What Windows 10 Means for the Modern Enterprise

v 1.1

MobileIron

Table of Contents

Executive Summary 3

Traditional vs. Modern: Introducing a New Era of Enterprise Computing 4
Evolution of the Modern Enterprise Architecture
Windows 10 Supports the New Enterprise Architecture

Windows 10: A Unified Platform for the Modern Enterprise 7
Device Management Evolves from GPO to MDM
Unified Set of MDM APIs
Consistent UI across Windows 10 Devices

The Windows 10 Device Lifecycle 9
Advanced Security and Data Loss Protection
Security That Follows Data Anywhere
Secure Connectivity and Remote Access

Windows 10 Unified Application Management 14
Application Distribution in Windows 10
Business Store for Windows 10
Distributing LOB Applications through the Business Store
Volume Purchasing through the Business Store
Windows Updates
Controlling Device Access through Azure Active Directory Integration

Conclusion 18

Executive Summary

The release of Windows 10 offers more than just new enterprise features — it is a major OS overhaul that accelerates the evolution of Windows from a PC-centric to a modern enterprise architecture. With Windows 10, enterprise IT can truly begin to shift from a security-focused legacy infrastructure to a modern enterprise architecture that prioritizes a highly productive, secure, and unified user experience across multiple devices.

Key to this transformation is the shift from using Group Policy Objects (GPOs) to enterprise mobility management (EMM) as the primary means to secure and manage enterprise devices. GPOs require a persistent local area network (LAN) environment in which users frequently power cycle their devices to activate the policies for that device. This approach lacks the flexibility required by the modern enterprise, where users often need access to business resources outside of the corporate network. EMM is quickly becoming the core device management platform in the modern enterprise because it enables business users to securely access enterprise data from any device, on any network, without compromising data security.

To support the shift from a traditional to a modern enterprise architecture, Windows 10 also includes these key enhancements:

- Convergence of mobile device management (MDM) APIs across all devices
- Unified employee experience across Windows phones, tablets, and laptops
- Single Windows Store and bulk license purchasing and distribution across disparate devices
- EMM distribution of both Win 32 and modern apps without the need for System Center
- Advanced Enterprise Data Protection (EDP)
- Device posture integration with Azure Active Directory (Azure AD) to control Office 365 access

> *Key to the transformation of traditional Windows to a unified mobile OS is the shift from using Group Policy Objects (GPOs) to enterprise mobility management (EMM) as the primary means to secure and manage enterprise devices.*

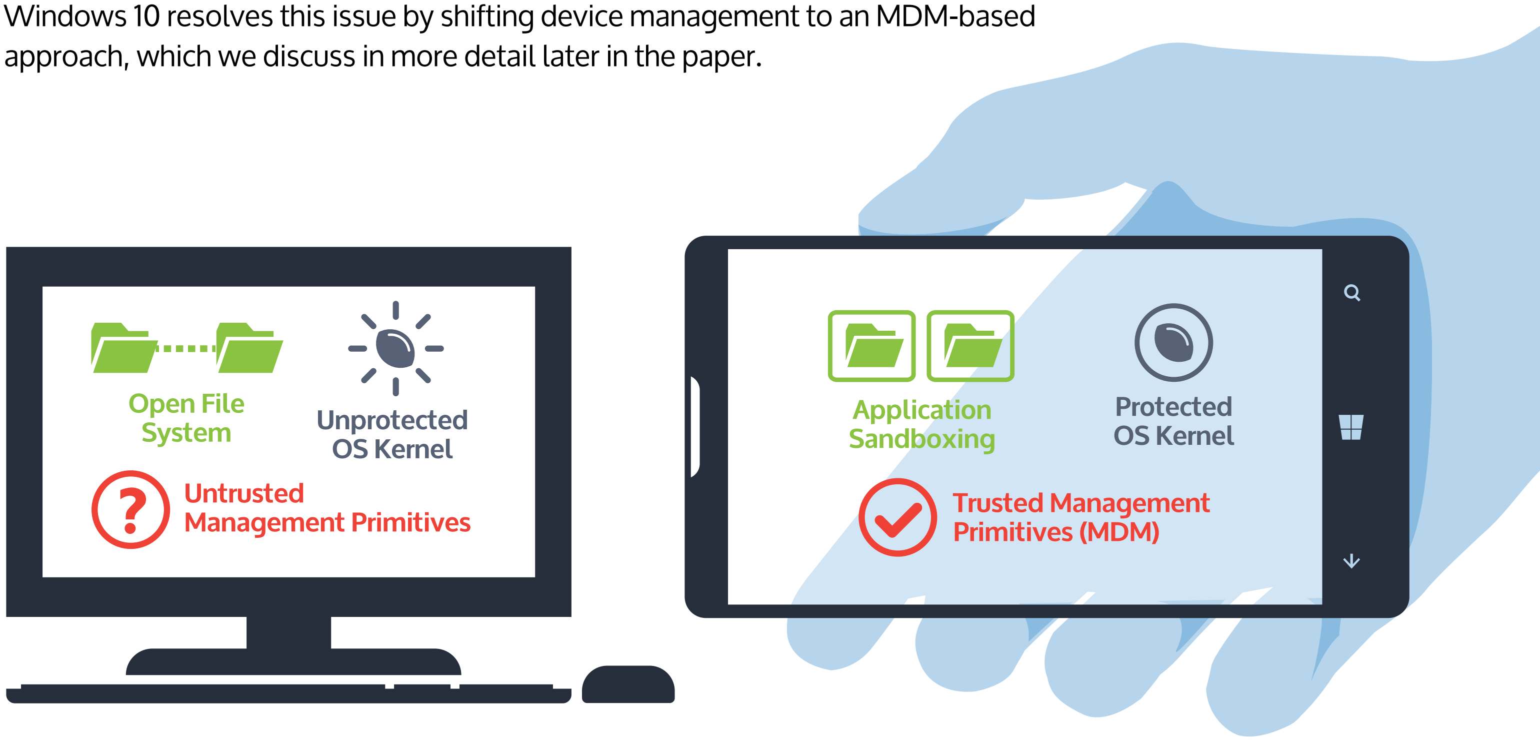
To better understand what Windows 10 means for the modern enterprise, this white paper provides a technical overview of these and other new features in the latest OS release. It also includes a brief overview of how the enterprise architecture has evolved and how Windows 10 enables IT leaders to use this fundamental architecture shift as a catalyst for business transformation.

Traditional vs. Modern: Introducing a New Era of Enterprise Computing

Windows 10 is ushering in a whole new era of enterprise computing. With Windows 10, previously separate OS versions on traditional Windows PCs, tablets, and phones are converging onto a unified platform managed by an EMM provider. For enterprise developers, this means that applications can be written once and run on any form factor and screen size. Windows 10 is also converging UIs so users will have a familiar interface on every device. As a result, the release of Windows 10 is a huge evolutionary step for Windows in the enterprise, but to fully grasp the impact it's important to first understand where it came from.

For the past 20-plus years, the traditional enterprise IT architecture centered around the Windows desktop model, which included an open file system and OS kernel vulnerable to modifications by other apps. For desktop security, IT focused on controlling the flow of data by maintaining a network perimeter and an arsenal of security technologies such as anti-malware, system management, virtualization, VPN, and remote desktops.

In addition, the traditional model required devices to join a domain governed by a set of GPOs, which control what users can and can't do on a computer system. For instance, a GPO can be configured to prevent users from setting an overly simplistic password or it can restrict access to certain folders. This model functions when all devices are connected to a persistent LAN, but it lacks the flexibility needed to manage intermittently connected devices in a modern mobile enterprise. Windows 10 resolves this issue by shifting device management to an MDM-based approach, which we discuss in more detail later in the paper.



Evolution of the Modern Enterprise Architecture

The enterprise architecture has been evolving ever since it was first introduced, but today's technology landscape is more dynamic than ever before. In the past, IT issued corporate-owned desktops and laptops burned with a system image. All software was preinstalled and several security agents ran on the device to protect the system, but performance often suffered in the process. Now employees can choose their own devices, select from a catalog of IT services, and update the OS on their own devices.[1] This evolution has been enabled by fundamental changes in the underlying architecture, which include:

> *"By 2020, smartphone security and management architectures will dominate the endpoint computing environment, while traditional PC image management will decline except on dedicated appliance-style devices."* [2]

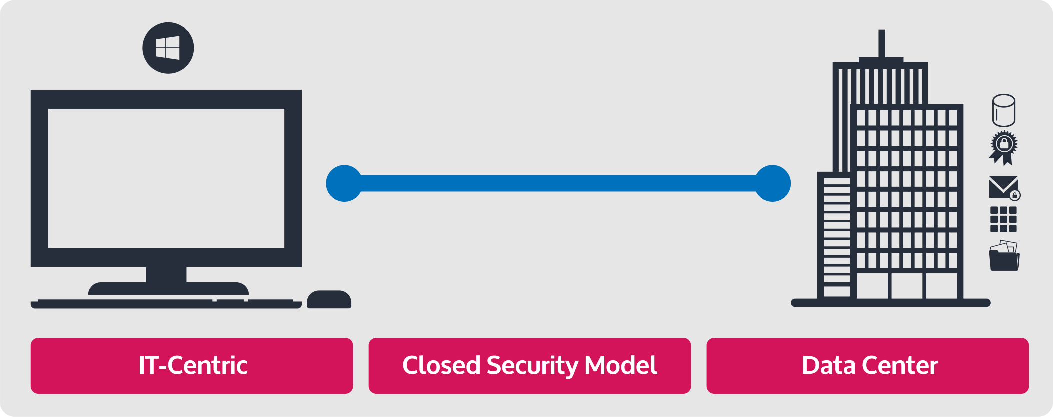
- **Sandboxed Architecture and Protected OS Kernel:** One of the biggest changes in modern enterprise IT is the shift to the sandboxed architecture and protected OS kernel in modern operating systems, including Windows 10. Modern operating systems use isolated storage and isolated memory for each app, so the data of each app is protected from the actions of other apps on the device. This model of a protected file system and kernel also protects against traditional malware threats, which minimizes the need for anti-virus software on mobile devices.

- **Management Primitives (MDM APIs):** Modern mobile architectures, including Windows 10, have introduced the concept of enterprise management primitives. Management primitives are ways to take certain OS-level actions, such as installing or deleting an app, storing a certificate, or configuring connectivity, that can only be accessed by a trusted EMM platform. As a result, management primitives establish EMM as the core security platform for the modern OS because they allow the OS kernel to remain secure while providing the enterprise with appropriate controls.[3]

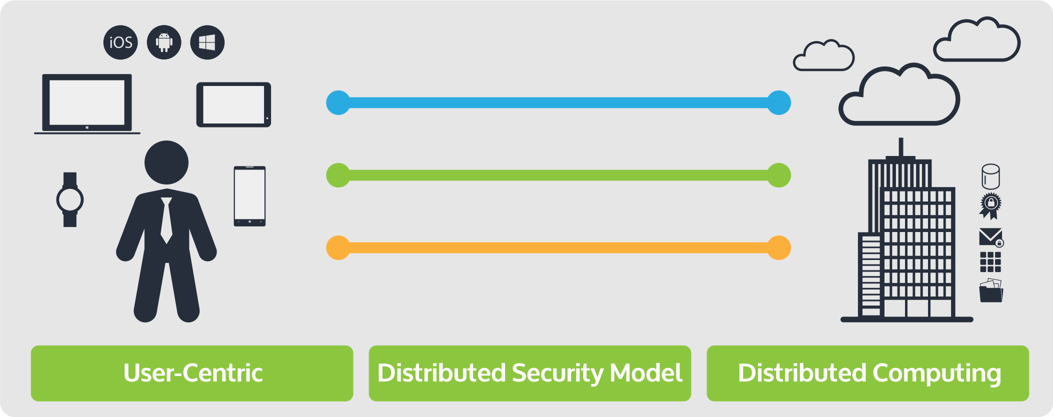
As a result of these fundamental architecture changes, the old model of Windows desktop computing, with its anti-virus software, cumbersome patches, license management, long deployment cycles, and locked-down devices is fading away. Windows PCs will no longer be required to join a domain to experience increased security and access policies once dictated by GPOs and desktop agents. Instead, EMM will be preferred over domain-joining as a central mechanism for managing devices. This will allow companies to move from the traditional, time-consuming, and costly full imaging of a device to a distributed security model that enables business users to upload and retrieve enterprise data from anywhere on multiple devices. And all of this data will be easier to secure and manage with application sandboxing, a protected kernel, and faster OS upgrades enabled by modern operating systems.

[1] Rege, Ojas. "Mobile App Mentality: 4 Ways IT Must Change." May 12, 2015. http://www.informationweek.com/software/enterprise-applications/mobile-app-mentality-4-ways-it-must-change/a/d-id/1320372
[2] Dulaney, Ken and Terrence Cosgrove. "Managing PCs, Smartphones and Tablets and the Future Ahead." Gartner Research, May 5, 2014.
[3] Rege, Ojas. May 12, 2015.

Old Enterprise Architecture



New Enterprise Architecture



Windows 10 Supports the New Enterprise Architecture

The release of Windows 10 is one of the crucial pillars supporting the modern enterprise architecture where mobile security and consumer choice are top priorities. By providing a single, converged OS and a unified set of MDM APIs, Windows 10 enables IT to manage all types of Windows devices as well as develop and manage universal apps that can run on any Windows device including phones, tablets, laptops, and PCs.

> *By providing a single, converged platform and a unified set of MDM APIs, Windows 10 enables IT to manage all types of Windows devices as well as develop and distribute universal apps that can run on any Windows device including phones, tablets, laptops, and PCs.*

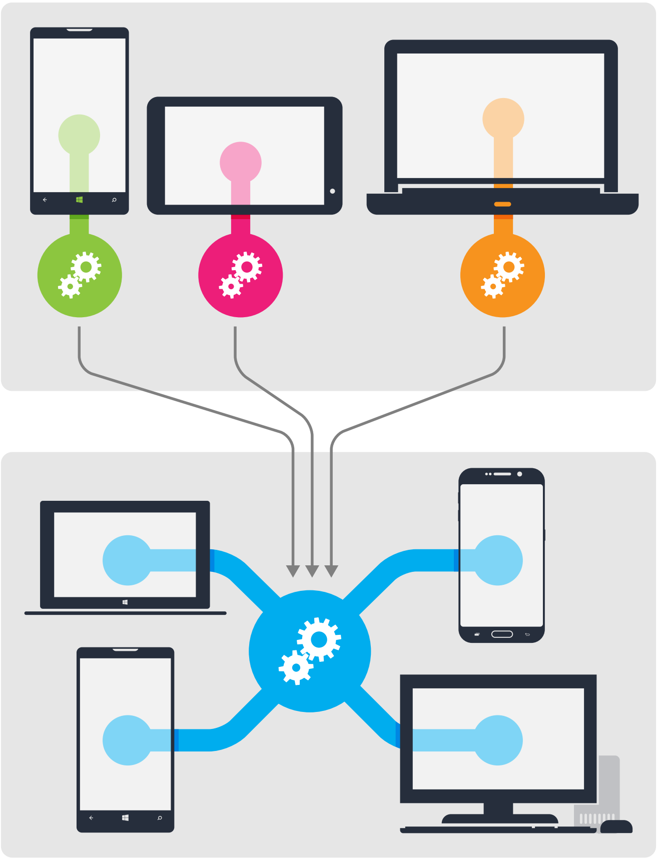
Windows 10: A Unified Platform for the Modern Enterprise

Device Management Evolves from GPO to MDM

In the old enterprise architecture, the GPO-based approach was used primarily because most computers were connected to a LAN and users regularly powered their workstations on and off to trigger the management policies configured for the device. This approach also allowed IT administrators to create, modify, and apply thousands of GPOs to users, applications, additional computers, specific groups, and the whole company.

In the modern enterprise, the GPO security model is becoming obsolete because users no longer have persistent connections to corporate LANs, nor do they regularly power cycle their devices. With the emergence of cloud services and applications, mobile employees no longer connect exclusively through the corporate network, but they still need to access business content wherever it resides. MDM protocols are specifically designed to secure and manage mobile devices regardless of how they access corporate resources. As a result, MDM is the path forward for the modern enterprise architecture.

Windows Phone 8.1 and Windows 8.1



Windows 10

Unified Set of MDM APIs

The release of Windows 10 supports the widespread industry shift toward MDM. Windows 10 converges traditional Windows operating systems to allow for security and management through a unified set of MDM APIs across mobile, desktop, and embedded products. Although Microsoft had previously released MDM protocols for Windows Phone 8.1 and Windows 8.1 for laptops and tablets, they were not the same and therefore required separate APIs and control interfaces.

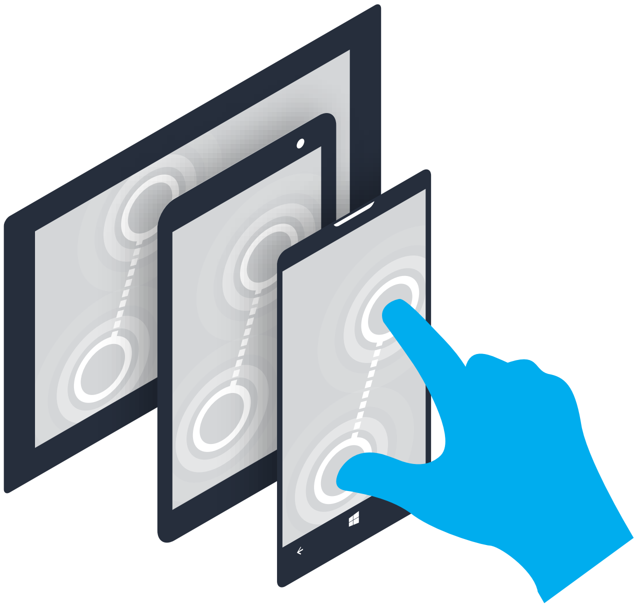
For instance, enforcing a policy such as a complex passcode requirement once required admins to use a separate configuration for a Windows phone vs. a PC. For example, let’s say IT wanted to enforce a complex passcode policy for Windows Phone devices. This same policy couldn't be applied to PCs without using a different configuration for the PC. The need to use different configurations for each device sometimes led to policy conflicts if, for example, a tablet administrator created one policy to enforce a complex passcode, but a mobile phone administrator created another policy that did not have this requirement. There was no easy way to locate or resolve the conflict.[4]

To address these challenges, Windows 10 converged all the MDM APIs and app development tools onto a single platform. With this convergence, IT can access unified MDM protocols through an EMM provider to manage any Windows 10 device. As a result, MDM policies configured for Windows 10 can be applied consistently across Windows devices. So if IT decides to create a complex passcode requirement, that policy will be enforced across tablets, PCs, and phones without the need to create separate policy configurations for each type of device.

If IT still needs to use both GPO and MDM configurations for different devices in legacy architectures, Windows 10 enables the device itself to resolve the conflict by automatically choosing the most secure configuration. It's important to note that Microsoft has resolved similar policy conflicts in the past by combining Active Sync and MDM policies. So if, for example, an Active Sync policy required a device to have a six-character password, and the MDM policy required eight characters, the Active Sync policy would be overruled by the more secure MDM policy. Microsoft is now taking this conflict resolution capability to the next level with MDM and GPO in Windows 10.

Consistent UI across Windows 10 Devices

Windows 10 resolves one of the biggest hurdles for end users by enabling a unified UI across all Windows devices. This means the desktop will have the same UI as a Windows Phone, allowing the user to have a similar experience on any device. This also saves time by eliminating the need for the user to relearn how to navigate on separate devices.

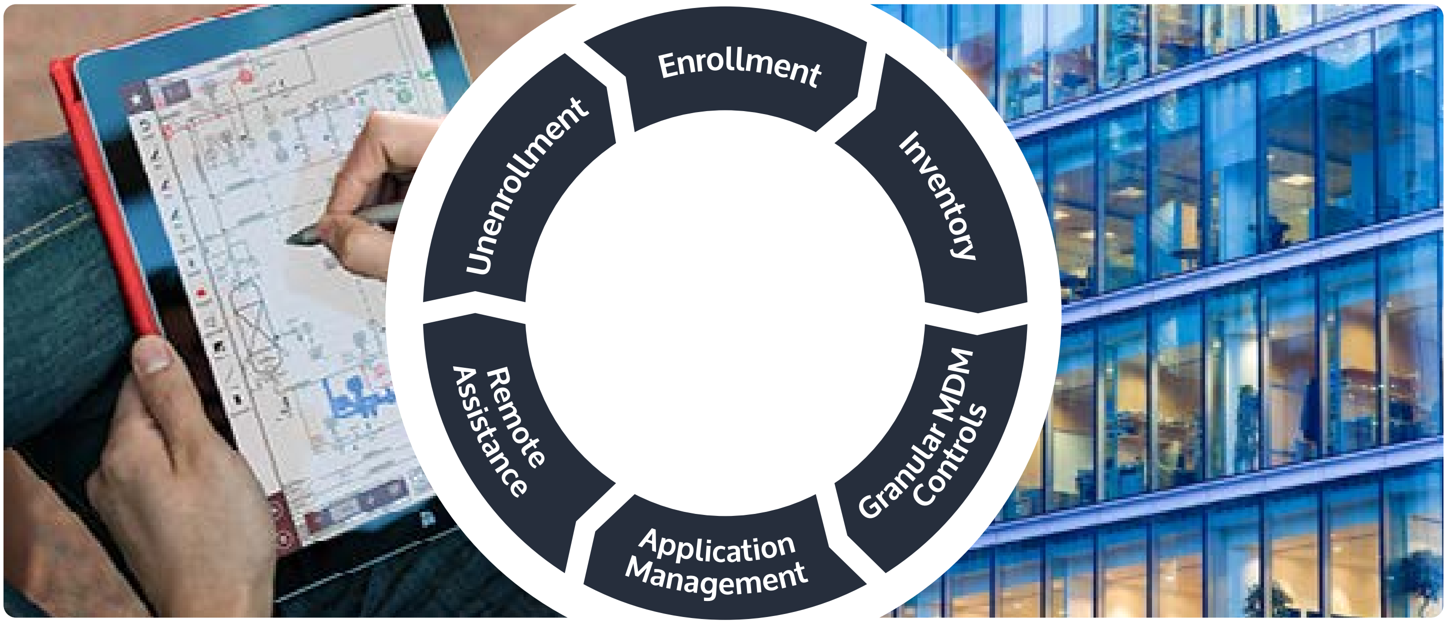


The new UI features in Windows 10 also allow the device screen to be customized for particular business uses. For example, a retail business may distribute several kiosk devices that employees use to assist store customers with questions and purchases. It's extremely important for these devices to be configured with a familiar UI and consistent applications tailored for the particular job function. With Windows 10, the UI can be configured through MDM to customize the tile layout, Start screen, and application filters so the look and feel is consistent across all the devices issued to that group.

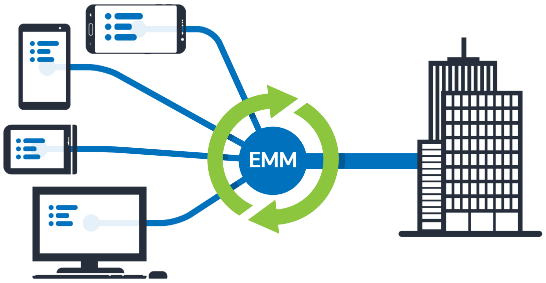
[4] Vasudevan, Janani. "Windows 10 Mobile Device Management (MDM) In Depth." May 7, 2015. https://channel9.msdn.com/Events/Ignite/2015/BRK3313

The Windows 10 Device Lifecycle

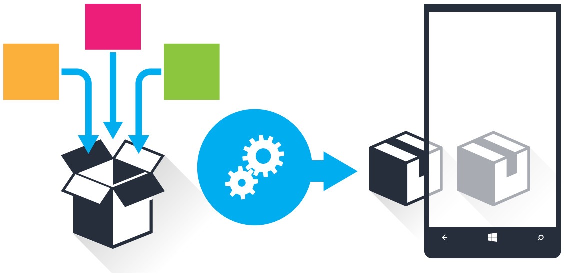
Windows 10 supports the lifecycle of a typical enterprise device through these phases:



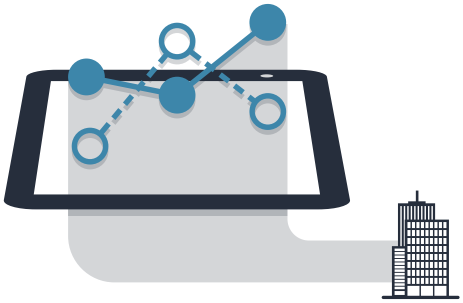
- **Enrollment:** Windows 10 greatly simplifies the setup process. Because the platform is now converged, users benefit from a unified UI and consistent set of enrollment instructions on every device. For IT, the enrollment process is automated through the EMM console and either an Active Directory or Azure Active Directory (Azure AD) join process.



- **Bulk Provisioning:** When IT needs to provision several devices to a group of users at the same time, devices can be preconfigured through bulk provisioning in Windows 10. This allows all the MDM configurations to be pre-loaded onto multiple devices, and then IT enrolls the device on behalf of the user. As soon as the device is turned on it is automatically enrolled using certificate-based authentication, which doesn't require the user to take any action on the device to enroll it.

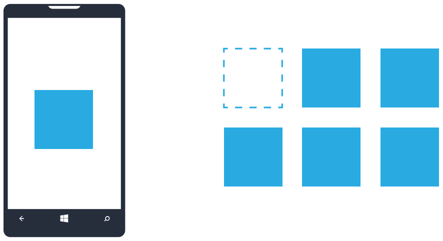


- **Inventory:** Windows 10 will provide additional device inventory on key device metrics such as security and compliance status, password compliance on desktops, battery level and serial numbers, and media access control (MAC) addresses for both LAN and Bluetooth devices. The IT admin can view this data through the EMM console and generate reports or take compliance actions on a device if required.



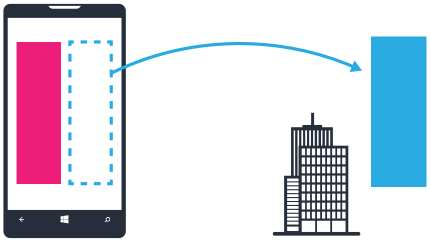
- **Granular MDM Controls:** Windows 10 offers more than 100 new policies for granular device management control beyond what is already available in Windows Phone 8.1 and Windows 8.1 for laptops and PCs. Some of these policies include new controls for email profiles and remote wipe — policies which already existed for Windows Phone but will now be available for PCs in Windows 10. All of the new policies can be leveraged by EMM providers and include: Microsoft Passport for Work policies, email provisioning for desktop, sync settings, Firewall and Defender policies for desktop, and AppLocker-enabled whitelisting and blacklisting of applications, drivers, and dynamic link libraries (DLLs).

- **Application Management:** Windows 10 fully integrates with the Windows Store and the Business Store portal to enable automated app management. IT can take advantage of volume licensing in the Windows Store to distribute hundreds or thousands of app licenses through an EMM provider. Admins can also configure and enforce application allow/deny lists through AppLocker and maintain an accurate inventory of apps on the device.



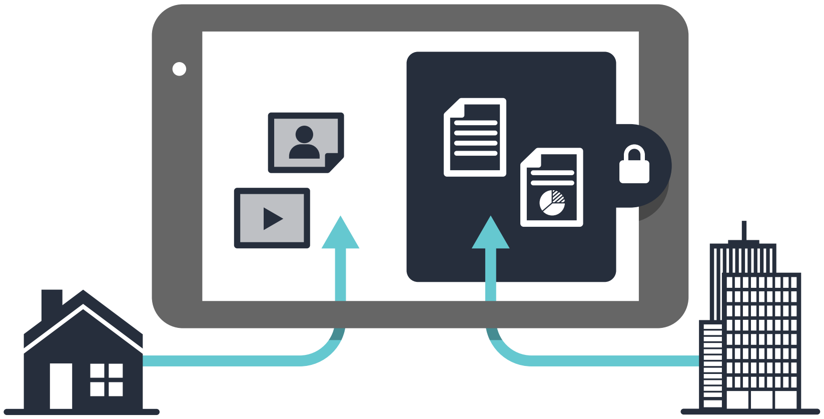
- **Remote Assistance:** If an employee loses a device, IT can attempt to ring or locate the device to help the user retrieve it. If the device is stolen, IT can reset the PIN, lock the device, or perform a full device wipe to prevent unauthorized users from accessing corporate data. IT can also perform ongoing inventory checks to ensure the device is in compliance.

- **Unenrollment:** When an employee leaves the company or upgrades to a different device, IT can retire the current device and remove all enterprise configurations, including apps, certificates, VPN access, Wi-Fi, email profiles, policies, and data that has been encrypted with EDP.



Advanced Security and Data Loss Protection

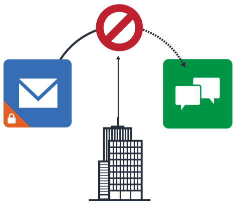
To help protect business apps and data on Windows devices, Microsoft introduced EDP in Windows 10. This capability is built into the OS and can be administered through a company's EMM console, where IT can specify exactly what constitutes enterprise data, which apps are for business, and how data can be shared. Here's how it works: Once the device has been set up through one of the enrollment options described previously, EDP helps prevent data loss from that mobile device with advanced security controls for:



1. **Resources:** An IT admin can configure a list of business resources in the MDM server. This list can include IP addresses, domains, and accounts such as a business email address. Whenever information flows from any of these resources, such as a filesharing IP address, a SharePoint domain, or a company email account, it is automatically recognized as business data inside the OS. This means Microsoft will encrypt and protect the information by default and store the data in a secure virtual container on the device.
2. **Authorized Applications:** This list is created inside the MDM server. IT can specify that content in the Resources list can only be accessed by authorized applications, such as Microsoft Suite, Outlook, PowerPoint, SharePoint, Salesforce, and in-house applications such as expense reporting.

Once the lists are created, the device will be able to see which apps are allowed to access certain data or files. For example, if an employee downloads a business attachment in Outlook, and then tries to post an image of that attachment on a personal Facebook page, the device could block the action.

> *As part of EDP in Windows 10, devices can determine whether or not to protect data depending on where it comes from.*



Copy/Paste Restrictions

EDP can also restrict copy/paste functions. If a user copies content from a Word doc or other business app, the system can block that content from being pasted in another application if it's not authorized. Or it can allow the content to be pasted, but warns the user that an audit log will be generated to document the action. EDP provides critical data loss protection because it prevents employees from distributing sensitive business data through a personal email account or other unauthorized app.

Security That Follows Data Anywhere

As part of EDP in Windows 10, devices can determine whether or not to protect data depending on where it comes from. For example, EDP can automatically encrypt data that comes from SharePoint but not from a personal email account on the device. This means that regardless of how data is transferred — from a tablet or PC to a USB drive, email, or the cloud — it stays secure. Not only does this add a much-needed layer of protection at the file level, the security mechanism is invisible and seamless to the end user. No special actions, apps, or locked-down devices are required to meet corporate security requirements. By taking security out of the hands of employees, IT can ensure corporate data is always safe wherever it travels.[5]

Enterprises should also note that Windows 10 does not include a "timebomb" option for enterprise data. This means there is no mechanism to eliminate enterprise apps and data if a device has not checked in after a specific interval, like one week. Companies should evaluate their own security policies to determine if they will need another option to enforce data loss prevention.

Secure Connectivity and Remote Access

The widespread adoption of mobile devices in the enterprise has created a multi-faceted challenge for every IT organization. On the one hand, IT needs to ensure that any device coming into the enterprise, whether employee- or corporate-owned, is secure, not jailbroken, and free of malware that can put business data at risk. On the other hand, the role of IT in the modern enterprise is quickly shifting from a pure technology and security focus to one that drives business productivity and user enablement. So while the traditional enterprise security model of locked-down devices and desktop VPN is giving way to securely enabled mobile devices, IT must still meet enterprise security requirements and address privacy concerns for mobile employees.

> *The role of IT in the modern enterprise is quickly shifting from a pure technology and security focus to one that drives business productivity and user enablement.*

Windows 10 directly addresses these concerns with new security upgrades that include: [6]

- **Application Allow/Deny Lists:** New in Windows 10, both Windows Store and Win 32 apps will be able to execute application allow/deny lists through AppLocker. AppLocker is a Windows feature that allows IT admins to define rules to allow or deny applications based on unique file identities, group policy, or user role.

> *New in Windows 10, both Windows Store and Win 32 apps will be able to execute application allow/deny lists through AppLocker.*

[5] Alkove, Jim. "Introducing Windows 10 for Business." Sept. 30, 2014. http://blogs.windows.com/business/2014/09/30/introducing-windows-10-for-business/
[6] Tiwari, Abhishek. "Windows 10: Remote Access Connectivity." October 30, 2014. http://channel9.msdn.com/Events/TechEd/Europe/2014/WIN-B345
[7] Tiwari, Abhishek. http://channel9.msdn.com/Events/TechEd/Europe/2014/WIN-B345

- **New VPN Platform:** Available for Windows Phone, laptops, and PCs, this platform provides a reliable way for third-party VPN solution providers to implement their VPN inside of Windows. The VPN client app runs in the same secure app container on the device just like any other Windows Store app.[7] This also allows IT to create a secure list of applications that have access to the VPN on any Windows 10 device.

Always-on VPN: Once configured, the VPN is always connected until the user manually disconnects. This feature can be pushed to mobile devices through MDM APIs. Although always-on VPN isn't recommended for mixed-use, BYOD devices, it's an option for corporate-owned devices, such as a kiosk or point-of-sale (POS) device.

App VPN: In Windows 10, a new VPN configuration service provider (CSP) will allow the EMM provider to configure the VPN profile of the device.[8] App VPN will also use application-based filters that allow only traffic from authorized applications, such as Outlook, Excel, and PowerPoint, to use the VPN connection. In Windows 10, IT can configure application filters and auto-connect through the VPN, which is invisible to the user.

- **Certificate Management:** IT can enable the Simple Certificate Enrollment Protocol (SCEP) for initial device provisioning and enrollment instead of relying on traditional username/password credentials. The MDM server sends SCEP instructions and a challenge to the device, which uses the challenge to request a certificate from the SCEP server. With Windows 10, IT can also directly install a certificate via MDM by sending the certificate and a private key through the MDM channel. This process does not require a SCEP server because it can use a self-contained certificate authority.

- **Microsoft Passport for Work:** In cases where IT wants to ensure the device is being enrolled by the intended user, IT can deploy a Microsoft Passport for Work certificate through MDM. In this case, the user will be required to submit a credential such as a PIN or fingerprint swipe to authenticate the user's identity to enroll the device.

- **Device Health Attestation:** Health attestation is a standard procedure used to verify the integrity of each step in the device bootup process. Windows 10 now includes a device health attestation service that customers can view through an EMM console to ensure devices are not compromised before granting access to corporate resources.

> *Windows 10 now includes a device health attestation service that customers can view through an EMM console to ensure devices are not compromised before granting access to corporate resources.*

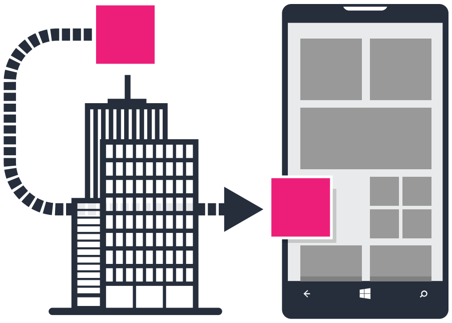
[8] Windows Hardware Dev Center: https://msdn.microsoft.com/en-us/library/windows/hardware/dn904978(v=vs.85).aspx

Windows 10 Unified Application Management

In Windows 10, programmers can develop universal apps that are written once with a single set of business logic and one UI so they can run on any Windows 10 device.[9] Furthermore, developers will now be able to run existing Android applications (Java and C++) natively on Windows 10, and iOS developers will be able to easily transition their apps and publish them in the Windows Store. Not only will these apps look the same on every device, IT will be able to create and enforce security and device management policies that apply equally to phones, laptops, and PCs. Perhaps most importantly, the user enjoys a consistent experience across all Windows 10 devices.

Application Distribution in Windows 10

Prior to Windows 10, there were two models for in-house app distribution. For Windows Phone, IT used application enrollment tokens (AET) to distribute apps to smartphones. For the desktop, IT used code-signing certificates to verify application identity and assign a key. Windows 10 will eliminate this fragmented approach by creating a unified Windows Store for all Windows apps, including in-house and third-party apps, where EMM providers can distribute and manage them over the air (OTA).



In addition to creating a single unified app storefront, Windows 10 will also enable IT to distribute Win 32 applications through the EMM console instead of System Center — a significant upgrade in the new platform. In Windows 10, IT admins can distribute and silently install (or uninstall) Windows Store apps, in-house apps, and Win 32 applications using MDM APIs — the same as they do for mobile apps. No action is required from the end user and IT can enable certain apps for specific users and groups.

Business Store for Windows 10

The Business Store for Windows 10 is a dedicated business portal that gives users a familiar shopping experience in an enterprise app store. The Business Store also gives IT the controls and configurations they need to effectively manage and distribute all the apps in the store via an EMM platform. The Business Store portal supports flexible business scenarios and a range of application types, including customized line-of-business (LOB) apps. In Windows 10, a sideloading key will no longer be necessary to download these apps on the device.

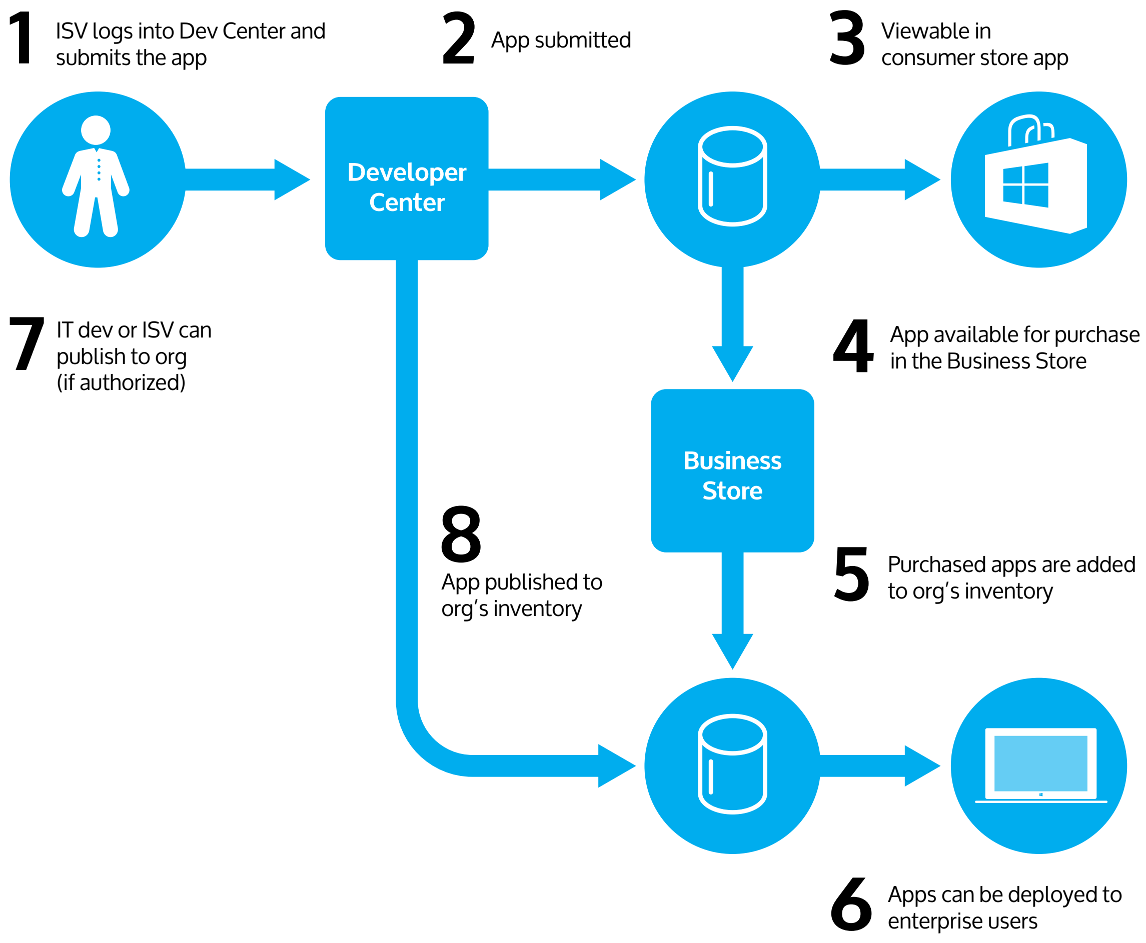
> *In Windows 10, Win 32 applications will no longer need to be packaged for distribution through System Center — they can be administered directly through the EMM console via MDM APIs.*

[9] Krill, Paul. “Microsoft to developers: Practice Windows 10 convergence.” InfoWorld, March 3, 2015.
http://www.infoworld.com/article/2891716/microsoft-windows/microsoft-developers-windows-10-convergence.html

The Business Store complements the Windows Store by supporting the same universal Windows applications that can run across multiple device form factors. It also supports existing Windows 8.x apps for both desktop and phones, as well as Windows platform "bridge" apps that enable Win 32 and Android apps in the store. (Note: "Bridge" apps will only work on Windows 10 devices and up going forward.) Also, apps submitted to the Windows Store will be available by default in the Business Store as well.[10]

Distributing LOB Applications through the Business Store

In-house LOB apps, such as a custom internal HR guide, can be submitted to the Business Store directly by the developer and available only to the business organization. This means they can't be distributed in the retail catalog or accessed by users outside the organization. The Business Store will also enable the IT admin to authorize developers who are allowed to submit applications to the store. Once apps are submitted from a developer, the IT admin can go into the Business Store and accept (or block) those applications submitted to the catalog.


1 ISV logs into Dev Center and submits the app
2 App submitted
3 Viewable in consumer store app
Developer Center
4 App available for purchase in the Business Store
7 IT dev or ISV can publish to org (if authorized)
Business Store
8 App published to org's inventory
5 Purchased apps are added to org's inventory
6 Apps can be deployed to enterprise users

[10] McKinstry, Ford and Tejas Patel. "Using the Business Store Portal with Windows 10 Devices." May 7, 2015. https://channel9.msdn.com/Events/Ignite/2015/BRK3338

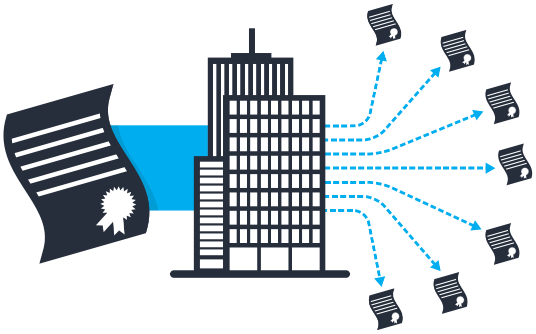
Volume Purchasing through the Business Store

Windows 10 will not only enable the ability to buy multiple licenses and distribute them via an EMM, it takes bulk purchasing a step further by offering two different options:

- **Online mode:** An enterprise can purchase licenses from the Windows Store, upload them to the MDM server, and allow devices to access them through the store.

- **Offline mode:** The customer purchases licenses through the Business Store portal and uploads them to the MDM server. Unlike online mode, offline devices don't require an Internet connection to connect to the app store. Instead, IT can create private networks, such as a supply warehouse, remote location, or law enforcement agency, where the device doesn't connect to the public store at all. It only connects to the MDM server to install the apps. With offline mode, public applications coming from the Windows Store can be distributed on private networks through an EMM provider without the need for the device to connect to the public network.

Volume purchasing also offers the ability to upgrade and downgrade device SKUs. For example, let's say an employee buys the least expensive version of Windows Home for personal use. The employee brings his device to work and decides to upgrade and expense it to the company. If the employee retires the device or leaves the company, the original Windows license can be reclaimed by the enterprise and reused on another device.



Windows Updates

In Windows 10, devices will be continually updated and kept current, and all updates can be managed through the EMM provider. IT can configure when the device should scan for updates and notify the user of restart before the update is installed. The device can be configured to automatically approve updates so that when they are installed, the user is not disrupted by an end-user license agreement (EULA) prompt.

Enrolled devices frequently connect through multiple networks, including corporate and home networks. To enable updates regardless of the network, IT can configure how the device installs the updates and where they are installed from. For example, IT can configure updates to come directly from the Microsoft Update server over the Internet, or they can be installed from the Windows Server Update Services (WSUS) server. A fallback can also be configured if one of these is not available.

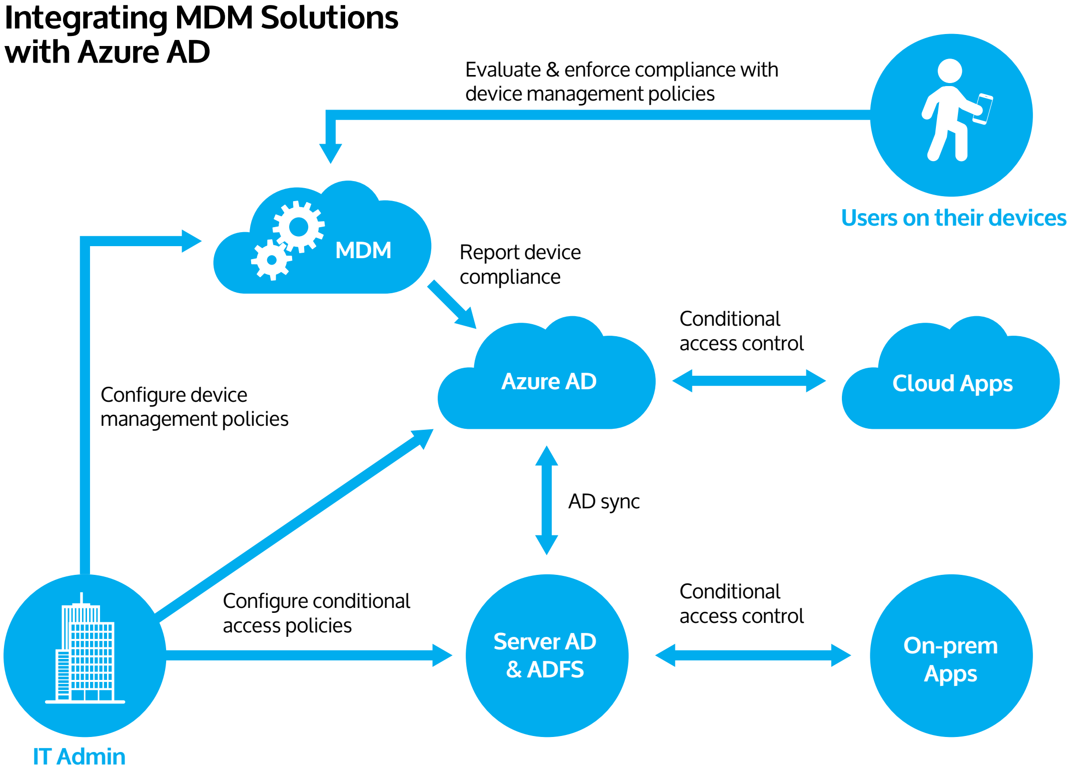
Just as important, Windows 10 delivers compliance status updates back to the MDM. This allows IT to see which updates have been downloaded, successfully installed or failed, and which are pending a reboot. IT can also control which OS and app updates are deployed based on the device type and user role.

Controlling Device Access through Azure Active Directory Integration

In Windows 10, IT can create a set of policies through the EMM console that will send device compliance status to Azure AD, which can then use this information to allow or block access to corporate resources protected by Azure AD credentials. For example, IT might want to configure a policy that labels a device non-compliant if it is found to be jailbroken. An API then allows the EMM provider to send the global device ID and compliance status to Azure AD. If the device is out of compliance, Azure AD can block device access to cloud resources such as Office 365, Salesforce.com, or any federated service authenticating through Azure AD. Any Windows 10 device that uses Azure AD credentials can be managed this way. The IT admin can also set up AD Sync between Azure AD and Windows Server AD to control access to on-premise apps.

> *EMM integration with Azure Active Directory enables IT to block access to corporate cloud services, such as Office 365, if a device falls out of compliance.*

Azure Active Directory Access Control for Office 365: Windows 10 EMM plays a central role in monitoring and reporting device status to Azure Active Directory, which grants or denies account access based on information from the EMM provider.


Integrating MDM Solutions with Azure AD
Evaluate & enforce compliance with device management policies
Users on their devices
MDM
Report device compliance
Conditional access control
Azure AD
Cloud Apps
Configure device management policies
AD sync
Configure conditional access policies
Server AD & ADFS
Conditional access control
On-prem Apps
IT Admin

It's important to note that, while Windows 10 is adding support for Azure AD, it will continue to support Active Directory. This means that IT can leverage both directory services without needing to choose one over the other.

Securing Office 365

Through MobileIron, IT admins can secure Office 365 with the ability to:

- Protect Office 365 app data when it's at rest on the device and in motion from the device to the backend application service.
- Configure the native email and PIM apps on mobile devices so they can connect to Office 365.
- Securely distribute Office 365 apps to mobile devices through the enterprise app store.
- Enforce operating system containerization controls such as data separation, Open In restrictions, and selective wipe to protect Office 365 data on the mobile device.
- Securely tunnel data from the device to the cloud through app VPN.
- Block rogue devices and browsers from accessing Office 365 by using Microsoft Active Directory Federation Services (ADFS) to limit authentication paths.

Conclusion

The release of Windows 10 is a major milestone in the evolution of the modern enterprise architecture. Now organizations can meet their mobile first goals with key capabilities such as: Converged MDM APIs across multiple form factors, a unified user experience across disparate Windows devices, EMM distribution of both Win 32 and modern apps, and greater data security through EDP and Azure AD access control. Together with an EMM platform, Windows 10 offers an exciting breakthrough for organizations ready to deliver unified device and security management for the modern enterprise architecture.

For More Information

To learn more about Windows 10 and what it means for your enterprise, please visit https://www.mobileiron.com/windows10 .

For questions regarding your Windows implementation, please contact us at globalsales@mobileiron.com .