WHITE PAPER – **DECEMBER 2018**

DEVELOPING A MODERN MANAGEMENT ADOPTION PROCESS

vmware®

Table of Contents

Windows 10 is rapidly becoming the operating system (OS) of the future for organizations. Microsoft made a strategic investment in mobilizing the Windows OS. With the approaching end-of-life date for Windows 7[1], organizations need to accelerate their OS upgrades. Microsoft built the Windows 10 OS to function as a mobile OS, similar to those made by Apple and Google. Windows 10 needs to be manageable from any network to enable a mobile workforce and provide users with secure access to an organization's resources from anywhere.

To make the most of these new capabilities, Microsoft requires customers to move to a new cloud-based management framework for their devices. This approach is called modern management. Modern management introduced numerous features and new technologies into the OS that are available to the administrator. An organization needs to understand what these technologies are, the impact of such technologies on their business, and how to create a modern management adoption plan that fits into their technology adoption processes and minimizes risk in that adoption.

This white paper explains a recommended process for IT architects so they can determine the appropriate aspects of modern management that can be implemented. This paper will help IT architects understand the factors that go into transforming to modern management by asking a set of discovery questions that address issues such as scale, complexity, security, and operations. This will help them to make the right decisions for their organization based on their change readiness, technology maturity, and risk profile.

This white paper includes:

- An introduction to modern management for Windows 10
- Discovery questions to best understand a Windows 10 deployment and integration points
- An explanation of the modern management adoption process
- A sample modern management adoption process based on average change readiness and an organization's risk profile
- A blank adoption process template

1. Microsoft. Windows lifecycle fact sheet. November 2018. https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet

What Is Modern Management for Windows 10?

Modern management represents the shift in the Windows OS management process to support the delivery of policies, Windows patches, and applications from the cloud. With traditional PC management, devices connect to a corporate network and IT security settings are applied to devices on the network. As users and devices have become mobile, the Windows 10 OS has been augmented to allow cloud-based delivery of security policies, configurations, and apps. Figure 1 shows an overview of the main differences between traditional and modern management across five PC management areas.

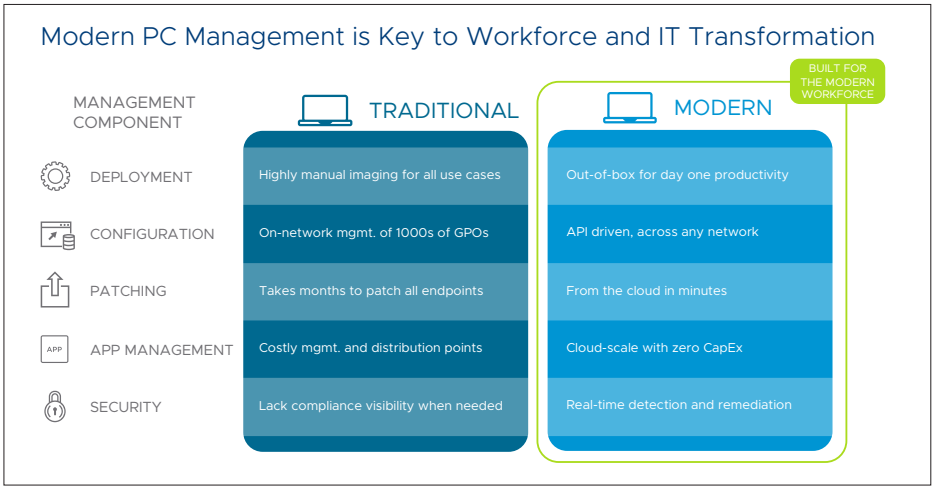

Figure 1: Comparison of Traditional and Modern Management

This white paper assumes that the reader understands the following technical aspects of Windows 10 modern management:

- Principles of the mobile device management (MDM) framework for Windows 10
- Windows configuration service providers (CSPs) for setting configuration policies on Windows
- Traditional PC lifecycle management (PCLM), including Group Policy Objects (GPOs), Windows updates, software distribution, and so on
- Traditional PCLM tools, such as System Center Configuration Management (SCCM) or the equivalent
- New features and functionality available in the Windows 10 OS, such as Windows Information Protection (WIP), health attestation, and Windows as a service
- Knowledge of both current and upcoming modern application types for Windows, such as Universal Windows Platform (UWP) and MSIX

Modern Management Readiness Discovery Questions

There are many considerations when planning how to transform to modern management. This section sets out a list of discovery questions.

The most effective method to complete discovery is to facilitate a group discussion with the right audience. Transitioning to modern management takes input from many different stakeholders in the organization, including desktop engineering, application packaging, networking, security, change management, help desk, and support. Modern management transformation requires input and engagement from all these teams to make informed decisions and make the transformation successful.

The first part of discovery is understanding what the current environment looks like:

- Describe the size of your device fleet, device models, and what Windows versions are running.
- How tech-savvy are your users? Do they use self-service, or are they open to self-service to get applications?
- How many applications are in use in your environment? How many are deployed by IT? How many are managed by IT?
- How do you set and manage configuration policies on your Windows devices?
- Do you currently deploy a corporate standard operating environment (SOE) through imaging? How many images do you have for your business units? How many applications are typically preinstalled in the image? How often are images refreshed?
- At a high level, explain your network topology. How many remote sites do you have? How many users are at each site? How is external Internet access made available to your branch offices? What are the download/upload speeds and bandwidth available?
- How dependent are you on existing PCLM tools? Which features of PCLM are being used? How many distribution nodes exist? How frequent are system updates and patches applied?

In addition, there are specific questions you need to answer to determine the right approach for your organization. The following table lists and organizes these questions by seven key components to Windows management.

COMPONENT	KEY QUESTIONS
Device and OS Lifecycle	• What is the breakdown of laptops and desktops? • Do you have a standard device model from a hardware OEM? If so, how many? • Do you deploy a standard corporate image to your devices? • How long does your total Windows imaging process take? How long does it take from unboxing to end-user ready? • What is your hardware refresh cycle? Are you getting new hardware as part of this Windows 10 migration project? • Are you using or looking to use Azure Active Directory? • Is a bring-your-own-device/bring-your-own-PC program in place or an upcoming project?
Configuration Policies	• Are your machines joined to an on-premises domain? • What percentage of devices do not actively check in to a domain controller within 30 days? • How do you deliver the configuration for Wi-Fi and virtual private network (VPN) access? • How do you configure certificates for your Windows devices? • Are users a local administrator on their computers? • Do you deploy mapped network drives? • Do you allow local file storage or leverage folder redirection? • Do you leverage cloud storage repositories, such as OneDrive? • How do you manage printer drivers and other driver updates?
GPOs	• How many GPOs are configured for your device fleet? • How many GPOs are specific to the Windows 10 OS? • How often do you change GPOs in your organization? • Who is responsible for implementing GPOs? • Do you apply different GPOs based on user profiles in your organization? • Is there a requirement to set different personalization settings for your users? • What steps have you taken to rationalize your GPOs to prepare for migration? • How do your configured GPOs compare to those that are configurable by MDM?
Patch Management	• What product are you using to deploy Windows patches? • How often are your patches released to devices? • Who is responsible for testing patches? • Do you complete application testing before new patches are released to your fleet? • Are you allowing for client devices to get Windows patches from the cloud? • On average, how long is it before 90 percent of your client devices report back that they have the appropriate patches? • Have you investigated/tested the distribution rings available in Windows as a service?

COMPONENT	KEY QUESTIONS
Application Deployment	• What tool do you use to deploy IT-distributed applications? • What is the breakdown of application types (MSIs, EXEs, scripted installs)? • What percentage of your applications are internally developed versus third-party software? • Do you repackage third-party software using a tool such as Flexera or Microsoft Orca? • How does a user request access to an application? • Are these applications available to users via self-service? • How many of your applications need to be refactored/modified to work on Windows 10? • What is your rollback plan for app updates that don't work successfully? • Do you have an application testing process? Is it integrated into image creation?
Security Policies	• Is there a Windows endpoint security framework or list of security requirements that are published and enforced by your information security team? • What password requirements do you enforce (minimum password length, password strength, password history)? • What are the most common policies configured on your Windows devices? • How do you manage device-level encryption? Where do you store your recovery keys? • What antivirus software do you apply to your endpoints? • What specific policy definitions are set in the antivirus platform? • What are your Windows Firewall settings for Windows endpoints? • What specific client firewall rules are being set? • What are your policies for unknown devices accessing the organization's data?
Reporting	• How are you reporting on your Windows device fleet? • What device/event information is being collected in your reporting tool? • How often are devices checking in and statistics being uploaded to this tool? • What percentage of clients check in within a timely manner (daily)? • Are your Windows device events being aggregated into a centralized security information and event management (SIEM) tool? • How long does it typically take to remediate a device once an IT admin gets the reporting data? • Can you trigger automated actions based on the status of the device? • Do you have application reporting specific to usage and licenses consumed? • Does your reporting contribute or integrate to asset management services? • Does your reporting tool create events in other business systems based on device information (e.g., create an IT service desk ticket, emails to managers/administrators, etc.)?

Organizations need to be aware that implementing Windows 10 modern management will also augment other processes around their OS management. These changes affect everything from application development and testing cycles, engagement with the business units, service-level agreements (SLAs), change management processes, and how information is communicated to IT and respective business units.

Some of the most important process transformation questions to consider when undertaking this project are:

- What are the steps in your IT change process?
- Who needs to approve changes that go into your Windows OS platform?
- Do changes need business and technical signoff? Are multiple approvers required for high-impact changes?
- What is the standard lead time for changes to occur?
- What is the process around expedited changes for urgent updates to the platform?
- How does IT inform the business about major changes or transformations to understand impacts on business unit–specific technology and people?
- What is the extent of consultation between IT and business units around major changes or transformations?

VMware Workspace ONE—Enabling Windows 10 Modern Management

VMware enables IT to leverage modern management to change how an organization approaches PC lifecycle management. By leveraging new technologies in Windows 10 and strong hardware OEM partnerships, VMware Workspace ONE® enables modern management across five main areas:

- **Device onboarding** – Enable co-management of endpoints with existing PCLM tools, such as SCCM, and integrations into the Windows 10 Out of Box Experience (OOBE) and Windows Autopilot.
- **Configuration management** – Apply MDM-based CSP policies to Windows endpoints and apply specific GPOs from the management console.
- **OS patch management** – Leverage the Windows as a service framework to create and update distribution rings for Windows patches, set deferment periods, and define which updates should be automatically approved by the administrator. Distribution rings can be configured based on the requirements of the organization.
- **Software distribution** – Deliver applications from different sources to users via the Workspace ONE catalog. Administrators can deliver EXE and MSI applications from the Workspace ONE UEM console and integrate directly into the Microsoft Store for Business to deliver public apps.
- **Client health and security** – Enable IT to enforce BitLocker encryption and set security policies on the endpoint. Administrators will also have access to setting policies related to WIP, Windows Hello, and other OS security features.

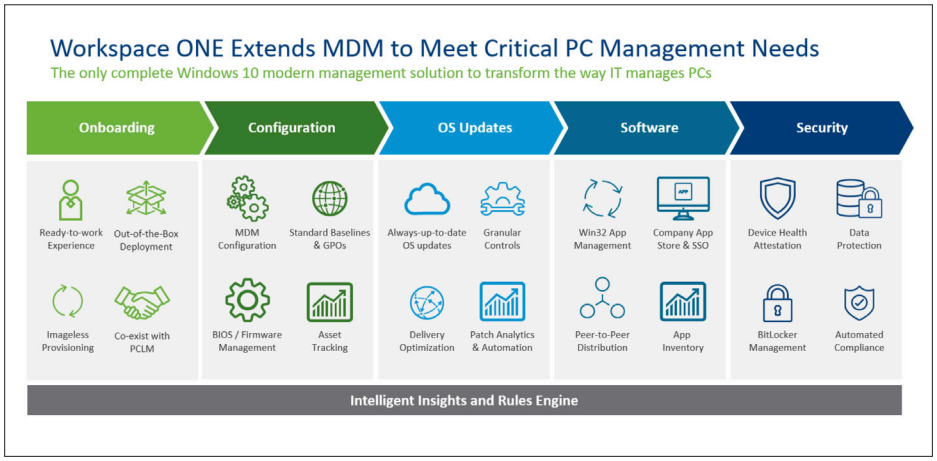

Figure 2: VMware Workspace ONE for Modern Management

Modern Management Adoption Process

The modern management adoption process provides a framework for organizations to adopt Windows transformation. This process aims to help organizations determine what modern management components can be deployed within a representative timeframe. The discovery questions in the previous section provide an indicative guideline of the complexity of core Windows components and identify which services have minimal work effort to transition.

There are five stages in the modern management adoption process. Figure 3 presents and further explains the process framework.

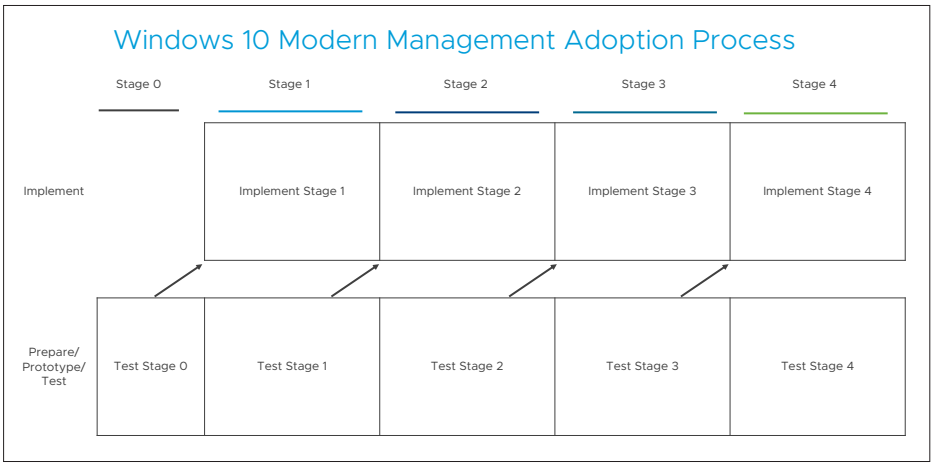

Figure 3: Modern Management Adoption Process

The key features of the adoption process are:

- Staged approach – The overall project plan for implementing modern management is broken into stages. Stage 0 occurs before the implementation starts, and Stage 4 is the final stage.
- Transformation timeframe – An organization can vary the number of stages if they choose. Typically, that's based on the speed at which they adopt technology and the overall risk profile of the organization. It is to be expected that industries such as banking and insurance minimize the risk of change and would be prime candidates for additional stages.
- Concurrent workstreams – Each stage is broken into two concurrent tasks: implementation and plan/prototype/test. The expectation is that items that fall into a stage happen concurrently. One dedicated team rolls out a tested capability, and another team tests modern management capabilities that will be rolled out in the future.
- Systematic deployment – Capabilities tested in a previous stage are candidates for rollout in the next stage. For example, an item tested in Stage 1 should be implemented in Stage 2. There are always exceptions, and certain functionality may need multiple stages to test before rolling out. Some of those functions have certain dependencies that also need to be changed before a successful rollout.
- Prerequisites – Some functionality adoption could have prerequisite components that need to be done prior to adoption and completed before testing.

Each organization will prioritize the functionality in modern management differently. They will ultimately decide to implement different capabilities at different times based on factors, such as:

- Size of deployment
- End-user impact of the change
- Use cases
- Business value
- Potential business impact
- Impact on other technologies implemented
- Whether new products need to be acquired
- Impact on IT staff and workload

Sample Adoption Process

Figure 4 illustrates a sample adoption process for an organization looking to realize modern management benefits. This organization has an existing device fleet and invested heavily in PCLM-based configurations, such as GPOs and Windows Server Update Services (WSUS). They are undertaking a transition from traditional PCLM to modern management for these devices.

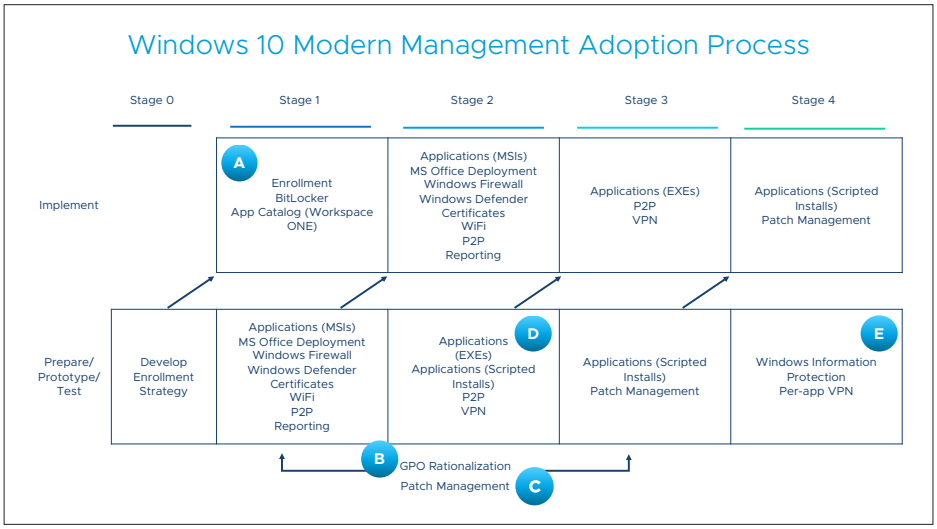

Figure 4: Sample Modern Management Adoption Process

Developing an adoption process involves a number of decisions and trade-offs between functionality, risk profile, and application adoption maturity. The following five examples explore decisions made and the rationale when building this sample adoption process.

A. Enrollment into Modern Management and BitLocker Configuration

Defining and testing an enrollment strategy in Stage 0 is critical to an organization's modern management journey. Enrollment enables other settings and functionality to be implemented during later stages of the adoption process. The goal of the enrollment strategy is to achieve co-management of Windows endpoints using a traditional PCLM tool and modern management.

Once the device has been enrolled into the modern management tool, IT decides what configurations need to be migrated. Common configurations such as device encryption are easy to implement and have no impact to existing devices encrypted with BitLocker. This can be enabled across the device fleet and allow IT flexibility to manage those policies in the modern management platform.

In addition, deploying apps such as Workspace ONE provide a platform for future delivery of corporate applications via self-serviced users.

B. GPO Rationalization

GPOs can be the most difficult component to transition to modern management. Most GPO policies are remnants of older OS versions, applications that have been decommissioned, and other past IT projects. GPOs represent a history of policies that have been configured into a Windows SOE and often are very time consuming in the migration process.

There are four steps to move GPOs to a modern framework for Windows 10:

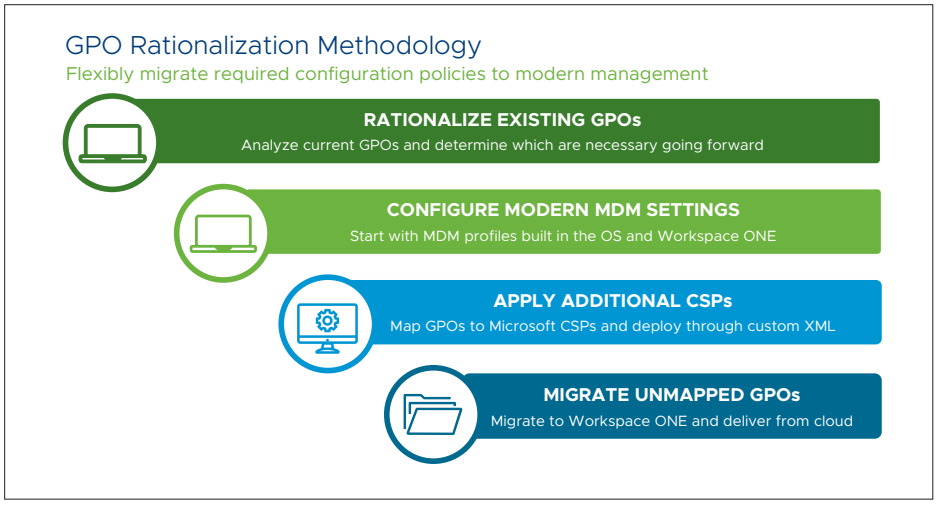

Figure 5: GPO Migration Strategy

1. Rationalize existing GPOs – Conduct a thorough assessment of the GPOs applied in an organization and determine if they are relevant/necessary. This involves engaging business owners to determine which specific GPOs have been set, whether they work on the Windows 10 platform, and whether those applications are still relevant to the organization. It is important to consolidate the list of necessary GPOs that need to be applied through modern management. Organizations can also use the security baselines technology provided in Workspace ONE if they want to create new security policies in modern management. Security baselines provide an organization with a set of best-practice configuration settings on Windows 10 that they can compare their consolidated GPO list against. In some cases, the security baseline may provide adequate coverage for most of a company's GPO settings.

2. Configure modern MDM settings – Using tools such as the MDM Migration Analysis Tool (MMAT) available from Microsoft, an organization can determine which GPOs map directly to configurable options in the MDM console. An administrator can use the console-enabled settings to easily identify which settings are applied on their device fleet.
3. Apply Microsoft CSPs via custom XML – MMAT will also identify which GPOs map to Microsoft CSP settings in the modern device management framework. Organizations can use VMware Policy Builder to generate the SyncML settings for the necessary CSPs that the GPO applies to.
4. Migrate unmapped GPOs – Certain GPOs will not map to CSPs but are still necessary to an organization. In these cases, alternative methods may need to be employed, such as GPO baselines or custom PowerShell scripts to apply specific registry settings. This should be employed as the last option to allow an administrator to use CSPs as the best practice for policy configuration.

The complexity of migrating GPOs to the modern framework is why GPO rationalization is shown as a multistage component in Figure 4. Organizations need to consolidate their current GPO settings and make decisions on the best approach to configure these in modern management.

C. OS Patch Management

The patch management process in Windows 10 is another significant shift for organizations to make. Microsoft introduced Windows as a service as the mechanism to simplify the servicing of Windows computers and reduce the resources needed to deploy and maintain Windows over time. Microsoft moved to a six-month cadence for major Windows releases (called feature updates) and a roughly monthly cadence for security and reliability fixes (called quality updates).

There are four considerations when implementing Windows as a service for modern patch management:

1. Servicing channels – Windows as a service introduced servicing channels to streamline the build and testing of Windows updates. IT administrators are responsible for deciding which servicing channel is suitable for their endpoint devices. As best practice, the majority of general-purpose PCs use the Semi-Annual Channel. Specialized devices that serve a critical function (such as ATMs, point-of-sale devices, and manufacturing control PCs) may use the Long-Term Servicing Channel. Many companies build deployment rings via modern management policies to set their user acceptance testing (UAT) devices in the Semi-Annual (Targeted) Channel or earlier.
2. Deferment period – Microsoft introduced configurable deferment periods for specific update types as part of the Semi-Annual Channel. Feature updates can be deferred for up to 365 days (for Windows 10 version 1703 and higher), and quality updates can be deferred for 35 days. Organizations need to set how long they want to defer updates from machines to give them time to test and deploy with minimal risk.

3. Application dependencies – Because many organizations develop their own applications for in-house use, changes to the Windows OS may have a direct impact on their application performance. Feature updates and major OS version changes now happen frequently and incrementally, when compared to large OS migrations that may have happened in the past (such as Windows XP to Windows 7, and Windows 7 to Windows 10). This now requires organizations to carefully analyze their application performance more regularly to coincide with the rollout of Windows feature updates. This will likely increase investments in automated testing and DevOps to reduce the burden on IT.
4. Impact on network performance – Delivering Windows updates from the cloud will impact network performance for remote offices. Traditional remote office architectures, such as hub-and-spoke, centralize performance and internet connectivity. This network architecture may be less advantageous for cloud delivery, and the overall impact on network performance should be measured before enabling Windows as a service. Organizations may need to invest in upgrading network connectivity at sites and test new delivery optimization models to coincide with Windows updates being delivered from the cloud.

Traditionally, companies have used services, such as WSUS, to triage available patches and deploy to corporate endpoints. Windows as a service removes the option to decline a Windows update. This requires an organization to test their applications before releasing every feature and quality update. Instead of completing these application tests for every major OS change, organizations need to match the feature and quality update cycle, which means testing as often as every 35 days.

As well as being prepared for the technical impact of cloud-based patch management, organizations need to be more agile in their change management and active in their engagement with business units. A clear UAT process for new versions of business applications for the Windows OS must be documented and allow for signoff by IT, business units, and leadership.

This process transformation is why patch management is shown as a multistage component in Figure 4. Organizations need to get comfortable with the new technology in Windows as a service and analyze the impact that the new mechanism has on their existing Windows application and OS testing procedures.

D. Migrating Applications (EXEs and Scripted Installs)

Applications such as EXEs and scripted installs are complicated to move to modern management because they may have legacy dependencies that introduce complexity when delivering the app. A consolidated application portfolio is critical to planning the app migration strategy.

MSI applications are significantly easier to deploy using modern management because the MSI includes the necessary installation command line, exit codes, and install completion parameters. It is recommended to begin the application deployment in modern management for MSI apps, and why it is shown as an earlier component in Figure 4, as compared to EXEs and scripted installs.

It is recommended to allow a longer timeframe to migrate EXEs and particularly scripted installs, so that an organization can consider these three factors:

LEARN MORE

VMware Workspace ONE lowers the cost of managing an organization's Windows deployments, secures endpoints and data on any network across any application, and delivers peak user experience across any device.

Contact your VMware Account Team to learn more about the transition to modern management.

AUTHORS AND CONTRIBUTORS

Adarsh Kesari, Staff Solutions Architect in VMware End-User Computing, authored this white paper. Adarsh's primary function is to provide transformational guidance to help organizations adopt Windows 10 modern management.

Contributors to this document include:

- Mike Nelson, Senior Solutions Architect, Windows Product Engineering, VMware
- Bryan Garmon, Senior Solution Engineer, AMER End-User Computing Systems Engineering, VMware
- Sean Hanrahan, Senior Solution Engineer, AMER End-User Computing Systems Engineering, VMware
- James Murray, Staff Solution Engineer, AMER End-User Computing Systems Engineering, VMware
- Justin Craig, Senior Solution Engineer, AMER End-User Computing Systems Engineering, VMware
- Mark Margevicius, Director of End-User Computing Strategy and Chief Customer Advocate, VMware

1. Application complexity – EXE and scripted-install apps are often very complicated, having many dependencies or referencing other applications or files on the endpoint. Many internal apps lack documentation as to how the app functions. An organization needs to fully understand how an EXE or scripted-install app works before trying to migrate it to modern management.
2. Network performance – App delivery from the cloud introduces complications to traditional network architectures, such as hub-and-spoke. IT needs to assess the impact of cloud-based delivery of apps on their network performance. Remote or non-domain-joined users are often the easiest use case for delivering apps from the cloud. These users are not often connected to the corporate network and often work with a direct connection to the Internet.
3. Application sustainability – The MSI platform is simpler to migrate to modern management and easier for app developers to make necessary incremental changes. The work effort required to move EXEs and scripted installs to MSIs should be assessed by organizations. This assessment will provide time and cost estimates to make an informed application migration decision.

Microsoft also introduced the MSIX platform, where organizations can package their apps and deliver from the Microsoft Store. This platform will continue to evolve with future Windows versions and may become the preferred migration path for EXEs and scripted installs.

E. Windows Information Protection and Per-App VPN

Newer technologies in Windows 10, such as WIP and per-app VPN, have been left to the final stages of testing in the example in Figure 4. WIP allows IT to delineate between the organization's applications and personal applications on a Windows device. Specifying an application as WIP-enabled forces it to be marked as managed, and data associated to the app is encrypted. There are some use cases where WIP may be implemented, such as a fully corporate endpoint. Organizations can develop strong use cases to implement this evolving technology once they understand the end-user behavior and apps that need to be targeted.

Per-app VPN is another new development for the Windows 10 OS that will continue to mature. Many organizations already implement a device VPN for Windows, especially for remote employees. Per-app VPN allows IT to designate what app traffic is routed through the company's data center. Changes to the VPN platform may impact end users. To avoid this risk, it is recommended that organizations understand user workflows for Windows applications before building a per-app VPN strategy.

Both WIP and per-app VPN on Windows 10 will continue to mature and present more use cases for customers. These use cases may accelerate the prototyping and testing of these functions, which may become tasks completed at earlier stages of the adoption process.

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

12/18