Windows 10, EMM, and the Future of PC Security and Management

Executive Summary

Managing your devices keeps getting more complex and your admins are juggling more complicated security and management tasks than ever before.   Until now, you have needed many complex and disparate tools to secure and manage your devices. But now Windows 10 and MobileIron makes your life much simpler and streamlines many traditional PC management responsibilities.

Table of Contents

415 East Middlefield Road Mountain View, CA 94043 USA
Tel. +1.650.919.8100 • Fax +1.650.919.8006 • info@mobileiron.com

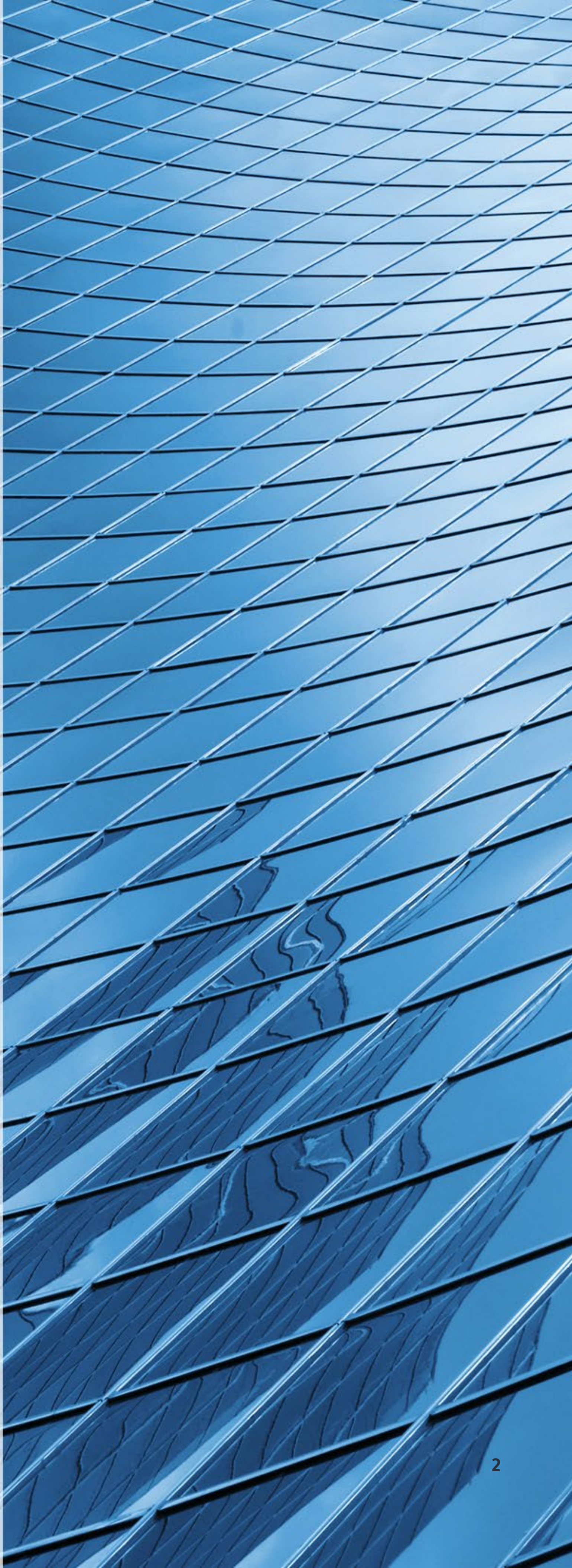
MobileIron

MKT-10389 v1.3

Windows 10 introduces a more unified approach that greatly simplifies many traditional PC management responsibilities.

The release of Windows 10 no longer requires admins to use a variety of desktop management tools such as LANDESK and Microsoft System Center Configuration Manager (SCCM) to manage legacy Windows PC clients. Instead, admins can use a single enterprise mobility management (EMM) platform to manage any Windows 10 device, including PCs and employee-owned or BYOD mobile devices. Windows 10 makes this possible by allowing admins to access a unified set of MDM APIs through an EMM provider like MobileIron. With EMM, admins can accelerate device setup and configuration, simplify app administration, and ensure seamless security across all enterprise devices managed with EMM.

To illustrate the difference between traditional desktop management and EMM capabilities, this paper explains how EMM can manage five of the most common desktop management use cases. It also includes recommendations for IT organizations looking to evolve their management infrastructure toward a more modern and unified EMM-based approach.



How Windows 10 is Changing the PC Management Game

PC management has evolved significantly over the years in an effort to support rapidly changing enterprise needs. Today, a common model of PC management requires devices to join a domain that's governed by a set of group policy objects (GPOs), which define what a system looks like and how it behaves for a certain group of users. Combined with tools such as LANDESK and SCCM, this model is most effective when all devices are connected to a persistent LAN. However, it lacks the flexibility needed to manage intermittently connected mobile devices — which enterprise users are adopting at a much faster rate than legacy, domain-joined devices. As a result, IT admins need a more consistent platform to manage the broad variety of devices across the enterprise.

Windows 10 addresses this gap by shifting device management from domain-joining to establishing EMM as a single point of trust in the enterprise. Windows 10 converges traditional Windows operating systems and provides a unified set of MDM APIs through a single platform. With this convergence, IT can manage any Windows 10 device by accessing MDM protocols through an EMM provider like MobileIron. Windows 10 also modernizes app deployment, because now Win32 applications can be deployed through EMM along with modern apps.

These changes make it easier for PC management teams to manage both PCs and mobile devices using the same platform for some of the most common use cases. Although traditional tools are still required for some situations, PC management teams will face more pressure to augment their current toolset with EMM, especially as more enterprise users upgrade to Windows 10 devices. In fact, Gartner Research estimates that by 2018, 40 percent of organizations will use EMM tools to manage at least a portion of their Windows PCs — a dramatic jump from less than five percent today.[1]

Gartner estimates that by 2018, 40 percent of organizations will use EMM tools to manage a portion of their Windows PCs — a dramatic jump from less than five percent today.

Think about that — in less than two years just under half of all companies today will move at least some of their PC management load to EMM. There are likely several reasons for this shift. In addition to Windows 10 support for EMM, global enterprises are looking for new ways to manage their rapidly changing security and agility requirements — and EMM has emerged as one of the top overall approaches.

[1] Saran, Cliff. "What Will Desktop Management Look Like in 2020?" Computer Weekly. http://www.computerweekly.com/feature/What-will-office-desktop-computing-look-like-in-2020.

Windows 10 + EMM Simplifies and Secures PC Management

The shift toward EMM as a PC management platform is actually very good news for administrators. It means that functionality doesn't have to be sacrificed for flexibility because an EMM provider like MobileIron can handle several common Windows 10 PC management tasks just as easily as a traditional toolset. This is because Windows 10 combines all the MDM APIs and app development tools onto a single integrated platform. With this shift, MDM policies configured for Windows 10 can be applied consistently across all Windows 10 devices through MobileIron's EMM platform.

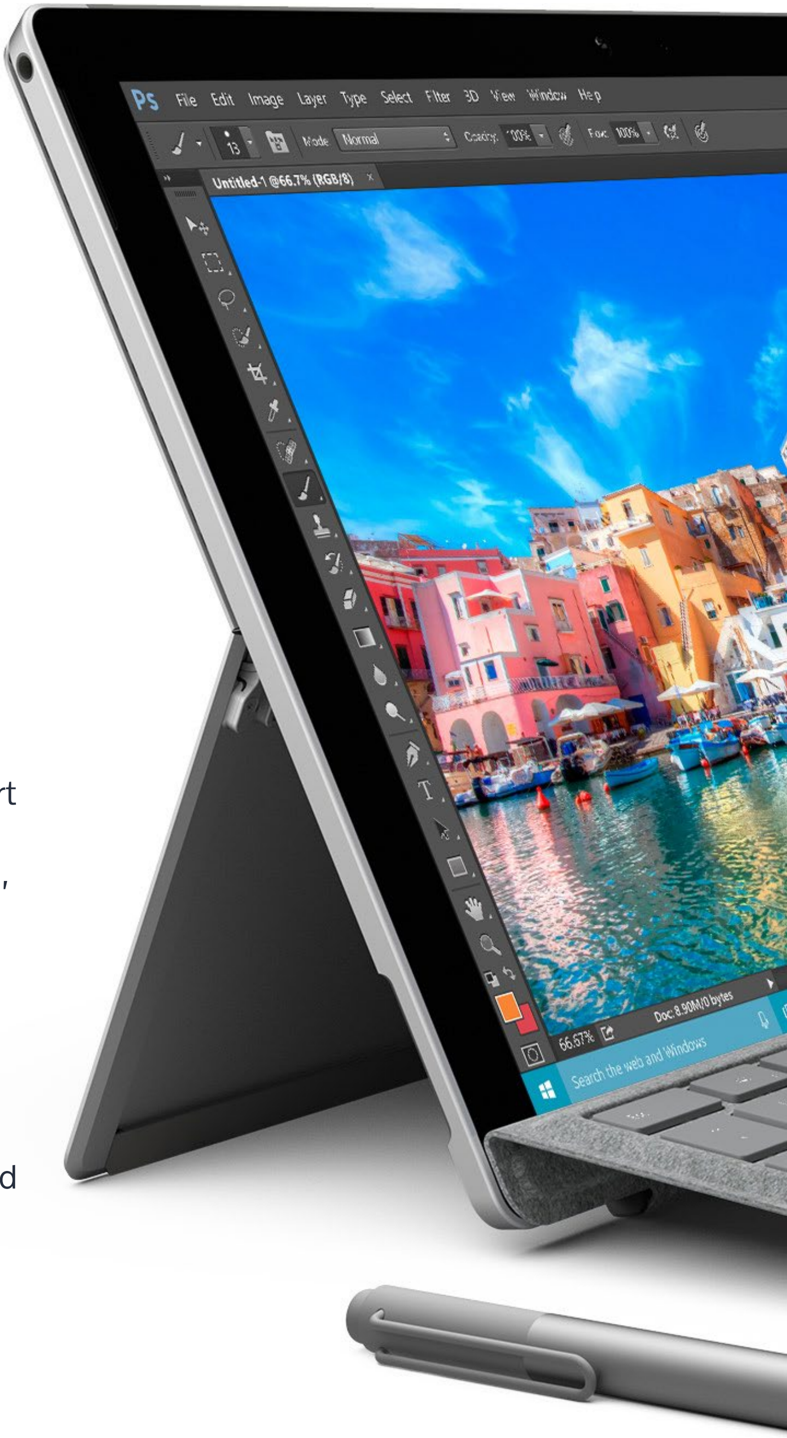
Functionality doesn't have to be sacrificed for flexibility because an EMM provider like MobileIron can handle several common Windows 10 PC management tasks just as easily as a traditional toolset.

For example, if IT creates 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. Microsoft had previously released MDM protocols for Windows Phone 8.1 and Windows 8.1 for laptops and tablets, but they were not the same and therefore required separate APIs and control interfaces. Windows 10 greatly simplifies management across all devices, and the following section illustrates how this particularly benefits PC administrators in five key management areas.

Top Five PC Management Capabilities of EMM

As mentioned previously, the existing model of domain-joining can't meet all the management requirements in today's rapidly changing enterprise. Together, Windows 10 and MobileIron offer a more comprehensive approach to PC and mobile management because they can easily support new devices, apps, and OS upgrades — flexibility that is absolutely essential to every IT organization.

Together, Windows 10 and MobileIron offer a more comprehensive approach to PC and mobile management because they can easily support new devices, apps, and OS upgrades — flexibility that is absolutely essential to every IT organization.


Ps File Edit Image Layer Type Select Filter 3D View Window Help
Mode: Normal
Untitled-1 @66.7% (RGB/8)
66.67%
Doc: 8.90M/0 bytes
Search the web and Windows

According to Gartner, the ability to manage and support a range of devices is becoming mission-critical for PC administrators. A recent report estimates that "by 2018, 40% of contact with the IT service desk will relate to smartphones and tablet devices — a leap from less than 20% today. This will put a heavy burden on desktop IT support, unless it works in a different way."[2]

This is where MobileIron can play a fundamental role in critical PC management processes. The following section details common PC management use cases and how EMM can perform them as well — or better — than current tools and processes.

[2] Saran, Cliff. http://www.computerweekly.com/feature/What-will-office-desktop-computing-look-like-in-2020

Use case #1: PC Setup and Enrollment

Traditional PC management

In the traditional PC setup model, an admin must physically access the device to enroll it through a high-cost, high-touch PC imaging process. This process requires IT to maintain a set of hardware drivers as well as a set of standard devices. If the company uses an image deployment service, which typically costs $20-25 per system, the cost of PC imaging can add up quickly.[3] Not only are traditional methods expensive, they are also time-consuming. For example, if a remote worker loses or damages his laptop, it can take several days to replace the device. With modern methods, IT can configure and secure a new device over the air, allowing the employee to be up and running the same day.

Windows 10 + MobileIron

With Windows 10 and MobileIron, IT can bypass many of the logistics necessary to deliver a traditionally imaged PC. With MobileIron, admins can support a broader range of devices, including BYOD and devices used by remote workers. Multiple devices can be configured and enrolled in EMM simultaneously without anyone needing to touch the device. This means devices can be enrolled anywhere, at any time, without being connected to a corporate network.

Windows 10 and MobileIron enable devices to be enrolled anywhere, at any time, without being connected to a corporate network.

Use case #2: Enterprise App Store Deployment

Traditional PC management

Enterprise app administration is relatively time-consuming because the admin needs to create a distribution package for each application[4] — a process that can take two to four days per application. Win32 applications may also require custom install scripts to support existing apps, which can create conflicts because some PC applications depend on other application versions to run. Also, unlike modern applications, legacy Win32 applications tend to leave unwanted artifacts after they are uninstalled. This can lead to sluggish performance due to issues such as an overblown registry. The device may also be less secure if certificates are not properly removed.

Windows 10 + MobileIron

IT can administer and distribute apps through an enterprise app store using MobileIron and Windows 10. Users can then select which apps they want installed on their PC or mobile device. Administering apps through EMM and a modern enterprise app store offers two key advantages:

1. **Faster app deployment.** With MobileIron, developers can distribute apps and updates to end users much faster. Users no longer need to search Google for an updated application or ask IT to push it to the device. Instead, admins can build enterprise app catalogs that allow apps to be automatically installed or recommended to end users. An enterprise app store managed by EMM also greatly simplifies app license management.

[3] Cosgrove, Terrence and Rich Doheny. "Manage PCs as Mobile Devices for the Right Use Cases." Gartner Research, March 23, 2016.

[4] Cosgrove, Doheny. March 23, 2016.

2. **Better app security.** Viruses and malware have traditionally plagued Windows platforms due to the inherent openness of the platform. By administering apps through a secure app store managed by MobileIron, developers can minimize security risks.

By administering apps through a secure app store managed by MobileIron, developers can minimize security risks.

Use case #3: Device Management

Traditional PC management

Conventional tools were not designed from the ground up to manage modern operating systems such as Android, iOS, and Windows 10. This results in a fractured management environment that forces admins to use multiple tools to manage legacy PC clients using one console and support mobile operating systems from another. In addition, because traditional PC management requires devices to be domain-joined, those devices must be connected to the corporate network to receive necessary updates. Not only does this add to management costs, it can impact productivity for mobile employees who only intermittently connect their devices to the corporate network and may not receive the latest updates right away.

Windows 10 + MobileIron

Unlike desktop management tools, MobileIron supports a “single pane of glass” multi-OS device management approach. This means critical updates can be distributed to devices on any network to ensure they are securely managed. MobileIron also automates essential management tasks, such as asset reporting and compliance, so IT can focus on more critical issues.

MobileIron automates essential management tasks, such as asset reporting and compliance, so IT can focus on more critical issues.

Use case #4: Certificate-Based Security

Traditional PC management

In many cases, it can take weeks or months to roll out security certificates on PCs. For example, in one common approach, the IT admin configures a customized web page or intranet portal where the user's identity can be verified. The verification process usually requires a few extra authentication steps for the end user. After authentication is completed, the user must then click on a link to generate the required certificates and store them on the PC. Alternately, the user may be instructed to run a script from a command line in order to produce the certificates — a highly unlikely scenario for someone with few technical skills.

Windows 10 + MobileIron

Certificates can be seamlessly deployed the same day in one of two ways:

SCEP certificate provisioning. IT uses 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.

Direct certificate installation. 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. It also simplifies the configuration process for services such as Wi-Fi and email because they can be assigned to a certificate rather than user credentials.

Unlike traditional desktop methods, Windows 10 and MobileIron can quickly and seamlessly deploy security certificates without requiring user intervention.

Use case #5: App Whitelisting/Blacklisting

Traditional PC Tools

Managing application blacklists and whitelists with today's PC management solutions requires the admin to specify all the applications through filenames. These configurations then need to be pushed to the device, which is a manual and time-consuming task.

Windows 10 + MobileIron

In Windows 10, both Windows Store and Win32 apps can 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.[5]

AppLocker makes it easy for IT admins to manage application allow/deny lists; no complex configurations are required.

[5] Cosgrove, Doheny. March 23, 2016.

Key Considerations in Adopting an EMM Platform

Although enterprise IT management is rapidly shifting toward an EMM-centric model, there are still gaps that IT should be aware of as they move in this direction. Some of these gaps may impact your EMM rollout:

- **GPOs vs. EMM policies.** While it's technically possible to manage a device with both GPO and EMM policies, it can create some management conflicts. GPOs and EMM offer completely different policy frameworks, which need to be evaluated before being applied to the same Windows machine. In general, EMM is better suited for remote users and employee-owned devices. On the other hand, GPOs provide more control because Microsoft has thousands of GPOs while EMM contains hundreds of policies. Organizations will need to analyze each framework to determine if they need certain GPO capabilities that EMM doesn't currently provide.[6]

- **Ability to edit and manage the registry.** PC admins are accustomed to tools that allow them to edit granular settings in the registry, but this is an error-prone process that can render the registry unusable. An EMM extension is needed to allow admins to securely edit the registry while minimizing the potential for human error. Admins should also prepare for a period of transition as they shift from established practices and become more familiar with the sandboxed modern architecture environment which offers more stability, protection, and security.

- **Enterprise app store requirements.** While the enterprise app store offers tremendous advantages for both admins and end users, Microsoft has certain requirements for applications distributed via the App Store. Organizations that don't meet these requirements currently have no easy way to distribute their applications and therefore can't leverage this feature. However, Microsoft's recent announcement of the "Centennial" desktop app converter may be good news for organizations. This release allows developers to convert their Win32 and .NET apps into the AppX app format for use in the Windows or Enterprise App Store. This means legacy apps can be deployed to the app store as Universal Windows Platform (UWP) apps, which can then be used on any mobile device, computer, surface-like device, devices without screens, or passive display devices.[7]

- **File system visibility and functionality.** EMM is unable to see which files are on the system, and therefore must have permission to access specific locations on the disk to take certain actions. This is because third-party applications may use files to manage issues such as licensing status. In some cases, the presence of a file controls or modifies the application's behavior, so the ability to view and manage files is an essential IT function. Industry efforts are underway to minimize this gap so EMM solutions can manage tasks at the file level.

[6] Cosgrove, Doheny. March 23, 2016.

[7] Jan Kamps, Haje. "Microsoft Introduces the Desktop App Converter for Bringing Win32 Apps to the Windows Store." TechCrunch, March 30, 2016. http://techcrunch.com/2016/03/30/desktop-app-converter

Next Steps: Recommendations

If you've been thinking of trying EMM, here are a few ways to introduce this management model to your organization:

1.

Start a pilot BYOD program with EMM.

Evaluate how your company is currently securing employee-owned devices. Can you fully support multi-OS devices, content, and apps? Consider exploring an EMM proof-of-concept designed to support a pilot program for select BYOD users in your organization.

2.

Manage new Windows 10 devices with EMM.

If you're planning to upgrade or order new Windows 10 devices, design a small pilot program to configure, secure, and manage these new devices with EMM instead of using your existing desktop management tools.

3.

Securely deploy Office 365.

If you're thinking of deploying Office 365, keep in mind that the domain-joined approach to desktop management simply can't support the Office 365 cloud-based model. EMM is by far the easiest and most secure way to enable Office 365 on any device in your organization.

Five IT Myths about EMM

Myth #1:

"We can't use EMM to manage all of our legacy applications."

Fact:

Microsoft announced that its new Centennial desktop app converter will be able to take existing Win32 apps and convert them to Universal Windows Platform (UWP) apps. According to Microsoft, Centennial will make it easy to bring legacy Win32 and .NET apps into the Windows Store where they can be securely administered by an EMM platform.

Myth #2:

"BYOD devices that are not domain-joined can't be managed because SCCM can't reach them. We have to use VPN to manage our distributed workforce."

Fact:

Traditional, device-wide VPNs disrupt workflow by requiring users to manually establish a VPN connection every time they want to access enterprise content. Additionally, device-wide VPNs allow any app on the device to access sensitive data. MobileIron offers a more intelligent and granular per-app VPN option that ensures only authorized business apps can access corporate resources behind the firewall. Unapproved and personal apps can be blocked, which prevents data loss, protects user privacy, and simplifies and secures distributed workforce management.

Myth #3:

"We just spent a lot of time and money writing scripts and we can't afford to throw out all of that work."

Fact:

EMM does not require the same level of investment as traditional PC management tools. With MobileIron, you don't have to throw away your current tools and start over from scratch. You can gradually add new or upgraded Windows 10 devices to your EMM deployment and scale the transition over time.

Myth #4:

"SCCM is more secure than EMM."

Fact:

In many cases, EMM is actually more secure than SCCM. For example, MobileIron is far more regular about checking device posture and taking corrective action than SCCM.

Myth #5:

"Cloud security isn't as robust as an on-premises infrastructure like SCCM or LANDESK."

Fact:

MobileIron combined with Azure Active Directory is a highly secure solution because it supports conditional access to backend resources. If a device falls out of compliance, the user is blocked from accessing corporate resources until the security issue is fixed.

Conclusion

The release of Windows 10 offers exciting possibilities for a new era of PC management. Together with an EMM provider like MobileIron, PC admins can access unified MDM APIs to manage any Windows 10 device and deliver a consistent, secure user experience regardless of form factor. Admins can also use MobileIron to administer both Win 32 and modern mobile apps through a secure enterprise app store. Access to enterprise resources such as Office 365 can be tightly managed by synchronizing device posture with Azure Active Directory access control. Just as important, admins can scale the transition to EMM over time, which protects current investments and allows IT to ensure its technology and management processes fully align with business requirements.

For organizations that have mostly relied on traditional desktop tools, now is the time to seriously evaluate the need for EMM to secure and manage a greater portion of enterprise devices and apps across the distributed workforce.

For More Information

To learn how MobileIron can help you manage your Windows implementation, please contact us at globalsales@mobileiron.com