MobileIron

DATA SHEET

AppConnect und AppTunnel: Mehr Sicherheit für mobile Apps

Die weltweit größten Unternehmen setzen im Bereich der mobilen IT Ihr Vertrauen in MobileIron®. Die hochgradig skalierbare standort- oder Cloud-basierte Lösung von MobileIron wurde speziell entwickelt, um mobile Apps, Dokumente und Geräte zu sichern und zu verwalten. MobileIron war das erste Unternehmen, das wegweisende Innovationen wie Multi-OS Mobile Device Management (MDM), Mobile Application Management (MAM) und Lösungen zum Schutz der Privatsphäre auf BYOD-Geräten bereitstellte.

Wenn mobile IT zur wichtigsten Computing-Plattform eines Unternehmens geworden ist, stellt jeder Fachbereich seine Kernfunktionen über Apps mobil zur Verfügung. Diese Apps können auch außerhalb des Unternehmensbereichs auf privaten oder minimal verwalteten Geräten genutzt werden. Die mobile IT muss die App-Daten schützen und darf dabei den Benutzerkomfort nicht beeinträchtigen.

Der verbundene Container

Für die geschützten Daten wird ein *„Container“* eingerichtet. Diese Daten werden an anderen Stellen als die restlichen Daten auf dem Gerät gespeichert und sind vor unberechtigten Apps oder Benutzern geschützt.

In der ersten Generation der Enterprise Mobility wurden alle geschäftlichen Daten und die damit verbundenen Apps in monolithischen, E-Mail-basierten Containern getrennt. Dadurch wurden die geschäftlichen Daten zwar geschützt, allerdings litt der Benutzerkomfort darunter.

Bei der neuen Generation der Enterprise Mobility spielt Benutzerkomfort eine wichtige Rolle und erfordert:

- Für Endbenutzer: Die Sicherheit muss unmerklich und das mobile Nutzungserlebnis reibungslos sein. Die Privatsphäre muss geschützt werden, besonders bei privaten Geräten.
- Für mobile IT: Geschäftliche Daten müssen geschützt und möglichst viele Geräte unterstützt werden. Der Aufwand für den Helpdesk muss minimal und die Lösung schnell einsatzbereit sein.

Die Architektur des *verbundenen Containers* von MobileIron erfüllt diese Anforderungen und schützt den Lebenszyklus mobiler Apps. Sie besteht aus zwei Komponenten:

1. MobileIron AppConnect:
MobileIron AppConnect containerisiert Apps, um gespeicherte App-Daten zu schützen, ohne persönliche Daten zu verletzen. Jede App wird zu einem sicheren Container, in dem Daten verschlüsselt und vor unberechtigtem Zugriff geschützt sind. Dieser Container kann jederzeit wieder entfernt werden. Da jeder Benutzer über mehrere geschäftliche Apps verfügt, sind die sicheren App-Container miteinander verbunden. Dies ermöglicht die gemeinsame Nutzung von Richtlinien (wie der einmaligen Anmeldung) und den Austausch von Daten (wie Dokumenten). Alle App-Container sind zur zentralen Richtlinienverwaltung mit MobileIron verbunden.

Herausforderung
Datenverluste verhindern, während mobile Apps in der Geschäftswelt eine immer wichtigere Rolle spielen

Die Lösung
MobileIron AppConnect MobileIron AppTunnel

Vorteile
- Sicherer mobiler App-Lebenszyklus
- Schutz für gespeicherte Daten (Data at Rest) ohne Verletzung persönlicher Daten
- Schutz von übertragenen App-Daten ohne VPN
- Schutz der Privatsphäre dank Datentrennung
- Automatische Konfiguration der Apps und dynamische Richtlinienaktualisierung ohne Benutzereingriff
- Unterstützung von SDK- und Wrapping-Methoden zur Nutzung von App-Containern
- Unterstützung von iOS und Android
- Unterstützung von internen und öffentlichen Apps

Aktuelle Auszeichnungen
Gartner: MobileIron im Leaders-Segment des Magic Quadrant for Mobile Device Management Software (Mai 2012)

Info-Tech: MobileIron wird als Champion unter den Anbietern für Mobile Device Management Suites Vendor Landscape positioniert (August 2012)

IDC: MobileIron als weltweit am schnellsten wachsender Anbieter im Bereich Mobile Enterprise Management bewertet (September 2012)

MAKING ENTERPRISE MOBILE FIRST

MobileIron

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

2. MobileIron AppTunnel:
MobileIron AppTunnel bietet sicheres Tunneling und Zugriffskontrolle, um übertragene App-Daten zu kontrollieren und zu schützen, ohne dass dafür VPN benötigt wird. Die MobileIron-Plattform unterstützt zwar auch VPNs von Drittanbietern, allerdings möchten viele Kunden nicht, dass VPN Zugriff auf alle Apps eines Geräts hat. Alternativ ermöglicht AppTunnel granulare Sicherheit für jede einzelne App, um jeden App-Container mit dem Unternehmensnetzwerk zu verbinden. Die Grundlage bildet die MobileIron Sentry-Technologie, die auf Tausenden Kundengeräten installiert ist. Sentry war das branchenweit erste intelligente Gateway für ActiveSync-E-Mail.

AppConnect

MobileIron AppConnect erstellt mithilfe eines SDK oder Wrappers für iOS bzw. eines Wrappers für Android einen sicheren App-Container. Um eine durchgängige Verwaltung zu ermöglichen, wird dieser Container auch mit anderen sicheren App-Containern und der MobileIron-Konsole verbunden:

- **Authentifizierung:** Bestätigung der Benutzeridentität durch Domain-Benutzername und Kennwort oder durch Zertifikate, sodass nur berechtigte Personen auf geschäftliche Apps zugreifen können
- **Single Sign-On:** Erzwungene zeitbasierte Anmeldung auf App-Ebene für mehrere App-Container
- **Autorisierung:** Zulassen oder Blockieren der App-Nutzung oder Datenspeicherung auf Basis des Gerätesicherheitsstatus
- **Konfiguration:** Automatische Konfiguration personalisierter Einstellungen wie Benutzername, Servername und spezifischer Attribute ohne Benutzereingriff
- **Verschlüsselung:** Verschlüsselung aller App-Daten auf dem Gerät
- **DLP-Kontrollen:** Festlegen von DLP-Richtlinien, z. B. für die Berechtigung zum Kopieren/Einfügen, Drucken oder Öffnen von Dateien, sodass sensible Daten den Container nicht verlassen können
- **Dynamische Richtlinien:** Dynamische App-Richtlinienaktualisierung
- **Berichterstellung:** Bereitstellung von Statistiken zur App-Nutzung
- **Selektives sicheres Löschen:** Sichere Remote-Löschung von App-Daten ohne Verletzung persönlicher Daten

AppTunnel

MobileIron AppTunnel bietet Tunneling und Zugriffskontrolle, um übertragene App-Daten zu kontrollieren und zu schützen, ohne dass dafür VPN benötigt wird. AppTunnel umfasst mehrere Sicherheitsebenen:

- **Eindeutige Verbindung:** Wird nur für berechtigte Apps, Benutzer und Geräte eingerichtet
- **Auf Zertifikaten basierende Authentifizierung:** Verhindert Man-in-the-Middle-Angriffe
- **Regeln zur Zugriffskontrolle:** Netzwerkzugriff blockieren, wenn die Sicherheit der App gefährdet ist

Über MobileIron

Wenn es um Enterprise Mobility geht, vertrauen Tausende Unternehmen auf MobileIron. Die Standort- oder Cloud-basierten Lösungen von MobileIron wurden speziell entwickelt, um die Verwaltung und Sicherung mobiler Apps, Dokumente und Geräte für Unternehmen auf der ganzen Welt zu optimieren. 7 der 10 wichtigsten Pharmaunternehmen, 4 der 5 größten Automobilhersteller, 3 der 5 größten Einzelhändler und die Hälfte der 10 renommiertesten Anwaltskanzleien weltweit haben sich für MobileIron entschieden.

Kundensicht

Apps: „MobileIron ist die ideale strategische Plattform zur Unterstützung und Verwaltung unserer mobilen Geräte und Apps.“
Life Technologies (Biowissenschaften)

BYOD: „MobileIron bietet genau die Systeme und Funktionen, die wir benötigen, damit unsere Mitarbeiter die Geräte ihrer Wahl nutzen können.“
Thames River Capital (Finanzdienstleistungen)

Innovation: „MobileIron unterstützt uns auf unserem Weg als Technologie-Innovatoren.“
Norton Rose (Rechtsanwaltskanzlei)

Betriebssystemunabhängigkeit: „Wir brauchten eine wirklich betriebssystemübergreifende Lösung. MobileIron bot eindeutig den größten Leistungsumfang.“
Colt Car Co./Mitsubishi (Automobilindustrie)

Skalierbarkeit: „[MobileIron] unterstützte uns nicht nur großartig bei der Produktskalierung, sondern auch bei der Behebung jeglicher Probleme.“
Lexington School District (Bildung)

Sicherheit: „In unserer Branche ist eine zuverlässige Lösung für mobile Sicherheit absolut unverzichtbar.“
National Health Service (Gesundheitswesen)

Support: „Guter Kundenservice ist heutzutage eine Seltenheit. Meine Erfahrungen mit MobileIron waren bisher absolut positiv.“
City of North Vancouver (öffentlicher Sektor)

Benutzerkomfort: „Die Stärke von MobileIron liegt in der einfachen Verwendung für iPad-Benutzer.“
KLA-Tencor (Technologie)

Hinweis: Einige Android Wrapping-Funktionen sind für eine zukünftige Version ausgelegt. Manche Funktionen können sich je nach Betriebssystem unterscheiden.

Gartner, Inc., Magic Quadrant for Mobile Device Management Software, Phillip Redman, John Girard, Monica Basso, 17. Mai 2012. Gartner gibt keine Empfehlung zu den in den Veröffentlichungen beschriebenen Anbietern, Produkten oder Dienstleistungen ab und empfiehlt Technologiebenutzern auch nicht, nur Anbieter mit der höchsten Bewertung zu wählen. Die von Gartner veröffentlichten Studien basieren auf den vom Gartner-Marktforschungsteam gewonnenen Einsichten und sollten nicht als faktische Aussagen gewertet werden. Gartner übernimmt keine Garantie für diese Studien, weder ausdrücklich noch implizit, insbesondere keine Garantie auf den Vermarktungserfolg oder die Tauglichkeit für einen bestimmten Zweck.

Info-Tech Research Group, Inc., Vendor Landscape: Mobile Device Management Suites, August 2012. Die „Vendor Landscape Reports“ der Info-Tech Research Group zeichnen außergewöhnliche Anbieter auf dem Technologiemarkt aus. Die Anbieter werden nach der Leistungsstärke ihres Angebots und der Richtung ihrer Unternehmensstrategie bewertet und in einer bestimmten Kategorie ausgezeichnet.