Windows 10 Endpoint Management Made Simple

How deploying modern Windows management with VMware Workspace ONE increases security and organizational effectiveness

Leveraging modern management for Windows 10 smooths the way for endpoints that are more secure and more frequently updated.

The Windows 10 operating system introduces major changes, with built-in mobile management APIs, more frequent cloud updates, modern apps, and more. These changes open up opportunities for cloud-based, modern management of enterprise endpoints at scale, similar to what organizations have done for many years for their mobile device deployments. Instituting modern management is one of the ways many organizations can overcome their constant struggle today to keep up with operating system upgrades, security patches, and configurations for their desktop PC users.

Traditional on-premises PC management relies on a cumbersome client/server infrastructure and labor-intensive methods that take more time than the fast pace of today's enterprise typically allows. In today's "perimeter-less" workplace, where users increasingly work remotely, these methods also reduce the security and overall effectiveness of large organizations, because security patches and feature updates don't get applied quickly enough. And this approach is especially inefficient when dealing with an agile operating system such as Windows 10, which receives frequent updates via the cloud.

Leveraging modern management for Windows 10, on the other hand, smooths the way for endpoints that are more secure and more frequently updated. It also solves the update crunch and handles every device and user through a single cloud-based platform.

Making the transition to modern management with Windows 10 does require some initial effort and planning. But a thoughtful, staged approach that takes into account an organization's legacy processes makes the job easier and ultimately frees up IT resources for more productive pursuits.

vmware®

The PC Management Challenge

Most IT departments today are still treated as cost centers, with admins squarely focused on run-of-the-mill operations—supporting endpoints, apps, and operating systems—for 80% of their time. These teams also face the pressure of shrinking IT budgets, a proliferation of new devices and apps, and increased employee expectations of a consumer-like experience on work PCs. The drain on productivity steals resources that organizations can better spend on new initiatives and innovation.

The traditional PC management scramble can also leave organizations open to security vulnerabilities as important patches and updates fall between the cracks, particularly for modern workforce devices that go off-network.

Additional challenges that come with traditional management include:

- Complex imaging processes that require significant time and expense to implement

- Managing fragmented app and OS ecosystems with a mix of legacy desktop apps alongside cloud-based and other modern apps

- An extensive app distribution and management infrastructure that needs to be kept up

- No self-service way for users to request and access apps and company resources

- The need to protect work data as devices go mobile and remote, creating more headaches

Depending on an organization's approach to management, Windows 10 can either compound these problems or help solve them.

Windows 10 is an all-new OS with more frequent updates. It comes with significant upgrades every six months and cumulative updates incorporating security patches and fixes pushed more frequently. That creates a struggle for IT, as it is now constantly dealing with testing and servicing new updates.

Given these challenges, fully 1 in 10 enterprises takes a year or longer to deploy patches across the organization. More critically than missed feature updates, delayed patching increases the security risk to organizations.

A Modern Endpoint Management Solution

A modern PC management approach enables cloud-based, API-driven desktop device administration via native OS mobile device management (MDM) hooks. But, importantly for organizations with long-standing processes, this MDM-based approach can be augmented with traditional PC lifecycle management capabilities under a unified console with solutions such as VMware Workspace ONE. This ensures management efficiencies and ease of use for users and IT in a transition from traditional PC lifecycle management (PCLM) tools to a modern approach. But the benefits go much further.

Modern management also:

- Greatly reduces IT time and cost across traditionally cumbersome PCLM tasks, such as onboarding, patching, app distribution, and managing remote endpoints

vmware®

- Secures Windows 10 devices in real time even off the corporate network, with innovations such as always-up-to-date policies and patches on any device

- Delivers the best user experience with powerful self-service enablement to reduce help desk costs and keep users productive

Overcoming Challenges to Transition

The challenges large organizations face in transitioning from traditional, high-touch endpoint management to modern management may include:

- Organizational inertia, built up over many years of managing endpoints in siloed management teams working without sufficient coordination or shared resources

- A significant investment in existing processes whose capacity to transition to modern management may not be readily apparent

- Fear of migration itself, borne of the perception of the significant cost, effort, and retraining that might result

Despite the challenges, transitioning to modern management doesn't have to be as challenging as you might think. Here's how to make the shift.

Prepare

To begin the transition from traditional to modern endpoint management, assess the current state of your endpoints and management processes. As part of the preparation process, clean house through policy and app rationalization, determining which you still need and which need to be replaced or retired.

Start with Specific Use Cases and Personas

Don't try to tackle everything at once. Instead, manage your organization's transition in stages, starting with the use cases that will return the biggest value in the shortest time.

It's also important to examine your organization's risk profile, potential trade-offs in functionality, and user group maturity. For example, it's always better to align the transition as part of your device refresh as you bring in new hardware or start with "friendly" personas such as the IT team or a trusted tester team of end users before rolling this out to executives. Also, an organization with a higher risk profile will most likely want to progress through more stages with fewer users than one with a higher tolerance for risk.

Prototype and Test

Run small-scale tests and prototype new configurations as you go, to avoid surprises. Think of implementation and testing as two parallel tracks that run in close coordination as part of the same stage. While one team tests the next set of capabilities for deployment, have another team launch already-tested capabilities.

Deliver Value to Users

At each stage, focus on upgrading the user experience with streamlined, intuitive functionality. For example, adopt a modern onboarding process to reduce costs and immediately show

vmware®

a positive end user experience impact. This will help with organizational buy-in, by giving the transition team successive wins that build on one another.

Marketing the benefits of the transition internally can help, for example, by encouraging users to consider the time savings and greater control they will have with self-serve, anytime, anywhere access to the apps they need in a company app store.

Demonstrating value starts at the top, by getting buy-in from business users and executives. Your transition team may be focused on technology, but your business partners will be focused on the user experience (i.e., what's in it for them?). Show them, by showcasing new capabilities in a prototype "experience center," for example. Among other capabilities, the prototype can demonstrate a modern OS update model and a modern security model.

You can also build anticipation and excitement by previewing future capabilities even before they're ready and providing frequent updates on what to expect when.

Modern Management with Workspace ONE

A modern management tool such as VMware Workspace ONE Unified Endpoint Management (UEM) can ease the transition. It does so by:

- Providing depth in management itself—both when it comes to modern MDM-based policy management and meeting traditional PC management requirements

- Providing automation tools to help ease and derisk the migration of complex traditional PC management workloads to modern management

Workspace ONE facilitates every step of the journey with modern management features such as the following:

- Turnkey provisioning that applies policies and settings across devices automatically

- Unbox-and-work user experiences that get users working immediately on any device without waiting for IT support

- Zero-IT-touch PC restores that get users back to work faster and with minimal hassle following incidents

- Cloud-based configuration across any network that provides anytime, anywhere setup across the enterprise

- Easy app publishing that gives users access to the applications they need when they need them, on any device

- Enhanced security through predictive patching that protects against all known vulnerabilities at all times

Workspace ONE goes beyond Windows modernization to deliver workspace modernization, and UEM enables IT departments to manage every endpoint and every use case with unified endpoint management in the cloud. That includes desktops, laptops, mobile phones, tablets, and even Internet of Things (IoT) devices.

Rules-based Automation

Workspace ONE's rules-based automation of patching, policy management, and user permissions offers IT departments fine-grained customization to suit the unique needs of their organizations and users through a state-of-the-art digital workspace platform.

vmware®

Security at its Core

With security at its core, Workspace ONE takes a holistic approach to security that encompasses users, endpoints, applications, and data as well as the networks on which they all depend. Robust access controls and comprehensive compliance policies help protect valuable data. It also stays on the job 24 x 7, reacting instantly to evolving cybersecurity threats with no need for intervention from IT professionals.

Improved Productivity

Workspace ONE improves the productivity of employees, by giving them secure, anytime access to the applications they need for getting their work done. That holds true whether those apps are native to the desktop or mobile device, are cloud-based, or run independently as virtual apps.

Analytics for a Complete View

In addition, Workspace ONE Intelligence delivers critical insights into application usage through analytics that correlate device, user, and application data for a complete view of the enterprise digital environment. Among other benefits, this enables IT departments to monitor application performance to help proactively resolve issues before support calls proliferate.

Making the Transition

VMware Workspace ONE provides powerful modern management capabilities for enhanced security and productivity for every endpoint, application, and user while reducing IT department workloads.

As Windows 10 becomes commonplace, sticking with traditional endpoint management saps time, money, and organizational effectiveness by requiring intensive hands-on interaction with devices and users through disk cloning, manual configuration, and other labor-intensive practices. At the same time, it increases security risks by putting up roadblocks to timely patching and proactive security updates as IT professionals struggle to keep up.

Modern management facilitates time-and-resource-saving, more secure, real-time endpoint management, thanks to cloud APIs and a significantly improved user experience.

Transitioning to modern management in a Windows 10 environment doesn't have to be as difficult as you might think. You can get there with a modern management platform such as VMware Workspace ONE UEM, which offers both the required depth in management and automated tools to get you there faster. This—along with preassessments, staged transitions, testing, and a focus on delivering value to users—will put you on the path to success in your modern management journey.

For more information about how modern management can streamline your operations, increase security, and free up valuable resources, visit the VMware Workspace ONE website.

vmware®