MobileIron

MobileIron AppConnect und MobileIron AppTunnel:

Erweiterte Sicherheit für mobile Apps und Daten

Die Verbreitung von mobilen und Cloud-Technologien hat es internationalen Unternehmen ermöglicht, die Produktivität wie nie zuvor zu steigern. Die Absicherung der Geräte, Apps und Cloud-Dienste, die auf kritische Unternehmensdaten zugreifen, stellt jedoch eine erhebliche Herausforderung für Ihr mobiles Sicherheitsteam dar. Sie müssen beispielsweise:

- Private Geräte für die berufliche Nutzung sicher aktivieren.
- Private Apps dürfen nicht auf Unternehmensdaten und Cloud-Dienste zugreifen können.
- Auf dem Gerät gespeicherte sowie in die Cloud oder an das Backend-Netzwerk des Unternehmens übertragene Daten schützen.
- Verhindern, dass Daten geteilt oder über nicht autorisierte Apps aufgerufen werden, beispielsweise über eine private Version von Office 365.

MobileIron AppConnect und MobileIron AppTunnel unterstützen Sie dabei, diese Anforderungen an die mobile und Cloud-Sicherheit zu erfüllen.

MobileIron AppConnect

MobileIron AppConnect kapselt Apps in Containern, um gespeicherte App-Daten zu schützen, ohne auf private Daten zuzugreifen. Jede App wird zu einem sicheren Container, in dem Daten verschlüsselt und vor unberechtigtem Zugriff geschützt sind, der wieder entfernt werden kann. Jeder App-Container ist außerdem mit anderen sicheren App-Containern über die Verwaltungsplattform von MobileIron verbunden, d. h. Richtlinien wie Single-Sign-On (SSO) für eine App können bequem geteilt und geräteübergreifend aktualisiert werden.

MobileIron AppTunnel

MobileIron Tunnel schützt Netzwerkdaten durch eine innovative App, die VPN-Verbindungen für Geräte mit iOS, Android und Windows 10 unterstützt. AppTunnel ermöglicht granulare Sicherheit für jede einzelne App und verbindet jeden App-Container mit dem Unternehmensnetzwerk. So können Unternehmen den Traffic von Unternehmens-Apps ohne Störung des privaten Traffics absichern, wenn beispielsweise ein Benutzer ein Familienfoto in Facebook veröffentlicht.

Hauptvorteile

- Sichern Sie App-Daten auf dem Gerät, bei der Übertragung in die Cloud oder ins Backend-Netzwerk des Unternehmens.
- Trennen Sie unternehmenseigene und private Apps und Daten auf dem Gerät.
- Erlauben Sie einen sicheren App-Zugriff ohne VPN.
- Konfigurieren, installieren und aktualisieren Sie Apps und Richtlinien ohne Eingriff des Benutzers.
- Unterstützen Sie SDK- und Wrapping-Methoden zur Nutzung von App-Containern.
- Stellen Sie Anwendungen für Geräte mit iOS, Android und Windows 10 bereit.
- Verwalten Sie interne und öffentliche Anwendungen.

MobileIron

Über MobileIron

MobileIron bietet eine sichere Basis für zeitgemäße Arbeit in Unternehmen jeder Größe in aller Welt. Weitere Informationen finden Sie unter **www.mobileiron.com**, Sie können sich natürlich auch an den Vertriebsmitarbeiter von MobileIron wenden.

Leistungsmerkmale

AppConnect

MobileIron AppConnect erstellt mit einem SDK oder Wrapper für iOS bzw. einem Wrapper für Android einen sicheren App-Container. Dieser Container ist mit anderen App-Containern über die MobileIron-Konsole verbunden und bietet folgende Verwaltungsfunktionen:

- **Authentifizierung:** Bestätigung der Benutzeridentität durch Domain-Benutzername und Passwort oder durch Zertifikate, sodass nur berechtigte Personen auf geschäftliche Apps zugreifen können.
- **SSO:** Vereinfachte Benutzerauthentifizierung über App-Container hinweg.
- **Autorisierung:** Zulassen oder Blockieren der App-Nutzung oder Datenspeicherung je nach Geräterisiko.
- **Konfiguration:** Konfiguration personalisierter Einstellungen wie Benutzername, Servername und anpassbarer Attribute ohne Eingriff des Benutzers, die per Push im Hintergrund übertragen werden.
- **Verschlüsselung:** Verschlüsselung aller App-Daten auf dem Gerät.
- **DLP-Kontrollen:** Definition von DLP-Richtlinien, z. B. der Berechtigung zum Kopieren/Einfügen, Drucken oder Öffnen von Dateien, sodass sensible Daten den Container nicht verlassen können.
- **Dynamische Richtlinie:** Aktualisierung von App-Richtlinien für alle oder eine Teilmenge der verwalteten Geräte, je nach Gruppe, Benutzerrolle und anderen Faktoren.
- **Berichterstellung:** Erzeugung detaillierter Statistiken zur App-Nutzung sowie von Audit-Protokollen und anderen Berichten zur Verbesserung der Verwaltung und Vereinfachung der Compliance.
- **Selektives sicheres Löschen:** Löschung von Unternehmens-Apps und Daten aus der Ferne, ohne private Daten zu verändern.

AppTunnel

AppTunnel bietet mehrere Sicherheitsebenen für die Daten mobiler Apps und benötigt kein VPN. Leistungsmerkmale sind u.a.:

- **Geschützte Verbindung:** Nur autorisierte Apps, Benutzer und Geräte dürfen Verbindungen mit Unternehmensressourcen aufbauen.
- **Zertifikatsbasierte Sitzungsauthentifizierung:** Schnelles Konfigurieren von Geräten mit Identitätszertifikaten und VPN-Konfigurationen, um einen sicheren und problemlosen Zugriff auf Unternehmensdaten für den Mitarbeiter sicherzustellen.
- **Regeln zur Zugangskontrolle:** Sperre des Netzwerk-Zugriffs, wenn auf der App-Seite die Sicherheit nicht gewährleistet ist.
- **MobileIron Sentry:** AppTunnel basiert auf der Sentry-Technologie, die ein Inline-Gateway zur Verfügung stellt, mit dem Sie den Traffic zwischen dem Mobilgerät und den Backend-Systemen im Unternehmen verwalten, verschlüsseln und absichern.
- **MobileIron Access:** AppTunnel unterstützt auch MobileIron Access. MobilIron Access erlaubt nur autorisierten Endgerätebenutzern, Apps und Cloud-Diensten, auf Unternehmensdaten zuzugreifen und bietet eine zusätzliche Sicherheit durch die Multi-Faktor-Authentifizierung.