

# Einfache und intelligente Sicherheit für die Unternehmens-Cloud



MobileIron  
**ACCESS**

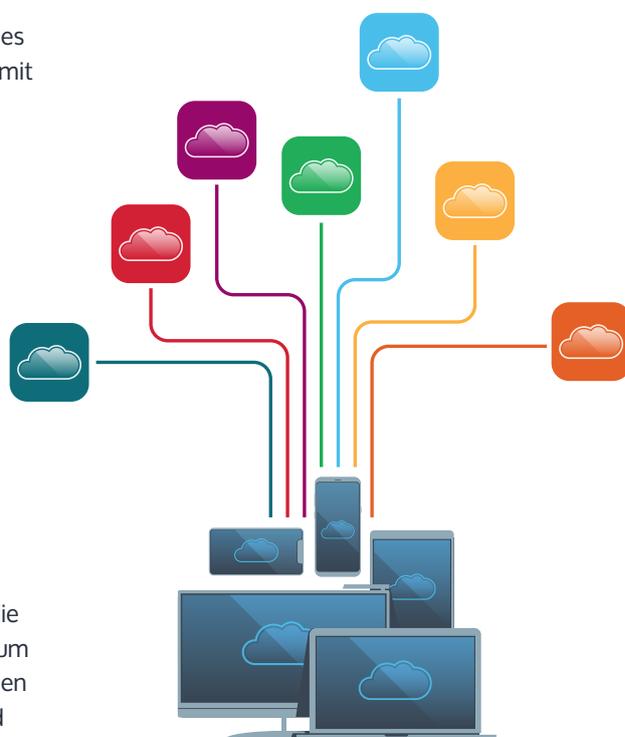
Der Schutz der mobilen und Cloud-Ressourcen vor dem Zugriff von Unbefugten oder Hackern ist eine der größten Herausforderungen, denen Unternehmen heute gegenüberstehen – eine Sicherheit, die sich nur auf die Kontrolle der Passwörter beschränkt, ist nicht mehr ausreichend. In der Tat waren 2018 gestohlene Benutzeranmeldedaten die Hauptursache für Datenschutzverletzungen in Unternehmen.<sup>1</sup>

In der PC-Ära arbeiteten die Mitarbeiter in einem genau definierten Unternehmensnetzwerk, und Passwörter reichten aus, um Benutzer zu identifizieren. In dem heutigen Umfeld mit mobilen Clouds hingegen ist die Trennlinie zum Unternehmensnetzwerk verschwunden, und Unternehmensinformationen stehen den Benutzern auf den unterschiedlichsten Endgeräten, Apps, Diensten, Netzwerken und Standorten zur Verfügung. In diesem Umfeld mit dynamischem Zugriff benötigen Unternehmen ein anderes Sicherheitskonzept, wenn sie:

- das Benutzervertrauen mit Multi-Faktor-Authentifizierung aufbauen,
- die Vertrauensstellung des Benutzers mit anderen Faktoren wie Endgerät, App, Netzwerk usw. vergleichen,
- adaptive Risikoricthlinien entsprechend der Benutzerumgebung nutzen wollen.

MobileIron Access bietet dieses neue Sicherheitskonzept, damit Unternehmen problemlos mobile Cloud-Technologien zur Erhöhung der Benutzerproduktivität und zur Verringerung des Risikos von Datenschutzverletzungen einführen können.

Mit Funktionen wie der Multi-Faktor-Authentifizierung (MFA), nahtlosem Single Sign-on (SSO) sowie einem modernen Richtlinienmodul verfügen Unternehmen über die richtige Sicherheitsplattform, um die wachsenden Anforderungen an Informationssicherheit und Compliance zu erfüllen.



## Hauptvorteile

MobileIron Access bietet eine auf Standards aufbauende Sicherheit für mobile Clouds, so dass Unternehmensinformationen nur für verifizierte Benutzer auf autorisierten Endgeräten, Apps und Cloud-Diensten zur Verfügung stehen.

## Einfach

Mit Merkmalen wie einmaliger Registrierung für die Multi-Faktor-Authentifizierung sowie passwortloser Anmeldung über mobile Apps bietet MobileIron Access den Benutzern das bestmögliche Benutzererlebnis.

## Intelligent

MobileIron Access erzwingt adaptive Risikoricthlinien, die die Art des Endgeräts, der App, des Netzwerks, den Benutzerstandort und vieles mehr berücksichtigen. Die Sicherheitsfunktionen berücksichtigen das Risiko der Benutzerumgebung und reduzieren die Gefahr von Datenschutzverletzungen.



## Über MobileIron

MobileIron bietet Unternehmen jeder Größe in aller Welt eine sichere Basis für moderne Arbeit. Zusätzliche Informationen über MobileIron Access finden Sie unter [www.mobileiron.com/Access](http://www.mobileiron.com/Access). Sie können sich auch an Ihren Vertriebsbeauftragten von MobileIron wenden.

<sup>1</sup> Verizon, Report über Datenschutzverletzungen 2018

# Leistungsmerkmale

## Multi-Faktor-Authentifizierung mit MobileIron Authenticator

Einfache MFA-App, die die umständlichen und teuren Hardware-Token durch eine sichere, mobile Multi-Faktor-Authentifizierung (MFA) ersetzt, die kostengünstig und benutzerfreundlich ist.

- **Konfiguration per Tastendruck**

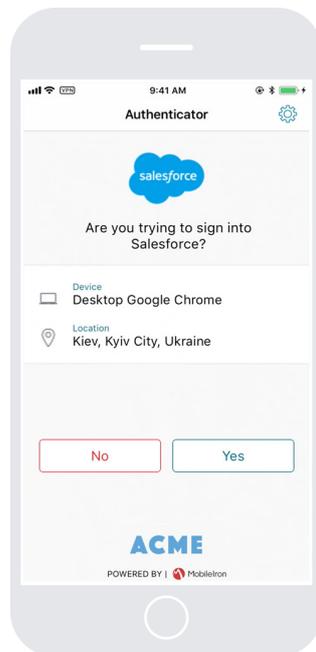
Konfiguration und Setup erfolgen automatisch über die MobileIron-Plattform. Der Benutzer muss die Authenticator-App lediglich einmal zur Aktivierung starten. Sobald die Aktivierung abgeschlossen ist, kann der Benutzer die Anmeldeversuche auf dem konfigurierten Smartphone verifizieren.

- **Push-Nachrichten**

MobileIron Authenticator sendet sofort Benachrichtigungen auf die Mobiltelefone der Benutzer, so dass diese Anmeldeversuche schnell und einfach bestätigen können.

- **Adaptive Authentifizierung**

MobileIron Authenticator bietet intelligente Authentifizierungsabläufe unter Berücksichtigung der unterschiedlichsten Aspekte, beispielsweise des Endgeräte-Risikoprofils, der App, des Netzwerks und des Benutzerstandorts.



## Natives Anmeldeerlebnis für moderne Endgeräte

Bieten Sie ein natives Anmeldeerlebnis für mobile Geräte, das die meisten Benutzer bereits kennen. Dank des nativen mobilen SSO verbinden sich die Benutzer über native mobile Apps sicher mit Unternehmensdiensten, ohne dass sie sich erst mit einer anderen SSO-App oder über ein Portal authentifizieren müssen.

- **Problemloses Single Sign-On**

Adaptive Richtlinien bieten den Benutzern eine passwortlose Authentifizierung, sobald diese mit genehmigten Apps und Endgeräten eine Verbindung aufbauen.

- **Intelligente Anmeldung**

Ein kontextabhängiges SSO verhindert, dass Benutzer eine Verbindung mit Unternehmensdiensten über nicht verwaltete Apps oder nicht genehmigte Dienste aufbauen.

## Intelligente Richtlinien durch Vertrauensstellungs-Modul

Nutzen Sie außer der Benutzeridentität intelligente Entscheidungen zur Zugangskontrolle, die auch Endgerät, App, Dienst, Benutzerstandort, Netzwerk usw. berücksichtigen.

- **Intuitive Arbeitsabläufe zur Risikominderung**

Mit anpassbaren, einfachen Schritten können die Benutzer die Risikominderung bei Verwendung nicht konformer Geräte selbst übernehmen; dadurch sparen sie Zeit und müssen keine Tickets für das Helpdesk registrieren.

- **Auf Standards aufbauende Sicherheit**

Sichern Sie jeden Cloud-Dienst mit einem auf Standards aufbauenden Konzept, um Sicherheitsmaßnahmen entsprechend den wachsenden Anforderungen des Unternehmens zu skalieren.