



Windows 10, EMM und die Zukunft der PC-Sicherheit und PC-Verwaltung

Zusammenfassung für die Geschäftsleitung

Die Verwaltung Ihrer Geräte wird immer komplexer und Ihre Administratoren kämpfen mit Sicherheits- und Verwaltungsaufgaben, die komplizierter sind als je zuvor. Bis heute brauchten Sie viele verschiedene komplexe Tools, um Geräte abzusichern und zu verwalten. Mit Windows 10 und MobileIron wird Ihr Leben einfacher. Diese beiden Produkte rationalisieren viele traditionelle Aufgaben der PC-Verwaltung.

Inhalt

Zusammenfassung für die Geschäftsleitung	1
Windows 10 ändert die Spielregeln für die PC-Verwaltung	3
Einfache und sichere PC-Verwaltung mit Windows 10 + EMM	4
Die fünf wichtigsten PC-Verwaltungsfunktionen der EMM-Plattform	5
Hauptüberlegungen für die Einführung einer EMM-Plattform	9
Nächste Schritte: Empfehlungen	10
Fazit	12

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



Mit Windows 10 ist ein vereinheitlichtes Konzept verfügbar, das viele Aufgaben der traditionellen PC-Verwaltung deutlich vereinfacht

Mit der Freigabe von Windows 10 müssen Administratoren nicht länger verschiedene Tools zur Verwaltung von Desktop-Computern wie LANDESK oder den Microsoft System Center Configuration Manager (SCCM) zur Verwaltung der Windows PC-Clients einsetzen. Stattdessen können die Administratoren mit einer Enterprise Mobility Management-Plattform (EMM) alle Geräte unter Windows 10 verwalten - auch PCs und Mobilgeräte, die im Rahmen einer BYOD-Initiative oder von den Mitarbeitern privat genutzt werden. Möglich wird dies in Windows 10, weil die Administratoren auf einen einheitlichen Satz von MDM APIs über einen EMM-Anbieter wie MobileIron zugreifen können. Mit EMM-Plattformen können Administratoren die Gerätekonfiguration und Geräte-Setups beschleunigen, die App-Verwaltung vereinfachen und eine nahtlose Sicherheit für alle über die EMM-Plattform verwalteten Unternehmensgeräte sicherstellen.

Um die Unterschiede zwischen der traditionellen Desktop-Verwaltung und den EMM-Möglichkeiten zu verdeutlichen, erläutert dieses Whitepaper die fünf wichtigsten Anwendungsfälle zur Verwaltung von Desktops durch eine EMM-Plattform. Sie finden hier außerdem Empfehlungen für Unternehmen, die ihre Verwaltungsinfrastruktur modernisieren und ein einheitliches EMM-Konzept einführen wollen.

Windows 10 ändert die Spielregeln für die PC-Verwaltung:

Die PC-Verwaltung hat sich über die Jahre signifikant entwickelt, um die dynamischen Anforderungen der Unternehmen zu erfüllen. Heute erfordert die Verwaltung von PCs häufig die Anmeldung bei einer Domain mit einer Reihe von Gruppenrichtlinienobjekten (GPOs), die festlegen, wie ein Computersystem auszusehen hat und wie es sich für eine bestimmte Benutzergruppe verhält. Zusammen mit Tools wie LANDESK und SCCM ist dieses Modell am effektivsten, wenn alle Geräte ständig mit einem LAN verbunden sind. Es fehlt jedoch die Flexibilität, um auch nur hin und wieder mit dem Netzwerk verbundene Mobilgeräte zu verwalten – und diese setzen die Benutzer in Unternehmen immer häufiger statt der bei einer Domain angemeldeten Geräte ein. Die IT-Administratoren benötigen daher eine konsistentere und sichere Plattform zur Verwaltung der vielen verschiedenen Geräte im Unternehmen.

Windows 10 berücksichtigt diese Lücke und verlagert die Geräteverwaltung aus der Domain in eine EMM-Plattform als den einzigen vertrauenswürdigen Verwaltungspunkt im Unternehmen. Windows 10 führt die traditionellen Windows-Betriebssysteme zusammen und bietet für eine einheitliche Plattform einen vereinheitlichten Satz MDM-APIs. Dank dieser Zusammenführung kann die IT jedes Gerät mit Windows 10 absichern und verwalten, indem sie die MDM-Protokolle über einen EMM-Anbieter wie MobileIron abrufen. Windows 10 modernisiert außerdem die App-Bereitstellung, da jetzt Win32-Anwendungen über die EMM-Plattform genauso bereitgestellt

werden können wie moderne Apps.

Diese Änderungen erleichtern den PC-Verwaltungsteams die Absicherung von PCs und Mobilgeräten mit der gleichen Plattform für die am häufigsten verwendeten Einsatzszenarien. Zwar sind traditionelle Tools in manchen Situationen weiter erforderlich, die PC-Verwaltungsteams sind jedoch gezwungen, ihre aktuellen Tools durch eine EMM-Plattform zu ergänzen, zumal immer mehr Benutzer im Unternehmen Upgrades auf Windows 10 durchführen. In der Tat geht Gartner Research davon aus, dass bis 2018 40 % der Unternehmen EMM-Tools mindestens zur Verwaltung eines Teils ihrer Windows-PCs einsetzen werden — diese Zahl liegt deutlich höher als die derzeit verwalteten 5 %.¹

In der Tat geht Gartner Research davon aus, dass bis 2018 40 % der Unternehmen EMM-Tools mindestens zur Verwaltung eines Teils ihrer Windows-PCs einsetzen werden — diese Zahl liegt deutlich höher als die derzeit verwalteten 5 %

Überlegen Sie, was das bedeutet – in nicht einmal zwei Jahren wird knapp die Hälfte aller Unternehmen mindestens einen Teil ihrer PC-Verwaltung in eine EMM-Plattform verlagern. Es gibt wahrscheinlich verschiedene Gründe für diesen Trend. Neben der Unterstützung von Windows 10 für EMM-Plattformen suchen internationale Unternehmen nach neuen Möglichkeiten, ihre dynamischen Sicherheits- und Agilitätsanforderungen zu verwalten – und als eines der besten Gesamtkonzepte hat sich EMM erwiesen.

¹ Saran, Cliff. „Wie wird die Desktop-Verwaltung 2020 aussehen?“ Computer Weekly.
<http://www.computerweekly.com/feature/What-will-office-desktop-computing-look-like-in-2020>.



Einfache und sichere PC-Verwaltung mit Windows 10 + EMM

Der Trend in Richtung EMM als PC-Verwaltungsplattform bringt für die Administratoren zahlreiche Vorteile. Funktionalität muss nicht für Flexibilität geopfert werden, weil ein EMM-Anbieter wie MobileIron mehrere Aufgaben zur Verwaltung von PCs unter Windows 10 genauso einfach wie mit den bisherigen Tools erledigen kann. Begründet ist dies darin, dass Windows 10 alle MDM-APIs und App-Entwicklungs-Tools in einer integrierten Plattform kombiniert. Aufgrund dieses neuen Konzepts können die für Windows 10 konfigurierten MDM-Richtlinien über die EMM-Plattform von MobileIron konsistent für alle Geräte mit Windows 10 verwendet werden.

Funktionalität muss nicht für Flexibilität geopfert werden, weil ein EMM-Anbieter wie MobileIron mehrere Aufgaben zur Verwaltung von PCs unter Windows 10 genauso einfach wie mit den bisherigen Tools erledigen kann.

Wenn die IT beispielsweise ein komplexes Passwort fordert, wird diese Richtlinie sowohl für Tablets als auch für PCs und Smartphones durchgesetzt, ohne dass separate Richtlinienkonfigurationen für jede Geräteart erstellt werden müssen. Microsoft hatte MDM-Protokolle schon für Windows Phone 8.1 und Windows 8.1 für Laptops und Tablets freigegeben, diese waren aber nicht identisch und benötigten daher separate APIs und Kontrollschnittstellen. Windows 10 vereinfacht die Verwaltung aller Geräte deutlich. Die folgende Abbildung zeigt, wie insbesondere PC-Administratoren in fünf Hauptverwaltungsbereichen davon profitieren.

Die fünf wichtigsten PC-Verwaltungsfunktionen der EMM-Plattform

Wie bereits erwähnt, kann das vorhandene Modell des Domain-Beitritts nicht alle Anforderungen an die Verwaltung in modernen, dynamischen Unternehmen erfüllen. Windows 10 und MobileIron bieten zusammen ein umfassenderes Konzept für die PC- und Mobilgeräteverwaltung, weil damit neue Geräte, Apps und Upgrades des Betriebssystems bequem unterstützt werden können – und diese Flexibilität ist in jeder IT-Abteilung absolut unverzichtbar.

Windows 10 und MobileIron bieten zusammen ein umfassenderes Konzept für die PC- und Mobilgeräteverwaltung, weil damit neue Geräte, Apps und Upgrades des Betriebssystems bequem unterstützt werden können – und diese Flexibilität ist in jeder IT-Abteilung absolut unverzichtbar

Nach Angaben der Gartner Group wird die Fähigkeit zur Verwaltung und Unterstützung von Geräten für PC-Administratoren zu einer kritischen Aufgabe. In einem aktuellen Bericht wird davon ausgegangen, dass bis 2018 40 % der Anrufe beim IT Service Desk wegen Smartphones und Tablet-Geräten erfolgen werden – ein enormer Sprung im Vergleich zu den maximal 20 % von heute. Dies wird den Desktop-IT-Support stark belasten, wenn er nicht andere Arbeitskonzepte findet.“²

Hier kann MobileIron eine fundamentale Rolle bei kritischen Prozessen zur PC-Verwaltung spielen. Der folgende Abschnitt erläutert typische Anwendungsfälle für die PC-Verwaltung und wie diese über eine EMM-Plattform mindestens genauso gut gelöst werden können wie mit den derzeitigen Tools und Prozessen.



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

Anwendungsfall Nr. 1: PC-Setup und Registrierung

Traditionelle PC-Verwaltung

Bei dem traditionellen Modell zur Konfiguration von PCs muss der Administrator direkten Zugang zu dem Gerät haben, um es zu registrieren; dazu ist die kosten- und arbeitsintensive Installation eines PC-Images erforderlich. Für diesen Prozess muss die IT eine Reihe von Hardware-Treibern sowie einen Satz Standardgeräte pflegen. Wenn das Unternehmen einen Dienst zur Bereitstellung eines PC-Images verwendet, entstehen in der Regel Kosten von 20 – 25 Dollar pro System. Die Kosten für PC-Images können sich damit schnell addieren.³ Die traditionellen Verfahren sind nicht nur teuer, sondern auch zeitaufwendig. Wenn ein Mitarbeiter mit Fernzugriff beispielsweise seinen Laptop verliert oder beschädigt, kann der Ersatz des Geräts mehrere Tage dauern. Mit modernen Methoden kann die IT ein neues Gerät „over the air“ konfigurieren und absichern, so dass der Mitarbeiter noch am gleichen Tag wieder arbeiten kann.

Windows 10 + MobileIron

Mit Windows 10 und MobileIron kann die IT viele logistische Engpässe umgehen, die bei der Bereitstellung eines PCs mit PC Image entstehen. Mit MobileIron können die Administratoren eine größere Gerätepalette (auch BYOD-Initiativen und Geräte von Mitarbeitern mit Fernzugriff) unterstützen. Es können in der EMM-Plattform gleichzeitig mehrere Geräte konfiguriert und registriert werden, ohne dass irgendjemand das Gerät in die Hand nehmen muss. Das bedeutet, die Geräte können zeit- und ortsunabhängig registriert werden, ohne dass eine Verbindung zu einem Unternehmensnetzwerk notwendig ist.

Mit Windows 10 und MobileIron lassen sich Geräte orts- und zeitunabhängig registrieren, ohne dass eine Verbindung zum Unternehmensnetzwerk notwendig ist

Anwendungsfall 2: Bereitstellung im Unternehmens-App-Store

Traditionelle PC-Verwaltung

Die Verwaltung von Unternehmens-Apps ist relativ zeitaufwendig, weil der Administrator für jede Anwendung ein Distributionspaket erstellen muss⁴ — dies kann zwei bis vier Tage pro Anwendung dauern. Für Win32-Anwendungen können außerdem kundenspezifische Installations-Skripts erforderlich sein, die die vorhandenen Apps unterstützen. Dabei kann es zu Konflikten kommen, weil manche PC-Anwendungen nur mit anderen Anwendungsversionen zusammenarbeiten. Außerdem neigen alte Win32-Anwendungen im Gegensatz zu modernen Anwendungen dazu, nach der Deinstallation unerwünschte Artefakte zu hinterlassen. Dies kann beispielsweise durch eine aufgeblähte Registry zu einer Verschlechterung der Leistung führen. Das Gerät ist außerdem weniger sicher, wenn die Zertifikate nicht ordnungsgemäß entfernt werden.

Windows 10 + MobileIron

Die IT kann Anwendungen durch einen Unternehmens-App-Store mit MobileIron und Windows 10 verwalten und verteilen. Die Benutzer können dann auswählen, welche Apps sie auf ihrem PC oder Mobilgerät installieren wollen. Die Verwaltung von Apps über eine EMM-Plattform und einen modernen Unternehmens-App-Store hat vor allem zwei Vorteile:

- 1. Schnellere Bereitstellung der App.** Mit MobileIron können Entwickler Apps und Updates für die Endbenutzer deutlich schneller verteilen. Die Benutzer müssen nicht mehr in Google nach einer aktualisierten Anwendung suchen oder die IT bitten, diese per Push auf das Gerät zu übertragen. Stattdessen erstellen die Administratoren Kataloge der Unternehmens-Apps. Die Apps werden entweder automatisch installiert oder den Benutzern wird die Installation empfohlen. Ein Unternehmens-App-

³ Cosgrove, Terrence und Rich Doheny. „Anwendungsfälle zur richtigen Verwaltung von PCs als Mobilgeräte.“ Gartner Research, 23. März 2016.

⁴ Cosgrove, Doheny. 23. März 2016.

Store, der über eine EMM-Plattform verwaltet wird, vereinfacht außerdem deutlich die Verwaltung der App-Lizenzen.

- Höhere App-Sicherheit:** Viren und Malware sind aufgrund der unsicheren Windows-Plattform seit langer Zeit ein Problem. Durch die Verwaltung der Apps über einen sicheren App Store von MobileIron können Entwickler Sicherheitsrisiken minimieren.

Durch die Verwaltung der Apps über einen sicheren App Store von MobileIron können Entwickler Sicherheitsrisiken minimieren.



Anwendungsfall Nr. 3: Geräteverwaltung

Traditionelle PC-Verwaltung

Traditionelle Tools wurden nicht von Grund auf für die Verwaltung moderner Betriebssysteme wie Android, iOS und Windows 10 konzipiert. Dies führt zu einer inkonsistenten Verwaltungsumgebung und die Administratoren müssen zur Verwaltung von PC Clients mehrere Tools für die verschiedenen Mobilsysteme einsetzen. Bei der traditionellen PC-Verwaltung müssen zudem die Geräte einer Domain angehören, d. h. sie müssen mit dem Firmennetzwerk verbunden sein, wenn sie die erforderlichen Updates erhalten sollen. Dies erhöht nicht nur die Verwaltungskosten, sondern kann auch die Produktivität mobiler Mitarbeiter beeinträchtigen, die nur hin und wieder mit ihren Geräten eine Verbindung mit dem Firmennetzwerk aufbauen und möglicherweise nicht sofort die aktuellsten Updates erhalten.

Windows 10 + MobileIron

Im Gegensatz zu den Verwaltungs-Tools für Desktop-PCs unterstützt MobileIron die Verwaltung von Geräten mit unterschiedlichen Betriebssystemen nach dem Konzept einer „zentralen Anzeige“. Das bedeutet, dass kritische Updates auf Geräte über beliebige Netzwerke verteilt werden können, damit diese verwalteten Geräte sicher sind. MobileIron automatisiert außerdem wichtige Verwaltungsaufgaben, beispielsweise die Berichterstellung über den Gerätebestand und die Compliance, so dass sich die IT auf kritischere Probleme konzentrieren kann.

MobileIron automatisiert außerdem wichtige Verwaltungsaufgaben, beispielsweise die Berichterstellung über den Gerätebestand und die Compliance, so dass sich die IT auf kritischere Probleme konzentrieren kann

Anwendungsfall Nr. 4: Sicherheit mit Zertifikaten

Traditionelle PC-Verwaltung

In vielen Fällen kann die Implementierung der Sicherheitszertifikate auf PCs Wochen oder Monate dauern. Üblicherweise richtet der IT-Administrator dabei eine benutzerspezifische Webseite oder ein Intranetportal ein, in dem die Identität des Benutzers überprüft werden kann. Die Verifizierung erfordert in der Regel einige zusätzliche Authentifizierungsschritte des Endbenutzers. Nach Abschluss der Authentifizierung muss der Benutzer auf einen Link klicken, um die erforderlichen Zertifikate zu erzeugen und auf dem PC zu speichern. Es ist auch möglich, dass der Benutzer aufgefordert wird, ein Script in der Befehlszeile zu starten, um die Zertifikate zu erstellen – ein sehr unpraktisches Szenario für Personen mit begrenzten technischen Fähigkeiten.

Windows 10 + MobileIron

Zertifikate können problemlos auf zwei Wegen innerhalb des gleichen Tages bereitgestellt werden:

Bereitstellung des SCEP-Zertifikats: Die IT stellt mit dem Simple Certificate Enrollment Protocol ([SCEP]) erstmals das Gerät bereit und registriert es, statt die üblichen Anmeldeinformationen wie Benutzername und Passwort zu verwenden. Der MDM-Server sendet die SCEP-Anweisungen und eine Anfrage an das Gerät, das diese Anfrage dann zur Anforderung eines Zertifikats vom SCEP-Server verwendet.

Direkte Zertifikatinstallation: Die IT kann auch direkt über MDM ein Zertifikat installieren, wenn sie das Zertifikat und einen privaten Schlüssel über den MDM-Kanal sendet. Bei diesem Prozess wird kein SCEP-Server benötigt, da eine eigene Zertifizierungsstelle verwendet werden kann. Damit wird auch der Konfigurationsprozess für Dienste wie WLAN und E-Mail vereinfacht, weil statt der Benutzeranmeldeinformationen ein Zertifikat zugeordnet werden kann.

Im Gegensatz zu den traditionellen Verfahren für Desktop-PCs lassen sich mit Windows 10 und MobileIron schnell und problemlos Sicherheitszertifikate bereitstellen, ohne dass der Benutzer eingreifen muss

Anwendungsfall Nr. 5: Eintragen von Apps in die Whitelist/Blacklist

Traditionelle PC-Tools

Um Blacklists und Whitelists von Anwendungen für die heutigen Lösungen zur PC-Verwaltung zu pflegen, muss heute der Administrator alle Anwendungen mit ihren Dateinamen definieren. Diese Konfigurationen müssen dann per Push auf das Gerät übertragen werden. Dies ist eine manuelle, zeitaufwendige Aufgabe.

Windows 10 + MobileIron

In Windows 10 können über AppLocker sowohl der Windows Store als auch Win32-Apps Listen ausführen, welche die Ausführung von Anwendungen zulassen oder verweigern. AppLocker ist eine Windows-Funktion, mit der die IT-Administratoren definieren können, welche Anwendungen erlaubt oder verboten sind. Dazu werden eindeutige Dateientitäten, die Gruppenrichtlinie bzw. die Benutzerrolle ausgewertet.⁵

Mit AppLocker können IT-Administratoren die Listen bequem verwalten, mit denen Anwendungen erlaubt oder verboten werden. Komplexe Konfigurationen sind nicht erforderlich

⁵ Cosgrove, Doheny. 23. März 2016.

Hauptüberlegungen für die Einführung einer EMM-Plattform

Obgleich die IT-Verwaltung in Unternehmen sich schnell in Richtung eines EMM-zentrierten Modells bewegt, existieren noch Lücken, die die IT kennen sollte, wenn sie sich für diesen Weg entscheidet. Einige dieser Lücken können die EMM-Einführung beeinträchtigen:

- **GPOs und EMM-Richtlinien.** Es ist zwar technisch möglich, ein Gerät sowohl mit GPOs als auch EMM-Richtlinien zu verwalten, es kann dabei jedoch zu Verwaltungskonflikten kommen. GPOs und EMM definieren grundverschiedene Rahmenbedingungen für Richtlinien, die bekannt sein müssen, bevor sie auf dem gleichen Windows-Gerät verwendet werden. Im Allgemeinen ist eine EMM-Plattform besser für Remote-Benutzer und private Geräte der Mitarbeiter geeignet. GPOs dagegen bieten eine bessere Kontrolle, da Microsoft über Tausende GPOs verfügt, während eine EMM-Plattform nur einige hundert Richtlinien besitzt. Unternehmen müssen die jeweiligen Rahmenbedingungen analysieren und klären, ob sie bestimmte GPO-Funktionen benötigen, die eine EMM-Plattform derzeit nicht anbieten kann.⁶
- **Fähigkeit zur Verwaltung und Bearbeitung der Registry.** PC-Administratoren sind es gewohnt mit Tools Detailsinstellungen in der Registry zu bearbeiten; dies ist jedoch ein fehleranfälliger Prozess, der dazu führen kann, dass die Registry nicht mehr verwendbar ist. Wenn Administratoren die Registry sicher bearbeiten und die Gefahr menschlicher Fehler minimieren wollen, brauchen sie eine EMM-Erweiterung. Administratoren sollten sich auch auf eine Übergangsphase vorbereiten, in der sie von bewährten Praktiken abweichen und sich stärker mit der modernen Sandbox-Architekturumgebung vertraut machen, die eine höhere Stabilität, mehr Schutz und mehr Sicherheit bietet.

- **Anforderungen an den Unternehmens-App-Store.** Der Unternehmens-App-Store hat zwar enorme Vorteile sowohl für Administratoren als auch für Endbenutzer, Microsoft stellt jedoch bestimmte Anforderungen an die Anwendungen, die über den App-Store verteilt werden. Unternehmen, die derzeit diese Anforderungen nicht erfüllen, haben es schwer, ihre Anwendungen zu verteilen und können daher diese Funktion nicht umfassend nutzen. Für solche Unternehmen ist die jüngste Ankündigung des „Centennial“-Desktop-App-Konverters von Microsoft eine gute Nachricht. Mit diesem Konverter können Entwickler ihre Win32- und .NET-Apps in das AppX-App-Format umwandeln und im Windows- oder Enterprise-App-Store anbieten. Das heißt, spezifische eigene Apps können im App Store als UWP-Apps der Universal Windows Plattform angeboten werden. Diese können dann auf jedem Mobilgerät, Computer, Surface-ähnlichen Gerät, Geräten ohne Bildschirm oder passiven Anzeigegeräten verwendet werden.⁷
- **Transparenz und Funktionalität des Dateisystems.** Die EMM-Plattform kann nicht erkennen, welche Dateien sich im System befinden und muss daher für bestimmte Aktionen Zugriffsrechte auf bestimmte Teile der Festplatte erhalten. Der Grund dafür sind Anwendungen von Drittanbietern, die beispielsweise mit Dateien den Lizenzstatus verwalten. In manchen Fällen steuert oder modifiziert die Existenz einer Datei das Anwendungsverhalten, beispielsweise die Anzeige, daher ist die Möglichkeit zur Anzeige und Verwaltung von Dateien eine wichtige IT-Funktion. In der Branche werden derzeit Anstrengungen unternommen, um diese Sicherheitslücke zu minimieren, so dass EMM-Lösungen Aufgaben auf Dateiebene verwalten können.

⁶ Cosgrove, Doheny. 23. März 2016.

⁷ Jan Kamps, Haje. „Microsoft stellt Desktop-App-Konverter vor, mit dem Win32-Apps im Windows Store angeboten werden können.“ TechCrunch, 30. März 2016. <http://techcrunch.com/2016/03/30/desktop-app-converter>



Nächste Schritte: Empfehlungen

Wenn Sie bereits eine EMM-Plattform in Betracht ziehen, hier einige Möglichkeiten, wie Sie dieses Verwaltungsmodell in Ihrem Unternehmen einführen:

1.

Beginnen Sie mit einem Pilot-BYOD-Programm mit einer EMM-Plattform.

Prüfen Sie, wie Ihr Unternehmen zurzeit die Geräte der Mitarbeiter absichert. Können Sie Geräte mit mehreren Betriebssystemen, Content und Apps voll unterstützen? Sie sollten ein Pilotprogramm für ausgewählte BYOD-Benutzer in Ihrem Unternehmen starten und dafür die Möglichkeiten einer EMM-Plattform sondieren.

2.

Verwalten Sie neue Geräte mit Windows 10 mit einer EMM-Plattform.

Wenn Sie ein Upgrade auf Windows 10 durchführen oder neue Geräte mit Windows 10 installieren wollen, sollten Sie ein kleines Pilotprojekt zur Konfiguration, Absicherung und Verwaltung dieser neuen Geräte mit einer EMM-Plattform statt mit den vorhandenen Tools zur Verwaltung der Desktop-Computer planen.

3.

Planen Sie eine sichere Bereitstellung von Office 365.

Wenn Sie die Bereitstellung von Office 365 in Betracht ziehen, sollten Sie berücksichtigen, dass das Domain-Konzept von Desktop-Computern für das Cloud-Modell von Office 365 nicht geeignet ist. Die schnellste und sicherste Möglichkeit zur Unterstützung von Office 365 auf jedem Gerät in Ihrem Unternehmen ist eine EMM-Plattform.

Fünf IT-Mythen über EMM

Mythos Nr. 1:

„Wir können mit EMM nicht all unsere eigenen Anwendungen verwalten.“

Fakt:

Microsoft informierte kürzlich, dass der neue Centennial-Desktop-App-Konverter in der Lage sein werde, vorhandene Win32-Apps in das Universal Windows Plattform-Format (UWP) zu konvertieren. Nach Angaben von Microsoft wird es mit Centennial ganz einfach sein, vorhandene Win32- und .NET-Apps im Windows Store anzubieten, wo sie durch eine EMM-Plattform sicher verwaltet werden können.

Mythos Nr. 2:

„BYOD-Geräte, die nicht zu einer Domain gehören, können nicht verwaltet werden, weil SCCM sie nicht erreichen kann. Wir müssen VPN verwenden, um die Geräte unserer verteilten Belegschaft zu verwalten.“

Fakt:

Konventionelle Geräte-VPNs stören den Arbeitsablauf, da die Benutzer eine VPN-Verbindung immer manuell herstellen müssen, wenn sie auf Unternehmens-Content zugreifen wollen. Außerdem kann bei Geräte-VPNs jede App auf dem Gerät auf sensitive Daten zugreifen. MobileIron bietet mit Per-App-VPN-Verbindungen ein intelligenteres, granulares Konzept, so dass nur berechtigte Unternehmens-Apps auf Unternehmensressourcen hinter der Firewall zugreifen können. Nicht genehmigte oder private Apps können gesperrt werden. Dadurch wird ein Datenverlust verhindert, die Privatsphäre des Benutzers geschützt und die sichere Verwaltung der verteilten Belegschaft vereinfacht.

Mythos Nr. 3:

„Wir haben viel Zeit und Geld in die Programmierung von Scripts investiert und können es uns nicht leisten, auf diese Investitionen zu verzichten.“

Fakt:

Eine EMM-Plattform erfordert nicht so umfangreiche Investitionen wie die traditionellen Tools zur PC-Verwaltung. Mit MobileIron müssen Sie auf Ihre derzeit verwendeten Tools nicht verzichten und komplett neu beginnen. Sie können schrittweise neue oder auf Windows 10 umgestellte Geräte in Ihrer EMM-Plattform bereitstellen und die Übergangsphase zeitlich strecken.

Mythos Nr. 4:

„SCCM ist sicherer als EMM.“

Fakt:

In vielen Fällen ist eine EMM-Plattform heute sicherer als SCCM. Beispielsweise prüft MobileIron weit regelmäßiger als SCCM das Risikoprofil der Geräte und leitet entsprechende Gegenmaßnahmen ein.

Mythos Nr. 5:

„Cloud-Sicherheit ist nicht so robust wie die im Firmennetzwerk vorhandene Infrastruktur, beispielsweise SCCM oder LANDESK.“

Fakt:

MobileIron ist in Kombination mit Azure Active Directory eine sehr sichere Lösung, da sie den bedingten Zugriff auf Backend-Ressourcen unterstützt. Falls ein Gerät die Compliance-Anforderungen nicht mehr erfüllt, wird dem Benutzer der Zugriff auf Unternehmensressourcen verweigert, bis das Sicherheitsproblem beseitigt ist.

Fazit

Mit der Freigabe von Windows 10 bieten sich interessante Möglichkeiten für eine neue Ära der PC-Verwaltung. Gemeinsam mit einem EMM-Anbieter wie MobileIron können die PC-Administratoren auf vereinheitlichte MDM-APIs zugreifen und damit alle Geräte unter Windows 10 verwalten sowie unabhängig von der Größe des Geräts ein konsistentes und sicheres Benutzererlebnis bereitstellen. Die Administratoren können mit MobileIron sowohl moderne, mobile Apps als auch Win-32-Apps in einem sicheren Unternehmens-App-Store verwalten. Der Zugriff auf Unternehmensressourcen wie Office 365 kann durch Synchronisation der Geräterisikoprofile mit Azure Active Directory als Zugriffskontrolle präzise verwaltet werden. Genauso wichtig ist, dass die Administratoren den späteren Übergang auf die EMM-Plattform skalieren können. Damit werden wichtige Investitionen geschützt und die IT kann sicherstellen, dass die technischen und Verwaltungsprozesse genau den Unternehmensanforderungen entsprechen.

Für Unternehmen, die sich bisher vor allem auf traditionelle Desktop-Tools verließen, wird es jetzt Zeit, gründlich die Notwendigkeit einer EMM-Plattform zur Absicherung und Verwaltung eines größeren Anteils der Unternehmensgeräte und Apps für die verteilte Belegschaft zu prüfen.

Weitere Informationen

Wenn Sie genauer wissen wollen, wie MobileIron Ihnen bei der Verwaltung Ihrer Windows-Implementierung helfen kann, wenden Sie sich bitte an globalsales@mobileiron.com.