Anleitung für Führungskräfte

Die fünf wichtigsten Fakten zum Enterprise Mobility Management

v1

MobileIron

Inhalt

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

Zusammenfassung für die Geschäftsleitung

Ob sie es wollen oder nicht, der Trend zur Mobiltechnologie zwingt Unternehmen, mobile Mitarbeiter mit Produktivitätstools auf jedem Gerät unabhängig von dem jeweiligen Betriebssystem auszustatten. Da Benutzer von Mobilgeräten zunehmend ihre eigenen Geräte sowohl für private Zwecke als auch für ihre berufliche Tätigkeit nutzen wollen, betreffen Technologieentscheidungen der Endbenutzer auch schnell die IT-Abteilung. Unternehmen können diese Realität nicht länger ignorieren, insbesondere nicht angesichts der enormen globalen Nachfrage nach Mobilgeräten. Nach Angaben des IDC erreichte "der weltweite Smartphone-Markt im 2. Quartal 2014 mit mehr als 300 Millionen Geräten erstmals in seiner Geschichte einen neuen Rekord." IDC stellt außerdem fest, dass die Auslieferung von BlackBerry-Geräten gegenüber dem Vorjahr um 78 Prozent sank, dies ist das vierte Quartal eines schrittweisen Niedergangs. Eines ist offensichtlich: Die Tage der Firmengeräte mit beschränktem Funktionsumfang sind vorbei. Wie können sich Unternehmen auf die Zukunft vorbereiten?

Verweigern Sie sich nicht der Ära der Unternehmensmobilität

Sie können die Umstellung auf Mobiltechnologie nicht verweigern oder verhindern. Diese Anleitung soll Ihnen zeigen, wie Unternehmensleiter durch Mobiltechnologie für die Benutzer das Unternehmen risikolos voranzubringen. Antivirenprogramme für Desktop-PCs und Firmengeräte mit beschränktem Funktionsumfang verlieren im modernen Unternehmen an Bedeutung. Die Unternehmen brauchen neue Strategien und Technologien, um sich zu Mobile-First-Unternehmen zu entwickeln, ohne Risiken einzugehen.

Enterprise Mobility Management (EMM) ist eine umfassende Lösung, die Unternehmen hilft, mehrere Betriebssysteme zu unterstützen, sodass die Mitarbeiter ihre bevorzugten Geräte für Unternehmens-Apps und Unternehmensdaten verwenden können und zugleich die kritischen und Compliance-Anforderungen erfüllt werden. Aus den drei Komponenten der EMM-Plattform – mobiles Gerätemanagement (MDM), mobiles Anwendungsmanagement (MAM) und mobiles Content-Management (MCM) – entsteht eine sichere, skalierbare und für Unternehmen geeignete Architektur, bei der die Benutzererfahrung Vorrang hat.

Warum ist Benutzererfahrung so wichtig?

Der Erfolg oder Misserfolg jeder Mobilitätsinitiative hängt wesentlich von der Akzeptanz der Benutzer ab. Jede EMM-Plattform muss daher dem Unternehmen erlauben, kritische Unternehmensprozesse durch Mobilanwendungen zu unterstützen, die leicht zugänglich sind und auf jedem Gerät verwendet werden können. Bei EMM geht es jedoch nicht nur darum, die Benutzer zufriedenzustellen. EMM sollte auch die Arbeit der IT-Abteilung erleichtern, indem Zugangskontrolle und Authentifizierung vereinfacht werden und die Benutzer ihre Geräte selbst verwalten und Probleme selbst beheben können, ohne das Helpdesk in Anspruch zu nehmen.

Umstellung auf ein Mobile-First-Unternehmen beschleunigen

Diese Anleitung beschreibt nicht nur, wie Enterprise Mobility Management funktioniert, sondern zeigt auch an einem typischen Implementierungsbeispiel, wie ein Unternehmen die Einführung plant und alle Teile einer EMM-Lösung verwaltet. Diese Anleitung enthält einen detaillierten Bereitstellungsprozess unter Verwertung der gesammelten Erfahrungen und Empfehlungen zur Suche nach dem richtigen EMM-Anbieter und Schritt für Schritt umsetzbare Erkenntnisse aus der Praxis, die jedem Unternehmen bei der Umwandlung zum Mobile-First-Unternehmen helfen können.

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

Einführung

Unternehmensmobilität: Was ist der Grund für diese Entwicklung?

Die PC-Ära ist vorbei.

Mobilgeräte werden weltweit immer häufiger eingesetzt, und es ist nicht zu erkennen, dass dieser Trend nachlässt. 2015 dürften Tablets erstmals häufiger verkauft werden als PCs, dieser Zeitpunkt markiert das Ende der PC-Ära.[1]

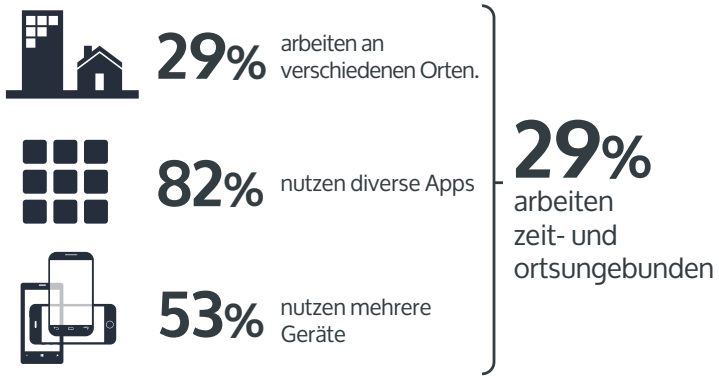
Diese und weitere Verbraucher-Technologietrends beeinflussen eindeutig die Entwicklung der Mobilität in Unternehmen. Da die Verbraucher (das heißt, die Mitarbeiter) mobiler sind, möchten sie auch am Arbeitsplatz genauso flexibel sein und schnell reagieren können. Sie möchten ihr eigenes Gerät– kein firmeneigenes Gerät – sowohl für ihren privaten Gebrauch als auch für berufliche Zwecke verwenden. Infolgedessen bestimmen jetzt die Verbraucher, welche Mobilgeräte Unternehmen verwenden, und die Nachfrage nach den bisher eingesetzten, von Unternehmen im Funkltionsumfang beschränkten Mobilgeräten sinkt schnell.

Mobiler Content explodiert geradezu.

Die Entwicklung und Verteilung von mobilem Content , von digitalen Dokumenten bis zu viralen Videos, ist ohne Beispiel. Dieser Trend wird sich fortsetzen, da es immer einfacher und kostengünstiger wird, Unternehmens-Apps und Content zu erstellen und zu verwalten. Die Unternehmensproduktivität lässt sich damit deutlich steigern. Zwischen 2005 und 2020 dürfte der Umfang digitaler Informationen um den Faktor 300 wachsen.

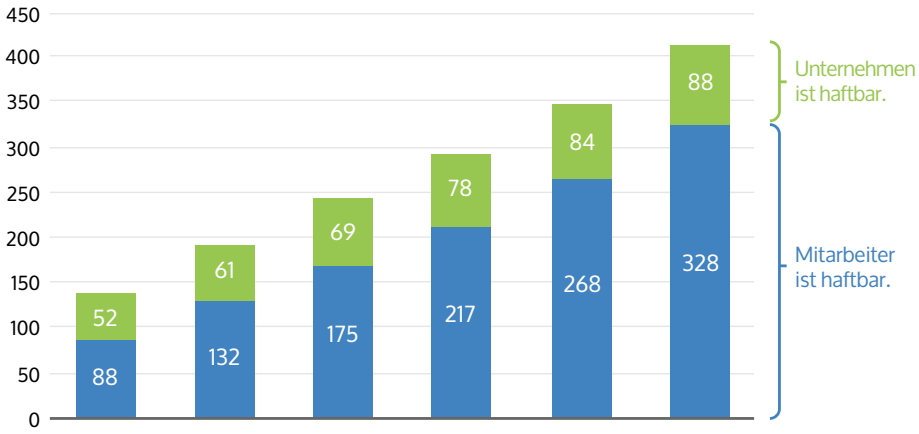
1 IDC-Pressemitteilung "Weltweite Auslieferung von Smartphones im zweiten Quartal bei über 300 Millionen Geräten; Android##

Mehr Benutzer, die zeit- und ortsungebunden arbeiten.



Forrester Februar 2013
"Trends 2013 für mobile Mitarbeiter"

BYOD wird umfassend genutzt



IDC Dezember 2013
"Prognose zum weltweiten Einsatz von Smartphones 2013-2017 in Unternehmen"

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

Es wird weiter mehrere Betriebssysteme geben.

Da der Markt für Mobiltechnologie sich weiter ändert, werden Umgebungen mit mehreren Betriebssystemen zur Norm. Die Endbenutzer möchten selbst entscheiden, welches Gerät sie für ihre Arbeitsaufgaben verwenden. Das heißt, die Unternehmens-IT muss jetzt in der Lage sein, mehrere mobile Betriebssysteme abzusichern und zu verwalten. Vor dem Wechsel zur Mobiltechnologie war die Situation für die IT-Abteilung einfacher: verwaltet werden mussten nur Endbenutzer mit Windows und Blackberry. Das hat sich enorm geändert. Es gibt alle paar Jahre eine neue Version von Windows, und die Intervalle verkürzen sich. Es gibt diverse Varianten von Android, iOS und Windows Phone, die sich im Unternehmen immer schneller verbreiten. Das heißt, die IT-Abteilung muss agiler arbeiten als je zuvor und Änderungen der sich laufend weiter entwickelnden Mobilgeräte schnell berücksichtigen. Es ist jedoch schwierig, zu prognostizieren, wie dieser Technologie-Mix sich entwickelt wird. Das erschwert der IT die Entscheidung, welche Geräte sie unterstützen soll. Die Antwort ist einfach: Schauen Sie sich den Verbrauchermarkt an. Wenn Sie wissen, welche Geräte Ihre Mitarbeiter kaufen, können Sie eine Mobilstrategie zur Unterstützung dieser Geräte konzipieren.

2 McCafferty, Dennis. "12 Amazing Facts about Mobility." CIO, 1. Sept. 2014.
http://www.cioinsight.com/it-strategy/mobile-wireless/slideshows/12-amazing-facts-about mobility.html/ 3 McCafferty, 1. Sept. 2014.

Mobilitätsverwaltung: die Herausforderungen

Unterstützung der Geräte der Wahl

Die Mobiltechnologie ändert dramatisch die Rolle der IT im Unternehmen. Statt vorzuschreiben, welche Technologien die Mitarbeiter verwenden sollen, muss die IT jetzt die verschiedenen Technologien implementieren, die die Mitarbeiter in das Unternehmen bringen. IT-Organisationen, die mobile Benutzer oder deren bevorzugte Geräte nicht unterstützen, werden schnell feststellen, dass sie keine Rolle mehr spielen, weil Mitarbeiter mit Mobilgeräten unkooperative IT-Abteilungen einfach ignorieren können.

Verwaltung mobiler Apps und mobilen Contents

Das Wachstum der mobilen Apps steht noch ganz am Anfang. Bis Ende 2017 werden 4,4 Milliarden Menschen mobile Apps verwenden; dies ist ein Anstieg von fast 30 Prozent pro Jahr.[2] Heute bieten Google Play und der App Store von Apple zusammen mehr als 1,6 Millionen Apps an, der Markt dürfte sich bis 2017 verdreifachen.[3]

Was bedeutet das für das Unternehmen? Die Nachfrage nach mobilen Apps explodiert nahezu, und die Endbenutzer erwarten mehr als nur einen Zugriff auf Unternehmens-E-Mails über ihre Smartphones. Die Mitarbeiter möchten auf alle kritischen Unternehmensprozesse und den Content zugreifen, den sie täglich benutzen. Da weitere Plattformen, beispielsweise iOS 8, die Entwicklung von Unternehmens-Apps unterstützen, dürfte die Nachfrage noch zunehmen. Um diese Nachfrage abzudecken, können Unternehmen nicht mehr wie bisher erst eine PC-Anwendung entwickeln und dann für Mobilgeräte bereitstellen. Die gesamte App- und Contententwicklung muss in Zukunft zuerst für Mobilgeräte erfolgen.

3 McCafferty, Dennis. "12 Amazing Facts about Mobility." CIO, 1. Sept. 2014.
http://www.cioinsight.com/it-strategy/mobile-wireless/slideshows/12-amazing-facts-about mobility.html/

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

Sicherheit und Compliance

Eine der größten Herausforderungen für die IT ist die Absicherung von Daten und Apps (auch Apps von Drittanbietern) auf allen Mobilgeräten ohne Beeinträchtigung der nativen Benutzererfahrung. Vor der Mobilgeräte-Ära waren die größten Sicherheitsrisiken Malware und Viren, welche Sicherheitslücken der offenen Dateisysteme und des ungeschützten Kerns nutzten. Heute besitzen mobile Betriebssysteme ein Sandbox-Dateisystem und einen geschützten Kern, sodass traditionelle Sicherheitsbedrohungen keine große Gefahr mehr sind. Mobilgeräte sind jedoch aus drei anderen Richtungen bedroht: durch Benutzer, durch Geräte und durch das Netzwerk.

Die Bedrohungen durch Mobilgeräte unterscheiden sich von den Bedrohungen auf PCs.

Mobile Sandbox-Betriebssysteme sind sicher. Bedrohungen, beispielsweise Malware, werden durch das Konzept des Betriebssystems reduziert. Datenverluste auf Mobilgeräten können vermieden werden, wenn die verschiedenen Bedrohungskategorien berücksichtigt werden.

Datenverlust

*Datenverlust in Cloud-Diensten und Anwendungen zur Steigerung der Produktivität durch Funktionen zum **Öffnen, Kopieren und Einfügen** sowie Weiterleiten*

Always-On-Vernetzung

*Mobilgeräte sind immer vernetzt und greifen oft über unsichere Netzwerke auf sensible Daten zu. Damit erhöht sich das Risiko von Datenverlust durch **WLAN-Sniffing, unsauber konfigurierte Zugangspunkte und Man-in-the-Middle-Angriffe (MitM).***

Manipulation von Geräten

*Schwachstellen im Betriebssystem werden genutzt, um **Jailbreaks oder Rootkits** auf Geräten zu installieren, Sicherheitsfunktionen zu umgehen und Schadsoftware von nicht genehmigten App-Stores zu installieren.*

Baugröße

*Durch die kleinen Abmessungen werden Mobilgeräte **leicht gestohlen und gehen leicht verloren.***

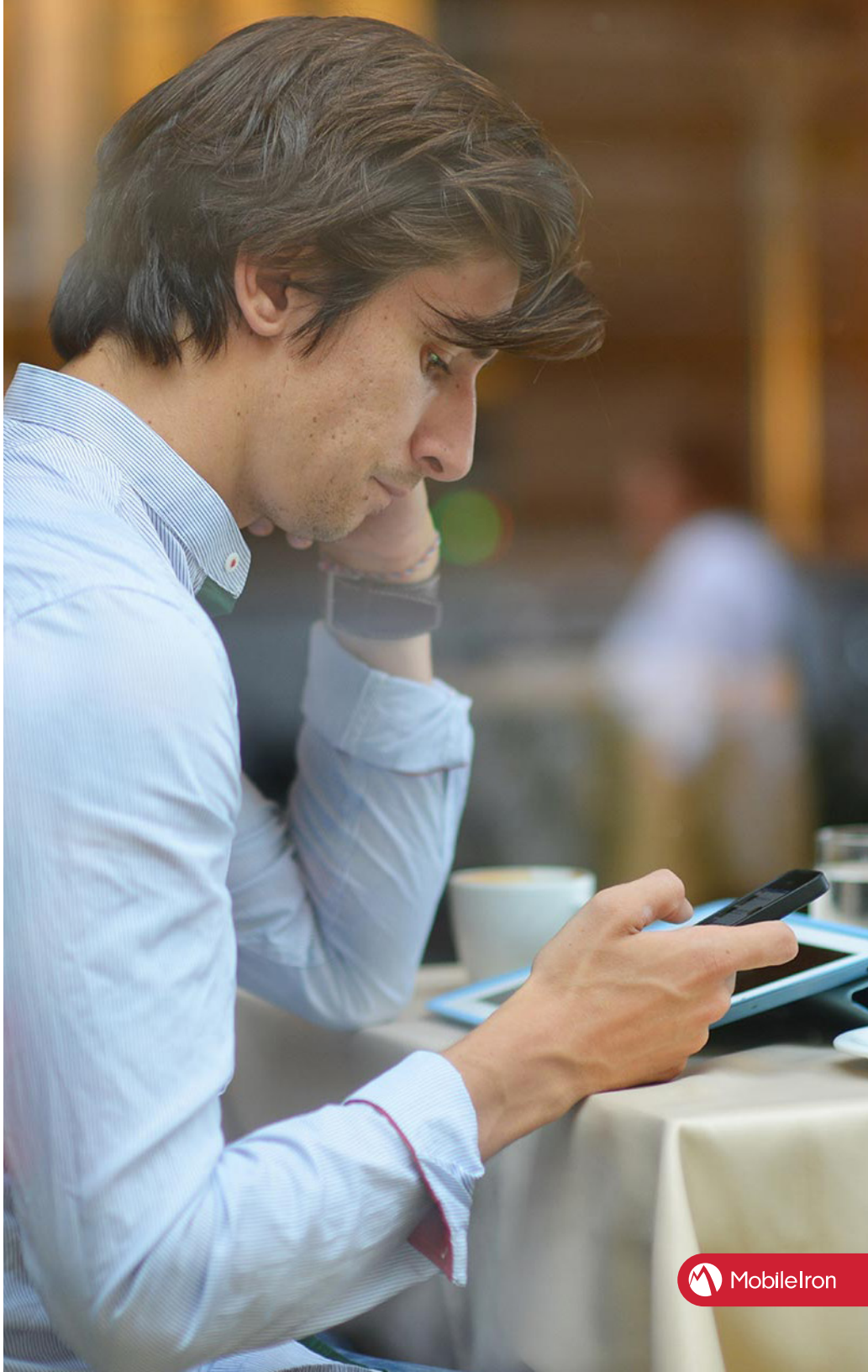
Unsichere oder riskante Apps

*Erfassung und Austausch von Daten, beispielsweise **personenbezogenen Daten (PII)** und Angaben zum Gerätestandort mit Werbe- und Analysesystemen von Drittanbietern.*

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

Um diese Sicherheitsrisiken zu beseitigen, muss die IT mit einem bewährten und konsistenten Ansatz:

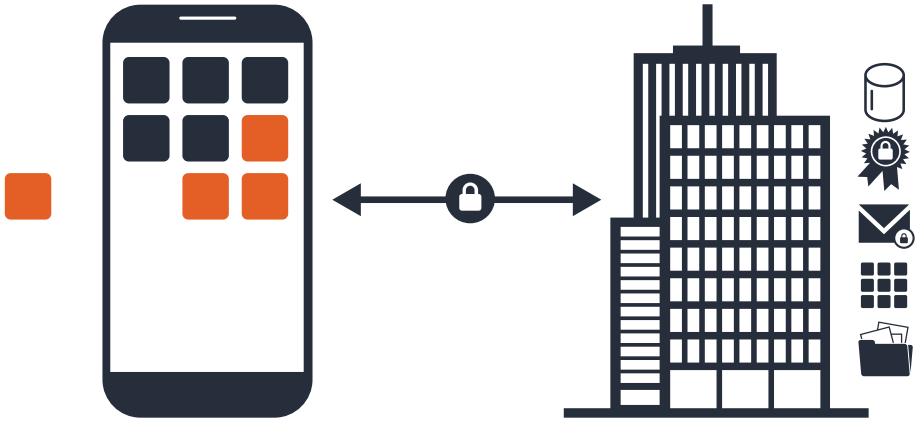
- Mobilgeräte für die Benutzer sicher bereitstellen.
- Benutzer auf deren Geräten authentifizieren.
- Unternehmens-Apps konfigurieren und sicherstellen, dass diese nur auf autorisierten Geräten laufen.
- Maßnahmen zur Vermeidung von Datenverlusten definieren, um die Compliance sicherzustellen.
- Ein sicheres Tunneling zum Unternehmensnetzwerk anbieten.
- Unternehmens-Apps und Daten bei Bedarf löschen, ohne den Datenschutz des Endbenutzers und dessen private Daten zu verändern.



Enterprise Mobility Management (EMM)

Was ist das?

Enterprise Mobility Management (EMM) ist eine umfassende Lösung zur Verwaltung von Mobilgeräten, mobilen Anwendungen und Content im gesamten Unternehmen. EMM-Lösungen wurden entwickelt, um Unternehmen bei der umfassenden Nutzung der Mobiltechnologie als Mittel zur Umgestaltung des Geschäfts zu unterstützen, damit die Endbenutzer unabhängig vom Ort und vom Gerät produktiver werden und die IT die kritischen Sicherheits- und Compliance-Anforderungen erfüllen kann.



Drei Komponenten des EMM

Verwaltung von Mobilgeräten (MDM)

MDM ist die Grundlage für jede EMM-Lösung und erlaubt es der IT:

- Mitarbeiter mit den Geräten produktiver zu machen, die diese gern verwenden,
- Mobilgeräte für mehrere Betriebssysteme abzusichern und zu verwalten,
- sichere Unternehmens-E-Mail, automatische Konfiguration von Geräten und Sicherheit durch Zertifikate anzubieten,
- selektiv Unternehmensdaten aus dem Gerät zu löschen, ohne private Daten zu verändern.

Mobile Application Management (MAM)

Mit MAM kann die IT:

- einen App-Store für Unternehmens-Apps aufbauen und pflegen,
- die Anwendungen auf jedem Gerät absichern,
- Endbenutzer auf dem Gerät authentifizieren,
- Unternehmens- und persönliche Apps auf Mobilgeräten trennen.

Mobile Content Management (MCM)

Mit MCM kann die IT:

- Unternehmensdaten auf Mobilgeräten absichern, ohne dadurch die Benutzererfahrung des Endbenutzers zu beeinträchtigen,
- eine intuitive Möglichkeit für den Zugriff, die Freigabe und

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

Kommentierung von Dokumenten aus E-Mails, SharePoint oder anderen Content-Managementsystemen des Unternehmens sowie für Unternehmens- und private Cloud-Dienste anbieten.

- DLP-Kontrollen zum Schutz von Unternehmens-Content vor unbefugter Weitergabe einführen,
- E-Mail-Anhänge verschlüsseln, sodass diese nur durch autorisierte Anwendungen angezeigt werden können.

Vorteile des Enterprise Mobility Managements

Bereitstellung einer sicheren, skalierbaren Architektur für Unternehmen

Obgleich Mobilgeräte gegen traditionelle PC-Viren immun sind, werden sie auf andere Weise bedroht. Die Verwaltung dieser Bedrohungen erfordert einen mehrstufigen Sicherheitsansatz, der Unternehmensdaten schützt, ohne die Produktivität des Benutzers oder die native Geräteumgebung zu beeinträchtigen.

EMM-Lösungen sind so konzipiert, dass sie spezifische Sicherheitsanforderungen von mobilen Unternehmen wie folgt berücksichtigen:

- **Sicherheit für Unternehmens-E-Mail, Unternehmens-Apps und Content** ohne Überwachung oder Veränderung der privaten Daten auf dem Gerät;
- **Identitätsverwaltung mit Zertifikaten,** damit nur autorisierte Benutzer auf das Gerät zugreifen können;
- **Absicherung mehrerer Benutzerprofile**, damit Benutzer ein Gerät sicher gemeinsam verwenden können;
- **Kapselungen von Anwendungen in Containern,** damit Daten in jeder App verschlüsselt werden können, vor unbefugtem Zugriff geschützt sind und ohne Veränderung der privaten Benutzerdaten von dem Gerät entfernt werden können.
- **VPN-Verbindungen pro App**: Damit können nur autorisierte Apps auf das Unternehmensnetzwerk zugreifen.
- **DLP-Funktionen**: DLP-Funktionen erlauben es den IT-Administratoren, die Funktionen zum Öffnen sowie zum Kopieren und Einfügen von Dokumenten zu begrenzen.
- **Funktionen zur automatischen Steuerung**: Diese lösen automatisch Benachrichtigungen aus, stellen Anwendungen und Dokumente in Quarantäne oder starten andere Maßnahmen zur Zugriffskontrolle, wenn Geräte die Compliance oder Richtlinien verletzen.
- **Selbstbedienungsfunktionen**: Diese vereinfachen die IT-Verwaltung, da die Benutzer sich selbst registrieren, die Compliance überprüfen und wiederherstellen sowie andere Aufgaben zur Geräteverwaltung und Fehlerbehebung ausführen können.

Unterstützung der Wahl der Endbenutzer durch eine native Geräteerfahrung

Damit die Mitarbeiter mit Mobilgeräten während ihrer Tätigkeit produktiv bleiben, muss die Benutzererfahrung für jede mobile Initiative höchste Priorität haben. Zur Unterstützung dieses Ziels sind die EMM-Lösungen so gestaltet, dass sie:

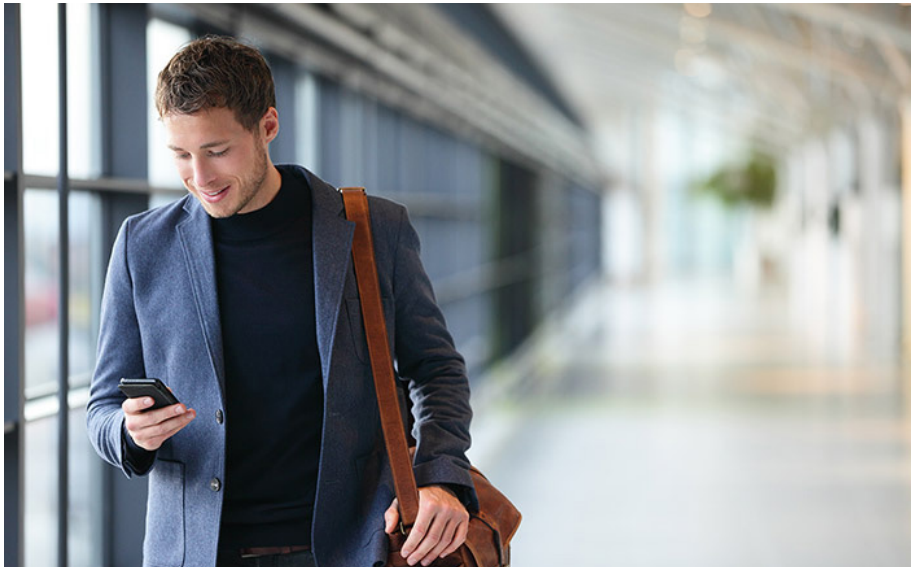
- **mehrere Betriebssysteme unterstützen,** sodass die Mitarbeiter mit ihrem bevorzugten Gerät arbeiten können, unabhängig davon, ob es unter iOS, Android oder Windows Phone läuft.
- **Benutzern erlauben, kritische Unternehmensanwendungen zu suchen und zu installieren,** beispielsweise die Unternehmens-E-Mail, Kalender oder andere Produktivitäts-Apps.
- **Hochsensible private und Unternehmensdaten** auf Mobilgeräten trennen und verwalten, ohne die native Erfahrung zu beeinträchtigen.
- **Sicherheitsmaßnahmen implementieren,** die hocheffektiv, aber für den Endbenutzer unsichtbar sind.
- **Benutzern** bei der Einhaltung der Compliance und Unternehmensrichtlinien helfen.

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

Anforderungen an die EMM-Plattform

Entwickeln und gestalten Sie die Plattform unter Berücksichtigung der Bedürfnisse des Benutzers.

Die Benutzererfahrung muss im Zentrum jeder Mobilitätsinitiative stehen. Wenn die Benutzer das Gerät, die App oder den Content nicht brauchen oder nicht verwenden können, liegt die Akzeptanz bei null, einerlei, wie viel Druck Ihre IT-Abteilung ausübt. Die EMM-Plattform muss daher folgende Anforderungen der Benutzer unterstützen:



Der Benutzer muss Gerät und Betriebssystem wählen können.

Damit die IT die Geräte unterstützen kann, die die Mitarbeiter verwenden wollen, muss die IT eine EMM-Lösung für mehrere Betriebssysteme implementieren und unterstützen. Wie bereits erwähnt, entscheidet nicht die IT, was die Verbraucher brauchen, sondern umgekehrt: Die Verbraucher entscheiden, welche Geräte sie nutzen wollen.

Bieten Sie einen sicheren Zugriff auf mobile Apps und Daten.

Mitarbeiter möchten nicht mehrere Geräte für ihre betrieblichen Aufgaben und ihren Privatgebrauch mit sich herumtragen. Statt also die Geräte zu trennen, ist es Aufgabe der IT, Unternehmens-Apps und private Apps und Daten auf einem Gerät zu trennen. Weil die Benutzer zunehmend ihre eigenen Geräte mit sensiblen persönlichen Informationen verwenden, muss die IT die Sicherheit dieser Daten und den Datenschutz unbedingt gewährleisten. Wenn beispielsweise ein Mitarbeiter das Unternehmen verlässt, wäre eine komplette Löschung des Geräts für diesen Benutzer eine Katastrophe. Die EMM-Lösung sollte daher die Möglichkeit bieten, selektiv Anwendungen und Daten zu verwalten, mit bewährten Verfahren die Unternehmens-Apps und Unternehmensdaten zu schützen und den Datenschutz für den Endbenutzer gewährleisten, indem private und Unternehmensdaten auf dem Gerät getrennt bleiben.

Stellen Sie sicher, dass die EMM-Funktionen benutzerfreundlich sind.

Der vielleicht wichtigste Aspekt ist die Benutzerfreundlichkeit der Funktionen des Geräts und der App-Verwaltung der EMM-Lösung. Die Benutzer sollten beispielsweise in der Lage sein, sich schnell zu authentifizieren und schnell Zugriff auf Unternehmens-Apps und Daten über ihre Geräte zu erhalten. Die Benutzer sollten auch Zugriff zu Selbstbedienungstools haben, mit denen sie einfache Gerätefunktion verwalten und Fehler schnell beseitigen können.

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

IT-Verwaltung vereinfachen

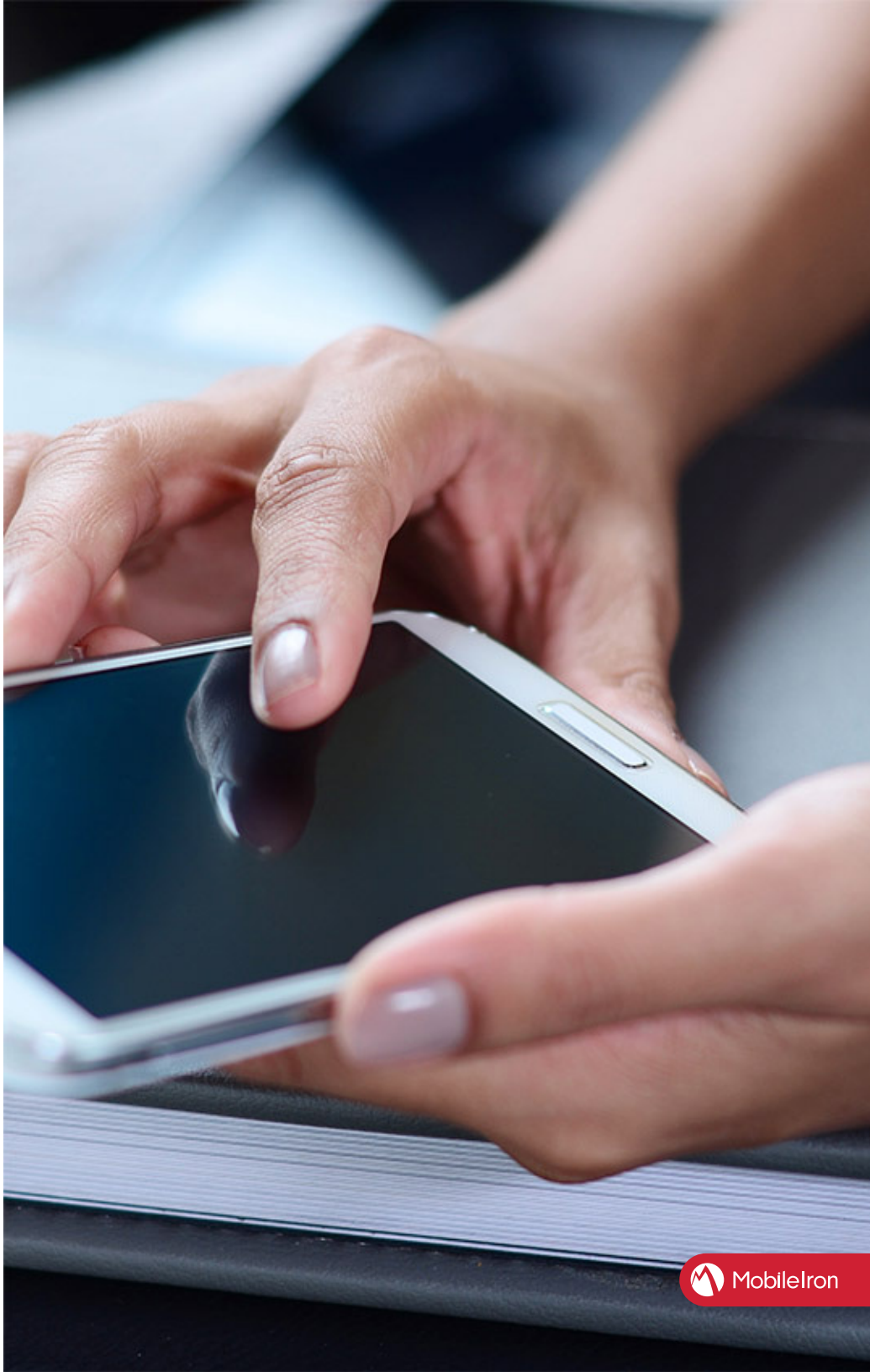
Komplexität ist eines der größten Probleme der IT bei der Verwaltung von Mobilgeräten. Die Verwaltung und Absicherung mehrerer Betriebssystemumgebungen mit diversen Geräten, Apps und Content ist nicht einfach. Aus diesem Grund sollte jede EMM-Lösung der IT folgende Möglichkeiten bieten:

Vereinfachte Zugangskontrolle und Authentifizierung

Zugriff der Benutzer auf Apps und Content mit dem gewünschten Gerät. Dazu muss nicht nur der Benutzer auf dem Gerät authentifiziert, sondern auch der Zugriff auf einzelne Unternehmens-Apps geschützt werden. Wenn der Benutzer jedoch jedes Mal ein Passwort eingeben muss, wenn er eine App öffnet oder Zugang zu einem Unternehmensdokument haben möchte, ist dies für die Benutzer schnell ermüdend und frustrierend. Die EMM-Lösung sollte daher der IT die Möglichkeit bieten, die Benutzer so schnell und schmerzfrei wie möglich zu autorisieren.

Aktivierung kritischer Unternehmensprozesse

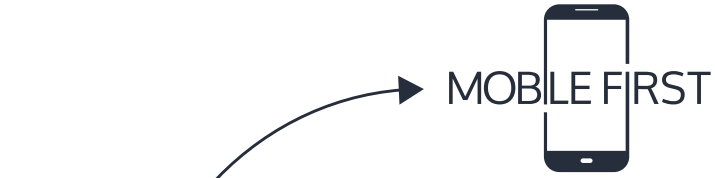
Die wichtigsten mobilen Apps sind die Apps, mit denen Mitarbeiter Zugriff auf essenzielle Daten für wichtige geschäftliche Entscheidungen erhalten. Im Einzelhandel beispielsweise können die Verkäufer mit mobilen Apps Kunden im gesamten Ladengeschäft besser beraten. Sie können beispielsweise den Bestand durchsuchen oder Kundenkäufe abschließen und so Warteschlangen an den Kassen vermeiden und die Kunden zufriedenstellen. Darüber hinaus sollte die IT eine EMM-Lösung einsetzen, um Unternehmens-Apps bereitzustellen, die die Produktivität im Unternehmen steigern, indem die Benutzer Zugriff auf die kritischen Prozesse haben, die sie jeden Tag brauchen.



Etappen der EMM-Implementierung

Die meisten Unternehmen beginnen auf dem Weg zum mobilen Unternehmen damit, dass sie zunächst einen Zugriff auf E-Mails und die Gerätekonfiguration bereitstellen. Unternehmen, die noch neu im Bereich Unternehmensmobilität sind, beginnen mit kleinen Schritten, um Erfahrungen zu sammeln. Es ist wichtig, dass die Endbenutzer Vertrauen entwickeln, damit die übrigen Schritte zum Enterprise Mobility Management erfolgreich sind. Die eigentlichen Vorteile des Enterprise Mobility Management entstehen jedoch, wenn die Mobilgeräteplattform zur primären IT-Plattform für die Bereitstellung von Anwendungen und Content wird. Auf diese Weise wird Mobilität zum Katalysator für eine echte Umgestaltung des Unternehmens.

Etappen auf dem Weg zum Ziel



Etappe 3

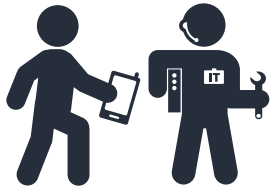
Geschäftstransformation
Neue Benutzer & Unternehmenserfahrung

- Helpdesk
- Datennutzung
- Überwachung der Datennutzung

Etappe 2

App & Content Enablement
- *Mobile Apps der ersten Generation*
- *Mobile Dokumente*
- *Cloud-Schutz*

- Verwaltung mobiler Anwendungen (Mobile Application Management, MAM)
- Verwaltung von mobilem Content



Etappe 1

Gerätesicherheit
- *BYOD*
- *E-Mail-Zugriff (sicheres ActiveSync)*
- *Sicherheit für mehrere Betriebssysteme (Ersatz für BlackBerry)*

- Verwaltung mobiler Geräte (MDM)

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

Bewährte Methoden der EMM-Bereitstellung

Die Bereitstellung einer EMM-Lösung erfolgt am besten in vier Prozessschritten (Planung, Entwurf, Bereitstellung und Einführung). Diese werden im Folgenden beschrieben.

Planen

Für den Planungsprozess müssen Sie zunächst wissen, was "Erfolg" für Ihr Unternehmen bedeutet und wie schnell Sie ihn erreichen können. Sammeln Sie Feedback von den wichtigsten Entscheidungsträgern im Unternehmen: Dies ist in der Planungsphase enorm wichtig. Beispielsweise definieren manche Unternehmen "Erfolg" als eine problemlose Bereitstellung, die den Benutzern die erforderliche Sicherheit, E-Mail-Zugriff und WLAN-Profile zur Verfügung stellt. Bei einer einfachen Bereitstellung wird die Geräteregistrierung vor allem über die IT-Mitarbeiter vorgenommen, die mit mobilen Betriebssystemen und deren Funktionen vertraut sind.

Unternehmen, die sich nicht auf eine einfache EMM-Bereitstellung beschränken wollen, müssen in der Planungsphase folgende Fragen beantworten:

1. Haben Ihre Mitarbeiter Erfahrung mit Mobilgeräten?

Technisch versierte Mitarbeiter sind pflegeleichter als Mitarbeiter, die noch nie mit Mobilgeräten gearbeitet haben. Benutzer mit weniger technischer Erfahrung benötigen mehr Support durch die IT.

2. Welche mobilen Betriebssysteme und Geräte will Ihr Unternehmen unterstützen?

Um diese Frage zu beantworten, müssen Sie wissen, welche Geräte unter den Mitarbeitern am beliebtesten sind. Möglicherweise können Sie zu Beginn der Einführung der Mobiltechnologie nicht alle bevorzugten Geräte unterstützen. Was Sie allerdings gar nicht brauchen, ist die Bereitstellung von Ressourcen zur Unterstützung von Geräten, die nur wenige Benutzer verwenden.

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

3. Wie komplex ist Ihre Netzwerkinfrastruktur?

Eine einfache Bereitstellung in einem Rechenzentrum mit internen Netzwerkdiensten erfordert weniger Ressourcen als eine Einführung in mehreren Rechenzentren mit komplexem Netzwerk und komplexer Infrastruktur. Die Auslagerung von IT-Diensten erfordert zusätzliche Planung.

4. Wie ausgereift ist Ihre Definition der IT-Governance, der Richtlinien und Prozesse?

Eine effektive IT-Governance erfordert in der Regel eine pünktliche Programmentwicklung und Lösungsbereitstellung unter Einhaltung des Budgets, um die Ziele des Unternehmens zu erfüllen. Unternehmen, denen ein definiertes oder ausgereiftes IT-Governance-Programm fehlt, benötigen mehr Zeit und mehr Mitarbeiter zur Implementierung ihrer EMM-Lösung.

5. Wie effektiv sind Ihre Ressourcen für die Mitarbeiterschulung und Weiterbildung?

Unternehmen mit vorhandenen Schulungs- und Weiterbildungsprogrammen und Infrastrukturen können die EMM-Einführung und die Akzeptanz des Programms sowohl durch die Mitarbeiter als auch durch das Helpdesk beschleunigen. Die Entwicklung einer Initiative zur Mitarbeiterweiterbildung erfordert vorab mehr Anstrengungen, zahlt sich jedoch durch die Weiterbildung von Mitarbeitern aus, die mit Mobilgeräten besser umgehen können und das Helpdesk seltener in Anspruch nehmen.

6. Hat Ihr IT-Team Erfahrung mit der Zertifikatsauthentifizierung?

Zertifikatsauthentifizierung entwickelt sich zu einer Standardfunktion bei Mobiltechnologieinitiativen. Wenn Sie interne Erfahrung in diesem Bereich haben, können Sie die Bereitstellung und Konfiguration beschleunigen.

7. Kann Ihre IT-Abteilung mobile Unternehmens-Apps entwickeln und bereitstellen?

Jeder Programmierer, der Apps für Ihr Unternehmen entwickelt, sollte über die Erfahrung und das Know-how verfügen, eine hervorragende mobile Benutzerumgebung bereitzustellen. Dies entscheidet über den Erfolg Ihrer Mobilstrategie. Wenn Sie keine erfahrenen App-Entwickler im eigenen Haus haben, müssen Sie diese Schlüsselfunktion auslagern.

8. Welche Sicherheitsanforderungen bestehen in Ihrem Unternehmen?

Der Schutz von Informationen und die Datensicherheit auf Mobilgeräten sind kritische Komponenten jeder EMM-Installation. Unternehmen in stark regulierten Branchen unterliegen strengeren Richtlinien für die Risikokontrolle und haben daher höhere Sicherheitsanforderungen als Unternehmen mit höherer Risikotoleranz.

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

Entwerfen

Diese Phase der EMM-Bereitstellung definiert die Richtlinien für Ihre Mobilitätsstrategie. Diese Etappe enthält vier Schritte, die im Folgenden erläutert werden.

1 Rollen definieren

Wie viele Admins? Welche Zuständigkeiten?

2 Transparenz definieren

Welche Benutzer und welche Geräte darf jeder Admin sehen und melden?

3 Aktionen zuweisen

Welche Aktionen kann jeder Admin ausführen?

4 Verteilung verwalten

Welche Apps, Richtlinien, Konfigurationen kann jeder Admin für die Benutzer / Geräte verteilen?

1. Rollen definieren:

Ermitteln Sie zunächst, wie Sie administrative Aufgaben organisieren wollen, beispielsweise Support durch das Helpdesk, Benutzerregistrierung und Gerätekonfigurationsmanagement. Wie viele Ebenen des Supports durch das Helpdesk brauchen Sie beispielsweise? Wer entwickelt und verwaltet Ihre hauseigenen Apps – eigene Mitarbeiter oder unabhängige Entwickler? Wer verwaltet die Richtlinien- und Konfigurationsprozesse?

2. Transparenz definieren

Zweitens müssen Sie festlegen, welche Benutzer und Geräte jeder IT-Administrator verwaltet, und wie viel Kontrolle und Transparenz diese Administratoren haben. Auch die Richtlinien zur Benutzerverwaltung und Geräteverwaltung können je nach Geschäftseinheit oder geografischer Region abweichen. In manchen Ländern beispielsweise existieren strengere Bestimmungen zum Datenschutz, und Ihre Geräterichtlinie muss diese Anforderungen berücksichtigen.

3. Aktionen zuweisen

Weisen Sie drittens jeder IT-Rolle die Aktionen zu, die diese ausführen soll. Welche Administratoren verwalten beispielsweise in Zukunft die Bereitstellung von Apps, Richtlinien und Konfigurationen entsprechend Ihren Transparenzrichtlinien?

4. Verteilung verwalten:

In diesem letzten Schritt legen Sie fest, welche Apps, Richtlinien und Konfigurationen Sie durch wen wann bereitstellen. Legen Sie fest, welche IT-Administratoren für die verschiedenen Verteilungsrollen zuständig sind und verhindern Sie, dass Administratoren nicht genehmigte Aktionen ausführen können.

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

Bereitstellen

In der Bereitstellungsphase Ihrer EMM-Einführung müssen Sie festlegen, ob Ihre Plattform im Unternehmensnetzwerk oder in der Cloud installiert werden soll. Diese Entscheidung kann auch mit den verschiedenen Tarifmodellen zusammenhängen, beispielsweise mit Abozahlungen oder einer ewigen Lizenz.

- **Installation im Netzwerk:**
  Eine Netzwerklösung erfolgt eine benutzerfreundliche Installation einer Software-Appliance im Unternehmensnetzwerk, die in weniger als einem Tag betriebsbereit sein kann. Lösungen für Installationen im Netzwerk können entweder unbefristet lizenziert oder nach einem Abomodell abgerechnet werden.
- **Cloud-Installation:**
  Eine EMM-Cloud-Bereitstellung integriert sich eng in die Messaging- und Sicherheitssysteme des Unternehmens für das eigene Netzwerk, beispielsweise die Unternehmens-E-Mail und Unternehmensverzeichnisse. Installationen in der Cloud werden auf Abobasis angeboten.

Einführen

Sobald Ihre EMM-Lösung eingeführt werden kann, müssen Sie sicherstellen, dass Ihre Mitarbeiter für das Helpdesk entsprechend vorbereitet sind. Sie müssen in der Lage sein:

- **Probleme bei der Verwaltung mehrerer Betriebssysteme** zu verstehen. Dazu müssen Sie die Mitarbeiter des Helpdesks zu den verschiedenen Geräten, Servern und Netzwerkproblemen schulen, die wahrscheinlich autreten und klar, welche Schritte für die Fehlerbehebung und den Eskalationsprozess auszuführen sind und wer für jede Problemart zuständig ist.
- **Geräteexperten einzubeziehen**, die die Geräte besser kennen als die Mitarbeiter des Helpdesks.
- **Auf die benötigten Ressourcen** für den erbrachten Support zuzugreifen. Sorgen Sie dafür, dass die Mitarbeiter über benutzerfreundliche Ressourcen zur Fehlerbehebung verfügen, beispielsweise über Skripts zur Problembeseitigung und eine Online-Wissensbasis.
- **Laufende Weiterbildungsmöglichkeiten umfassend zu nutzen,** um sicherzustellen, dass Sie bei Upgrades der Mobilgeräte, der Infrastruktur usw. auf dem neusten Stand sind.

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

Worauf Sie bei einem EMM-Anbieter achten sollten

Eine der am häufigsten gestellten Fragen zu EMM-Anbietern lautet: Wie finde ich einen Anbieter, der alle meine spezifischen Anforderungen erfüllen kann? Hier die wichtigsten Kriterien, mit denen Sie Ihre Suche eingrenzen und beschleunigen können:

Plattformneutralität

Erinnern Sie sich daran, wie Mobilgeräte vor fünf oder zehn Jahren aussahen? Einige der damaligen Anbieter existieren heute gar nicht mehr. Es bestehen gute Chancen, dass in fünf Jahren die Mobiltechnologie ganz anders aussieht als heute. Sie sollten also nicht versuchen, zu prognostizieren, welche Mobilgeräteplattformen in einem extrem wettbewerbsintensiven Verbrauchermarkt erfolgreich sein werden; viel einfacher ist es, wenn Sie sich für einen Anbieter entscheiden, der eine plattformneutrale Verwaltung mehrerer Betriebssysteme unterstützt. Dann müssen Sie sich nicht darum kümmern, welche Geräte unterstützt werden sollen, weil Ihr Anbieter jedes gewünschte Gerät unterstützen kann.

Spezielle Mobilgeräteplattform

Mobilität in Unternehmen ist die Zukunft, und mobile IT entwickelt sich schnell zu dem Weg, über den Apps und Daten verwaltet und bereitgestellt werden. Suchen Sie nach einem Anbieter, dessen Plattform für dieses Konzept entwickelt wurde. EMM-Lösungen, die lediglich Ergänzungen oder Einzelkomponenten einer vorhandenen Infrastruktur sind, sind möglicherweise nicht umfassend genug oder berücksichtigen nicht alle Aspekte und können daher nicht die Skalierbarkeit und Zuverlässigkeit bieten, die Sie brauchen.

Umfangreiches Ökosystem

Sie sollten nicht nur einen Anbieter auswählen, der eine solide Vision und eine spezielle EMM-Plattform besitzt, sondern Ihr Lösungsanbieter sollte auch ein Ökosystem von Anbietern pflegen, die Zusatzlösungen für mobile Unternehmen entwickeln. Ein umfassendes Partner-Ökosystem stellt sicher, dass Ihr Anbieter die breiteste Palette von Mobilgeräten, Betriebssystemen, Geräten und Bereitstellungskonfigurationen unterstützen und eine breite Palette von Einsatzfällen aus der Praxis berücksichtigen kann.

Starker und wachsender Kundenstamm

Nicht zuletzt sollten Sie sich das Kundenportfolio des Anbieters anschauen. Unterstützt der EMM-Anbieter Unternehmen in den verschiedensten Branchen? Wächst der Kundenstamm oder betreut er nur ein Nischensegment im Markt? Die Recherche zum Kundenstamm eines EMM-Anbieters ist eine kritische Due-Diligence-Komponente Ihrer Anbieterauswahl.

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

Zusammenfassung

Bei Unternehmensmobilität geht es nicht nur um den Kauf der modernsten Technologie oder darum, Mitarbeitern den Abruf von E-Mails auf dem Mobiltelefon zu gestatten. Mobilität betrifft die Umgestaltung des gesamten Geschäfts, um die Produktivität auf ganz neue Weise zu erhöhen. Obgleich der Start einer Mobilitätsinitiative wie die Erkundung eines unkartierten Territoriums sein kann, hilft Ihnen die richtige EMM-Lösung, schnell zu einem Mobile-First-Unternehmen zu werden.

Über MobileIron

MobileIron ist ein führendes Unternehmen für Enterprise Mobility Management (EMM); über 7.500 Kunden weltweit haben sich für MobileIron entschieden, darunter mehr als 400 der weltweit wichtigsten 2000 Unternehmen ("Forbes Global 2000"). Diese Unternehmen richten ihr Geschäft durch Unternehmensmobilität neu aus und beschleunigen Innovationen. MobileIron wurde speziell zur Absicherung und Verwaltung mobiler Apps, Dokumente und Geräte internationaler Unternehmen in Form einer Cloud-Lösung bzw. als Lösung für das Unternehmensnetzwerk entwickelt. MobileIron arbeitet mit mehr als 130 AppConnect-Partnern sowie mehr als 36 Technologie Alliance-Partnern zusammen, die unsere Plattform integriert haben oder gerade integrieren. Unsere Kunden haben mit AppConnect über 1.000 intern entwickelte Anwendungen abgesichert. Nicht zuletzt verfügt unser internationales Customer Success-Team über umfassende Erfahrung, um unseren Kunden den nötigen Support bei der Entwicklung zum Mobil First-Unternehmen zu bieten.

www.mobileiron.com

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