Overcoming the Top 5 Challenges to Windows 10 Adoption

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Ivanti

April 2017

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Executive Summary

The introduction of Windows 10 promises a wealth of advantages for enhancing user experiences. Most notably, it unifies the operating environment across mobile and PC endpoints. However, organizations faced with performing mass migrations to the new platforms face a number of significant challenges, the top five of which include:

- Too many software components to update
- Business environment disruptions
- Enabling rapid patch deployments
- Meeting security requirements
- Managing heterogeneous devices

Only with the adoption of comprehensive automated migration solutions can these challenges be overcome in a controlled manner that ensures a successful and reliable transition to Windows 10.

Are You Ready for Windows 10?

The latest release of Microsoft flagship operating system, Windows 10, is here, promising a wealth of usability improvements wrapped up in a familiar user interface. With a look and feel more akin to Windows 7, most users will find this environment a refreshing change from the much reviled Windows 8 tiles-based interface. Windows 10 is poised to be the dominant PC operating system (OS) for the next decade and is notable for unifying the application and desktop environments across all endpoint device types (i.e., desktop, laptop, tablet, and smartphone). The new OS also allows applications to be easily ported from other platforms (e.g., Linux, iOS, Android, etc.), establishing a common user environment that can run any application on any device. Enhanced security in Windows 10 includes multifactor identification and data loss prevention (DLP) through the use of containers. If all these new features in Windows 10 are not enough, Microsoft is providing additional incentives for rapid adoption by offering free upgrades for one year on any devices currently running Window 7 or Windows 8, and it has guaranteed a 10-year support lifecycle for the platform.

While one might think the advantages to Windows 10 would entice organizations to embrace the new OS, there is still substantial apprehension to initiating enterprise-wide migration processes. The central problem is the sheer complexity of coordinating large numbers of disparate people and devices while ensuring controlled and secure OS deployments. Naturally, the larger and more complex the organization is, the greater the likelihood it will experience slow migration times and business disruption. Organizations relying on manual migration processes have an increased likelihood of introducing human errors that further affect business productivity. Ultimately, these negative user experiences with the migration process will detract end users from employing Windows 10 and will reflect badly on the IT operations team responsible for deploying it.

> While one might think the advantages to Windows 10 would entice organizations to embrace the new OS, there is still substantial apprehension to initiating enterprise-wide migration processes.

Faced with the prospect of a painful transition, many organizations will choose not to migrate some or all of existing devices, but instead will allow the OS introduction to occur through natural attrition processes—that is, to introduce Windows 10 only with new or replacement devices. While this approach avoids the migration process entirely, it means IT organizations will have to indefinitely maintain a number of older OS editions. This becomes a particular problem as those older environments reach end-of-life (as has already occurred with Windows XP). Additionally, multiplatform support exponentially increases management efforts proportional to the number of environments that need to be maintained. For instance, each platform will need to be independently patched, provisioned, and configured with separate deployment processes. A more pragmatic approach is to take advantage of the current migration incentives and strategically employ automation to transition existing devices with little or no impact to business productivity.

Top Five Challenges to Windows 10 Adoption

Listed below, in no particular order, are the top five challenges organizations encounter with Windows 10 migrations along with recommended solutions for avoiding or negating these pitfalls. Each organization is different, and some will find a particular challenge more critical than others. These unique enterprise requirements should be carefully considered when prioritizing the requirements for adopting or developing a migration solution.

#1 Too Many Software Components to Update

The problem…

A typical endpoint hosts hundreds of software elements, including applications, drivers, patches, firmware, email, databases, and graphics enablement software. Each of these software elements must be updated to the latest edition that is compatible with Windows 10. Microsoft's User State Migration Tool (USMT) is only able to install and configure the base operating system and desktop; it relies on a post migration execution of Windows Update to transition any additional software elements. However, Windows Update does not support all applications and any proprietary or unsupported software elements will need to be manually installed by the administrator. In some cases, the OS migration tool overwrites portions of existing software code leaving it in an "installed" but not operational state. Windows Update will not reinstall or report these damaged applications as it does not recognize them as being faulty. This is a particular problem with device drivers, which have proven to be particularly unreliable post migration and almost always need to be completely reinstalled.

Lacking an understanding of which software elements will be impacted by a Windows 10 migration, many organizations blindly perform the migration with the belief that they can remediate any issues post migration. Unfortunately, damaged or incompatible software elements are time-consuming to identify, diagnose, and reinstall, even for experienced IT administrators and the larger the support stack, the greater the number of potential problems. Non-technical workers will be severely inconvenienced by an inability to access critical apps and software services post migration and may further damage their environment if they attempt to repair these issues themselves.

The solution…

The first step in any migration process must include an audit of all hardware and software assets to ensure they will be compatible with the new OS. This information should be recorded in an asset database to enable centralized reporting. From this, the most common applications employed by the company should be easily identified. These applications should be tested prior to the mass distribution of Windows 10 to identify any compatibility or migration issues. Any challenged software elements should be flagged for post-migration reconfiguration or reinstallation. Additionally, it is important to perform a financial analysis to identify any costs that will be necessary to upgrading the infrastructure in order to meet compatibility requirements for Windows 10.

An automated, centralized deployment packaging or imaging solution is essential to controlling the mass migration of Windows environments. It is important to adopt a solution with built-in migration capabilities and that can bundle in pre- and post-migration tasks—including software deployments, updates, patching, and configurations—enabling complete migration processes to be built on a centralized environment and customized to meet unique user requirements. To ensure all software deployments and updates complete successfully and uninterrupted (and also to eliminate administrator interaction with the migration processes) the automated solution should be able to manage installations through numerous reboots and should monitor the migration process through completion to ensure final system configurations meet predetermined standards for compatibility. Any errors encountered during migrations should be immediately reported to IT administrators for remediation.

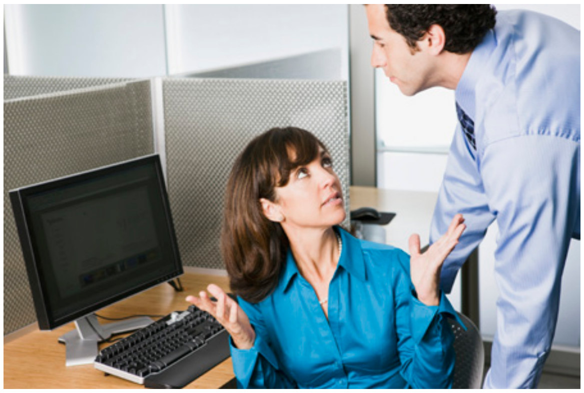
#2 Business Environment Disruptions

The problem…

Mass operating system migrations are extremely disruptive to business productivity. A single installation process can temporarily saturate a network segment as it downloads the numerous system, patch, application, and driver updates. Since standard migration processes deploy directly from Microsoft and third-party drivers, and applications are also installed from remote systems, the primary bottleneck for network activity is the local internet access point. Should hundreds or even thousands of migrations occur simultaneously for instance through a mass upgrade, an entire business production network could scream to a halt. Local servers may similarly be impacted if they host software elements necessary for a migration.

Perhaps most impacted by a migration process are the users themselves. Installing Windows 10 takes time, especially if there are a number of additional applications or drivers that need to be reinstalled after the OS migration process completes. Since most workers are dependent on their devices to perform their job functions, migration processes may incapacitate those users for as much as a day—or perhaps several days—if a problem arises that is not easily resolved.

Even after the migration process has completed, users will need to take the time to familiarize themselves with the new environment, particularly if they are transitioning from an environment that is very different from Windows 10, such as Windows 8 or Windows XP. The amount of time it will take users to adjust to the new environment will depend on their individual technical knowledge and skills, but could be counted in days or even weeks. Aggregated across an entire enterprise, this translates into a stunning loss of workforce productivity that could result in lost revenue and/or an inability to meet business requirements.



The solution…

Windows 10 migrations must be controlled centrally by IT operations. Prior to deployment, all pre-existing user applications, data, and configurations should be backed up to preserve a known, safe environment for recovery in the event of an unexpected migration problem. IT operations should schedule migrations so that they occur out-of-hours (i.e., evenings and weekends) without requiring any user interactions. Wherever possible, elements of a migration—including application, patches, drivers, and the Window 10 operating system—should be staged on a server on the local network to prevent unnecessary WAN and internet traffic. Also, while "multicasting" solutions will allow multiple migrations to be implemented simultaneously for speedy migration schedules, groups of deployment should be carefully distributed to ensure network bottlenecks are never fully saturated.

To simplify user transitions to a potentially unfamiliar environment, migration processes should export personal settings (e.g., file locations, shortcuts, preferences, etc.) from the users' pre-existing environments into the new Windows 10 environment. Additionally, remote access capabilities should be employed that allow administrators to see and control user desktops to enable remote training and problem remediation following migrations. In the event a major and unexpected issue should occur during or following a migration, the affected user environments should be rolled back to the pre-existing environment. The issue can then be resolved while users continue to function in the old environment, and migrations may be reinitiated after a solution is found.

#3 Enabling Rapid Patch Deployments

The problem…

It should be no surprise that even with the most ardent testing new software environments are invariably riddled with unexpected performance and security issues. Previous Windows releases adhered to this rule, and there is no reason to expect Window 10 will be an exception. As issues arise, patches are distributed by both Microsoft and third-party vendors to support applications and device drivers. However, the challenge is for organizations to rapidly distribute these updates as any lag time between patch availability and deployment is time when the business is at risk. The reason for this is that malicious hackers monitor for the release of a new patch, evaluate it to identify the vulnerability that is being repaired, and then target that vulnerability with malware and other breach attempts with the expectation that most businesses will take days or weeks to actually deploy the newly published patch. Often called "zero day vulnerabilities," this significant security risk is extenuated by the reality that manual patch deployments are time-consuming and are often dependent on direct connectivity with all devices in the support stack (which is unlikely due to an increasingly mobile workforce).

Similar to the problems encountered with multiple OS migrations, mass patching of devices can also impact business productivity. Microsoft's much reviled "Patch Tuesday" processes are a great example of this. Since the vendor releases major patch releases on that particular day each week, the majority of devices—particularly those running Windows Update—will download and install updates at the start of the Tuesday workday when workers turn on their PCs. Since patches are downloaded from remote vendor hosting environments, simultaneous patch deployments commonly create network bottlenecks and severe performance degradation. These conditions are symptomatic of organizations that lack control over their patch deployments.

The solution…

The delivery of system and application patches should be automated and centralized. Vulnerability management solutions should proactively monitor for vulnerabilities from all critical system, driver, and application providers. As soon as new vulnerabilities are detected, they should download patches automatically onto a local staging area in preparation for mass distribution. If any supported systems require multiple patch deployments, they should be bundled into a single installation along with any required pre- or post-installation automated configuration processes. If possible, patches should be scheduled to be deployed during the earliest convenient off-hour time period (such as evenings or weekends) to minimize impacts on the production network and user productivity. Patch deployments should also be monitored to ensure they complete successfully, and audits should be continuously monitored to ensure they are on all the latest patch versions to minimize risks.

#4 Meeting Security Requirements

The problem…

It is an unfortunate but predictable problem that the amount of targeted malware and other security attacks are directly related to the popularity of the supported platform. Simply put, hackers know they can maximize the attention they receive from their malicious deeds when they focus on high-profile environments. It then follows that an intensified number of zero-day and other targeted attacks can be expected for the highly publicized Windows 10 OS. It must also be recognized that antivirus scanners alone cannot combat the predicted rise in vulnerabilities.

With Windows 10, Microsoft has introduced a number of new security features that should be leveraged with revised or new support practices. For example, security, maintenance, and alert settings have been relocated to the new Action Center—a centralized tool for managing all system notifications—so existing scripts or automated processes will need to be redirected to accommodate the change. Additionally, Windows 10 is recording a wealth of sensitive information on user activities that could be used maliciously if inappropriately acquired. Cortana, an interactive indexing and organization tool, is arguably the most significant potential security violator native to Windows 10. Among the data Cortana is collecting are all websites visited, online purchases made, and a user's geographical location. Fortunately, Microsoft does provide privacy settings that allow these features to be disabled, but they are on by default, and it is unlikely users will make any adjustments to these on their own. Additional settings, such as for those defining password and access permissions, will also need to be set for every Windows 10 device in the support stack. It is essential that all security configurations be deployed during the migration process to enable users to easily transition between the two environments.

The solution…

Security policies for Windows 10 deployments should be strategically standardized to reflect the new threat environment. Any automated security management solutions adopted to support the environment should include tools specifically designed to support Windows 10. This will remove the guess work from security management by targeting the threats unique to the new environment. The management platform should also proactively monitor for any potential breaches or policy violation. While this includes virus and malware detection, proactive monitoring must extend beyond these to provide full control over devices and applications. Recorded status data will also provide critical proof-of-compliance to help meet regulatory requirements. To standardize and control access privileges, employ role-based management solutions that are customized to meet the businesses unique security requirements.

#5 Managing Heterogeneous Devices

The problem…

One of the core value promises of Windows 10 is that it unifies the operating system across multiple endpoint device types—including smartphones, tablets, laptops, and desktops—using common application and accessing common data files. From an IT management perspective, however, this requires a fundamental change in how user devices are supported and managed. Traditionally, IT organizations support PCs and mobile devices with independent management solutions. This was principally because the operating systems were radically different between the two platforms (e.g., iOS and Android devices versus Windows and Mac devices). However, with a unified Windows 10 environment, it no longer makes any sense to maintain separate interfaces to support different device types. Often called "swivel-chair management," managing with multiple interfaces is both time-consuming and error-prone because it relies on the manual, independent execution of monitoring, configuration, and provisioning tasks. Each unique interface requires different support processes and practices that extenuate management complexities. It is also nearly impossible to standardize policies and privileges across multiple interfaces because profiles would need to be manually synchronized on a continuing basis.

Heterogeneous device management is further challenged when also needing to support non-Windows and virtual devices. For instance, application deployment solutions—such as an app store, service catalog or packaging solution—may not be centralized for all managed environments. This is a particular problem for adopters of the Windows 10 Business Store as it does not support non-Windows devices, requiring organizations to adopt a mix of methods for deploying applications.

The solution…

Unified endpoint management (UEM) solutions enable centralized management for all PC, mobile, and virtual devices in the support stack. With this approach, a single console interface is employed to configure, monitor, and maintain all essential system, security, and application support elements. This allows configurations to be standardized for simplified management and to help establish a common user experience across devices. In particular, the ability to employ common user profiles for all support devices will allow administrators to set access privileges and authorization settings in a single location. Additionally, consolidated monitoring and reporting enables the generation of comprehensive health status and usage reports for SLA and compliance attainment.

Effective Migration Solutions

The successful and controlled transition of enterprise clients to Windows 10 can only be accomplished with the assistance of an automated management solution with comprehensive migration capabilities. While the native Microsoft migration tools and other migration point solutions may be sufficient for home users, they lack the configuration and security management support essential to achieve business operations requirements. Also, these basic tools fail to provide sufficient visibility into compatibility issues and installation errors, making any unexpected problems difficult to diagnose and remediate. Instead, a fully-integrated management solution suite should be employed that ensures Windows 10 deployments are secured, configured, and maintained through every stage of the migration, including pre installation, deployment, provisioning, and post installation.

As an example, Ivanti's flagship platform, the Ivanti Unified Endpoint Management suite, delivers a consolidated solution for endpoint and security management with purpose-built features to simplify migration processes. The platform is designed to manage physical, virtual, and mobile clients across their entire lifecycle through a true UEM experience administered from a centralized console that includes compliance overviews, reports, and alarms. Fully automated migration capabilities are included with the Ivanti Endpoint Management module. Beginning with asset detection and full system auditing, the solution records endpoint information and includes granular details on hardware and software configurations as well as compatibility checks and upgrade cost assessments. Armed with this information, the entire migration process can be centrally managed for all devices in the support stack. Migrations may be run in the background or scheduled to perform off-hours to minimize impacts to business productivity. The automated deployment and provisioning tasks may be performed though multiple reboots with continuous monitoring to ensure administrators are alerted to any issues and receive confirmation of migration successes. With user state migration functionality, all pre-existing configurations and user environment settings are ensured to be correctly mapped to the new environment, and through direct integration with Active Directory, role-based user profiles are enabled to simplify management and enhance user experiences. Applications can be provisioned, configured, and updated during the migration or hosted on a corporate app store. After the migration, the Ivanti solution provides remote troubleshooting features to simplify user problem remediation and training. Should all else fail, backup and restore capabilities are included with the platform to roll systems back to a state prior to migration.

> Ivanti's flagship platform, the Ivanti Unified Endpoint Management suite, delivers a consolidated solution for endpoint and security management with purpose-built features to simplify migration processes.

Fully integrated with Ivanti Endpoint Management is the Ivanti Endpoint Security module which adds additional layers of risk mitigation during migration processes from a single unified console. Employing a "defense-in-depth" strategy, the platform provides a multilayered security solution to enable persistent threat protection. OS, configuration, and third-party application patches are continuously monitored for availability and can be rapidly deployed to heterogeneous endpoints, minimizing zero-day vulnerability risks. Application controls ensure enterprise software is only accessible by authorized users, and device controls restrict the inappropriate use of removable devices (e.g., USP flash drives) and media (e.g., DVDs/CDs) to prevent data loss and theft. Additionally, the solution includes full malware prevention, including centrally managed scans and removal of viruses, worms, spyware, adware, and other malicious threats. Knitting together endpoint and security management functionality, the Ivanti Unified Endpoint Management suite delivers all the essential capabilities necessary for ensuring a successful enterprise-wide Windows 10 migration process.

EMA Perspective

The impact Window 10 can be expected to have on enterprise mobility cannot be understated. It is arguably the single most critical release of the OS Microsoft has delivered in 15 years, so it is no wonder that Microsoft has been so aggressive with providing incentives for migration. Over the past decade, the focus of PC and mobile device platforms has shifted towards facilitating the "consumerization of IT," focusing more on meeting home user requirements while broadly neglecting enterprise requirements. Windows 10, however, is a game changer. A unified OS across all device types means that common desktop environments, applications, and data can be accessed from any endpoint without requiring any code rebuilds or translation software. This directly addresses the needs of the enterprise market and particularly for business that rely on proprietary software to support unique job functions. EMA expects that the availability of Windows 10 will broadly expand adoption of Windows-based tablets across many industry verticals but especially among health care, financial, and educational institutions.

Given the inevitability of Windows 10 dominance (at least in the PC market), early adopters of the platform will have an advantage over slower competitors. The ability to push out a single software release to all user devices dramatically increases business agility to respond to customer requests and to meet changing business requirements. Technological superiority has always been a boon to business profitability as it results in improved products and services while increasing operational efficiencies. Since the lifespan of Windows 10 will undoubtedly be counted in decades, broad transition to the platform is simply a matter of time, but the greatest benefits will be achieved by those who get there first.

Enterprise-wide OS migrations can seem a daunting task. However, the primary decision for IT managers is whether to approach Windows 10 migration challenges in a controlled or uncontrolled manner. If an organization fails to plan a strategic migration, updates will occur in a random, chaotic fashion that will disrupt business operations, reduce user productivity, and overwhelm IT operations with time-consuming incident requests. The adoption of automated unified endpoint management solutions, such as those offered by Ivanti, enable centralized control of every step in the deployment and management process to enable reliable and secure migrations allowing organization to rapidly and most effectively attain value from their Windows 10 adoption.

About Ivanti

Ivanti is IT *evolved*. By integrating and automating critical IT tasks, Ivanti helps IT organizations secure the digital workplace. For more than three decades, Ivanti has helped IT professionals address security threats, manage devices and optimize their user experience. From traditional PCs, to mobile devices, virtual machines and the data center, Ivanti helps discover and manage your IT assets wherever they are located, improving IT service delivery and reducing risk. Ivanti also ensures that supply chain and warehouse teams are effectively leveraging the most up-to-date technology to improve productivity throughout their operation. Ivanti is headquartered in Salt Lake City, Utah, and has offices all over the world. For more information, visit www.ivanti.com.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
3268.040417