SOPHOS
Security made simple.

Mobile Device Management Buyers Guide

Kontrolle durch die IT-Abteilung 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 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 Mobilplattform kann die Arbeit der IT-Abteilung vereinfachen. Beobachtet man die derzeitige Entwicklung, wird dies aber eher keine realistische Lösung sein. In der Praxis werden zahlreiche verschiedene Plattformen genutzt, was die ohnehin knappen Ressourcen der IT-Abteilungen noch stärker beansprucht. Viele IT-Experten prüfen daher Mobile Device Management-Systeme (MDM), die Ihnen helfen sollen, BYOD-Programme zu verwalten und komplexe Verwaltungsaufgaben zu vereinfachen.

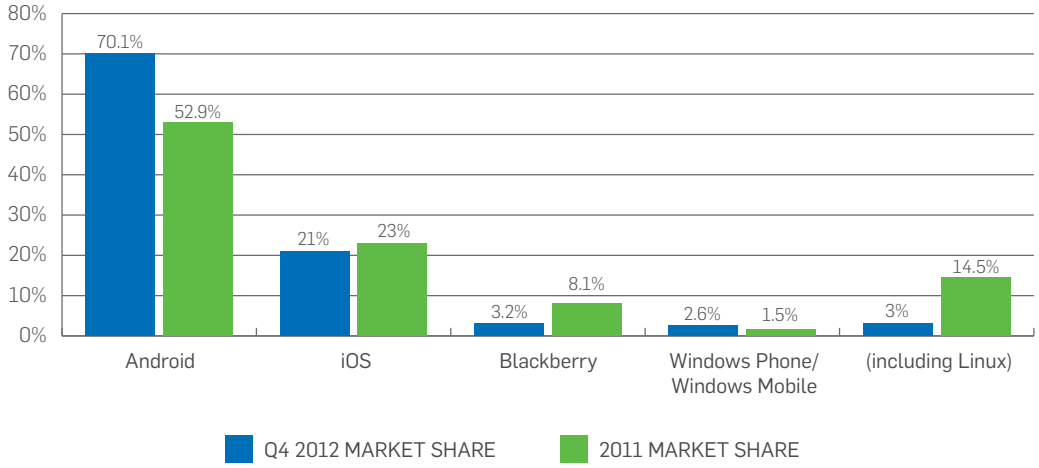

Abbildung 1: Marktanteile mobiler Betriebssysteme in den Jahren 2011 und 2012

Dieser MDM Buyers Guide hilft Ihnen bei der Auswahl der richtigen Mobile Device Management-Lösung für das BYOD-Programm Ihres Unternehmens. Hier finden Sie Informationen darüber, wie effiziente MDM-Systeme die BOYD-Strategien von Unternehmen optimal unterstützen, Konformität sichern und eine einfache zentrale Verwaltung von Geräten und Anwendungen ermöglichen. Darüber hinaus enthält dieser Leitfaden eine detaillierte Tabelle, in der die Funktionen der wichtigsten MDM-Anbieter verglichen werden.

Compliance- und Richtliniendurchsetzung

Eine MDM-Lösung schützt Unternehmensdaten durch die Durchsetzung unternehmensinterner Sicherheitsrichtlinien. 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-Experten können für die Richtliniendurchsetzung und Risikominderung MDM-Lösungen einsetzen.

Bevor ein Datenzugriff gewährt wird, muss das jeweilige mobile Gerät registriert sein. Verbindet sich ein registriertes Gerät, überprüft das MDM-System, ob das Gerät die Unternehmensrichtlinien einhält, z. B. bezüglich Jailbreaking, Passwortkonfiguration und unzulässiger Apps. Zusätzlich zur Standard-Compliance-Prüfung gibt es MDM-Lösungen, mit denen Sie unternehmensinterne Richtlinien zur Nutzung mobiler Geräte über ein Self-Service-Portal bereitstellen können. So gewährleisten Sie, 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

MDM-Lösungen lassen sich sehr gut einsetzen, um Maßnahmen zur Risikominderung zu ergreifen. Außerdem können Sie der Durchsetzung Ihrer Richtlinien mehr Nachdruck verleihen. Maßnahmen zur Risikominderung können je nach Schweregrad einer Richtlinienverletzung festgelegt werden. Bei kleineren Verstößen reicht es u. U. aus, den Benutzer zu informieren. Alternativ können Sie nicht richtlinienkonforme Geräte sperren, so dass diese keine Daten oder E-Mails aus dem Unternehmensnetzwerk mehr erhalten. 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 MDM-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, Ausführung eines Malware-Scans. Eine automatische Benachrichtigung des Benutzers bei Compliance-Problemen kann den Arbeitsaufwand für die IT-Abteilung erheblich reduzieren. Denn die Benutzer sind dann in der Lage, die meisten Fehler direkt selbst zu korrigieren – ohne das IT-Helpdesk zu bemühen.

Sicherheit für Daten und digitale Inhalte

Eine MDM-Lösung dient der zentralen Bereitstellung von Sicherheits- und Verwaltungsfunktionen für mobile Geräte, um auf diesen Geräten gespeicherte oder über sie abgerufene Unternehmensdaten zu schützen. Eine umfassende Strategie für die Nutzung mobiler Geräte muss alle Anwendungsbereiche abdecken und berücksichtigen, dass die Nutzer dabei mit Unternehmensdaten arbeiten.

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

Die Möglichkeit, verlorene gegangene Geräte remote zurückzusetzen, ist unverzichtbar und fester Bestandteil der meisten MDM-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. Das reduziert nicht nur den Arbeitsaufwand für die IT, sondern erhöht auch die Effizienz. Denn in der Regel weiß der Benutzer als erster, dass sein Gerät verloren gegangen ist oder gestohlen wurde, und kann dann sofort die entsprechenden Maßnahmen ergreifen.

Über die Sicherung der auf den Geräten gespeicherten Daten hinaus sollte die IT auch sämtliche Möglichkeiten der Benutzer kennen, mit denen diese auf Daten zugreifen, sie weiterleiten oder bearbeiten können. Versenden sie Dokumente per E-Mail an sich selbst? Nutzen sie cloudbasierte Dateifreigaben? Um Datenverluste zu verhindern, müssen Sie Ihre Daten überall verschlüsseln und Geräte vor Malware schützen. Im Idealfall bietet ein Anbieter ein Komplettpaket aus Lösungen, das all diese Anforderungen abdeckt. Ein solches Komplettpaket vereinfacht die Verwaltung der IT-Sicherheit und senkt die Gesamtkosten. Ein Beispiel hierfür ist eine Verschlüsselungslösung, die Daten verschlüsselt, bevor diese in der Cloud hochgeladen werden, autorisierten mobilen Geräten aber weiterhin erlaubt, auf die in der Cloud gespeicherten Informationen zuzugreifen.

Schutz vor mobiler Malware

Schädliche Apps oder Anwendungen mit Sicherheitslücken sowie mobile Malware bereiten IT-Experten große Sorgen. Um die Sicherheit Ihrer mobilen Geräte unter Kontrolle zu haben, sollten Sie sich für eine Lösung entscheiden, bei der Sie mobile Sicherheitsanwendungen in Ihre MDM-Konsole integrieren können. So verwalten Sie alle Sicherheitsbereiche von einer Konsole aus.

Darüber hinaus ist für Android-Benutzer eine Sicherheitslösung mit Web-Schutz dringend zu empfehlen, da die meisten Infektionen aus dem Internet stammen. Im Folgenden finden Sie eine kurze Liste der Funktionen, die für die Mobile Security App in einer MDM-Lösung empfohlen werden:

- Verwaltung des Malware-Schutzes
- Auslösen eines Scans, wenn die Mobile Security App nicht mehr aktuell ist
- Automatisches Sperren infizierter oder sicherheitstechnisch veralteter Geräte
- Blockieren oder Zulassen verdächtiger bzw. potenziell unerwünschter Apps (PUAs)
- Schutz für Android-Benutzer vor gefährlichen Webseiten
- Schutz der Benutzer vor störendem Text- und Anrufer-Spam

Sicherheitsfunktionen auf einen Blick

Sicherheitsanbieter mit MDM

✓= JA X = NEIN

Funktion	Sophos	Symantec	McAfee	Kaspersky	Trend
COMPLIANCE-ÜBERPRÜFUNG UND -DURCHSETZUNG					
Geräte mit Jailbreak/gerootete Geräte zulassen oder nicht zulassen	✓	✓	✓	✓	✓
Auf Side-Loading überprüfen	✓	✓	✓	X	✓
Mindestversion des Betriebssystems durchsetzen	✓	✓	✓	X	✓
Geräte-Verschlüsselung durchsetzen	✓	✓	✓	✓	✓
Whitelist- oder Blacklist-Apps	✓	✓	✓	✓	✓
Erforderliche Apps durchsetzen	✓	✓	✓	✓	X
FUNKTIONEN ZUR RISIKOMINDERUNG					
Sperrung des E-Mail-Zugangs basierend auf Compliance-Status	✓	✓	✓	X	X
Administrator benachrichtigen	✓	✓	✓	✓	✓
Möglichkeit zur Kontrolle der Netzwerkfreigabe	✓	✓	X	X	X
Automatische Ausführung risikomindernder Maßnahmen	✓	✓	✓	X	X
SICHERHEIT FÜR GERÄTE, DATEN UND INHALTE					
Orten, Sperren und Zurücksetzen	✓	✓	✓	✓	✓
Unternehmensseitiges Zurücksetzen	✓	✓	✓	✓	✓
FUNKTIONEN ZUM MOBILEN MALWARE-SCHUTZ (INTEGRIERT IM MDM)					
Apps bei der Installation scannen	✓	✓	X	X	✓
Anti-Malware-Scans remote auslösen	✓	✓	X	X	✓
Schadanwendungen (Malware) blockieren	✓ (SMSec 3.0)	✓	X	X	X
Sicheres Surfen im Internet	✓	✓	X	X	✓
UMFASSENDE SICHERHEITSLÖSUNG/INTEGRATIONSFÄHIGKEIT DES ANBIETERS					
Complete Security-Anbieter	✓	X Mobile Suite, ohne vollständige EP+Mobile Suite	✓ Per EPO	✓	✓

Sicherheitsfunktionen auf einen Blick

Reine MDM-Anbieter

✓= JA X = NEIN

Funktion	Sophos	AirWatch	MobileIron	Good Technology
COMPLIANCE-ÜBERPRÜFUNG UND -DURCHSETZUNG				
Geräte mit Jailbreak/gerootete Geräte zulassen oder nicht zulassen	✓	✓	✓	✓
Auf Side-Loading überprüfen	✓	✓	✓	✓
Mindestversion des Betriebssystems durchsetzen	✓	✓	✓	✓
Geräte-Verschlüsselung durchsetzen	✓	✓	✓	✓
Whitelist- oder Blacklist-Apps	✓	✓	✓	✓
Erforderliche Apps durchsetzen	✓	✓	✓	✓
FUNKTIONEN ZUR RISIKOMINDERUNG				
Sperrung des E-Mail-Zugangs basierend auf Compliance-Status	✓	✓	✓	✓
Administrator benachrichtigen	✓	✓	✓	✓
Möglichkeit zur Kontrolle der Netzwerkfreigabe	✓	✓	✓	X
Automatische Ausführung risikomindernder Maßnahmen	✓	✓	✓	✓
SICHERHEIT FÜR GERÄTE, DATEN UND INHALTE				
Orten, Sperren und Zurücksetzen	✓	✓	✓	✓
Unternehmensseitiges Zurücksetzen	✓	✓	✓	✓
FUNKTIONEN ZUM MOBILEN MALWARE-SCHUTZ (INTEGRIERT IM MDM)				
Apps bei der Installation scannen	✓	X	X	X
Anti-Malware-Scans remote auslösen	✓	X	X	X
Schadanwendungen (Malware) blockieren	✓ (SMSec 3.0)	X	X	X
Sicheres Surfen im Internet	✓	✓	✓	✓
UMFASSENDE SICHERHEITSLÖSUNG/INTEGRATIONSFÄHIGKEIT DES ANBIETERS				
Complete Security-Anbieter	✓	X	X	X

Nativer Ansatz oder Container-Ansatz

Nahezu alle MDM-Lösungen auf dem Markt bieten Funktionen zur Sicherheit, Geräte- und Anwendungsverwaltung sowie zur Compliance. Dabei gibt es zwei verschiedene Herangehensweisen: den nativen Ansatz und den Container-Ansatz.

Anbieter, die mit dem nativen Ansatz arbeiten, nutzen die systemeigenen Funktionen des Geräts. Welche Funktionen des Geräts genutzt werden können, hängt jedoch davon ab, was das installierte Betriebssystem zulässt. Vorteil dieses Ansatzes: Der Benutzer kann sein Gerät wie gewohnt ohne Einschränkungen verwenden.

Ebenfalls für diesen Ansatz spricht die rasante Weiterentwicklung mobiler Betriebssysteme. Die neueren mobilen Geräte werden bereits über viele zusätzliche Sicherheitsfunktionen verfügen. Wenn Sie sich für den nativen Ansatz entscheiden, können Sie von neuen Sicherheitsfunktionen profitieren, die bei Betriebssystem-Updates automatisch hinzukommen. Es ist daher sinnvoll, sich für einen flexiblen Anbieter zu entscheiden, der mit den schnellen Entwicklungen bei mobilen Geräten und Betriebssystemen Schritt halten kann.

Beim Container-Ansatz werden Anwendungen, die auf Unternehmensdaten zugreifen können, in einem "Container" von anderen Anwendungen isoliert.

Da E-Mails, Kalender und Kontakte die am häufigsten verwendeten mobilen Anwendungen darstellen, konzentrieren sich die meisten Anbieter von Container-Apps auf die Bereitstellung eines separaten E-Mail-Clients und die Bereitstellung separater Funktionen für Kalender und Kontakte. Der Nachteil dieses Ansatzes ist die eingeschränkte Benutzerfreundlichkeit. So kann sich z. B. die Akkulaufzeit des Geräts erheblich verringern.

Endnutzer möchten durch die Verwendung des eigenen mobilen Geräts eine möglichst ausgewogene Work-Life-Balance erzielen. Da der Container-Ansatz die Benutzerfreundlichkeit und die Gerätefunktionen beeinträchtigt, ist es nicht verwunderlich, dass viele Benutzer diesen Ansatz ablehnen.

Bevor Sie sich für einen der beiden Ansätze entscheiden, sollten Ihre IT-Experten sorgfältig zwischen Risiko und Benutzerfreundlichkeit abwägen. Wenn es in Ihrem Unternehmen nicht zwingend erforderlich ist, Risiken um jeden Preis auszuschließen, ist der Container-Ansatz für Sie wahrscheinlich nicht die beste Wahl.

Zentrale Verwaltung mobiler Geräte und Anwendungen

In der Praxis zeigt sich, dass Endnutzer durchaus bereit sind, ein bestimmtes Maß an Kontrolle über ihre mobilen Geräte abzugeben, 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

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 MDM-Lösung, die es Ihnen leicht macht, die mobilen Geräte in Ihrer Umgebung während der gesamten Lebensdauer 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 Application Management

Stellen Sie Ihren Mitarbeitern die Tools zur Verfügung, die diese für ihre Arbeit brauchen. In einer BYOD-Umgebung kann das bedeuten, dass Sie eine Vielzahl an Apps bereitstellen müssen. Das Mobile Application Management (MAM), das in Ihrer MDM-Lösung enthalten ist, unterstützt Sie bei der Verwaltung dieser Apps. So können Sie zum Beispiel erforderliche Unternehmensanwendungen per Push-Übertragung an die Geräte senden, zulässige Apps auf eine Whitelist und unzulässige Apps auf eine Blacklist setzen.

Enterprise App Store

Ein Enterprise App Store ermöglicht es Ihnen, Ihren Benutzern empfohlene und erforderliche Apps direkt auf dem mobilen Gerät bereitzustellen. Sowohl Ihre unternehmenseigenen Apps als auch solche aus dem App Store werden auf dem mobilen Gerät des Benutzers angezeigt, und dieser kann durch einen einfachen Klick die Installation starten.

Darüber hinaus bietet ein Enterprise App Store folgende Vorteile:

- Sichere Verteilung empfohlener und vom Unternehmen entwickelter Apps
- Festlegen zulässiger Softwarepakete in der Verwaltungskonsole und Übertragung an einzelne Geräte, Gruppen oder Plattformen
- Verteilung iOS-verwalteter Apps an Benutzer und bei Bedarf Löschen der Apps einschließlich aller zugehörigen Daten
- Sperrung alternativer App Stores
- Anzeige aller Apps, die auf einem bestimmten Gerät installiert sind

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 Ihnen, sich für eine MDM-Lösung zu entscheiden, die ein integriertes Self-Service-Portal beinhaltet. 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 Richtlinienkonformität erreicht werden kann
- Ihre Geräte per Fernabfrage zu orten, zu sperren, Daten zu löschen oder ihr Passwort zurückzusetzen

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 MDM 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?
- Bietet das System die Möglichkeit, den Gerätestatus automatisch in den Compliance-Status zu setzen, und können Sie festlegen, ob der Benutzer für den E-Mail-Empfang autorisiert ist?
- Können Sie alle Ihre Geräte, einschließlich iOS, Android- und Samsung SAFE-Geräte, direkt im MDM-System konfigurieren? Oder benötigen Sie ein separates iPhone-Konfigurations-Dienstprogramm?
- Ist der Workflow optimiert, und wie einfach finden Sie die Daten, die Sie für die Verwaltung von Geräten und Richtlinien benötigen?
- Können Richtlinien over-the-air bereitgestellt werden?
- Können Sie mobile Geräte jederzeit und von überall 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?
- Unterstützt das System das Simple Certificate Enrollment Protocol (SCEP) zur Bereitstellung von Zertifikaten, die Ihre unternehmenseigenen und privaten Mitarbeitergeräte benötigen, um auf Ihr Netzwerk und weitere Ressourcen zugreifen zu können?

Bietet Ihnen Ihr MDM-Anbieter all diese Optionen?

Sie sollten auch andere Faktoren in Ihre Entscheidung für einen MDM-Anbieter mit einbeziehen. Stellen Sie Ihrem Anbieter folgende Fragen:

1. **Flexibilität bei der Bereitstellung:** Bietet Ihr MDM-Anbieter sowohl eine lokale Verwaltung als auch eine cloudbasierte Version an?
2. **Benutzerbasierte Lizenzierung:** Da viele Benutzer mehrere mobile Geräte mitbringen (Smartphone, Tablet), können die Lizenzierungskosten rasch außer Kontrolle geraten. Rechnet Ihr Anbieter pro Gerät (pro Knoten) ab oder bietet er eine benutzerbasierte Preisgestaltung an?
3. **Support:** Erhalten Sie bei Ihrem Anbieter einen Rund-um-die-Uhr-Support?
4. **Langfristige Überlebensfähigkeit:** Mobile Device Management ist noch relativ jung und wird von vielen kleinen Start-Up-Anbietern angeboten. Sie sollten sicherstellen, dass Ihr Anbieter auch langfristig überlebensfähig ist und nicht schon bald vom Wettbewerb übernommen wird.
5. **Innovationsfähigkeit:** Bewerten Sie die Geschwindigkeit, mit der Ihr Anbieter innovative Lösungen auf den Markt bringt und sich an neue Entwicklungen anpassen kann. Hersteller mobiler Geräte bringen in rasanter Geschwindigkeit immer neue Modelle und Versionen auf den Markt. Ist Ihr MDM-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) ?
6. **Umfassende IT-Sicherheit:** Bietet Ihr Anbieter Komplett-Lösungen für alle Bereiche der IT-Sicherheit? Ist er in der Lage, zusätzliche und integrierte Sicherheitslösungen für Ihre gesamte unternehmensinterne IT bereitzustellen?

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

Oxford, GB | Boston, USA

7.13.GH.bgna.simple

SOPHOS