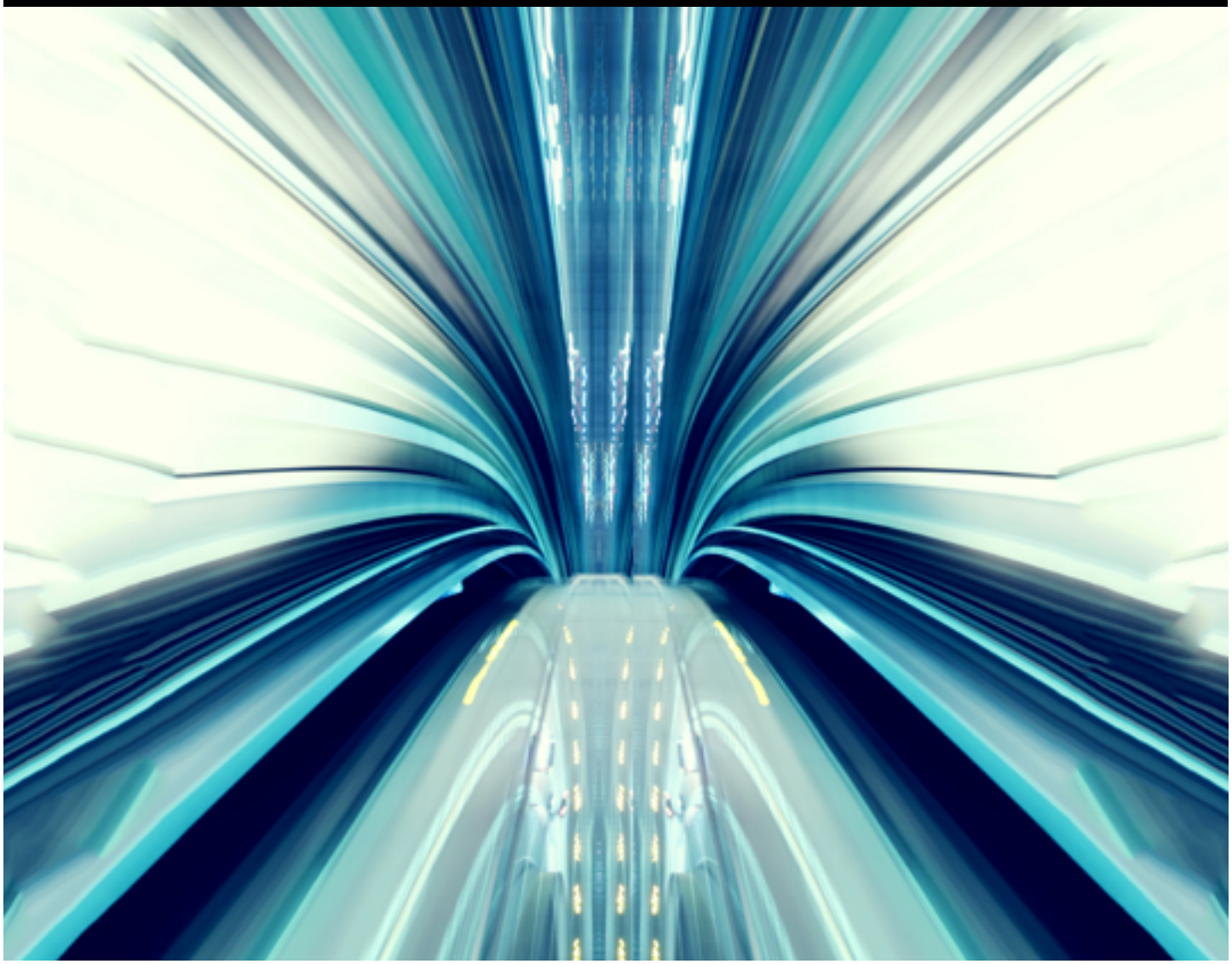
BlackBerry

Whitepaper



Unified Endpoint Management (UEM) – ein Leitfaden für CIOs

10 wichtige Qualitätskriterien

Wie entwickelt man eine belastbare Mobilitätsstrategie?

Je mobiler Ihr Unternehmen wird, desto tiefer muss Ihre Mobilitätsstrategie greifen. Die Voraussetzung zur Mobilisierung von Business Apps ist dabei in jedem Fall eine sichere, umfassende, einheitliche und zukunftsfähige Plattform.

Was kann UEM leisten?
Eine durchdachte Unified Endpoint Management (UEM) Lösung umfasst mobile Apps für fast jede Aufgabe sowie ihre Verwaltung, Sicherheit und Integrität auf mobilen Geräten, Desktops und an allen anderen Endpunkten sowie in der Cloud. Inklusive des Internet of Things (IoT).

Sie ermöglicht:

- Höhere Produktivität und Effizienz
- Mehr Mitarbeiterzufriedenheit
- Kosteneinsparung und Maximierung des mobilen ROI
- Bessere Kundenbindung
- Neue Ertragsmöglichkeiten
- Zuverlässiges Digital Rights Management (DRM)
- Vereinfachte Administration

Definieren Sie Ihren gewünschten Mobilitätsgrad

Stufe 1: Unified Endpoint Management (UEM) & Messaging
Stufe 2: Mobile Zusammenarbeit
Stufe 3: Mobilisierung bestehender Geschäftsprozesse
Stufe 4: Entwicklung neuer Geschäftsprozesse

Überprüfen Sie Ihre UEM-Plattform auf 10 Schlüsselfaktoren

1. **Multi-Plattform Endpoint Management**
2. **Mobile Sicherheit und Verwaltung geschäftlicher Apps**
3. **Sicherheitszertifikate und Zugangsdaten**
4. **Schutz der Privatsphäre**
5. **Dokumentenkontrolle**
6. **Bereitstellungsmodul (Cloud/On-Premise)**
7. **Migration und Implementierung**
8. **Technischer Support**
9. **Schulung und Anwenderfunktionen**
10. **Preise und Kosten**

Leistungsmerkmale der BlackBerry Enterprise Mobility Suite

16 der G20-Regierungen, die 10 größten Anwaltskanzleien, 5 von 5 der größten Öl- und Gasunternehmen und über die Hälfte der Fortune 100 Unternehmen einschließlich aller F100 Geschäftsbanken haben sich aus guten Gründen für BlackBerry UEM12 entschieden:

- Sichere mobile Apps
- Konsistente Multi-Plattform Richtlinien
- Umfassende Kontrollen für Betriebssysteme iOS, Android, Android for Work, Samsung Knox, Windos, macOS, BlackBerry – unabhängig vom Eigentumsmodell und Nutzergruppe
- Schlüsselfertige Lösung
- Sicher durch Container- und Sicherheitsrichtlinien über das Betriebssystem hinweg sowie Trennung geschäftlicher und persönlicher Inhalte
- Tools, APIs, Infrastruktur und Software für plattformübergreifende App-Entwicklung
- Höchste Sicherheit auch für streng regulierte Branchen
- Kontrolle durch integriertes DRM
- Flexible und kostengünstige Anpassung
- Unterstützt Einhaltung höchster Sicherheitsanforderungen und gesetzlicher Vorschriften

So nutzen Sie diesen Leitfaden

Dieser Leitfaden basiert auf den Erfahrungen erfolgreicher Fortune 500 Unternehmen und gewährt Ihnen einen Einblick in die Erkenntnisse führender Analysten und Experten. Er unterstützt Sie dabei, eine belastbare Mobilitätsstrategie für Ihr Unternehmen zu entwickeln.

Neben individuellen Anforderungen müssen Sie aber noch vieles mehr beachten. Auch wenn der Weg steinig erscheint, sollten Sie ihn gut planen und in Ruhe gehen. Sie sparen auf lange Sicht viel Zeit, Geld und schonen Ihre Nerven. Und erreichen sicher ein lohnendes Ziel.

Vor nicht allzu langer Zeit sahen Unternehmen Mobilität noch als isoliertes Projekt. Die Herausforderung der Anfangszeit bestand in der Mobilisierung von E-Mails. Seither hat sich viel getan. Mobilität ist eine zentrale Strategiefrage geworden. Das Hauptaugenmerk liegt auf der Mobilisierung von Business Apps. Einzellösungen für das Mobile Device Management sind nicht länger gefragt. Alles dreht sich um eine sichere, umfassende, einheitliche und zukunftsfähige Plattform für mobile Apps.

Da cloudbasierte Unternehmensanwendungen die mobile Produktivität signifikant verbessern sollen, benötigen Mitarbeiter jederzeit und überall Zugriff auf sensible Unternehmensinhalte. Dadurch verschieben sich die traditionellen Sicherheitsgrenzen. Denn wichtige Dokumente müssen auch außerhalb der eigenen Firewall sicher geteilt werden können.

Mittlerweile befinden sich auch die vertraulichsten Daten auf mobilen Geräten. Sie werden auf Desktops und Laptops übertragen und in öffentlichen, privaten oder persönlichen Clouds gespeichert.

Diese Entwicklung bietet hervorragende Möglichkeiten zur Steigerung von Produktivität, Mitarbeiterzufriedenheit, Kundenbindung und unternehmerischer Effizienz. Doch um die Herausforderungen der Mobilität bewältigen zu können, braucht es eine gründliche Vorbereitung.

Wie sehr die neuen technischen Möglichkeiten die Mobilität verändern, zeigt sich an den Abkürzungen und Bezeichnungen. Was gestern noch MDM oder EMM hieß, nennt sich nun UEM und umfasst Verwaltung, Sicherheit und Identität von mobilen Geräten, Desktops und anderen Endpunkten. Die wachsende Zahl von Anwendern und die immer neuen Anforderungen des Internet of Things sind eine große Herausforderung. Die modernsten Lösungen sorgen mit einer einheitlichen Plattform für die nötige Transparenz und Kontrolle über alle Endpunkte hinweg.

Eine belastbare mobile Strategie bietet Ihnen erhebliche Vorteile. Sie ermöglicht es Ihnen, mit den neuesten Mobilitätstrends Schritt zu halten. Sie verbessert die mobile Produktivität und sorgt für Sicherheit sowie den Schutz der Privatsphäre. Zudem vereinfacht sie die Administration. Ein wesentlicher Aspekt angesichts der wachsenden Zahl an Rollen, Apps, Betriebssystemen und Gerätetypen.

Mobilität ist wie eine Reise. Bevor Sie starten, sollten Sie erst einmal eine Bestandsaufnahme machen und herausfinden, welchen Grad der Mobilität Ihr Unternehmen erreicht hat. So finden Sie leichter eine Lösung, die Ihre aktuellen und zukünftigen mobilen Anforderungen erfüllt.

Vorbereitung der Mobilitätsstrategie

Ohne eine mobile Strategie ist die richtige Entscheidung über eine langfristige Lösung nahezu unmöglich. Halten Sie deshalb die wichtigsten Anforderungen und Erwartungen Ihres Unternehmens an Mobilität detailliert fest. Führen Sie im ersten Schritt eine Bedarfsanalyse durch und klären Sie die Anforderungen mit Ihren Stakeholdern ab. Wenn Sie alle Beteiligten einbeziehen, laufen Sie nicht so schnell Gefahr, wichtige Anforderungen zu übersehen. Folgende Fragen sollten Sie unbedingt beantworten:

1. Haben Sie bereits eine Lösung, die Ihre aktuellen und künftigen Anforderungen erfüllt? Sind bereits Lücken bekannt und wo muss nachgebessert werden?

2. Kennen Sie Ihre Kosten für Mobilität?

3. Gelingt es Ihnen mühelos, Ihre Compliance- und Sicherheitsanforderungen zu erfüllen?

4. Wie sichern Sie Ihre geschäftlichen Daten – und auch die Ihrer Kunden – mobil und in der Cloud?

5. Wie sichern Sie die Zugangsdaten und Benutzerkonfigurationen Ihrer Mitarbeiter auf mobilen Geräten?

6. Wie gut schützen Sie die Privatsphäre Ihrer Mitarbeiter?

7. Wie begegnen Sie dem stetigen Wachstum bei Anwendern, Geräten und Daten?

8. Wie gehen Sie mit der Vielzahl der Anbieter und Lösungen in Ihrer mobilen Umgebung um? Haben Sie schon eine umfassende und einheitliche Lösung?

9. Welche Arten mobiler Apps (Native Apps, Web Apps, Hybride Apps) verwenden Sie bzw. brauchen Sie, um die Produktivität in Ihrem Unternehmen zu verbessern?

10. Bieten Sie Ihrer IT, den Eigentümern und Entwicklern von Apps eine gemeinsame Sicherheitsgrundlage? Können verschiedene Entwicklerteams die gleichen Sicherheits-funktionen für alle Arten von Apps anwenden?

Mobilitätsgrad

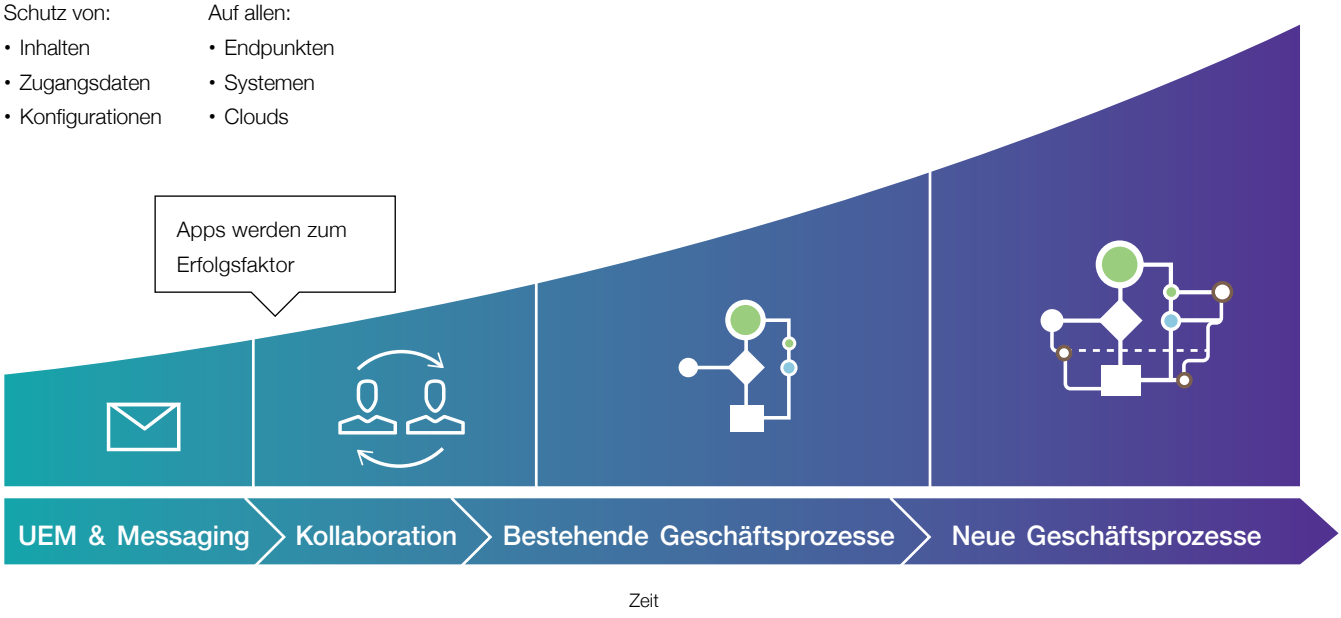
Es gibt vier Stufen des mobilen Reifegrades. Je mobiler Ihr Unternehmen wird, desto tief greifender die Maßnahmen. Konkret bedeutet das: neue Strategien annehmen, neue Tools integrieren, bestehende Geschäftsprozesse überarbeiten und neue Geschäftsmodelle entwickeln.

Gleichzeitig steigen die Sicherheitsanforderungen, da immer mehr Unternehmensanwendungen mobilisiert werden.

Der mobile Reifegrad

Schutz von:
- Inhalten
- Zugangsdaten
- Konfigurationen

Auf allen:
- Endpunkten
- Systemen
- Clouds



Basismobilität

Zu den ersten Investitionen gehören die Basisversion eines Endpoint Managements und mobile E-Mail. Hier kann schon ein kleines Budget zu schnellen Produktivitätsgewinnen führen, vor allem durch die Einführung von Bring Your Own Device (BYOD). Allerdings gehen mit der Gerätevielfalt auch neue Gefahren einher.

Herausforderungen dieser Phase

- Grundlegende geschäftliche Daten (E-Mails, Anhänge) auf mobilen Geräten schützen
- Den Nutzen mobiler Geräte erkennen
- Intern technisches Fachwissen aufbauen

Merkmale dieser Phase

- Sie haben erst kürzlich eine Lösung für das Device Management implementiert. Ihre Investitionen in Mobilität sind minimal und erfolgen nur projektbezogen.
- Sie haben die mobile App-Entwicklung noch nicht in Betracht gezogen.
- Sie haben verstanden, dass Mobilität für Ihre Geschäftsziele entscheidend ist, aber wissen noch nicht, wo Sie anfangen sollen.

Mobile Zusammenarbeit

Nutzen Mitarbeiter E-Mails und Anhänge regelmäßig mobil, wächst oft der Wunsch nach weiteren mobilen Anwendungen. Und angesichts der vielen Möglichkeiten fällt ein Verzicht schwer. Der nächste logische Schritt ist die Optimierung der mobilen Zusammenarbeit. Aber nur die wenigsten MDM-Plattformen können mobile Anwendungen zuverlässig sichern und geschäftliche Daten effizient schützen.

Herausforderungen dieser Phase

- Die wichtigsten Microsoft®-Anwendungen mobilisieren: Exchange, Office 365, SharePoint™, OneDrive for Business, Skype for Business, Dynamics CRM usw.
- Sicherheit und Kontrolle in den Workflow von Dokumenten implementieren
- Angenehmer mobiler Bedienkomfort
- Die Privatsphäre der Mitarbeiter schützen

Merkmale dieser Phase

- Ihre Investitionen in die Mobilität sind nach wie vor minimal bis moderat.
- Sie mobilisieren horizontale Business Apps für eine bessere Zusammenarbeit, wie SharePoint und Enterprise Instant Messaging (EIM).
- Je mehr Business Apps eingesetzt werden, desto mehr fürchten Sie sich vor Datenverlusten.
- Die Geschäftsbereiche fordern rollenbasierte, spezifische Anwendungen, um erfolgreicher zu arbeiten.

Mobilisierung bestehender Geschäftsprozesse

Mittlerweile können Ihre Mitarbeiter dank der mobilisierten Tools für Kollaboration und Kommunikation von nahezu überall aus komfortabel zusammenarbeiten. Die spürbaren Erleichterungen im Arbeitsalltag führen gewöhnlich dazu, dass Sie auch weiterhin mit der Unterstützung der Geschäftsbereiche rechnen können. Im nächsten Schritt geht es um die Mobilisierung bestehender Geschäftsprozesse und Anwendungen im großen Stil. Das ist der Zeitpunkt, an dem die meisten Unternehmen Lücken in ihrem App-Inventar entdecken und mit der Entwicklung eigener mobiler Apps beginnen.

Herausforderungen dieser Phase

- Mobile Apps und Initiativen mit bestehenden Geschäftsprozessen in Einklang bringen und Lücken mit individuellen Projekten füllen
- Neue Datenformen entstehen, neue Nutzung existierender Daten
- Mobile Anwendungen oder Prozesse in bestehende Infrastrukturen integrieren
- Sicherheitsrichtlinien und regulatorische Vorschriften zuverlässig einhalten

Merkmale dieser Phase

- Collaboration Apps werden gut angenommen. Die Mitarbeiter verlangen nach weiteren Apps.
- Sie mobilisieren bestehende Geschäftsprozesse und planen langfristig mobile Investitionen.
- Ihre Investitionen in die Mobilität sind moderat.
- Sie stellen Anwendungen zur Unterstützung wichtiger betrieblicher Einheiten wie Vertrieb, Führungskräfte und Außendienst bereit.
- Sie planen in naher Zukunft die Entwicklung von eigenen Anwendungen.
- Sie füllen Lücken mit benutzerdefinierten Apps für Geräte, Betriebssysteme und Clouds.
- Sie können mit Ihrer mobilen Plattform die drei wichtigsten Faktoren für sichere Mobilität verwalten: geschäftliche Inhalte, Zugangsdaten und Anwendungskonfigurationen.

Entwicklung neuer Geschäftsprozesse

Nach der Mobilisierung bestehender Geschäftsprozesse steht die Realisierung von Wettbewerbsvorteilen auf dem Plan. Es geht um Kosteneinsparungen, verbesserte Kundenbindung und die Schaffung neuer Ertragsmöglichkeiten. Jetzt können Sie Ihren mobilen ROI maximieren. Mobilität durchdringt Ihr gesamtes Unternehmen. Sie haben mobile Anwendungen für fast jede Aufgabe. Vorsicht ist aber angesagt, wenn die Vernetzung so weit fortgeschritten ist, dass die Verwaltung der Geräte und Applikationen kaum noch zu meistern ist. Wenn sie ineffizient und inkonsistent wird. In diesem Fall befinden Sie sich in der mobilsten Phase, im Pervasive Computing. Sensible geschäftliche Daten finden sich überall: auf Smartphones, Tablets, PCs und Wearables, auf Backend-Systemen, in öffentlichen und auch persönlichen Clouds. Sie brauchen jetzt ein zuverlässiges Digital Rights Management (DRM). Möglichst auf Dateiebene, um Ihre Daten umfassend zu schützen.

Herausforderungen dieser Phase

- Unternehmensanwendungen im großen Stil über Geräte, Betriebssysteme und Clouds hinweg verwalten
- Backend zur Unterstützung neuer mobiler Anwendungen, Geschäftsmodelle und Geräte entwickeln
- Aufbau und Entwicklung von Identitätsmanagement und Mechanismen zur Authentifizierung mit Single Sign-on, einschließlich Cloud Services
- Mobile App-Entwicklung mit bestehenden geschäftlichen Anforderungen in Einklang bringen

Merkmale dieser Phase

- Ihre Endpoint Management Lösung ist ein wesentlicher Teil der Mobilitätsverwaltung.
- Sie verwalten Daten, Dokumente und Rollen zusammen mit Anwendungen und Geräten.
- Sie haben begonnen, benutzerdefinierte, interne Anwendungen bereitzustellen.
- Ihre Investitionen in die Mobilität sind moderat bis hoch.
- Ihr Unternehmen nutzt neue Geschäftsmodelle und maximiert damit den Return on Investment bei der Mobilität.

Sieben zentrale Herausforderungen

1. Sicherheit für Unternehmensinhalte, Zugangsdaten und Gerätekonfigurationen inklusive Schutz vor Datenverlusten.

2. Anpassungsfähigkeit an aktuelle und zukünftige Anforderungen bei gleichzeitiger Integration von UEM in die wichtigsten Systeme und Prozesse.

3. Bedienkomfort, damit die mobile Arbeit nicht unnötig erschwert wird und Mitarbeiter auf eigene Faust nach Lösungen suchen.

4. Schutz von Dateien in Cloud-Anwendungen und auf mobilen Geräten.

5. Konsistente Sicherheitsmodelle über Anwendungen hinweg trotz unterschiedlicher Entwicklungstechnologien (für native Apps, HTML5, hybride Entwicklungsumgebungen usw.).

6. Skalierung der Mobile Management Infrastruktur.

7. Bereitstellung des mobilen technischen Supports für das gesamte Unternehmen.

Schlüsselfaktoren bei der Auswahl einer UEM-Plattform

Wenn Sie den Mobilitätsgrad Ihres Unternehmens kennen, dann können Sie die Probleme eingrenzen, die Sie in naher Zukunft lösen müssen. Und durch vorausschauende Planung sorgen Sie dafür, dass Ihre Mobilitätsstrategie auch langfristig mit den Unternehmenszielen übereinstimmt.

Die folgende Liste erhebt keinen Anspruch auf Vollständigkeit. Sie gibt Ihnen aber einen Überblick über die wichtigsten Faktoren, die Sie berücksichtigen müssen, um die beste Lösung für alle Beteiligten zu finden.

1. Multi-Plattform Endpoint Management
2. Mobile Sicherheit und Verwaltung von Apps
3. Sicherheitszertifikate und Zugangsdaten
4. Schutz der Privatsphäre
5. Dokumentenkontrolle
6. Bereitstellungsmodell (Cloud oder On-Premise)
7. Migration und Implementierung
8. Technischer Support
9. Schulung und Anwenderfunktionen
10. Preise und Kosten

1. Multi-Plattform Endpoint Management

Sind bei Ihnen mehrere mobile Betriebssysteme, Gerätetypen und Eigentumsmodelle gleichzeitig im Einsatz, müssen Sie sicherstellen, dass Ihre UEM-Lösung all diese Geräte verwalten kann. Je nach Rolle und Anwendungsfall. Für interne und externe Mitarbeiter, für vertrauliche und weniger sensible Daten, für gemeinsam genutzte Geräte, Desktop- und Kiosk-Systeme. Denken Sie perspektivisch. Behalten Sie sowohl Ihre aktuellen Plattformen als auch mögliche Neue im Auge wie beispielsweise Android™ for Work, Samsung Knox Workspace und iOS Managed Apps.

Deshalb sollte Ihre neue Plattform alles über eine einheitliche Konsole verwalten können: Benutzergruppen, administrative Rollen, Softwarekonfigurationen, E-Mail-Profile, IT-Richtlinien und vieles mehr. Angesichts der Tatsache, dass Ihre IT schon mehr als genug Herausforderungen meistern muss, sollte Ihre neue Plattform außerdem eine benutzerfreundliche und intuitive Benutzeroberfläche besitzen.

Dies sind die wichtigsten Anforderungen an eine nachhaltige UEM-Lösung:

Anwender einfach einrichten und registrieren. Ihre Mitarbeiter sollten sich selbst und einfach Over-the-Air anmelden können. Die Optimierung dieses Prozesses erhöht die Zufriedenheit der Anwender und senkt die Supportkosten.

Umfangreiche Richtlinienkontrollen aktivieren. Sie müssen alle Richtlinien für Ihr Unternehmen definieren und bereitstellen können: seien es Passwörter, Geräteverschlüsselung, Kamera, Wi-Fi®, VPN und vieles mehr. Bei Verlust, Diebstahl oder Ersatz eines Geräts sollten Sie geschäftliche Daten löschen können, ohne persönliche Inhalte oder Apps zu beeinträchtigen.

Support zur Einhaltung gesetzlicher Vorschriften oder hoher Sicherheitsanforderungen. Regulierte Branchen wie Finanzdienstleistungen, Gesundheitswesen, Recht und Regierung müssen für die Sicherheit von Kunden-, Finanz- und sonstigen vertraulichen Daten zahlreiche Bestimmungen erfüllen. Dies kann nicht mal schnell nebenbei erledigt werden, sondern ist oft mit einem enormen Aufwand verbunden. Ihre UEM-Lösung sollte daher gesetzeskonform angelegt sein. Anhand der Sicherheitszertifikate und Akkreditierungen können Sie erkennen, welche Lösungen Ihre spezifischen Anforderungen erfüllen.

Jailbreak/Rooting automatisch erkennen. Für Anwender kann das „Hacken“ eines Geräts durchaus verlockend sein. Es bietet mehr Freiheit bei der Funktionsauswahl auf einem Smartphone oder Tablet. Zugleich stellt es ein erhebliches Sicherheitsrisiko dar, wenn integrierte Sicherheitsvorkehrungen eines Betriebssystems deaktiviert werden. Diese Geräte werden sehr anfällig für Malware und gezielte Angriffe. Ihre UEM-Lösung muss diese Attacken automatisch erkennen und beseitigen können. Und zwar mit einer Software, die den Status eines Geräts tarnt. Zudem sollten Jailbreak und Root Detection nicht auf Standortdienste angewiesen sein. Denn das schont den Akku und schützt die Privatsphäre der Anwender.

2. Mobile Sicherheit und Verwaltung von Apps

Sicherheit durch Containerization

Containerisierte Apps bieten Ihnen detaillierte Kontrolle, denn jede App befindet sich mit den dazugehörigen Daten in einem eigenen, verschlüsselten Dateispeicher. Dadurch können Sie jeden App-Container mit eigenen Nutzungsregeln und Richtlinien belegen, separat schützen und nach Bedarf löschen. Persönliche Apps, die vom Besitzer des Geräts installiert werden, können sich gefahrlos neben genehmigten fremden oder firmeneigenen Apps befinden, die auf das geistige Eigentum des Unternehmens zugreifen. Denn sie werden strikt voneinander getrennt. Native Funktionen wie Kopieren und Einfügen können so unterbunden werden. Trotz der inhaltlichen Trennung kann der Anwender alle Apps auf dem Gerät beliebig anordnen.

Mit dem passende Software Development Kit (SDK) Ihrer UEM-Lösung können Sie Sicherheitsbibliotheken vor der Kompilation direkt in den Quellcode der App integrieren. Obwohl die Containerization den Quellcodezugriff und die Codierung durch die Entwickler erfordert, bieten SDKs einige Vorteile, die weit über die Sicherheit hinausgehen: Entwickler können ganz einfach Funktionen wie Disaster Recovery und Hochverfügbarkeit in die Apps integrieren. Und auch die Verwendung schlüsselfertiger Funktionen wie Anwesenheit und Drucken werden zum Kinderspiel.

Jede Container-Lösung sollte mindestens über die folgenden Funktionen verfügen:

App-Berechtigung – die App darf nur auf dem Gerät eines autorisierten Anwenders bereitgestellt werden.

App-Verschlüsselung – selbst wenn ein Hacker das Gerätepasswort entschlüsselt hat, bleiben die Daten in der App durch eine zweite Ebene der Verschlüsselung noch geschützt.

App-Authentifizierung – erweiterte Optionen für die Authentifizierung mit einem Passwort auf App-Ebene, wie zum Beispiel Support für die Zwei-Faktor-Authentifizierung.

Single Sign-on – bei Bedarf können sich Anwender für eine containerisierte App anmelden und zugleich Zugang zu allen containerisierten Apps erhalten. Für einen besseren Bedienkomfort.

Umfassende Sicherheitsrichtlinien – wie beispielsweise sichere Passwörter, Schutz vor Datenverlusten („Öffnen in“, Ausschneiden/Kopieren/Einfügen, Dateiverwaltung) und Compliance-Kontrollen (Fernsperre/-löschen, Erkennung von gehackten Geräten, Durchsetzung der OS-Version).

Sicherer Zugriff – auf Server und Ressourcen hinter der Firewall ohne offene eingehende Firewall-Ports oder eine unnötige Übertragung über das Firmennetzwerk.

Digital Rights Management (DRM) – Sicherheitsrichtlinien auf Dateiebene, die geschäftliche Inhalte schützen, die sich zwischen Geräten, Systemen und Clouds bewegen.

Apps bereitstellen und verwalten

Mithilfe der richtigen Mobile Application Management (MAM) Lösung können Sie Ihren Anwendern maßgeschneiderten Zugriff auf Anwendungen und Daten bieten. Und zwar auch über ein Privatgerät, ohne dass Sie die Sicherheit und regulatorischen Vorschriften des Geräts ständig kontrollieren oder einschränken müssen.

Wichtig ist vor allem, dass Sie MAM-Richtlinien und -Technologien haben, mit denen Sie selektiv geschäftliche Apps und deren Daten löschen können, ohne persönliche Inhalte zu berühren. Denn Mobilität wird erst zu einem echten Erfolgsfaktor, wenn Sie Ihren Anwendern einen hohen Bedienkomfort bieten können und sensible Daten zuverlässig zu schützen wissen.

Von großem Vorteil kann auch ein firmeneigener App Store sein, der Sie beim Verteilen individueller und betreuter Apps an Mitarbeiter sowie externe Berater und Partner unterstützt. Dafür müssen Sie die Geräte nicht einmal selbst verwalten.

Einige Lösungen verfügen auch über grafische Dashboards, die detailliert die App-Nutzung im gesamten Unternehmen aufzeigen. So können Sie leicht auf Kennzahlen wie registrierte Nutzer, Anzahl der Apps, App-Verteilung über OS-Plattformen, beliebteste Apps und vieles mehr zugreifen.

Betrachten Sie den gesamten Lebenszyklus einer mobilen App

Ihre EMM-Lösung sollte ein Framework für die Sicherheit und Verwaltung über den gesamten Lebenszyklus einer App bieten. Hierzu gehören:

- **Entwicklung und Beschaffung von extern und intern entwickelten Apps**
- **Bereitstellung und Implementierung von Apps**
- **Sicherheit von Apps und Richtlinienverwaltung**
- **Nutzung von Apps und Feedback der Anwender**
- **Deaktivierung von Apps und selektive Datenlöschung**

Die folgenden Funktionen sind ein Beweis dafür, dass Sie auf dem richtigen Weg sind:

- **Single Sign-on, damit sich Ihre Anwender nur einmal authentifizieren müssen, um über Apps Zugriff auf Inhalte zu erhalten.**
- **Verschlüsselung geteilter Daten zwischen Apps und bei der Nutzung, ob auf dem Gerät, hinter der Firewall oder in der Cloud.**
- **Einfache Containerization jeder Applikation.**
- **Ein SDK für Entwickler mit erweiterter Funktionalität, wie beispielsweise sicheres Teilen von Dokumenten von App-zu-App oder ein Shared Services Framework zum einfachen Hinzufügen von Funktionen, ohne dass eigens ein neuer Code geschrieben werden muss.**

3. Sicherheitszertifikate und Zugangsdaten

Welche Sicherheitszertifikate muss eine UEM-Plattform vorweisen können, um in die engere Auswahl zu kommen? Welche Anbieter gelten als zuverlässig? Beachten Sie: Je nach Branche können Sie auch gesetzlich zu einer Plattform verpflichtet sein, die HIPAA, HITECH, GLBA, FISMA oder andere Sicherheitsanforderungen unterstützt.

Achten Sie darauf, welche Unternehmen, Analysten, Kunden und Branchen die Plattform positiv bewerten. Die meisten Anbieter rühmen sich mit hoher Sicherheit und vielen Funktionen. Aber nur die wenigsten können mit einer unabhängigen Validierung durch Dritte diese Behauptungen untermauern.

Mobile Apps begünstigen Datenverluste, wenn Mitarbeiter geschäftliche Inhalte an ihre persönliche Cloud oder E-Mail senden und Gerätesicherungen an PCs ausführen. Mobile Sicherheit bedeutet mehr als nur den Schutz geschäftlicher Daten auf dem Gerät und während der Übertragung. Sie müssen auch Konfigurationsdetails und Zugangsdaten sichern, die auf mobilen Geräten gespeichert sind. Fehlt dieser Schutz sind Ihr Netzwerk und wichtige Applikationen in Gefahr. Die Sicherung des Geräts allein verhindert nicht den Verlust geschäftlicher Daten. Sie müssen die drei wichtigsten Faktoren der Mobilität schützen: Inhalte, Zugangsdaten und Konfigurationen.

4. Schutz der Privatsphäre

Das Phänomen BYOD macht deutlich, wie sensibel und sorgsam Geräte und Daten verwaltet werden müssen. Mitarbeiter wollen ihre Privatsphäre aus den gleichen Gründen schützen wie Unternehmen sensible Daten. Was vertraulich ist, soll auch vertraulich bleiben und geht keinen Dritten etwas an.

Außerdem sorgen in zahlreichen Ländern Antidiskriminierungsgesetze dafür, dass der Zugriff auf ein Gerät, dessen Apps oder Standortinformationen einen Rechtsstreit zur Folge haben.

Eine Datenschutzverletzung liegt beispielsweise dann vor, wenn Ihre geschäftlichen Daten in Gefahr sind und Sie alle Daten auf dem privaten Gerät eines Mitarbeiters löschen. Zum Beispiel bei Verlust oder Diebstahl des Geräts oder wenn der Mitarbeiter das Unternehmen verlässt.

Standortdienste zur Durchsetzung von Compliance-Vorschriften belasten nicht nur den Akku. Sie stellen auch einen Verstoß gegen den Schutz der Privatsphäre dar. Das gleiche gilt für die Speicherung von Telefon- und Standortprotokollen.

Suchen Sie daher nach einer vertrauenswürdigen Lösung. Sie sollte Ihre geschäftlichen Daten ebenso schützen wie die persönlichen Daten Ihrer Mitarbeiter. Und das unabhängig vom Betriebssystem oder Eigentumsmodell.

5. Dokumentenkontrolle

Das Teilen von Dateien – vor allem über mobile Geräte – ist ein wesentlicher Bestandteil der Zusammenarbeit geworden. Je mehr Unternehmen ihre Prozesse mobilisieren, desto mehr sensible Daten befinden sich auch auf mobilen Geräten.

Nicht geschützte Dateien, die sensible Angaben wie zum Beispiel geistiges Eigentum, Finanzdaten und regulierte Informationen enthalten, stellen eine Gefahr dar. Dies gilt unabhängig davon, ob sie innerhalb Ihres Unternehmens bleiben oder extern geteilt werden. In einer Umfrage des Ponemon Institute[1] gaben 61 % der Mitarbeiter an, dass sie E-Mails unverschlüsselt gesendet, vertrauliche Dokumente nicht gelöscht oder versehentlich sensible Daten an unberechtigte Empfänger weitergeleitet haben.

Um zu verhindern, dass regulierte oder geschäftskritische Daten in die falschen Hände geraten, müssen Sie Ihre Dokumente direkt schützen. Suchen Sie eine UEM-Plattform, die eine sichere Enterprise File Synchronization and Sharing (EFSS) Lösung mit DRM-Funktionen auf Dateiebene bietet oder sich mit einem solchen Tool leicht integrieren lässt. In regulierten Branchen brauchen Sie zusätzliche Funktionen zur Nachverfolgung von Dokumenten sowie für die Prüfung und Compliance.

6. Bereitstellungsmodell (Cloud oder On-Premise)

Viele Endpoint Management Lösungen bieten Ihnen eine Cloud-Version (auch Software as a Service oder SaaS genannt) und eine On-Premise-Version. Beides hat Vorteile. Folgende Faktoren sollten Sie bei Ihrer Entscheidung beachten:

Einrichtungszeit: Cloudbasierte Lösungen sind sehr oft schnell eingerichtet und betriebsbereit.

Instandhaltung: Cloudbasierte Lösungen können die Arbeitsbelastung für die IT bei Updates und Upgrades reduzieren. Dies ist insbesondere dann hilfreich, wenn die internen technischen Ressourcen begrenzt sind.

Zugriff und Kontrolle: Eine On-Premise-Lösung sitzt serverseitig in Ihrem Rechenzentrum. Etliche IT-Unternehmen nutzen dies zur besseren Kontrolle über Daten, Disaster Recovery und eine engere Integration mit anderen Systemen.

Compliance: Für hochsichere oder regulierte Unternehmen wie Regierungsbehörden oder das Militär ist eine Lösung On-Premise die bessere Wahl. Auch wenn Cloud-Anwendungen sicherer geworden sind und sich weiterentwickelt haben.

Im Idealfall bietet Ihnen Ihre UEM-Lösung beide Bereitstellungsoptionen, ohne Verzicht auf Sicherheits- oder Leistungsmerkmale. Möglicherweise brauchen Sie für verschiedene Standorte auch unterschiedliche Modelle.

7. Migration und Implementierung

Die Migration zu einer neuen Plattform erfordert meist viel Zeit und Ressourcen, muss aber nicht zwangsläufig in Stress ausarten. Denn entscheidend ist die Herangehensweise. Schließlich soll Ihre Lösung so schnell und unterbrechungsfrei wie möglich den Mitarbeitern zur Verfügung stehen.

Ihre UEM-Strategie muss diesem Prozess Rechnung tragen. Beantworten Sie sich folgende Fragen: Welche Ressourcen brauchen Sie und wo kommen sie her? Ein typischer Firmenkunde hat Tausende Geräte verteilt auf mehrere Büros in der ganzen Welt im Einsatz.

Daher brauchen Sie für die Migrationsphase einen konkreten Plan. Mit Terminen für die Migrationen sowie für die Schulungen der IT und der Mitarbeiter.

8. Technischer Support

Guter Support ist für Sie erfolgsentscheidend, wenn Sie auf Ihre mobile Plattform angewiesen sind. Wenn es beispielsweise darum geht, Entscheidungsfindungen zu beschleunigen, Umsatz und Gewinn zu steigern, Workflows zu vereinfachen oder Kontakt zu Mitarbeitern, Teams, Kunden und Lieferanten zu halten. Bringen Sie in Erfahrung, welche Leistung zu welchen Kosten verfügbar ist. Was vor allem Planung, Implementierung, Optimierung und kontinuierliche Fehlerbehebung kosten. Ihre neue UEM-Lösung sollten Sie so auswählen, dass der Anbieter auch den passenden Support übernehmen kann.

9. Schulung und Anwenderfunktionen

Welchen Support brauchen Sie für das Training, wie greifen Sie auf die Trainingseinheiten zu und was wird es kosten? Je einfacher Ihre UEM-Lösung für die IT und den Mitarbeiter bei der ersten Bereitstellung und der laufenden Verwaltung ist, desto weniger Zeit brauchen Sie für die Schulung. Fragen Sie genau nach, wie der UEM-Anbieter Sie bei diesem Prozess unterstützt. Und was getan wird, um die Schulungen so straff und einfach wie möglich durchzuführen.

10. Preise und Kosten

Durch die Migration zu einer einzigen, einheitlichen Endpoint Management Plattform kann Ihr Unternehmen die Infrastruktur standardisieren, die Komplexität reduzieren und den ROI erhöhen.

Ihre Lösung sollte eine kostengünstige und flexible Mobilität bieten, die sich im Laufe der Zeit nach oben oder unten skalieren lässt. Beharren Sie auf Einzelheiten, wenn es um die Anzahl der Geräte geht, die Sie pro Domain hinzufügen können. Betrachten Sie auch die Zahlungsbedingungen. Statt einer hohen Anfangsinvestition bevorzugen Sie vielleicht ein Abonnement-Modell mit jährlich vorhersehbaren Betriebskosten. Die Umverteilung der Kosten auf diese Weise kann für den Cashflow hilfreich sein.

Für ein realistisches Bild der Kosten müssen Sie die direkten und indirekten Kosten betrachten. Je mehr Ihre Mobilisierung voranschreitet, desto wichtiger wird der Faktor Zuverlässigkeit.

Erstklassige Mobilität durch die BlackBerry Enterprise Mobility Suite

BlackBerry
Enterprise Mobility Suite

Mit der BlackBerry Enterprise Mobility Suite werden Sie den Erwartungen und Anforderungen Ihrer Mitarbeiter an sichere mobile Apps gerecht. Die BlackBerry Enterprise Mobility Suite bietet Ihnen konsistente Multi-Plattform Richtlinien für Endgeräte und die App-Verwaltung. Außerdem umfassende Kontrollen für die Betriebssysteme iOS®, Android™, Android™ for Work, Samsung Knox™, Windows®, macOS und BlackBerry®. Unabhängig vom gewählten Eigentumsmodell oder der Nutzergruppe.

Die BlackBerry® Enterprise Mobility Suite:

- bietet eine schlüsselfertige Lösung für das Rollout von Apps zur Kollaboration, Line of Business Apps und eigenen Apps. Die Daten Ihres Unternehmens und die Privatsphäre Ihrer Mitarbeiter bleiben stets geschützt, indem Sie konsistente Container- und Sicherheitsrichtlinien über Betriebssysteme hinweg bereitstellen, um geschäftliche und persönliche Inhalte getrennt zu halten.
- bietet Tools, APIs, Infrastruktur und Software Development Kits für die App-Entwicklung, um eine konsistente Sicherheit über Geräte und Betriebssysteme hinweg zu gewährleisten.
- hat strenge Tests einschließlich der Common Criteria Security Zertifizierung für App-Verwaltung und die zugrunde liegende App-Sicherheitsplattform bestanden, sodass es die Lösung der Wahl für Versicherungen, Finanzen, Recht, Luft- und Raumfahrt, Verteidigung, Militär und alle sicherheitsbewussten Unternehmen ist.
- kann präzise Kontrolle über Inhalte durch integriertes Digital Rights Management (DRM) bieten. So lassen sich Daten immer und überall schützen und nachverfolgen, auch wenn sie heruntergeladen und extern geteilt werden.
- passt sich flexibel und kostengünstig an. So können im Laufe der Zeit neue Funktionen ohne Unterbrechung oder teure Ersatzinvestitionen hinzugefügt werden.
- unterstützt Unternehmen bei der Einhaltung höchster Sicherheitsanforderungen und/oder gesetzlicher Vorschriften. BlackBerry Enterprise Solutions unterstützen:
- 16 der G20-Regierungen
- die 10 größten Anwaltskanzleien
- 5 von 5 der größten Öl- und Gasunternehmen
- über die Hälfte der Fortune 100 Unternehmen, einschließlich aller F100 Geschäftsbanken

Die BlackBerry Enterprise Mobility Suite bietet Ihnen passende Produkte für alle Anforderungen an Mobilität und Produktivität

Management Edition

Für Unternehmen, die Kontrolle und Verwaltung auf Geräteebene wollen, bietet die Management Edition mit BlackBerry® UEM eine komplette, plattformübergreifende, hochsichere und einheitliche Endpoint Management Lösung.

Enterprise Edition

Für Unternehmen, die neben einer UEM-Lösung auch ausgewählte Funktionen zur Zusammenarbeit nutzen wollen, bietet die Enterprise Edition ein mobilisiertes Microsoft® Exchange mit höchstem Bedienkomfort, Ende-zu-Ende Sicherheit und dem Schutz geschäftlicher Daten.

Collaboration Edition

Für Unternehmen, die von einer erweiterten mobilen Produktivität profitieren wollen, bietet die Collaboration Edition mobilisierte Microsoft-Anwendungen – Exchange, Office 365, Office, SharePoint, Skype for Business – und andere wichtige Anwendungen (wie CRM) über ein führendes App-Ökosystem.

Application Edition

Für Unternehmen, die bereits erweiterte Endpoint Management Funktionen zusammen mit Apps zur Zusammenarbeit und Business Apps von Drittanbietern nutzen, bietet die Application Edition eine Plattform für die Sicherheit, Entwicklung und Bereitstellung von Apps. Denn durch individuelle Apps lassen sich eine breitere Palette von Geschäftsprozessen realisieren.

Content Edition

Für Unternehmen, die ihre UEM-Funktionen und ihre vielfältigen eigenen und fremden Apps optimal schützen wollen, bietet die Content Edition mit BlackBerry Workspaces die sicherste Enterprise File Synchronization and Sharing (EFSS) Lösung auf dem Markt. Workspaces integriert DRM in Dateien, damit Inhalte überall geschützt bleiben. Das Anzeigen, Bearbeiten, Kopieren, Drucken, Herunterladen und Weiterleiten von Dateien kann jederzeit kontrolliert werden. Selbst wenn die Datei mit externen Dritten geteilt wurde.

Weitere Informationen zur BlackBerry Enterprise Mobility Suite finden Sie unter www.blackberry.com/suite.

* Stand: Oktober 2015

[1] Die komplette Studie finden Sie unter: https://www.complianceweek.com/sites/default/files/Ponemon-Intralinks%20File%20Sharing%20Report.pdf