MobileIron

Unified Endpoint Management

Absicherung des modernen Unternehmens mit UEM

Mobile und Cloud-Technologien haben die Arbeitsweise moderner Unternehmen verändert. Informieren Sie sich über die umfassende Sicherheitsplattform, die MobileIron mit Unified Endpoint Management (UEM) anbietet, um kritische Unternehmensprozesse durch moderne Endgeräte, Apps und Cloud-Dienste umzugestalten.

Umfassende Sicherheitsplattform

Die MobileIron-Plattform bietet fundamentale Transparenz und die Kontrollen zur Absicherung, Verwaltung und Überwachung unternehmenseigener bzw. mitarbeitereigener Mobilgeräte oder Desktops, die auf unternehmenskritische Daten zugreifen. Unternehmen können damit eine Vielzahl von Mitarbeitergeräten im Unternehmen absichern und zugleich den gesamten Lebenszyklus des Geräts verwalten. Dies betrifft:

- Konfiguration und Durchsetzung von Richtlinien
- Verteilung und Verwaltung von Unternehmens-Apps
- Zugriffskontrolle und Multifaktor-Authentifizierung (MFA) mit MobileIron Access
- Erkennung und Eindämmung von Bedrohungen mit MobileIron Threat Defense

MobileIron UEM ist eine bewährte, sichere, skalierbare und für Unternehmen geeignete Architektur, bei der das Benutzererlebnis Priorität hat und zugleich höchste Sicherheitsstandards erfüllt werden.

Sichere Unternehmensexpansion in der Cloud und Mobiltechnologie

Unternehmens- und Benutzerkontrolle:
Mit MobileIron können Unternehmen individualisierte Mobilitäts- und Sicherheitsstrategien implementieren und die Unternehmensanforderungen nach eigenem Wunsch anpassen. Wir gewährleisten außerdem den Datenschutz für die privaten Daten der Benutzer und schützen die Unternehmensdaten - Benutzer und Administratoren erhalten jeweils die Kontrolle über ihre Informationen.

Freie Wahl:
MobileIron UEM ist für alle modernen Betriebssysteme und Geräte gleichermaßen offen. Die Administratoren können UEM entweder in der Cloud oder im LAN bereitstellen und die Benutzer ihre bevorzugten Geräte für die Arbeit verwenden.

Erlebnisgesteuerte Akzeptanz:
MobileIron beschleunigt die Akzeptanz des Konzepts durch ein natives Benutzererlebnis für die Produktivitäts-Apps, die beruflich genutzt werden. Dies vereinfacht die Compliance und reduziert Sicherheitsbedrohungen und die sogenannte Schatten-IT. Je höher die Akzeptanz der Benutzer, umso stärker kann die IT Produktivität und Wachstum im gesamten Unternehmen beschleunigen.

Sicheres, krisenfestes Unternehmen:
Unsere Plattform verhindert eine Unterbrechung des Geschäftsbetriebs, ohne den Benutzer zu stören. Unsichtbare, automatische Sicherheitsfunktionen gewährleisten die Sicherheits-Compliance und ermöglichen es Ihrem Unternehmen, sich auf die Zukunft vorzubereiten.

Wichtige Anwendungsszenarien

Nutzung von Profilen für Mobilgeräte
Automatisierung und Rationalisierung der Gerätebereitstellung durch skalierbare Vorinstallation per Tastendruck.

Aktivierung eines nativen Benutzererlebnisses
Vertrautes mobiles Benutzererlebnis auf den für berufliche Zwecke eingesetzten Geräten mit problemloser Authentifizierung für Unternehmens-Apps und -Daten.

Schutz der Unternehmensdaten
Sicherung der Unternehmensdaten auf jedem Endgerät, in jedem Netzwerk und jeder Anwendung, Trennung privater und beruflicher Daten auf den Geräten.

Sicherheitsstandards und Zertifizierungen*

- Common Criteria Certification
- CSA STAR
- CSfC
- DISA STIG
- EU-US Privacy Shield
- FedRAMP Authority to Operate
- FIPS 140-2 Affirmation
- SOC 2 Type II

Weitere Informationen über die Zertifizierungen von MobileIron finden Sie hier: https://www.mobileiron.com/en/certifications-and-uptime

Über MobileIron

MobileIron bietet die sichere Basis für moderne Arbeit. Weitere Informationen finden Sie unter www.mobileiron.com.

Hinweis:
- Die Verfügbarkeit bestimmter Funktionen und Leistungsmerkmale hängt von der Bereitstellungsart ab, das heißt, ob Sie im LAN oder in der Cloud installieren.
- Die Verfügbarkeit kann je nach Betriebssystem und Geräteart abweichen.
- ServiceConnect-Integrationen mit dem Platinum-Bundle schließen von MobileIron entwickelte Software zur Integration mit spezifischen Produkten und Diensten von Drittanbietern ein. Für die API-Integrationen muss kein Platinum-Bundle erworben werden.

Unified Endpoint Management (UEM) von MobileIron	Silver	Gold	Platinum
Verwaltung und Sicherheit von Mobilgeräten			
Verwaltung von Mobilgeräten (MDM): Sichern und verwalten Sie Endgeräte mit den Betriebssystemen Apple iOS und Google Android. Verfügbar im eigenen Netzwerk sowie als Cloud-Dienst.	✓	✓	✓
Einfache Implementierung: Nutzen Sie umfassend Dienste wie das Geräteregistrierungsprogramm DEP von Apple, Android Zero-Touch oder die Mobilregistrierung von Samsung KNOX, um den Benutzern den Einstieg zu erleichtern.	✓	✓	✓
Verteilung und Konfiguration mobiler Apps: Apps@Work, eine anpassbare App für einen Unternehmens-Store, erleichtert in Kombination mit dem Volumenkaufprogramm (VPP) von Apple die sichere Verteilung mobiler Apps. Darüber hinaus erleichtern Funktionen wie die verwalteten iOS-Apps und Android Enterprise die Konfiguration der Einstellungen auf App-Ebene sowie der Sicherheitsrichtlinien.	✓	✓	✓
Sicheres E-Mail-Gateway: MobileIron Sentry ist ein Inline-Gateway, das den Traffic zwischen dem Mobilgerät und den Backend-Systemen des Unternehmens verwaltet, verschlüsselt und absichert.	✓	✓	✓
Verwaltung und Sicherheit von Desktopgeräten			
Verwaltung unter Windows 10: Einheitliche Plattform zur Verwaltung moderner Windows-Endgeräte mit Windows MDM APIs und konventionellen Gruppenrichtlinienobjekten.		✓	✓
Mac-Verwaltung: Verwalten Sie macOS-Endgeräte mit MDM APIs nach dem neuesten Stand der Technik, um Registrierung, App-Verteilung und Lebenszyklusverwaltung von Mac-Geräten zu vereinfachen.		✓	✓
Sichere Produktivität			
App für sichere E-Mail und persönliche Informationsverwaltung (PIM): MobileIron Email+ ist eine plattformübergreifende, sichere PIM-Anwendung für iOS und Android. Die Sicherheitskontrollen umfassen beispielsweise eine Verschlüsselung, die auch die Ansprüche von Behörden erfüllt, die Authentifizierung mit Zertifikaten, S/MIME, eine Verschlüsselung auf Anwendungsebene und die Durchsetzung von Passcodes.		✓	✓
Sicheres Surfen: Web@Work ermöglicht sicheres Surfen im Internet, indem es sowohl Daten bei der Übertragung als auch auf dem Endgerät gespeicherte Daten schützt. Dank anpassbarer Lesezeichen und sicherem Tunneling können die Benutzer schnell und sicher auf Unternehmensinformationen zugreifen.		✓	✓
Sichere gemeinsame Arbeit an Inhalten: Docs@Work ermöglicht es den Benutzern, auf Inhalte von Repositories wie SharePoint, Box, Google Drive usw. sicher zuzugreifen und Dokumente zu erstellen, zu bearbeiten, zu markieren und zu teilen.		✓	✓
Kapselung von mobilen Apps in Containern: Stellen Sie die AppConnect SDK bzw. den App Wrapper als zusätzliche Sicherheitsebene für eigene mobile Apps bereit oder wählen Sie aus unserem Ökosystem AppConnect-integrierte Apps aus.		✓	✓
Abgeleitete Anmeldeinformationen: Unterstützen Sie eine Zwei-Faktor-Authentifizierung mit üblichen Zugangskarten (CAC) und der Verifizierung der persönlichen Identität (PIV).		✓	✓
Sichere Konnektivität			
VPN pro App: MobileIron Tunnel ist eine für mehrere Betriebssysteme geeignete VPN-Lösung, mit der Unternehmen spezifische mobile Apps für den Zugriff auf Unternehmensressourcen hinter der Firewall autorisieren können, ohne dass der Benutzer eingreifen muss. MobileIron Tunnel ist für iOS, Android, macOS und Windows 10 verfügbar.			✓
Skalierung der IT-Operationen			
IT-Systemintegrationen: ServiceConnect erlaubt zur Rationalisierung der IT-Operationen über die UEM-Plattform die Freigabe von Daten von MobileIron für andere IT-Systeme, beispielsweise Splunk oder ServiceNow.			✓
Serverüberwachung und Verwaltung: MobileIron Monitor zeigt in einem Dashboard die Systemleistung und die Trendentwicklung für MobileIron Core und Sentry-Server.			✓
Helpdesk-Tools: Help@Work ist eine App, mit der die IT, bei Zustimmung des Benutzers, aus der Ferne dessen Display anzeigen und kontrollieren kann, um Probleme effizient zu lösen.			✓

MobileIron Threat Defense (MTD)	MTD	MTD+
Abwehr mobiler Bedrohungen für iOS und Android		
Erkennung von Bedrohungen: Schützen Sie sich gegen bekannte und unbekannte Bedrohungen und aktive Attacken mit einer modernen, auf künstlicher Intelligenz basierenden und das Systemverhalten auswertenden Erkennung auf dem mobilen Endgerät.	✓	✓
Eindämmung von Bedrohungen: Begrenzen Sie die Zeit der Gefährdung durch noch unbekannte Angriffe und unterbinden Sie vom ersten Tag an Angriffe mit richtlinienabhängigen Compliance-Aktionen. Melden Sie riskantes Verhalten und wehren Sie Angriffe auf Endgeräte proaktiv mit oder ohne Netzwerkverbindung ab.	✓	✓
Moderne App-Analysedaten: Evaluieren Sie die Risiken mobiler Apps laufend, um Bedrohungen des Datenschutzes und der Sicherheit zu erkennen.		✓

MobileIron Access	MobileIron Access
Adaptive Sicherheit und bedingter Zugriff auf Cloud-Dienste und eigene Apps	
Benutzerverifizierung: MobileIron Authenticator ist eine MFA-App, die vor dem Diebstahl von Anmeldeinformationen schützt.	✓
Passwortlose Anmeldung: Problemloses Single-Sign-On (SSO) erlaubt den Benutzern den schnellen und sicheren Zugriff auf die Dienste.	✓
Intuitives Benutzererlebnis: Nutzen Sie einen kundenspezifischen Zugriff und vordefinierte Arbeitsabläufe, damit die Benutzer Probleme selbst lösen können, ohne Hilfe vom IT-Helpdesk anzufordern.	✓

MobileIron 401 East Middlefield Road, Mountain View, CA 94043, USA • globalsales@mobileiron.com • www.mobileiron.com • Tel: +1.877.819.3451 • Fax +1.650.919.8006