

When was the last time you tuned up your Windows environment? The first step to a modern Windows environment is to augment your existing processes, technology and reporting to make your life and the lives of your end users better. Do you know how many machines in your fleet have successfully implemented the patch you sent last Tuesday? Do you know how many users are running an app that has missed a critical vulnerability update? Have you explored innovations within the smartphone and tablet arena that could make your life with PCs easier?




The feedback we hear from customers is consistent. Users want to be productive wherever they are on whatever device they want to use. They are often accessing corporate resources off network on a variety of device types, which increases the number of threat vectors for the organization. IT needs real-time visibility into their Windows environment to know which devices are not up-to-date with the latest patches, running unsigned apps, or running older versions of app dependencies (e.g. Java, .NET) exposing the device and corporate network to potential attack. They need the ability to perform actions based on that information, such as deploying a patch, killing a rogue process, or performing a remote wipe of a device that poses a security threat.

### Real-time Visibility and Security into Your Environment

Imagine if you could get complete visibility across all of your endpoints in 15 seconds or less. Imagine typing a simple question in English like you would in Google to query your entire environment, get results in seconds—even across millions of endpoints—and be able to gather and act on critical insights at a moment's notice. Now you can. VMware® works with desktop and server versions of Windows 7, 8.1 and 10 whether virtual or physical and enables you to:

- Discover and take control of unmanaged endpoints
- Detect advanced threats in seconds across millions of endpoints
- Quickly remediate compromised endpoints at scale
- Restore compromised Windows endpoints to a golden image

The platform lays across the whole organization to secure endpoints, give IT operations visibility into live software inventory and detailed resource utilization, and distribute applications and patches at scale. As customers plan their move to Windows 10, VMware enables them to take a pulse on the existing environment to fix any issues and streamline transition to Windows 10.

VMware also gives customers a modern way to secure and manage mobile devices, Windows endpoints and servers. Integrations with the VMware ecosystem result in added compliance, faster threat containment and customizable remediation actions that adjust to threat levels, via dynamic configuration and management policies.

For example, you could use VMware to execute queries to detect endpoints that are out of compliance, and then quarantine those devices. Once the threat is contained, VMware can inform end users about the compliance breach and IT admins can deploy the necessary fix to bring the endpoints back to a compliant state.

### Over-the-air Configuration and Consolidated App Catalog

Do you remember the last time you received that phone call from a traveling executive who happened to "misplace" their laptop? Hopefully, you enforced BitLocker encryption, otherwise sensitive corporate information could be out in the wild, and there's nothing you can do. However, if you had deployed unified endpoint management (UEM), you could have performed a remote wipe to prevent data loss.

EMM solutions have historically given organizations the ability to configure Wi-Fi, set-up VPN, access a consolidated business app store and perform a remote wipe on iOS, Android and other mobile operating systems. By deploying EMM solutions compatible with traditional Windows environments, organizations can complement PC Lifecycle Management tools by extending the same capabilities from mobile operating systems to give users a better experience, improve security and to save IT time.

### Support Remote Workers and Deploy Applications with Virtualization

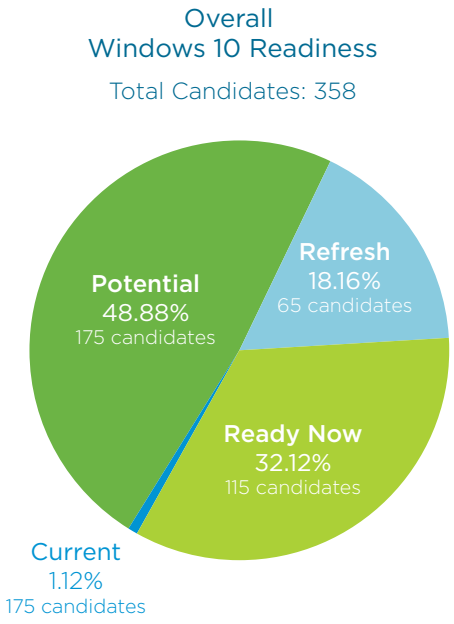
When was the last time you evaluated your end users' needs and use cases? Sure, you might have some virtual desktop populations for common scenarios such as call centers and remote developers, but have you thought about additional ways to extend resources to your employees, contractors and partners? With desktop and application virtualization, you could deliver resources users need to do on their personal device—or any device. Some of your applications might require a certain OS, browser or plugin version, and for those applications to be virtualized so they can run independently of the users operating system.

VMware lets you centrally deploy virtual desktops at scale, embrace BYOD and eliminate downtime due to lost or damaged endpoints, improve security by keeping data safe and secure in the datacenter, and can boost the bottom line by avoiding hardware refreshes or reducing endpoint cost. You get a simplified, secure, and scalable end user computing strategy.

## Discover a New World on Your Journey to Windows 10

It's been said that if Henry Ford asked his customers what they wanted, they would have said faster horses. Ford's automobile changed transportation by addressing the problem in a completely different way. Similarly, Windows 10 diverges from its predecessors in a dramatic way that redefines how IT manages the entire lifecycle of PCs, smartphones, tablets and any other endpoint that runs the last operating system from Microsoft.

Until the release of Windows 10, IT departments had to approach their environment like visiting a strip mall: piece together disparate technologies that don't operate well together to address various challenges around configuration, software distribution, patching, malware and security.




With Windows 10, Microsoft has introduced a new possibility that operates like eCommerce: It's convenient, the technology works well together and opens up new opportunities that didn't exist before. After speaking with hundreds of customers who have migrated to Windows 10 or are mapping out their rollout, we've found that after improving security within their existing environments, there are four key steps remaining on the path to a successful Windows 10 deployment:

Assess ▶ Migrate ▶ Manage ▶ Secure

## Step 2: Assess your existing environment to take the guesswork out of your physical and virtual deployments

Many organizations struggle on where to start with their path to Windows 10 from knowing which existing machines can handle Windows 10, what use cases might be better suited for desktop virtualization and everything in between. With the right desktop assessment tool, organizations can receive intelligent recommendations on what machines and uses cases are best suited for an in-place physical migration to Windows 10 and which ones are better suited to run a virtual desktop on premises or from the cloud. This gives you a baseline understanding of your existing environment to determine how you'll approach your migration to Windows 10. To learn more about the assessment tool, visit assessment.vmware.com.

Just like previous upgrades to new versions of Windows, IT admins responsible for physical or virtual desktop environments will need to test applications for any compatibility issues before migrating their fleet to Windows 10. If applications do not run on Windows 10, IT can deploy these as virtual apps, so they continue to work after the migration to Windows 10 and users can still get their jobs done. Legacy applications such as Internet Explorer 6 are an example of this.

## Step 3: Determine your migration plan for virtual and physical machines

According to Microsoft, 96 percent of businesses are piloting Windows 10. However, many are still just mapping out their plans for migration. There are several questions we ask customers as a baseline to guide their journey to Windows 10:

- Are you planning to adopt Windows 10 over the next 3 to 4 years as your PCs are refreshed?
- Are you planning to do an in-place or custom image migration of all existing machines?
- Do you plan to virtualize endpoints that cannot support Windows 10?
- Are you addressing use cases within your business where virtual desktops and applications bring efficiencies?
- Are you planning a combination of all of the above?

Every organization will need to determine the migration path that's best for them, but here are some common ways we help organizations approach their path to migration:

**Refresh**

As devices are refreshed over the next 3-4 years, organizations transition to Windows 10 and manage any new devices with the modern, unified endpoint management (UEM) framework that enables them to streamline IT, lower costs of management and deliver a peak end user experience.

**Migrate**

- In-place: organizations leverage in-place migration tools to move machines from previous OS versions to Windows 10 base image, and provision company recommended policies and apps using the UEM solution.
- Custom image: instead of the base OS image, organizations can also migrate to a company recommended image with custom apps and data, and auto enroll into management with UEM.

**Virtualize**

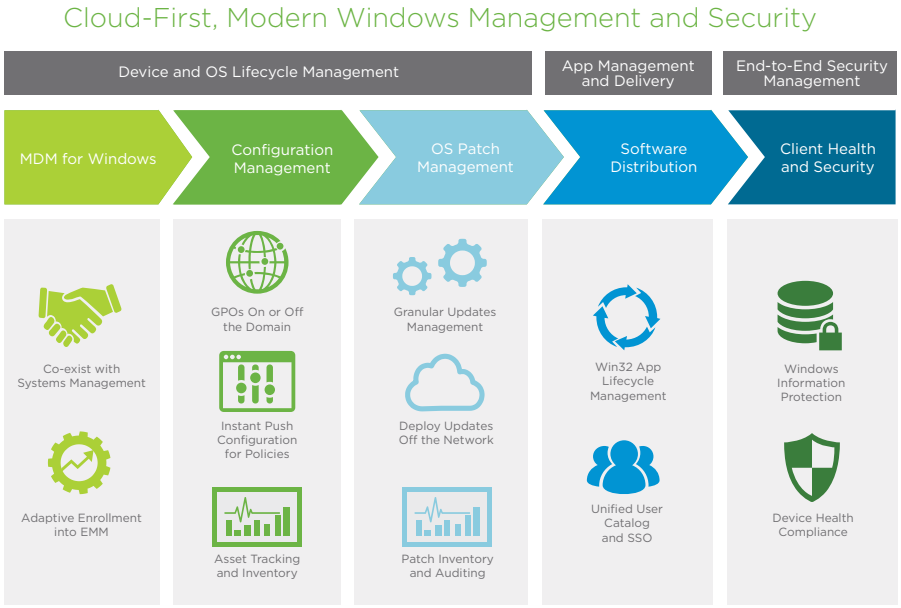
- Virtual desktops and apps are upgraded centrally and delivered to end users on their existing devices. This lets you support various use cases such as:
  - Existing machines that cannot support Windows 10 receive a virtual desktop
  - Organizations consider virtual desktops for BYO laptop scenarios
  - Virtualize mission-critical applications that aren't compatible with Windows 10
  - Organizations create internet or data isolation for security sensitive deployments

## Step 4: Evaluate UEM for physical machines in the new Windows framework

Traditional processes to image, configure and fully set-up a physical PC can take several hours. Over time, application and registry residue bogs down system performance causing image drift, results in performance issues for the end user, and often requires IT to go back and spend several hours re-imaging devices and inconveniencing users.

Most organizations use PC lifecycle management tools with hundreds of GPOs, custom scripts, and more cobbled together tools to manage their Windows environment. Unfortunately, there are several limitations with legacy PCLM tools, including the inability to perform actions on devices off domain and company network, costly infrastructure to maintain, labor intensive processes such as imaging and more.

The beauty of modern smartphones is that you can walk into a store, buy a device, enter your credentials and then automatically get access to all of your applications and services over-the-air in minutes. Why can't PC users get the same experience? Well, with Windows 10 they can. Windows 10 managed with UEM solution offers a new way for organizations to support their desktop fleet and provide a similar experience to what users get with their smartphones and tablets. Just enter your work email and password and the device will configure over the air in minutes with all of the applications, services and corporate policies needed to get work done. The new approach redefines the way IT manages the entire lifecycle of PCs, smartphones, tablets and any other endpoint consistently, from a unified console.




No more imaging every machine for hours. No more patch Tuesday's. No more inability to perform actions on users outside of the company walls. By deploying UEM to Windows 10 machines, IT has more time to focus on supporting the business and has a much more secure environment. Users get a unified application catalog across their Windows 10 PC, their tablet and their smartphone and they have a self-service portal to address common user issues instead of hogging time with IT.

## Step 5: Harden security with real-time visibility into your environment

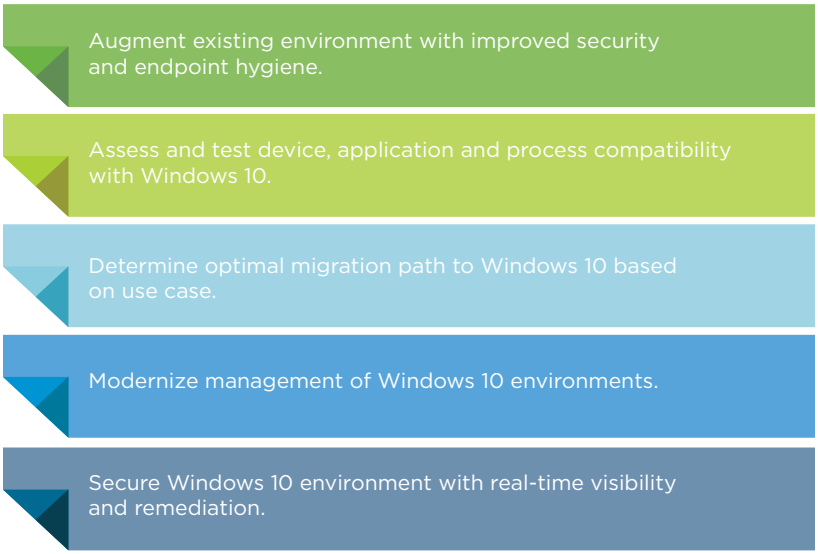
Andrew Grove, co-founder and former CEO of Intel Corporation, lived by a simple motto: Only the paranoid survive. The same principle that guided Intel's success must be the mantra of everyone in IT. In the past, organizations had a standard operating environment: one type of device running one operating system with a set of pre-approved applications on a specified network. Now, IT must support multiple types of operating systems running on all kinds of device types with unique mixes of applications running on or off the corporate network.

Facing this dynamic operating environment to support and an increasing array of cyber security attacks to combat, IT has been forced to adopt a zero trust model to protect corporate data. With VMware, IT can harden the operating system by enabling password-less authentications, preventing unapproved and unsigned apps, monitoring for compromised devices and performing automated remediation actions without the need for IT tickets. These actions can include restricting access to work resources instantly when an OS is determined to be compromised or even delivering a remote wipe command when a device is lost or stolen. VMware also delivers the capabilities mentioned previously around real-time visibility and security for devices running Windows 10.

To learn more about how VMware can help modernize your Windows Environment and get more out of your investments with Microsoft, visit www.WindowsUEM.com

## Extract More Value from your Environment

We've only scratched the surface of what's possible to get more value of your investments in Microsoft with VMware. As you look to complement your existing environment with additional capabilities and as you move to Windows 10, here's a quick recap on the five key ways VMware can support your initiatives:




In addition to supporting your Windows deployments, you may also be making other investments with Microsoft, such as moving to Office 365, Azure Active Directory and more. VMware end user computing solutions can enable you to more easily deploy and configure Office apps and services, and connect your Directory credentials and policies for federated identity and single sign on into your applications.

---

1.5 billion devices: http://www.computerworld.com/article/2919104/windows-pcs/where-will-microsoft-find-1-billion-devices-for-windows-10.html

**VMware, Inc.** 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com