Windows 10 with EMM:
TCO Toolkit

MobileIron

MobileIron BRIDGE

10

MKT-11239 EN v1.2

Table of Contents

MobileIron

415 East Middlefield Road

Mountain View, CA 94043

info@mobileiron.com

www.mobileiron.com

Tel: +1.877.819.3451

Fax :+1.650.919.8006

Mobile Disrupts the Desktop

For more than twenty years, the desktop PC dominated enterprise computing as the main productivity tool for knowledge workers. Now this dominance is being challenged as employee preferences shift to mobile experiences and modern operating systems. This new generation of computing has given rise to a powerful and agile model of security and management called enterprise mobility management (EMM). With Windows 10, Microsoft has re-architected the Windows operating system to adopt EMM.

Gartner describes EMM as "the operating system for the digital enterprise."[1] Gartner has also recommended that "EMM should be your first choice for managing Windows 10" for certain use cases because "it offers fundamentally more efficient management, addresses unmet use cases, and offers a better user experience for existing use cases."[2]

Here's why: With the rise of mobile computing, employees don't use a locked-down PC on the corporate network to do their jobs. Instead they use many different devices, some company-owned and some personally owned. These devices run a vast array of mobile apps and connect across networks that are outside of IT's control. Legacy Windows client management tools (CMTs), like Microsoft's System Center Configuration Manager (SCCM), LANDESK, and Symantec IT Management Suite (formerly Altiris), are too manual and inflexible for modern computing environments because they rely on installing and managing a complex system image on the PC.

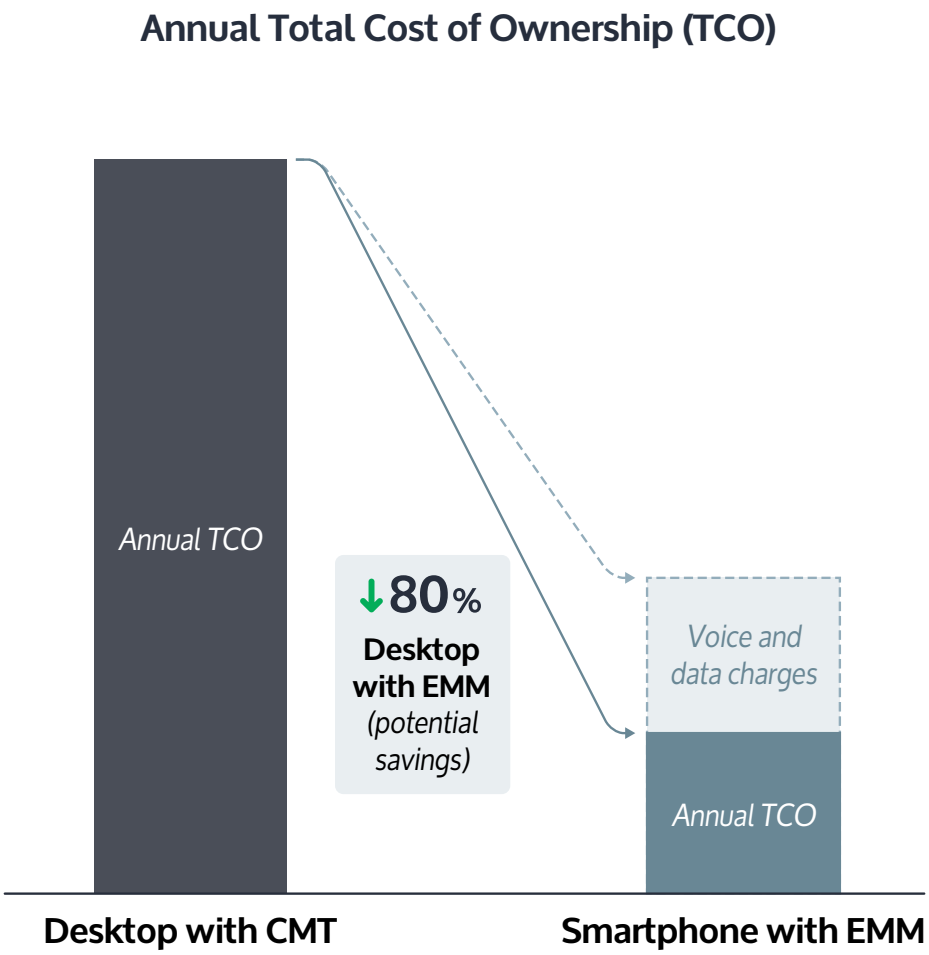
The era of the domain-joined PC is coming to a close.

1 http://blogs.gartner.com/manjunath-bhat/2016/06/14/why-is-enterprise-mobility-management-emm-so-difficult-to-get-right/

2 "EMM Should Be Your First Choice for Managing Windows 10 and Mac OS X," by Andrew Garver, August 15-18, 2016, Gartner, Inc., Gartner Catalyst Conference

With Windows 10, Microsoft is addressing the need for greater security and management flexibility in the enterprise. Windows 10 is revolutionary because it enables IT to migrate PCs from CMTs to modern EMM solutions like MobileIron. EMM moves the legacy PC paradigm from hard-coded image to context-based policy. One of the advantages of this migration is the reduction of up to 80% in the total cost of ownership (TCO) of a PC.

The savings will vary by organization, so this paper provides a TCO framework and detailed worksheet for IT professionals to calculate the potential savings for their particular deployment environment.



Evolution of Windows 10 Architecture

In 1994, Microsoft launched Systems Management Server (SMS) v1. This evolved to System Center Configuration Manager (SCCM) and became the dominant model for securing and managing PCs for the next two decades.

IT created a system image that was installed on PCs before they were given to employees. This image consisted of the operating system plus all the applications and configurations approved by IT for the employee. The result was a PC that was completely locked down, pre-configured, and controlled end-to-end by IT. It was secure as long as no further system changes were made by either the employee or any application on the PC.

The traditional Windows architecture offered a broad attack surface because both the file system and the operating system could be easily compromised. To mitigate the risk, IT had to install, as part of the image, several additional security agents to monitor threats and remediate appropriately. Maintaining data security on the PC was a constant challenge. Whenever a user downloaded an application, there was always a chance it could compromise the underlying system. If the application was deleted, it could still leave unwanted artifacts that could slow performance, create system instability, or obscure the root cause of any problem. In an enterprise with hundreds or thousands of PCs, all of these slight system variations increased both the complexity of data loss prevention and the cost of troubleshooting.

The traditional PC model required devices to join a domain governed by a set of group policy objects (GPOs) which controlled what employees could and could not do on a PC. This assumed the devices were corporate-owned, Windows-based, and connected to a persistent LAN. The modern enterprise no longer works this way. Today's employees work on any device and in a variety of environments — home, airports, coffee shops, hotels, etc. The traditional approach can no longer support this work style because mobile devices are not always on the LAN and are frequently owned by the employee, not the company. They tend to be mixed-use devices that are deeply embedded in every aspect of an employee's personal and work life.

To address these new requirements, Microsoft has re-architected Windows to move beyond CMT to support EMM. As further evidence of the increasing shift to EMM, Gartner retired the Magic Quadrant for Client Management Tools in March 2016. Gartner said it made the decision because of stalled market innovation and an overall industry evolution toward modern approaches.[3]

3 "Gartner Retires the Magic Quadrant for Client Management Tools," by Rich Doheny, Terrence Cosgrove, March 29, 2016, Gartner, Inc. https://www.gartner.com/doc/3267732/gartner-retires-magic-quadrant-client

The Real Value of EMM

EMM solutions provide an efficient and flexible way to provision services to employees and secure business data on modern operating systems. The move to EMM represents a major change in how the desktop will be secured and managed moving forward. As InfoWorld writes, "IT needs to start planning now for the day when PCs are managed and secured like mobile devices, and desktop apps are developed and deployed like mobile apps."[4]

The EMM model offers several benefits:

Lower cost:

EMM eliminates high-touch CMT processes for image management and device provisioning. EMM operates over the air and so does not require IT to manually configure a device. Along with simpler help desk and troubleshooting processes, EMM reduces TCO for PCs.

Secure BYOD:

EMM establishes a data boundary between work and personal information on a PC, which secures the former without compromising the privacy of the latter. This separation of personal and work data is essential for enabling bring-your-own-device (BYOD) programs. CMT cannot be used for personal PCs because it requires a device-wide corporate system image to be installed.

Real-time policy:

EMM allows policies to be updated and compliance to be maintained even when the PC is on an external network. CMT requires the PC to be joined to the domain and may depend on user login or VPN activation for policies to be updated.

Better user experience:

EMM supports self-service and puts more control and choice in the hands of the employee. It is far less intrusive than CMT and IT never has to physically touch the device. Unlike CMT, EMM also provides a consistent user experience across multiple operating systems, including Android, iOS, and Windows 10.

4 http://www.infoworld.com/article/3120505/computers/your-pc-is-simply-another-mobile-device.html

TCO Model for Windows 10 with EMM

An EMM solution like MobileIron can allow IT to perform desktop security and management functions for a fraction of the cost IT currently incurs using traditional CMT. This section outlines a comparative cost model across hardware, software, IT operations, and the service desk. While every IT organization has its own cost structure, this model and the TCO worksheet at the end of this document can provide a starting point for custom analysis.

Because the Windows 10 EMM transition is just starting, most organizations do not have cost data from their actual experiences yet. However, over the last several years, Gartner has published TCO analyses that provide directional guidance.

Published TCO for PCs and Smartphones

According to Gartner research, the annual TCO of a fully managed smartphone using EMM is almost 80% lower than the annual TCO of a fully managed desktop using CMT.

The annual desktop TCO is $3,126[5] and the annual smartphone TCO is $679.[6] Adding voice and data charges, which aren't relevant for the desktop, the annual smartphone TCO rises to $1,339, which is still almost 60% lower than annual desktop TCO.

Therefore, organizations can potentially save up to 80% as the desktop moves from Windows 7 to Windows 10, and the security and management model moves from CMT to EMM.

Gartner Analysis: TCO of CMT-Managed Desktops[5] and EMM-Managed Smartphones[6]

Annual cost	Fully managed desktop	Fully managed smartphone	Description
Total direct costs	$1,539	$245 ($905 with voice/data)	This represents the annual hardware, software, and labor costs of managing a PC or smartphone. Smartphones have an additional $660 annual cost for cellular voice and data, for which there is no PC equivalent. If that cost is added the smartphone annual TCO increases from $245 to $905.
Total indirect costs	$1,587	$434	This is the annual cost of downtime per end user. This cost can fluctuate depending on individual salaries (e.g., downtime for higher-paid executives would cost more). PC indirect costs are higher because CMT solutions require manual IT touch while smartphone provisioning and maintenance using EMM tends to be over-the-air and self-service by the employee.
Total cost of ownership	$3,126	$679 ($1,339 with voice/data)	Smartphone annual TCO is **78%** lower than PC annual TCO. Even including cellular voice and data charges, smartphone annual TCO is **57%** lower than PC annual TCO.

5 "Desktop Total Cost of Ownership: 2013 Update," by Federica Troni and Michael Silver, March 14, 2013, Gartner, Inc. http://www.gartner.com/document/2371417

6 "Use TCO to Assess Choice in Devices, Support Policies and Management Approaches," by Federica Troni and Michael Silver, Nov. 4, 2014, Gartner, Inc. http://www.gartner.com/document/2898217

The range of potential savings is broad and will vary by organization. Achieving even a portion of the potential will result in substantial savings that could be applied to strategic IT initiatives such as application modernization or business transformation.

There will also be a transitional investment of time and resources before the full value of the Windows 10 with EMM end state can be realized. The transition playbook at the end of this paper outlines migration considerations of moving from CMT to EMM.

TCO Components for Windows 10 with EMM

This section outlines the major costs associated with security and management in a CMT environment vs. security and management in an EMM environment. These costs are divided into four categories:

1. Hardware and software licensing
2. IT operations
3. Service desk
4. Employee downtime (indirect)

The first three are direct costs. The fourth is an indirect cost, but relevant to this analysis because the EMM model requires far less manual touch from IT. As a result, the employee rarely, if ever, has to give up his or her device to IT for installation or repair.

The goal of this section is to help each organization define its credible end state for PC TCO across each of these four cost components.

1. Hardware and Software Licensing

Hardware

- Hardware costs for the endpoint will be consistent across the CMT and EMM models because both support the same Windows 10 PCs. The EMM model will require less back-end server hardware and the CMT model will require less bandwidth for software distribution.

Software

- **CMT model:** In addition to the investment in the CMT solution, traditional PC security and management also requires licensing several secondary software components, such as encryption, anti-malware, VPN, content-aware data loss prevention (DLP), app sandboxing, virtual desktop infrastructure (VDI), patching agents, and backup agents.
- **EMM model:** With MobileIron controlling the embedded capabilities of Windows 10, many traditional secondary software components will no longer be required because they will either be embedded in the MobileIron solution, embedded in Windows itself, no longer technically possible, or replaced by other compensating controls. EMM, as a platform, has become central to enterprise security. In fact, one of Gartner's strategic planning assumptions is that "through 2020, the combined security capabilities of mobile platforms and EMM solutions will meet 80% of enterprise mobile security requirements."[7] Windows 10 is another proof point that EMM is becoming the policy hub for enterprise security.

7 "When and How to Go Beyond EMM to Ensure Secure Enterprise Mobility," by Manjunath Bhat, Dionisio Zumerle, June 10, 2016, Gartner, Inc. http://www.gartner.com/document/3343519

Traditional software (starting state)	Modern software and compensating controls (end state)
Client management tools (CMT)	**MobileIron + Windows 10** MobileIron integrates with Windows 10 to provision and configure endpoint services through policy-based controls and an enterprise app store. MobileIron Bridge extends these capabilities so admins can deploy granular GPO-style configurations, edit and manage the registry, deliver non-MSI Win32 apps through an enterprise app store, and view and manage the file system without requiring the PC to join the domain. MobileIron Bridge fills the GPO gap between traditional CMT systems and EMM to speed up migration from CMT to EMM.
Disk and file encryption	**MobileIron + BitLocker** Microsoft BitLocker is already becoming the default encryption method for Windows systems. MobileIron provides the monitoring mechanism to determine whether or not encryption is activated, and also provides the remediation mechanism to remove enterprise data if it is not. In parallel, organizations may use Microsoft BitLocker Administration (MBAM) for encryption deployment, key recovery, and reporting. Some organizations with highly sophisticated BitLocker management needs might use third-party tools instead of MBAM.
Anti-malware suite	**MobileIron + threat detection services** Traditional signature-based, anti-malware suites are not needed on modern sandboxed operating systems because the spread of file-based attacks is tightly constrained by the native data containerization embedded in the operating system. MobileIron checks device and OS integrity on an ongoing basis to ensure non-compliance is identified and appropriate remediation policies are enforced. However, Gartner predicts that by 2018, between 5-15% of organizations will, in addition, deploy a threat detection service to identify anomalous behavior and zero-day attacks.[8] MobileIron provides enforcement and remediation when such threats are detected by these services. Anti-malware suites scanning for anomalous behavior may also be useful if legacy Win32 apps are running on the device.
Device VPN	**MobileIron + Windows 10** Device-wide VPN is being replaced by per-app VPN. Separation of personal and work data across the network is essential to protect privacy. MobileIron Tunnel provides a secure tunnel for business applications so IT will not need separate dedicated VPN infrastructure.
App sandboxing	**MobileIron + Windows 10** Modern apps are sandboxed natively in Windows 10, so there is no need for secondary sandboxing tools. However, many organizations will have legacy Win32 apps. Microsoft's Desktop App Converter is a good first step to convert traditional Win32 apps to Universal Windows Platform (UWP) apps. This is more secure than running an unconverted app, but not as secure as an app without any Win32 code. Additional compensating controls in the transition period could include blacklisting known attack vectors, running only signed apps, and using, for the time being, an anti-malware product that scans for anomalous behavior. Whitelisting apps can add security as well, but at the substantial cost of flexibility. MobileIron also acts as a policy engine for Windows Information Protection (WIP) to prevent data leakage from authorized to unauthorized apps on the device.

8 "Market Guide for Mobile Threat Defense Solutions," by John Girard, Dionisio Zumerle, July 28 2016, Gartner, Inc. https://www.gartner.com/doc/3393617/market-guide-mobile-threat-defense

Traditional software (starting state)	Modern software and compensating controls (end state)
Content-aware DLP	**MobileIron + Windows 10** Content-aware DLP solutions inspect the file system on a device to identify sensitive information such as credit card numbers, so organizations can set policies to mitigate the risk of losing that data. These solutions are not technically feasible on hardened and sandboxed modern operating systems like Windows 10 because they require the operating system to allow an app to scan the content of other apps and the overall file system. The compensating control is to set DLP policies through MobileIron at the app level to prevent unauthorized data sharing. Some organizations may continue to use existing network DLP solutions to inspect traffic going to and from a mobile device in order to identify sensitive data.
Virtual desktop infrastructure (VDI)	**Modern apps + Windows 10** VDI is a transitional technology. VDI solutions run the desktop image on a server, not on the device itself, so that apps can be accessed remotely without any local data on the PC. This technology has two main drawbacks. It is expensive to deploy and it provides a poor user experience because the application is not optimized for a modern touch interface. Apps should be modernized, not virtualized. VDI can still act as a transitional mechanism to make legacy apps available on modern devices until those apps are modernized, but app streaming may be a more effective approach.
Patching	**MobileIron + Windows 10** Using MobileIron, the administrator can see which OS patches are available, see which ones apply to a particular device, and decide when and how to distribute them. MobileIron Bridge can allow the administrator to do rollbacks when necessary as well. Some OS builds are very large and could strain the network depending on the breadth of the distribution, so it is essential to have a good understanding of network capacity in order to structure the rollout.
Backup	**Modern apps + Windows 10** Modern apps sync data to a back-end service, either on-premises or in the cloud, so very little, if any, data resides only on the endpoint. Email apps and enterprise file sync and share (EFSS) apps already operate this way, and this is also the behavior that virtually all modern third-party business apps will follow. Full device backup is not necessary in the end state, and like iOS, may not even be possible through a third-party service because of the inherent sandboxing of the apps.

2. IT Operations

CMT/EMM platform administration

- Both types of platforms must be administered. MobileIron generally requires 1-2 FTEs per 10,000 devices for administration, while CMT systems generally require more. Most large organizations already have an installed CMT for PCs and an installed EMM for mobile devices so this cost component should be relatively easy to quantify.

Image management

- **CMT model:** With CMT, IT must create, test, and maintain a system image to deploy the operating system and company-authorized apps and configurations. Each image can take 40-60 hours to create and test. The system image must initially be installed manually on each new PC, which can take over an hour, and the PC must then be physically delivered to the employee. Additional admin and employee labor may be required to configure and install certificates on the machine. Images are usually updated at least twice a year. Ongoing image distribution and configuration updates can happen over the air but only when the machine is on the corporate network.
- **EMM model:** With MobileIron, there is no system image to create. Instead, IT sets policies for device configuration and deploys an enterprise app store. IT can simultaneously configure and secure large numbers of devices over the air across any wireless network. Employees can be up and running on their devices in a matter of minutes instead of days without the need for any IT intervention. Certificates can be provisioned automatically, eliminating the need for employee interaction. New configurations, policies, and changes require minimal effort from IT. They deploy automatically to the device and remain transparent to the employee. To do this, IT simply creates a per-app VPN configuration together with a Simple Certificate Enrollment Protocol (SCEP) profile on the MobileIron server and then assigns them to a group. The devices of all employees in that group are automatically enrolled with the appropriate settings and with access to the appropriate apps. In addition, the per-app VPN can be configured to automatically launch when the app is launched, find its own server, and authenticate (using certificates) without any action from the employee.

Training for employees

- **CMT model:** All roads lead to IT in the CMT model. Employees need to know how to file trouble tickets but have very little additional control over their PCs.
- **EMM model:** With MobileIron, self-service is the core of the deployment model. Employees enroll themselves and then select their apps, which will require some employee training.

Software distribution

- **CMT model:** With CMT, IT admins must create application distribution packages and (in some cases) custom install scripts to deploy applications to PCs. This process is labor-intensive and can take two to four days per application regardless of how many PCs receive the application. The time required and delivery success rate will depend on the complexity of the application, such as[9]:
  - Does it require special base configurations?
  - Does it have dependencies on operating system functions or other apps?
  - Does it require a reboot during or after installation?
  - Does it require multiple tests for system and integration testing?

9 "Sample App Package Benchmarking," by Terrence Cosgrove, Gartner, Inc. (unpublished)

- **EMM model:** With MobileIron, IT administers and distributes apps through an enterprise app store. Modern Windows apps leverage the Universal Windows Platform (UWP), and there is no additional packaging required for UWP apps. Employees go to the MobileIron enterprise app store to select and install the apps they want. The install process is far simpler for the employee, and there are minimal dependencies other than perhaps the OS version. When a new version of the app is available, IT publishes the update, which is then automatically installed on the device. MobileIron can also distribute traditional Win32 apps packaged as MSI, which makes the distribution simpler but would still require the laboriousness of traditional packaging.

Organizations willing to modernize their apps will gain the most cost savings and deliver the most value and best experience for their employees. In some organizations, this may not be possible in the short-term because an existing Win32 app may be essential to the business and not easy to modernize.

In these situations, IT has four options for distributing legacy apps:

1. Use MobileIron Bridge with scripting to deploy the non-MSI Win32 app.
2. Use one of many wrappers available to convert traditional "setup.exe" to the MSI file format, and then distribute the MSI version of the app directly through the MobileIron enterprise app store.
3. Use the Microsoft Desktop App Converter to convert Win32 applications into UWP applications without requiring a developer. These converted apps can be distributed via MobileIron, like MSI files, and they leave no artifacts. They can also take advantage of real-time notifications and other benefits of UWP apps. Once they are UWP apps, ongoing packaging work is dramatically reduced.
4. Provide remote access to the legacy apps through either VDI (virtualized desktop) or app streaming.

App conversion and remote access are, however, only short-term approaches to the legacy app challenge. The best long-term answer is to use Windows 10 migration as a catalyst to critically assess the existing legacy apps portfolio to determine which Win32 apps to modernize and which to retire.

3. Service Desk

Level 1/2/3 staffing

- **CMT model:** Service desk costs for traditional Windows deployments can be high due to ongoing management complexity and endpoint variability. File system vulnerabilities and OS dependencies expand the attack surface on the device and increase the complexity of troubleshooting. Root cause analysis is also challenging, but CMT does provide detailed information to aid troubleshooting activities. Ratios vary by organization and service levels but CMT-managed endpoints require approximately three support FTEs per 1,000 devices.
- **EMM model:** With EMM and modern operating systems like Windows 10, system stability should be higher and, in our experience, users report fewer incidents than for traditional PCs. Fewer dependencies and linkages between the app and OS minimize problems and simplify troubleshooting, so the technician-to-device ratio can be much smaller than with CMT. EMM-managed endpoints require approximately one support FTE per 1,000 devices.

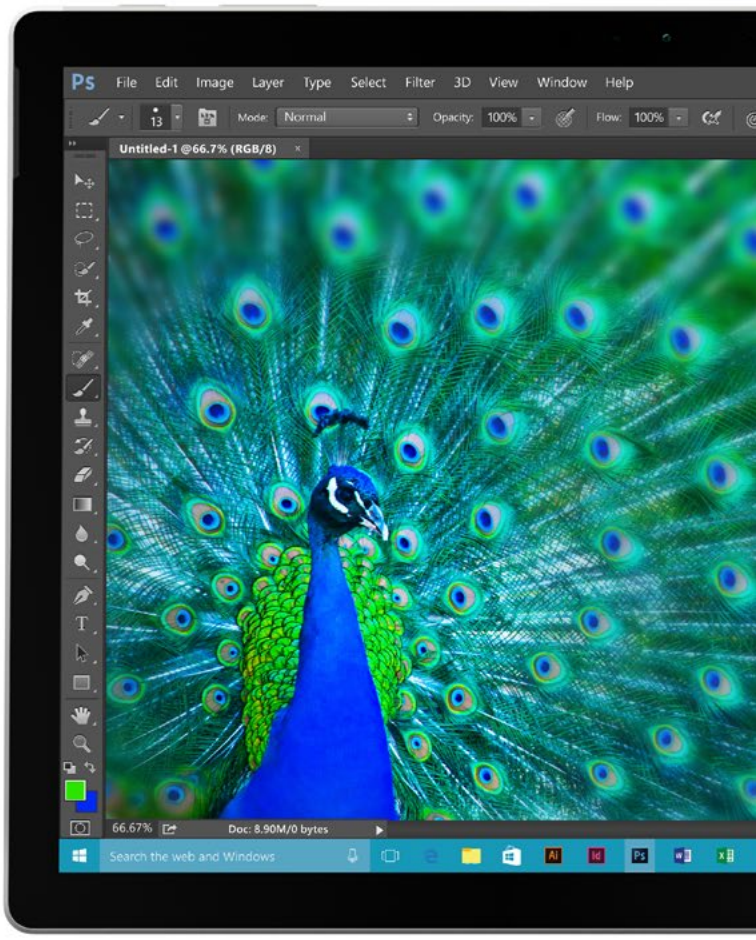
Training for support staff

- **CMT model:** Employee technical issues can be complex and hard to troubleshoot. To quickly and accurately resolve problems, support staff need a relatively sophisticated understanding of the underlying architecture of operating system and apps.
- **EMM model:** In our experience, root cause analysis is generally easier, because so many modern OS subsystems are black boxes to minimize dependencies.

4. Employee Downtime (Indirect)

Time without device

- **CMT model:** With CMT, IT processes are high-touch, very manual, and require the employee to give up his or her laptop, sometimes for extended periods. This impacts employee productivity.
- **EMM model:** With MobileIron, IT processes are low-touch and over-the-air. As a result, troubleshooting and repair logistics are easier for both employees and IT, and the device is almost never with IT.



Transition Playbook

The prior section outlined the TCO difference between the starting state of Windows with CMT and the end state of Windows with EMM. But transitions, no matter how beneficial in the long run, can be challenging for an organization without a structured playbook. Several factors will determine how quickly an organization can move from CMT to EMM and achieve its target cost savings:

- **Windows 10 adoption:** The legacy CMT system will need to be functional until all Windows endpoints are migrated to Windows 10. In most organizations, new Windows 10 devices, especially tablets such as Microsoft Surface or similar devices from HP or Lenovo, will be the starting point for EMM. Even after the migration, the CMT may still be used for back-end Windows server management.
- **GPO complexity:** EMM policies are new to Windows 10 and may not yet replicate the full set of GPOs that an organization has deployed to its existing PCs. MobileIron Bridge addresses this GPO gap and allows IT to apply these same granular policies without requiring CMT or requiring the PC to join the domain. However, the EMM transition is a good time to reconsider the complexity of existing GPOs. Many legacy policies may no longer be required. Even with the power of MobileIron Bridge, organizations should still critically evaluate their policy infrastructure to determine what is really required instead of deploying complex policies simply because that is what they did in the past.
- **Legacy apps:** The fewer legacy Win32 apps in an organization, the better the Windows 10 user experience and the faster the migration to EMM. Less than half the apps in an organization are now Windows-specific[10], and most organizations accept the inevitability of moving off Win32 apps. Many still struggle with the resources required for app modernization. There are several short-term options to ease legacy app deployment, like app conversion through Microsoft's Desktop App Converter or remote access through VDI or app streaming. These approaches can be effective stop-gap measures but shouldn't be viewed as a long-term application strategy. They are only a short resting point on the essential journey to app modernization.
- **Organizational inertia:** EMM is disruptive to existing desktop management practices and organizational silos. Some CIOs may have to address conflict between the desktop and mobile teams as new security and management architectures and operational processes are put in place. Change management is an important component of the EMM migration and will require the support of executive leadership within the organization.

10 "IBM's Internal Apple Mac Savings Started With New Processes," by Michael A. Silver, Terrence Cosgrove, Rich Doheny, May 4, 2016, Gartner, Inc. https://www.gartner.com/doc/3306418/ibms-internal-apple-mac-savings

Conclusion

The move to EMM is the most fundamental shift in Windows security and management in twenty years. It is not a question of if the world's business PCs will move to EMM, but when. InfoWorld has noted, "Maybe the benefits of EMM, coupled with the greater trends to cloud computing and mobile-first application development, will finally let IT cut loose all that technical debt that threatens to mire it in the past. It will need to, because operating systems, apps, and protocols are all moving targets that require periodic refreshing. Mobile management admins know that from the annual API updates from Apple and Google and the regular pace of OS and app updates. Desktop admins need to prepare for that reality as well."[11]

Planning the transition to EMM and quantifying potential cost savings require a detailed analysis of an organization's existing security and management infrastructure. The TCO model and worksheet in this paper can provide a good starting point.

But where does this transition fit in the priorities of an IT organization? When should planning start? InfoWorld has a recommendation: "Start now, if not sooner."[12]

To learn how MobileIron can reduce your PC TCO, please contact us at globalsales@mobileiron.com.

11 http://www.infoworld.com/article/3109247/microsoft-windows/why-and-how-you-should-manage-windows-pcs-like-iphones.html

12 http://www.infoworld.com/article/3120505/computers/your-pc-is-simply-another-mobile-device.html

MobileIron

Appendix: TCO Worksheet

Step 1: Quantify current actual costs for your Windows 7 desktop deployment using CMT

Step 2: Quantify current actual costs for your iOS mobile deployment using EMM

Step 3: Estimate, based on the framework in this paper, potential cost of Windows 10 desktop deployment using EMM

	Current state: Windows 7 with CMT		End state: Windows 10 with EMM		Current state: iOS with EMM
HARDWARE					
Annual purchase cost per device					
• Cost of purchasing device	$1,000+	→	$1,000+	←	$100+
• Amortization period (# of years)	3-4 years	→	3-4 years	←	2-3 years
Annual hardware cost per device	Calculate	→	Calculate	←	Calculate
SOFTWARE (Security and Management)					
Annual software licensing cost per device					
• Platform (CMT or EMM)	$20 per device per year	→	$40 per device per year	←	$40 per device per year
• Disk and file encryption	MBAM or 3rd party	→	MBAM or 3rd party	←	N/A
• Anti-malware suite	3rd party	→	For zero-day or legacy apps	←	For zero-day
• Device VPN	3rd party	→	Per-app VPN (EMM+)	←	EMM+ (per app VPN)
• App sandboxing	3rd party	→	Anti-malware if legacy apps	←	N/A
• Content-aware DLP	3rd party	→	N/A	←	N/A
• Virtual desktop infrastructure (VDI)	3rd party	→	Transitional till modern apps	←	Transitional till modern apps
• Patching	CMT+	→	EMM+	←	N/A
• Backup	3rd party	→	Minimal as modern apps	←	N/A
• Other security and management software	Company-specific	→	Company-specific	←	Company-specific
Annual software cost per device	Calculate	→	Calculate	←	Calculate
IT OPERATIONS					
Annual IT labor cost per device					
CMT/EMM platform administration:					
• # FTE	3-4 per 10,000 devices	→	1-2 per 10,000 devices	←	1-2 per 10,000 devices
• Annual cost per FTE	Company-specific	→	Company-specific	←	Company-specific
Annual total CMT/EMM platform admin cost	Calculate	→	Calculate	←	Calculate
Image management (create and test):					
• Hours to create and test new image	60 hours	→	N/A	←	N/A
• Number of new images created per year	Company-specific	→	N/A	←	N/A
• Total hours/year to create/test new images	Calculate	→	N/A	←	N/A
• Hourly labor cost	Company-specific	→	N/A	←	N/A
Annual total image creation and testing cost	Calculate	→	N/A	←	N/A
Image management (deploy):					
• Hours to install image on new PC	1-2 hours	→	N/A	←	N/A
• Number of new PCs deployed each year	25% of fleet	→	N/A	←	N/A
• Total hours/year to deploy images on new PCs	Calculate	→	N/A	←	N/A
• Hourly labor cost	Company-specific	→	N/A	←	N/A
Annual total image deployment cost	Calculate	→	N/A	←	N/A
Training for employees					
• Total annual cost of employee training sessions	Company-specific	→	Company-specific	←	Company-specific
• Total annual cost of employee training materials	Company-specific	→	Company-specific	←	Company-specific
Annual total employee training cost	Calculate	→	N/A	←	N/A

IT Operations continue on next page...

Software distribution:					
• Hours to package an app for distribution	16-32 hours	→	N/A	←	N/A
• Total app packages per year	Company-specific	→	N/A	←	N/A
• Total hours per year to package apps for distribution	Calculate	→	N/A	←	N/A
• Hourly labor cost	Company-specific	→	N/A	←	N/A
Annual total software distribution cost	Calculate	→	N/A	←	N/A
Total annual IT operations cost	Calculate	→	Calculate	←	Calculate
Number of devices under management	Company-specific	→	Company-specific	←	Company-specific
Annual IT operations cost per device	Calculate	→	Calculate	←	Calculate

SERVICE DESK

Annual service desk labor cost per device

Level 1/2/3 staffing:					
• # FTE	3-4 FTE per 1,000 devices	→	TBD	←	1 FTE per 1,000 devices
• Annual cost per FTE	Company-specific	→	Company-specific	←	Company-specific
Annual total Level 1/2/3 staffing cost	Calculate	→	N/A	←	N/A
Training for support staff:					
• Total annual cost of support training sessions	Company-specific	→	Company-specific	←	Company-specific
• Total annual cost of support training materials	Company-specific	→	Company-specific	←	Company-specific
Annual total support training cost	Calculate	→	Calculate	←	Calculate
Total annual service desk cost	Calculate	→	Calculate	←	Calculate
Number of devices under management	Company-specific	→	Company-specific	←	Company-specific
Annual service desk cost per device	Calculate	→	Calculate	←	Calculate

EMPLOYEE DOWNTIME (INDIRECT)

Annual labor cost of lost productivity

• Number of hours without device per year	Company-specific	→	Company-specific	←	Company-specific
• Hourly labor cost	Company-specific	→	Company-specific	←	Company-specific
Annual employee downtime cost per device	Calculate	→	Calculate	←	Calculate

Total annual cost per device	Calculate	→	Calculate	←	Calculate