vmware

A Definitive Guide to Windows 10 Management: A VMware Whitepaper

November 2015

Table of Contents

Executive Summary

With Windows 10, Microsoft introduces a consolidated operating system (OS) platform that changes how organizations treat the management of End-User Computing (EUC) environments.

Windows 10 mobile management technologies are easier, faster, and less complex than prior versions of Windows. These fundamentally different "mobile-first" changes are broad and far-reaching in terms of IT management issues involving platform updates, the cadence of change, application design and delivery, end-user autonomy, and enhanced security. This new way of managing Windows is more closely aligned to the enterprise mobile management (EMM) based approaches found in mobile management tools today.

Windows 10 has many important characteristics and features that will have a significant impact on organizations. The mobile and cloud features change Windows from a PC-centric OS to one that is device agnostic and critical to an organization's digital workplace.

The key management enhancements that Windows 10 introduces include:

- Dynamic and continuous updates
- Universal applications that work across different devices
- Cloud-based directory integration and services
- Enterprise Data Protection
- Seamless user experiences
- Windows Store and Business Store Portal

For many customers, implementing new ways to manage Windows can be overwhelming; the tools, processes, and skill sets for EMM management are different than that of PC management. Microsoft recognizes the value of not being overly aggressive when positioning new management technology with its current customers and allows IT administrators to manage Windows 10 much the same way as Windows XP, Windows 7, or even Windows 8. Customers who view Windows 10 exclusively as a PC platform often cite that management consistency between older versions of Windows is a top criterion when contemplating OS migrations.

This whitepaper provides an overview of how Windows management evolved from a rigid and disruptive PC-centric approach to one offering a flexible and light-touch model. It will also delve into the specific management technologies that Windows 10 introduces, as well as leveraging conventional Windows management tools that are in use today.

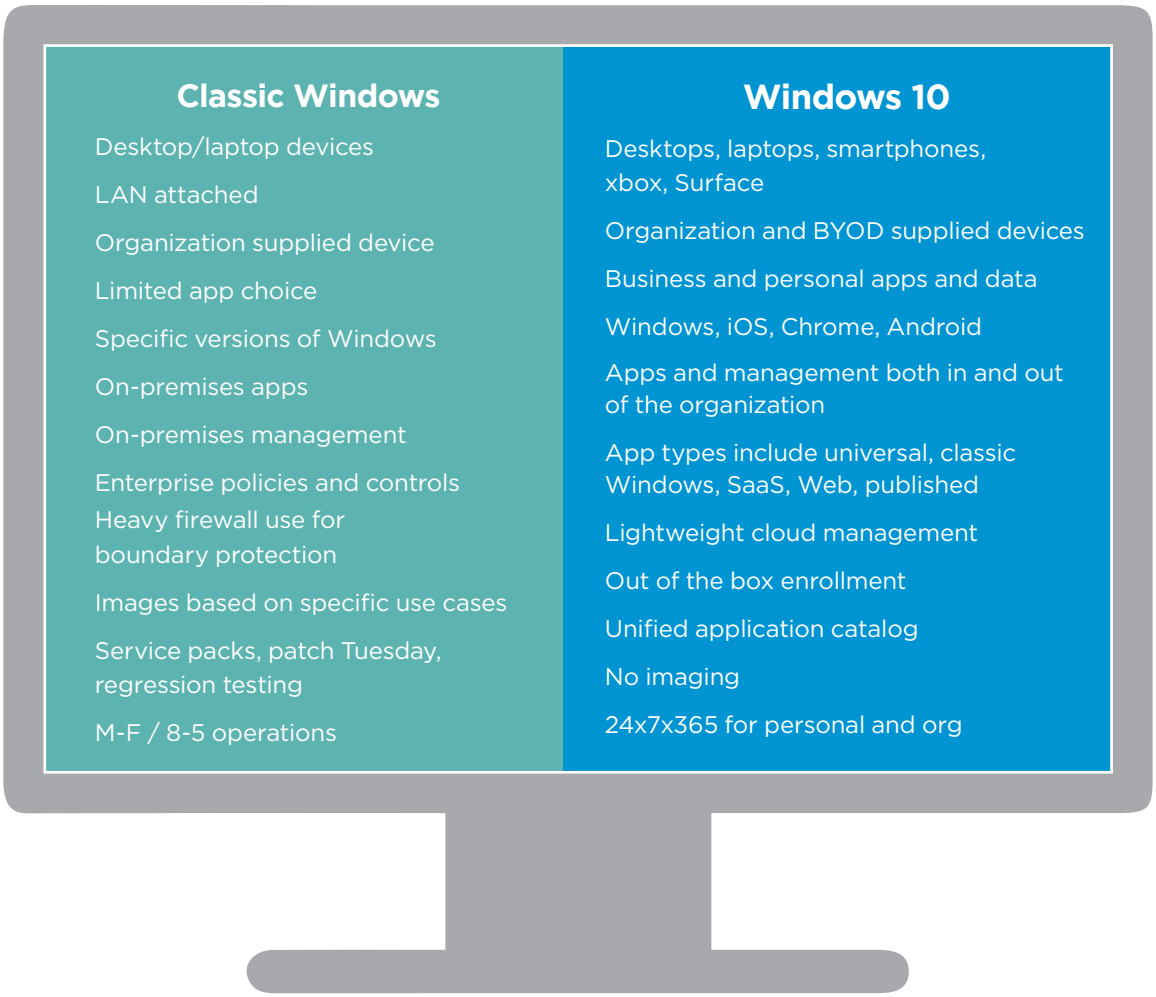
Challenges with Windows Management

Windows Management has been a long and difficult journey for IT organizations over the past 20 years – traditionally very complex, costly, siloed, heavy-weight, and error-prone. Further, the restrictions of being network connected, domain-joined, and running on either a desktop or laptop made Windows management restrictive in use and limited in capability. Through the decades, the dynamics of management evolved to where management requirements now include:

- Application delivery
- Patch management
- Inventory
- Reporting
- Analytics
- Security management
- Policy management
- Data backup

Despite the best efforts of vendors and customers, the principles that underpin Windows architecture remained largely unchanged, which resulted in organizations spending a disproportionate amount of their operational budget on maintenance and support for PCs, Windows, users, and their configurations – all with often minimal success.

For example, it is not uncommon that new PCs are delivered to users in a well-managed state, whereby the configuration, settings, applications, etc., are integrated for optimal use. Initial configurations work well enough for a while, or until things change. Over time, users often unknowingly make changes to their configuration, become targets to malware, or have new application requirements that make the standard configuration vulnerable, obsolete, or unstable. IT staff then begins a series of triage tactics to provide temporary fixes. It is not uncommon for PC performance to deteriorate to a point where IT admins need to completely refresh the machine by wiping and replacing the image.



The scenario above impacts nearly every customer with PCs in use. It is not uncommon for operational costs to represent nearly 40% of all PC-related costs, and with little or no benefit to either the user or enterprise. In addition, costs associated with lost productivity (e.g. downtime, help desk time, time lost to reboots because of system instability) further add to organizational burden. This includes indirect costs, which often go unmeasured or ignored.

Organizations and users need a better way – one that is easier, simpler, more reliable, and more secure. The new EMM technologies in Windows 10 introduce better ways to address many traditional management shortfalls and will elevate productivity and security of the user at a lower cost. Customers should be mindful to the inevitable impact this has on the organization; according to Gartner, "By 2018, the number of organizations managing a portion of their PCs/Macs with an EMM system will rise from less than 1% today to 40%."[1]

[1]Predicts 2016: Mobile and Wireless," Gartner Research G00273934, October 2015.

How Windows 10 Differs

Time waits for no man, or technology. EUC has had phenomenal growth beyond the PC; device diversity in the hands of users is the de facto standard today. The first choice for many users is often a mobile device (laptop, tablet, or smartphone), for use both in and out of the office.

Group Policy Object (GPO) transitioning to EMM

Managing this diversity requires a new approach that is fundamentally different to that of legacy PC management. Legacy Windows management is largely dependent upon GPOs, which while effective for PCs on an enterprise network, are difficult for devices not on the network. This means that emergency updates and fixes are inconsistently delivered, bringing unnecessary risk to organizational data and users. GPOs are also OS-version specific, which means that organizations embracing a BYOD strategy will have exposure and risk. Pre Windows 10 BYOD management requires a separate EMM-based management infrastructure, which adds cost, complexity, and redundant operations for organizations.

Sandboxes and Primitives

EMM employs a fundamentally different approach to platform control. Mobile operating systems, such as iOS, Android, and now Windows 10, have an underlying “sandbox” architecture that creates environments of separation and isolation on a device. Sandboxing protects the OS kernel from rogue applications, virus, malware, etc. Sandboxing touches all major components (including memory, storage, and data) so that each application is protected from the actions of any other application on the device. Windows 10, along with other mobile operating systems, also includes enterprise management primitives that offer more granular control of additional OS management functionality, such as adding and removing applications, network controls, certificate storage, and per-application VPN functionality. This means that organizations have much more latitude with configuring devices without compromising the integrity of the kernel.

Common APIs across all devices

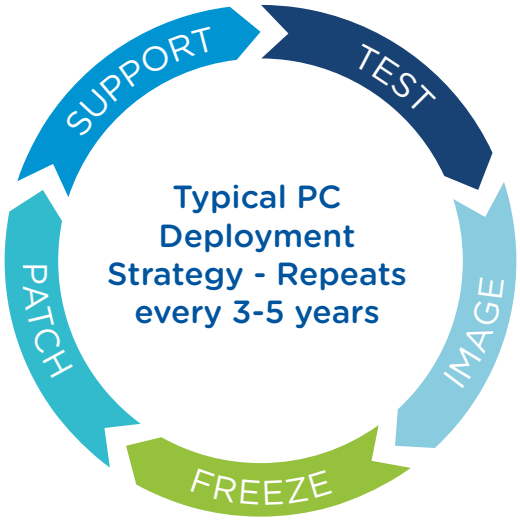
The success of an application is, in part, dependent upon the success of the underlying operating system. When PCs were the only devices, having a single version of Windows simplified application development, delivery, and management – ultimately making Windows a success.

As platforms and device types diversified, developers faced a choice of competing platforms. APIs were not unified across mobile, desktop, and embedded versions of Windows. With Windows 10, Microsoft has introduced a unified set of APIs ("Universal Applications") so that developers can write a single code base and have it run and managed on any device. This simplifies application development, platform support, and device management for organizations and users alike.

The introduction of EMM management, sandboxing, and universal APIs on all enterprise devices will have significant operational impact over time. Organizations will be able to approach all devices in the same way, which will dramatically simplify management and operations over lifetime use. IT administrators will spend less time managing devices and applications, and will instead be able to focus on users, use cases, and context of use. EMM introduces device portability, free-flowing data, and better protection at a lower cost.

Windows 10 Management Features

Pre-Windows 10 management features were designed in an era when the rate of change for the operating system was intended to produce a static and highly standardized environment. Major releases of the operating system occurred periodically (normally every 3-4 years), with intermittent updates (via hot fixes and service packs) happening as needed.



As a result, organizations built highly standardized processes around software/platform/image updates that typically aligned with the device refresh strategy for desktops and laptops (typically every 3-5 years). Today, this approach to management is costly, fraught with error, incomplete, and makes the deploying organization slow to react to new requirements. This all changes with Windows 10.

New Methods of Updates

Microsoft has made the cadence of Windows 10 updates more frequent and dynamic, where OS fixes, patches, updates, etc., are deployed in a variety of client servicing plans. This aggressive update strategy is used as a means to ensure users always have access to the latest and greatest OS features, updates, and fixes.

For many enterprises, this aggressive update strategy will not be ideal, and they will prefer to employ a more tempered approach to system updates. To help with this, organizations can pick from three different processes to maintain Windows 10 on PCs and mobile devices that require enterprise stability: the Current Branch, Current Branch for Business, and Long-Term Servicing Branch.

The Current Branch (CB) is designed for early/fast adopters of the latest and greatest, and is most valuable to consumers. New features will ship alongside security and other critical updates rather than being packaged within a future release of the OS or within a Service Pack.

Current Branch for Business (CBB) offers similar cycles to Current Branch, but is more appropriate for organizations adopting a BYOD policy for their users. Organizations using this method will receive the same critical updates that are delivered in Current Branch, but new features will be delivered at a later date. This delay will allow organizations to test new features before deploying them into production, which ultimately will improve interoperability with existing applications and infrastructures.

Long-Term Servicing Branch (LTSB) is designed for those use cases that are deemed mission critical, such as those in medical, financial, and kiosk type of deployments. As with CB and CBB, critical and security updates are delivered immediately through Windows Server Update Services. But new features are not delivered, and are instead packaged up as a future LTSB update that can be deployed when deemed ready. LTSB updates will allow organizations to receive long-term support on specific LTSB builds so that image stability can be guaranteed.

New Methods of Enrollment and Device Provisioning

Unlike prior versions of Windows, Windows 10 dramatically streamlines the process for device enrollment and provisioning. And while existing processes such as imaging and patching can be applied as they have been in the past, Windows 10 introduces new methods and tools that greatly simplify enrollment activities. Collectively, these run time provisioning tools enable users to enroll their devices simply and easily, via self-service, without the assistance of an IT administrator. They allow configuration of new off-the-shelf devices without re-imaging, work independent of network types, and are compatible with existing tools. The run time provisioning tools allow for:

Simplified Workspace Enrollment

This is achieved through the creation of a Provisioning Package that is a collection of settings (e.g. Wi-Fi settings), profiles (e.g. user groups, printer designations), and file assets (e.g. applications, certificates, wall papers, custom URLs) required for a given user or group. These packages are then applied to any number of devices in bulk as a first run experience, deployed via removable media, during run time, or embedded within an image.

Out of the Box Experience

Most organizations struggle with device proliferation and the velocity of device refreshes, and often temper the cadence of device changes in an effort to keep up with change management requirements. To help with this, Windows 10 offers an out of the box experience that allows a new device to be correctly configured and verified without the involvement of IT staff. Users simply enter their credentials and, once authenticated, receive the standard configuration.

Over the Air Configuration

Another limiting factor for many organizations was the requirement of being on the domain in order to complete a configuration. This requirement was rather perplexing to many, as having users on the domain (especially in remote scenarios) proved difficult and inconsistent. Windows 10 removes the on-domain requirement, and users can simply enroll the device over any public or private network.

Bulk Provisioning

Many organizations implement application and device-based projects for large numbers of individuals at once. Normal efforts for these projects require that each device be customized based on individual needs. Bulk provisioning capabilities allow for mass enrollment of users and devices so that the operational efforts normally needed are now delivered via policy. This means that users and administrators can dynamically add or remove applications, configure and provision settings, create local accounts, domain-join devices, and enroll devices into management.

Peer to Peer Delivery

Organizations also struggled with the mass quantities of PCs being configured at the same time, as complete images (often in excess of 50GB) were streamed to each PC from distribution nodes on a network. This approach consumes large amounts of bandwidth and can often choke a network. Now with Windows 10, PCs can be configured to act as distribution nodes to service other devices that are nearby (such as in a branch environment) without traversing the network for the complete image.

Unified Application Experiences

For many customers, the primary problems associated with PC management arise from app delivery, integration and support. These problems become more complex as organizations adopt more apps and the number of variables and configuration possibilities grows exponentially. Today's sophisticated user requires control over apps on both personal and corporate owned devices. To help solve such application integration woes, Microsoft introduced a variety of features and tools in Windows 10 that greatly assist app management. Users have the ability to install and run apps, so devices effectively support bimodal requirements (apps installed/run by users and administrators). Unified applications are designed to service administrators, developers, and most importantly users in ways that are difficult to achieve today.

Windows Store

Windows 10 exposes the Windows Store, which is a converged application portal that serves as a common repository for all apps – making it far more accessible than in previous versions. Developers can target applications with a single code base that offers a unified experience. The resulting applications are much simpler to deploy, and can be easily provisioned both internally and externally to the organization.

Business Store Portal

For many organizations, the existing PC application portfolio is rarely managed in ways that are ideal for cost and operational efficiencies. Windows 10 changes that by introducing the business store portal, which offers dramatic improvements in management in the areas of acquisition, metering, use, and reclamation. Applications can be enrolled for bulk purchase, reclaimed and recycled for use, and licensed for both on and offline use. Applications provisioned through the business store portal are available via Windows Store, third-party developed apps, and internally developed apps. The business store portal features will interest many parts of the organization, including (but not limited to) procurement, asset managers, audit, and IT administrators.

Unified Application Catalog

With Windows 10, Microsoft consolidated the application install experience by giving EMM providers the ability to install desktop applications along with native and web applications. The unified application catalog gives organizations the ability to deliver applications from any location, including locally installed universal applications, classic windows apps, cloud applications, web apps, reverse seamless VDI applications, and published applications using Remote Desktop Server Host (RDSH).

Having a unified app catalog is a requirement for many organizations today. Under Windows 10, IT administrators have the option to auto-provision their users, or allow users access to the catalog in self-service mode, where the application portfolio is customizable by the user. Users can also view, browse, search, and install applications defined by their administrator based on their role and user group.

Software Distribution

Windows 10 also allows for a wide variety of software distribution mechanisms that are either new or enhancements of existing techniques. These include:

- Remote delivery of applications, files, and commands
- The deployment of an enterprise application catalog
- Local network distribution from down-stream relay servers
- Enhanced logging used for installation and execution
- Conditional installation based on network, schedule, or power
- Automated workflows for product installation
- Remote execution of scripts and complex packages

The benefits of these software distribution options include the delivery of all applications via a unified catalog, increased capabilities involving software inventory, and an inventory that supports modern app delivery.

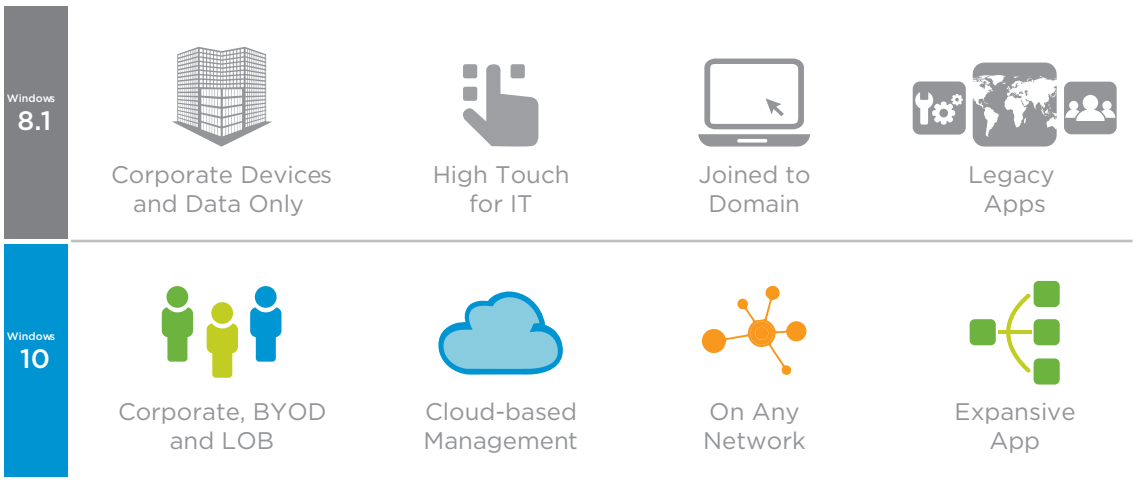
Classic Windows Applications

Windows 10 offers compatibility with Win32/Win64 applications. This means applications written for prior versions of Windows 7 and 8, and 8.1 can migrate to Windows 10 with minimal effort. Most organizations will perform regression testing as part of their effort, but will find that the amount of effort will be significantly less as compared to migration work required moving from Windows XP to Windows 7. Organizations can also provision classic Windows applications using existing PCLM (or other tools, such as PowerShell and login scripts) under Windows 10. Disk imaging, patch Tuesday, and software distribution tools, which are common today will work without incident in Windows 10.

Organizations also have the option of delivering entirely different versions of Windows on Windows 10 devices using a variety of technologies such as leveraging a type 1 virtual machine (VM) on the same device to provision an older version of Windows. Organizations can also deploy different versions of Windows by installing them on virtual machines as part of a VDI experience (with tools such as VMware's Horizon 6); users simply remote into the VM running Windows XP/7 etc. from a Windows 10 device. Customers will now have the opportunity to embrace cloud-based services for the purpose of using desktop as a service (DAAS). DAAS providers (such as VMware's Horizon Air) offer both legacy as well as Windows 10 access to their customers.

Domain Joined Management

Windows management has primarily centered around managing PCs (both desktops and laptops) through group policies that were "on the network" in a domain-joined way. And while this approach works well for PCs that are on an enterprise network (e.g. campus environment, branch office locations), increasingly devices off the network (predominantly traveling workers) needed to invoke a VPN in order for the device to be properly managed. Administrators often use VPNs to restrict and protect enterprise resources and isolate access to the infrastructure.



Windows 10 changes the domain-joined requirement by changing the focal point of security and access away from the network and onto the device. This approach allows organizations to protect corporate data at the device level where proper device attestation can be performed. In today's EUC environment, relying on VPNs and standard access methods and devices provides an incomplete and haphazard solution to the dynamic world of device diversity and BYOD.

Application Delivery

Applications are the life-blood of any organization and user; these tools allow for the creation of content, processing of work, and serve as the conduit to organizational growth. As organizations expand and evolve, so do application delivery requirements. Delivering applications in today's dynamic and fluid world need to be available at anytime, on any device, and across any network. As a result, most users require access to local apps, hosted apps, SaaS apps, classic apps, and cloud apps.

Universal Applications

One of the design goals that Microsoft established for Windows 10 is to increase the relevancy of Windows across different devices so that the OS can be used on desktops, laptops, smartphones, tablets, gaming platforms, and other devices. To accommodate this, Microsoft introduced the concept of universal applications. This is a new set of development primitives that allow applications to have commonality across all devices. For the developer, this means writing a single code base that can run on virtually any Windows device. Universal applications can be provisioned right to the device and can also be made available via the Windows Store.

Classic Windows Applications

Classic Windows applications (Win32 and Win64) constitute the majority of the application portfolio for most organizations. This portfolio can number in thousands for some large and complex enterprises; the applications are the foundation of a user's productivity. Microsoft made sure that the vast majority of classic Windows applications can easily migrate to Windows 10; in the rare case where it cannot run Windows 10, the OS gives notification of any incompatibilities prior to completing an in-place upgrade. Classic Windows applications are installed as they were before using exe's, MSIs, batch files, and scripts.

Cloud-based Applications

Cloud-based applications, such as those via SaaS providers (e.g. Salesforce.com) can easily integrate into the Windows 10 application catalog. Software providers can submit their applications to the Windows Store for signing so customers can reliably access cloud applications without incident.

Hosted/Remote Applications

Windows 10 can also remotely connect to published RDSH (Remote Desktop Server Hosted) applications residing on Horizon, XenApp, or Terminal Services servers. Highly standardized environments (e.g. call centers) with a fixed and finite need from their applications traditionally use these. Many clients will continue to use older releases of Windows while they test Windows 10 on devices by configuring Windows 10 devices to access to VDI-based desktops running legacy Windows (XP, 7, 8) images. These VDI environments can be provisioned on-premises or via service providers (aka Horizon Air). As VDI environments continue grow, Windows 10 devices will become more commonplace because of BYOD scenarios.

Identity Management

As application, device, and network access continues to diversify, there exists an increased capability for the delivery of a simple, easy, and secure way to access applications and data.

- Multiple user credentials
- Diverse delivery infrastructures
- Multi-factor authentication
- Binary access
- Diversity of device controls

Today's Identity Problem

Most enterprises today have at least one or two SaaS apps in use. Typically, a line of business owner manages app provisioning and user-access manually. At best, they may coordinate with IT for help desk and ticket management for new-user onboarding, separation, or password resets. While this might be OK for one or two SaaS apps, many enterprises are now deploying their third, fourth or fifth app, making the proliferation of user credentials overly complex. This complexity risks compliance and security as no one in IT can guarantee what employees have access to which apps, or what data might be saved on unmanaged, unencrypted devices. Identity management capabilities within Windows 10 make dealing with access and security across app types, networks, services, and data significantly more manageable. It does this by enabling:

Enterprise Single Sign-On
Simplify business mobility with included identity provider (IDP) or integrate with existing on-premises identity providers so you can aggregate SaaS, Native Mobile, and Windows 10 apps into a single catalog.

Self-Service App Store
Build a branded self-service app store so employees can subscribe to applications across devices with automated or manual provisioning.

Identity Management with Adaptive Access
Establish trust between users, devices and the hybrid cloud for a seamless user experience and enable powerful conditional access controls leveraging third-party device enrollment and SSO adaptors.

Enterprise-Grade Hybrid Cloud Infrastructure
Leverage VMware Identity Manager, the same identity management solution as vCloud Air and vCloud Suite, in the most advanced data centers and private clouds.

Security

The growth in security breaches continues to be an ever-present issue for every organization. These threats are very real and have the attention of CIOs today. Most attacks happen as result of improperly configured PCs or because users unknowingly expose their devices by downloading payloads or launching web pages that infect a system. Further, older releases of Windows were never designed to fully address the wide variety of spam, malware, or phishing that plague organizations today. Organizations also struggle balancing risk management, governance, and other security initiatives that impact business goals. Windows 10 ushers in many new changes that help address security and data concerns that exist with pre-Windows 10 environments:

	Windows 7	Windows 10	New Technology
Identity Protection	Theft of passwords possible/likely; multifactor too complex	Multifactor authentication is native and easy	Windows Hello Microsoft Passport
Data Protection	Disk encryption complex and difficult often requiring third-party integration	Disk encryption enabled by default; cross DLP functionality between Windows, Cloud, apps	BitLocker Enterprise Data Protection
Threat Resistance	Thousands of malware threats on a daily basis; AV can't keep up	Malware become irrelevant; Windows will only run trusted apps	Device Guard Windows Defender
Hardware Security	Device integrity nearly impossible; malware attacks holes in hardware configurations	System integrity maintained through hardware; hardware no longer exposed to malware	Secure Boot TPM Virtualization Health Attestation

The underlying philosophy for Windows 10 security is that all applications must earn trust before they can be used. This means a multitude of mechanisms are in order including protecting the device, application, transport, and scenario where applications can be executed.

Microsoft has introduced several advanced security and data loss prevention (DLP) features with Windows 10. One of the new features is Device Guard, which gives organizations the ability to lock down devices against malware. Secure Boot updates only allow trusted software to load when a device is turned on, while Health Attestation allows IT to determine the health of a managed device and take necessary compliance actions as needed.

Windows Hello leverages biometric capabilities for fingerprint, iris, and facial recognition as a means of completing a two-factor authentication (along with user ID and password credentials). Microsoft Passport replaces passwords with a private key available solely to its unique user.

Windows 10 DLP solution is Enterprise Data Protection (EDP) and protects data at the file-system level and is user transparent. EDP can differentiate between personal and corporate data on the device by classifying data by:

Tagging of Data

Enterprise data is tagged and classified based on a variety of attributes including IP address, email domain, internal resources (e.g. file shares).

Policy Levels

Policies are configured to establish how data is handled, including encryption, blocking, and auditing. Organizations can use this to track where files are, who accesses them, and what can be done with the files.

Defining Privileged Apps

Apps are configured with privileged levels to handle enterprise data.

Per-app VPNs

Apps establish which applications can access internal services independent of other device restrictions.

Windows 10 also enhances many existing EMM security features (such as white-listing, black-listing, encryption, antivirus configuration, passwords requirements, and certificate management). These features dramatically improve an organization's capability to more proactively manage devices in ways that offer better security at lower cost and higher user SLAs.

Summary

Windows 10 is a milestone release for the market at large – representing a fundamental shift in the way enterprises manage devices, apps, and operating system environments – and helping to keep the desktop as a critical piece of business technology with an essential role in how work gets done. Having EMM and legacy management technologies within the same platform have wide-reaching management implications for enterprise customers, and presents a unique opportunity for customers. Organizations who favor BYOD, device diversity, and app portability will likely embrace the EMM-based Windows management approach. Customers who favor domain-joined Windows management for PCs and Win32/Win64 apps will continue to manage Windows with the existing tools that have been in use for the prior versions of Windows, and will do so with the products that are in use today.

VMware offers unique opportunities to support customers today and to help them transition to a new era of endpoint and app management. VMware's unified endpoint management approach offers customers the beginnings of cross-platform management that is highly desired by customers. Having the ability to offer integrated app management solutions in either case means that the VMware EUC portfolio is relevant, unique, and is highly valued by organizations. VMware offers a blended solution that achieves the management solutions that are desired regardless of where the customer may be on their Windows 10 deployment. Organizations need flexibility in how to best manage Windows 10; using AirWatch with Horizon/FLEX offers capabilities that best meet those requirements, supporting the current and future needs of the organization while protecting existing and legacy investments. The value of having unified management under a single pane that addresses heterogeneous environments provides customers an elegant EUC management framework now and in the future.

VMware therefore offers the enterprise a unique opportunity to fully capitalize on the advantages of Windows 10, while ensuring that users can continue to move forward with device and apps models that are essential to modern End-User Computing. VMware ensures that users can continue to have the broadest choice of device environments, ubiquitous and continuous access to all essential apps across that portfolio of devices and support for "bring your own" models of device ownership, without sacrificing security or adding complexity to the IT process of managing devices and apps or preserving integrity of data and privacy.