SOPHOS
Security made simple.

Buyers Guide – Enterprise Mobility Management

Effiziente Nutzung von IT-Ressourcen und Datenschutz für mobile Geräte vs. mehr Freiraum für Benutzer

Um Flexibilität und Produktivität zu gewährleisten, kommen in der heutigen Berufswelt immer öfter mobile Geräte zum Einsatz – der durchschnittliche Mitarbeiter hat heute bereits drei mobile Geräte. IT-Abteilungen stehen vor der schwierigen Aufgabe, ein ausgewogenes Verhältnis zwischen der Sicherheit der Unternehmensdaten und der Produktivität der Mitarbeiter zu schaffen. Und zwar oft mit knappen IT-Ressourcen.

Bei BYOD geht es zum großen Teil darum, den Benutzern die Verwendung ihrer bevorzugten Geräte und Plattformen zu ermöglichen. Aktuelle Studien zeigen, dass Android und iOS mit mehr als 80 % Marktanteil derzeit marktführend sind, Windows Phone 8 jedoch immer mehr aufholt (siehe Diagramm unten). Die Festlegung auf eine einzige mobile Plattform kann die Arbeit der IT-Abteilung vereinfachen. Beobachtet man die derzeitige Entwicklung, ist dieser Ansatz aber wohl kaum eine realistische Lösung. In der Praxis werden zahlreiche verschiedene Plattformen genutzt, was die ohnehin knappen Ressourcen der IT-Abteilungen noch stärker beansprucht. Viele IT-Experten prüfen daher Lösungen zum Enterprise Mobility Management (EMM), die ihnen helfen sollen, die Flut mobiler Geräte in den Griff zu bekommen und komplexe BYOD-Verwaltungsaufgaben zu bewältigen.

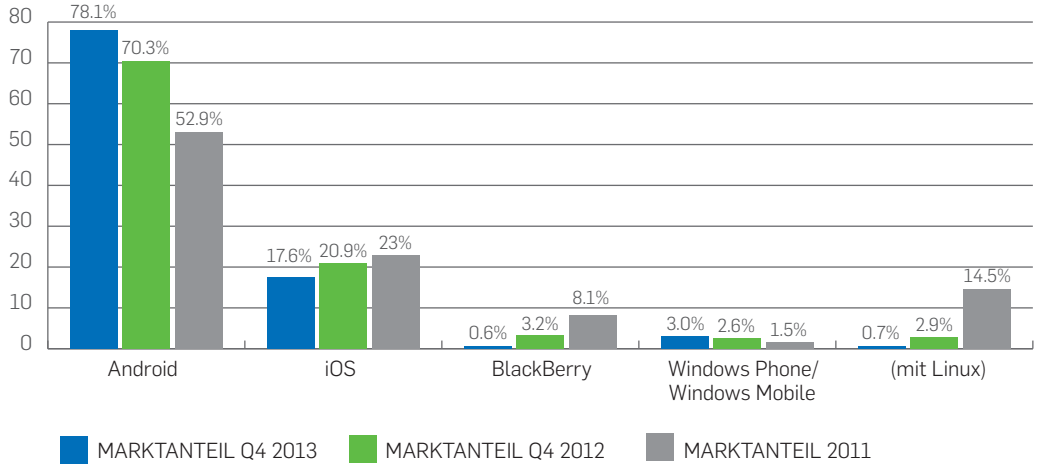

Abbildung 1: Marktanteile mobiler Betriebssysteme in den Jahren 2011–2013
Quelle: IDC Worldwide Mobile Phone Tracker, 12. Februar 2014

Dieser EMM Buyers Guide hilft Ihnen bei der Auswahl der richtigen Mobile-Lösung für das BYOD-Programm Ihres Unternehmens. Sie erfahren, wie effiziente EMM-Systeme die BYOD-Strategien von Unternehmen optimal unterstützen, die Compliance sicherstellen, Unternehmensdaten schützen und eine einfache zentrale Verwaltung von Geräten und Anwendungen ermöglichen. Außerdem enthält der Guide eine detaillierte Tabelle, in der Sie die Funktionen der wichtigsten Mobile-Security-Anbieter im Vergleich sehen.

Schutz für Unternehmensdaten

Mit einer EMM-Lösung lassen sich mobile Geräte von einer zentralen Stelle aus sichern und verwalten, damit die auf diesen Geräten gespeicherten oder über sie abgerufenen Unternehmensdaten geschützt sind. Eine umfassende Strategie zur sicheren Nutzung mobiler Geräte muss alle denkbaren Szenarien berücksichtigen, in denen die Nutzer auf ihren mobilen Geräten mit Unternehmensdaten arbeiten.

Viele Betriebssysteme für mobile Geräte verfügen über integrierte Sicherheitsfunktionen wie z. B. Einschränken von Gerätefunktionen (Deaktivieren der Kamera) und Verschlüsselung. Ihre EMM-Lösung sollte Ihnen helfen, diese Funktionen zu steuern, um alle Daten optimal zu schützen.

Die Möglichkeit, Maßnahmen für verloren gegangene Geräte zu ergreifen, ist unverzichtbar und fester Bestandteil der meisten EMM-Lösungen. Diese Funktion ermöglicht dem Administrator, ein Gerät zu orten, zu sperren und/oder Unternehmensdaten vom Gerät zu löschen. Idealerweise sollten Sie eine Lösung verwenden, die es Ihren Benutzern erlaubt, ihre Geräte über ein Self-Service-Portal selbst zu orten, zu sperren oder zurückzusetzen. Hierdurch wird nicht nur die IT entlastet, sondern auch die Effizienz gesteigert. Denn in der Regel weiß der Benutzer als erster, dass sein Gerät verloren gegangen ist oder gestohlen wurde, und sollte sofort die entsprechenden Maßnahmen ergreifen.

Außerdem muss die IT wissen, wie Benutzer Unternehmensdaten auf mobilen Geräten speichern, bearbeiten und austauschen. Laut einer Studie von Sophos nutzen 46 % aller Unternehmen Cloud-Speicher zum Austausch von Unternehmensdaten. 60 % dieser Unternehmen nehmen jedoch keine Verschlüsselung dieser Daten vor, die auf mobilen Geräten über die Cloud ausgetauscht werden. Um Datenverluste effektiv zu verhindern, muss der Datenschutz auch außerhalb des Büros greifen. Daten müssen an jedem Ort geschützt werden und eine Verschlüsselung einzelner Dateien ist unverzichtbar, damit unbefugte Personen sich keinen Zugriff auf sensible Unternehmensdaten verschaffen können. Mit einer EMM-Lösung, die jede einzelne Datei transparent verschlüsselt, können Sie sicher sein, dass Ihre Dokumente und Daten geschützt bleiben – nicht nur im Büro, sondern überall.

Compliance- und Richtliniendurchsetzung

Eine EMM-Lösung schützt Unternehmensdaten, indem sie die Compliance mit den Sicherheitsrichtlinien des Unternehmens durchsetzt. Compliance-Prüfungen stellen sicher, dass der Zugriff auf Unternehmensdaten ausschließlich für registrierte und richtlinienkonforme Geräte möglich ist.

Endbenutzer, die mit ihren mobilen Privatgeräten auf Unternehmensdaten zugreifen möchten, sollten sich darüber im Klaren sein, dass sie dabei zur Einhaltung unternehmensinterner Richtlinien verpflichtet sind. IT-Verantwortliche können funktionsstarke EMM-Lösungen einsetzen, um Richtlinien durchzusetzen und das Risiko von Datenverlusten zu verringern.

Bevor ein Datenzugriff gewährt wird, muss das jeweilige mobile Gerät registriert sein. Verbindet sich ein registriertes Gerät, überprüft das EMM-System, ob das Gerät die Unternehmensrichtlinien einhält, z. B. bezüglich Jailbreaking, Passwortkonfiguration und unzulässiger Apps. Manche EMM-Lösungen bieten Ihnen zusätzlich zur Standard-Compliance-Prüfung die Möglichkeit, unternehmensinterne Richtlinien zur Nutzung mobiler Geräte über ein Self-Service-Portal bereitzustellen. So können Sie sicherstellen, dass die Benutzer die Richtlinien kennen und akzeptieren, bevor der Zugriff gewährt wird.

Da Ihre Benutzer ggf. mehrere Geräte besitzen und für den Zugriff auf Unternehmensdaten verwenden, sollte Ihre Lösung außerdem die Erstellung gruppen- und benutzerbasierter Compliance-Regeln ermöglichen. Wenn in Ihrem Unternehmen sowohl unternehmenseigene Geräte als auch Privatgeräte zulässig sind, sollten Sie eventuell separate Regeln für die beiden Gerätegruppen erstellen.

Risikominderung

IT-Verantwortliche können mit einer EMM-Lösung Risiken mindern und dafür sorgen, dass ihre Richtlinie zur Nutzung mobiler Geräte erfolgreich durchgesetzt wird. Maßnahmen zur Risikominderung können je nach Schweregrad einer Richtlinienverletzung festgelegt werden. In weniger schwerwiegenden Fällen reicht es ggf. aus, die Benutzer lediglich zu informieren oder den Datenzugriff oder E-Mail-Empfang für nicht richtlinienkonforme Geräte zu sperren. Wenn Ihre Daten in Gefahr sind, ist u. U. nur noch ein Zurücksetzen des Geräts oder ein selektives Löschen der Unternehmensdaten per Remotezugriff eine sinnvolle Option.

Die Risikominderung wird für das IT-Team vereinfacht, wenn das EMM-System über vorkonfigurierte, automatisierte Antworten auf Compliance-Probleme verfügt, die ausgeführt werden, ohne dass der Administrator eingreifen muss. Beispiele für solche Antworten sind: Sperrung des E-Mail-Empfangs, Benachrichtigung an Benutzer und/oder Administrator oder Anwendung eines Lockdown-Profils. Automatische Benachrichtigungen der Benutzer bei Compliance-Problemen können den Arbeitsaufwand für die IT-Abteilung deutlich reduzieren. Denn die Benutzer sind dann in der Lage, die meisten Fehler direkt selbst zu korrigieren – ohne das IT-Helpdesk zu bemühen.

Integrierte Sicherheit: Anti-Malware und Web-Schutz

Mobile Geräte sind nichts anderes als kleine Computer, die Benutzer überall hin begleiten. Daher benötigen sie einen genauso stabilen und integrierten Virenschutz wie PCs, der sowohl mobile Malware abwehrt als auch Web Filtering für Android-Geräte beinhaltet.

Darüber hinaus ist für Android-Benutzer eine Sicherheitslösung mit Web-Schutz dringend zu empfehlen, da die meisten Infektionen aus dem Internet stammen. Zum Schutz vor mobiler Malware sollte eine EMM-Lösung unbedingt die folgenden Funktionen beinhalten:

- Automatische Malware-Scans für alle neu installierten Apps
- Verschieben infizierter Geräte in die Quarantäne
- Schutz vor schädlichen Websites und Sperren von Webseiten nach Kategorie

Network Access Control

Um das Datenpannen-Risiko zu senken, sollte eine EMM-Lösung den Gerätestatus konstant überwachen und den Netzwerkzugriff entsprechend kontrollieren. Eine EMM-Lösung sollte Jailbreaks, unzulässige Apps und unsichere Einstellungen erkennen und den Gerätestatus konstant überprüfen. Falls sich ein Gerät als nicht richtlinienkonform erweist, muss der Zugriff auf das WLAN und/oder VPN durch Integration mit Network-Security-Anbietern gesperrt werden. Idealerweise stammen Network-Security- und EMM-Lösung vom gleichen Anbieter, damit ein einheitliches Sicherheitsportfolio besteht, dessen einzelne Lösungen optimal aufeinander abgestimmt sind.

Sicherheitsfunktionen auf einen Blick

Anbieter von Sicherheitslösungen mit EMM

✔ = JA ✗ = NEIN

Funktion	Sophos	Symantec	McAfee	Kaspersky	Trend Micro
DATENSCHUTZ UND MOBILE VERSCHLÜSSELUNG					
Orten, Sperren und Zurücksetzen	✔	✔	✔	✔	✔
Unternehmensseitiges Zurücksetzen	✔	✔	✔	✔	✔
Verschlüsselung einzelner Dateien	✔	✗	✗	✗	✗
COMPLIANCE- UND RICHTLINIENDURCHSETZUNG					
Geräte mit Jailbreak/gerootete Geräte zulassen oder nicht zulassen	✔	✔	✔	✔	✔
Auf Side-Loading überprüfen	✔	✔	✔	✗	✔
Mindestversion des Betriebssystems durchsetzen	✔	✔	✔	✗	✔
Durchsetzung von Geräteverschlüsselung	✔	✔	✔	✔	✔
Whitelist- oder Blacklist-Apps	✔	✔	✔	✔	✔
Erforderliche Apps durchsetzen	✔	✔	✔	✔	✗
RISIKOMINDERUNG					
Sperrung des E-Mail-Zugangs basierend auf Compliance-Status	✔	✔	✔	✗	✗
Administrator benachrichtigen	✔	✔	✔	✔	✔
Möglichkeit zur Kontrolle der Netzwerkfreigabe	✔	✔	✗	✗	✗
Automatische Ausführung risikomindernder Maßnahmen	✔	✔	✔	✗	✗
ANTI-MALWARE UND WEB-SCHUTZ					
Apps bei der Installation scannen	✔	✔	✗	✔	✔
Anti-Malware-Scans remote auslösen	✔	✔	✗	✔	✔
Schadanwendungen (Malware) blockieren	✔	✔	✗	✔	✔
Web Filtering auf Basis von Kategorien	✔	✗	✔	✔	✔
Sicheres Surfen im Internet	✔	✔	✔	✔	✔
NETWORK ACCESS CONTROL					
Network Access Control	✔	✔	✗	✗	✗
Complete-Security-Anbieter	✔	✗ Mobile Suite, aber keine vollständige EP+Mobile Suite	✔ Per EPO	✔	✔

Sicherheitsfunktionen auf einen Blick

Reine EMM-Anbieter

✔= JA ✗ = NEIN

Funktion	Sophos	AirWatch	MobileIron	IBM (Fiberlink)
DATENSCHUTZ UND MOBILE VERSCHLÜSSELUNG				
Orten, Sperren und Zurücksetzen	✔	✔	✔	✔
Unternehmensseitiges Zurücksetzen	✔	✔	✔	✔
Verschlüsselung einzelner Dateien	✔	✗	✗	✗
COMPLIANCE- UND RICHTLINIENDURCHSETZUNG				
Geräte mit Jailbreak/gerootete Geräte zulassen oder nicht zulassen	✔	✔	✔	✔
Auf Side-Loading überprüfen	✔	✔	✔	✔
Mindestversion des Betriebssystems durchsetzen	✔	✔	✔	✔
Durchsetzung von Geräteverschlüsselung	✔	✔	✔	✔
Whitelist- oder Blacklist-Apps	✔	✔	✔	✔
Erforderliche Apps durchsetzen	✔	✔	✔	✔
RISIKOMINDERUNG				
Sperrung des E-Mail-Zugangs basierend auf Compliance-Status	✔	✔	✔	✔
Administrator benachrichtigen	✔	✔	✔	✔
Möglichkeit zur Kontrolle der Netzwerkfreigabe	✔	✔	✔	✔
Automatische Ausführung risikomindernder Maßnahmen	✔	✔	✔	✔
ANTI-MALWARE UND WEB CONTROL				
Apps bei der Installation scannen	✔	✗	✗	✗
Anti-Malware-Scans remote auslösen	✔	✗	✗	✗
Schadanwendungen (Malware) blockieren	✔	✗	✗	✗
Web Filtering auf Basis von Kategorien	✔	✗	✗	✗
Sicheres Surfen im Internet	✔	✗	✗	✗
NETWORK ACCESS CONTROL				
Network Access Control	✔	✔	✔	✔
Complete-Security-Anbieter	✔	✗	✗	✗

Zentrale Verwaltung von mobilen Geräten, Inhalten, E-Mails und Anwendungen

In der Praxis zeigt sich, dass Endnutzer durchaus bereit sind, ein bestimmtes Maß an Kontrolle über ihre privaten mobilen Geräte abzugeben, die sie beruflich nutzen, um mehr Flexibilität, Effizienz und Produktivität zu gewinnen. Gleichzeitig benötigen IT-Abteilungen genug Kontrollmöglichkeiten, um BYOD-Programme optimal verwalten und für Sicherheit sorgen zu können. So benötigen sie vielleicht die Möglichkeit, Richtlinien durchzusetzen, sowie einen Überblick über alle Geräte, die sich mit dem Unternehmensnetzwerk verbinden, über die Anwendungen, die auf den Geräten installiert werden, und darüber, wie auf Informationen zugegriffen wird und wie diese weitergeleitet werden.

Mobile Device Management (MDM)

Ganz gleich, ob Sie Ihren Mitarbeitern mobile Geräte zur Verfügung stellen oder ob diese ihre Privatgeräte mitbringen: Sie müssen den Überblick über alle Geräte im Netzwerk behalten. Entscheiden Sie sich für eine EMM-Lösung, die es Ihnen leicht macht, die mobilen Geräte in Ihrer Umgebung während der gesamten Lebensdauer der Geräte zu verwalten – von der ersten Einrichtung und Registrierung bis zur Außerbetriebnahme. Darüber hinaus benötigen Sie auch Tools, die Sie über den Gerätebestand informieren und Ihnen Reporting-Daten liefern. Übersichtliche Dashboards mit Informationen auf einen Blick, strukturierten Tabellen oder Tortendiagrammen zeigen Ihnen alle Geräte sowie deren jeweiligen Status, z. B. zu Inhaber, Plattform und Compliance.

Mobile Content Management (MCM)

Sorgen Sie dafür, dass Ihre Daten überall sicher sind – auch außerhalb des Büros. Mit einer mobilen Verschlüsselung auf beruflich genutzten Privatgeräten stellen Sie sicher, dass jedes Dokument geschützt bleibt, und ermöglichen gleichzeitig ein produktives und sicheres Zusammenarbeiten. Durch die Ausweitung einer stabilen Verschlüsselungslösung auf Ihre mobilen Geräte ermöglichen Sie Ihrer IT die Kontrolle über die Bearbeitung und den Austausch von Daten in der Cloud. Verschafft sich beispielsweise jemand Unbefugtes Zugriff auf den Dropbox-Account eines Mitarbeiters, so muss Sie dies nicht beunruhigen, wenn Sie eine Verschlüsselung einzelner Dateien implementiert haben. Denn ohne den entsprechenden Schlüssel ist kein Zugriff auf die verschlüsselten Unternehmensdaten möglich.

Mobile Email Management (MEM)

Ein sicherer Zugriff auf Unternehmens-E-Mails ist insbesondere in einer BYOD-Umgebung unverzichtbar. Mit MEM sorgen Sie für umfassende Sicherheit in der E-Mail-Infrastruktur Ihres Unternehmens: Sie verteilen E-Mail-Einstellungen, ermöglichen Ihren Benutzern innerhalb weniger Minuten ein produktives Arbeiten und können den E-Mail-Zugriff über ein sicheres E-Mail-Gateway auf Grundlage des Gerätestatus kontrollieren. Außerdem sollten Sie in der Lage sein, vertrauliche Unternehmens-E-Mails selektiv zu löschen, wenn ein Benutzer das Unternehmen verlässt.

Mobile Application Management (MAM)

Ihren Mitarbeitern die für ihren Job notwendigen Programme bereitzustellen, ist geschäftlich gesehen sicherlich sinnvoll. In einer BYOD-Umgebung kann dies jedoch schnell zu einer unkontrollierten Zunahme mobiler Anwendungen führen. Das in Ihrer EMM-Lösung enthaltene Mobile Application Module (MAM) sollte Sie bei der Verwaltung all dieser Anwendungen unterstützen. Es sollte Ihnen ermöglichen, erforderliche Unternehmensanwendungen per Push-Übertragung an die Geräte zu senden sowie zulässige Apps auf eine Whitelist und unzulässige Apps auf eine Blacklist zu setzen.

Zentrale Verwaltung

Android-Geräte sind besonders anfällig für Malware. Daher ist es wichtig, diese Geräte – und Ihr Netzwerk – mit einer EMM-Lösung zu schützen, in die Anti-Malware, Web-Schutz und Network Access Control integriert sind. Solche Lösungen können Android-Benutzer vor datenstehlender Malware und vor dem Zugriff auf schädliche Websites schützen.

Verwaltung

Da Sie heutzutage viele unterschiedliche mobile Geräte verwalten müssen, brauchen Sie unbedingt eine einfache Lösung, die Ihren Mitarbeitern erstens ein mobiles Arbeiten ermöglicht und zweitens Ihre IT entlastet.

Self-Service-Portal

Wir empfehlen eine EMM-Lösung mit einem umfassenden Self-Service-Portal. Das reduziert den Arbeitsaufwand Ihrer IT und ermöglicht es Ihren Benutzern, viele einfache Aufgaben selbst zu erledigen. Denn schließlich sind die Benutzer selbst die ersten, die wissen, ob sie ein neu gekauftes Gerät für die Arbeit verwenden möchten oder ob ein Gerät verloren gegangen ist bzw. gestohlen wurde. Ihr Self-Service-Portal sollte die Benutzer mit einfachen Schritten durch die selbst zu übernehmenden Aufgaben führen.

Ein Self-Service-Portal ermöglicht es Benutzern:

- Eigene Geräte selbst zu registrieren und den unternehmensinternen Richtlinien zur Nutzung mobiler Geräte zuzustimmen
- Den Compliance-Status im Self-Service-Portal und auf dem Gerät anzuzeigen
- Tipps zu erhalten, wie die Compliance erreicht werden kann
- Die eigenen Geräte per Fernabfrage zu orten, zu sperren, Daten zu löschen oder das Passwort zurückzusetzen
- Die eigenen Geräte außer Betrieb zu setzen

Konfiguration und Wartung

Bei der Wahl einer Lösung sollten Sie auch darauf achten, dass die Lösung, für die Sie sich entscheiden, einfach zu installieren, zu konfigurieren und zu warten ist. Ein System, das drahtlos von einer Web-Konsole aus eingerichtet und konfiguriert werden kann, beschleunigt die Bereitstellung und reduziert den Arbeitsaufwand Ihrer IT.

Im Folgenden finden Sie eine kurze Checkliste, die Ihnen helfen soll zu überprüfen, wie einfach die Konfiguration, Verwaltung und Wartung Ihres EMM ist.

- Wie schnell kann das System eingerichtet und in Betrieb genommen werden?
- Kann das System Benutzern oder Gruppen auf Basis ihrer AD-Gruppenzugehörigkeit automatisch Profile und Richtlinien zuweisen?
- Kann Ihre EMM-Lösung ein Gerät automatisch richtlinienkonform rendern und erhalten Sie die Kontrolle darüber, ob ein Benutzer Unternehmens-E-Mails abrufen/empfangen darf?
- Können Sie alle Geräte, z. B. iOS, Android und Samsung SAFE, direkt im EMM-System konfigurieren? Oder müssen Sie auf die separate iPhone Configuration Utility zurückgreifen?
- Ist der Workflow optimiert, und wie einfach finden Sie die Daten, die Sie für die Verwaltung von Geräten und Richtlinien benötigen?
- Können Sie mobile Geräte jederzeit und von überall aus verwalten?
- Wie sieht die Benutzeroberfläche aus? Werden die Informationen so angezeigt, dass Sie alle Daten schnell und problemlos finden und Probleme mit nur wenigen Klicks lösen können?

Bereitstellungsarten

Wir empfehlen eine EMM-Lösung mit einer Reihe von Bereitstellungsoptionen, da Sie so das ideale Bereitstellungsmodell für Ihr Unternehmen auswählen können.

- Lokal: Software, die auf lokalen Servern vor Ort installiert und verwaltet wird. Bei dieser Version bleiben alle Daten in Ihrem Unternehmen.
- SaaS: Bei dieser Variante erfolgt die komplette Verwaltung über eine webbasierte Konsole, ohne dass Software installiert oder aktualisiert werden muss.

Unternehmen, die nach einer einfachen, integrierten webbasierten Konsole und stabiler Sicherheit für mobile Geräte suchen, empfehlen wir Sophos Cloud Mobile (enthält auch Schutz für Windows und Mac). Weitere Informationen finden Sie unter www.sophos.de/cloud.

Wie gut ist das Angebot Ihres EMM-Anbieters?

Um herauszufinden, wie gut das Angebot Ihres EMM-Anbieters ist, sollten Sie noch weitere Faktoren berücksichtigen:

1. **Flexibilität bei der Bereitstellung:** Bietet Ihr EMM-Anbieter sowohl eine lokale Verwaltung als auch eine cloudbasierte Version an?
2. **Benutzerbasierte Lizenzierung:** Da viele Benutzer heutzutage mehrere mobile Geräte (Smartphone, Tablet) mit ins Büro bringen, können die Kosten für Lizenzen schnell ins Uferlose steigen. Zahlen Sie bei Ihrem EMM-Anbieter pro Gerät (pro Knoten) oder ist das Preismodell benutzerbasiert?
3. **Support:** Leistet Ihr EMM-Anbieter 24-Stunden-Support?
4. **Datenschutz:** Da Daten immer öfter auf mobilen Geräten ausgetauscht und bearbeitet werden, sollte der von Ihnen gewählte EMM-Anbieter unbedingt Daten auf mobilen Geräten verschlüsseln können, damit Ihre Unternehmensdaten auch dort sicher bleiben.
5. **Langfristige Überlebensfähigkeit:** EMM ist noch relativ jung und wird von vielen kleinen Start-ups angeboten. Sie sollten sicherstellen, dass Ihr Anbieter auch langfristig überlebensfähig ist und nicht schon bald vom Wettbewerb übernommen wird.
6. **Zusätzliche Sicherheit für Android-Geräte:** Achten Sie darauf, dass Ihr EMM-Anbieter zusätzliche Anti-Malware- und Web-Schutz-Funktionen zum Schutz von Android-Geräten bietet.
7. **Innovationsfähigkeit:** Verfolgen Sie, wie schnell Ihr Anbieter innovative Lösungen auf den Markt bringt und sich an neue Entwicklungen anpasst. Hersteller mobiler Geräte bringen ständig neue Modelle auf den Markt. Ist Ihr EMM-Anbieter flexibel genug, um sich die jeweils neuesten Vorteile der Betriebssysteme zunutze zu machen (z. B. Windows Phone 8, Samsung SAFE oder KNOX von SAFE)?
8. **Umfassende IT-Sicherheit:** Hat Ihr Anbieter Komplett-Lösungen für alle Bereiche der IT-Sicherheit im Angebot? Ist er in der Lage, zusätzliche und integrierte Sicherheitslösungen für Ihre gesamte unternehmensinterne IT bereitzustellen?

Sophos Mobile Control

Kostenlose Testversionen auf
www.sophos.de/mobile

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

7.14.GH.bgde.simple

SOPHOS