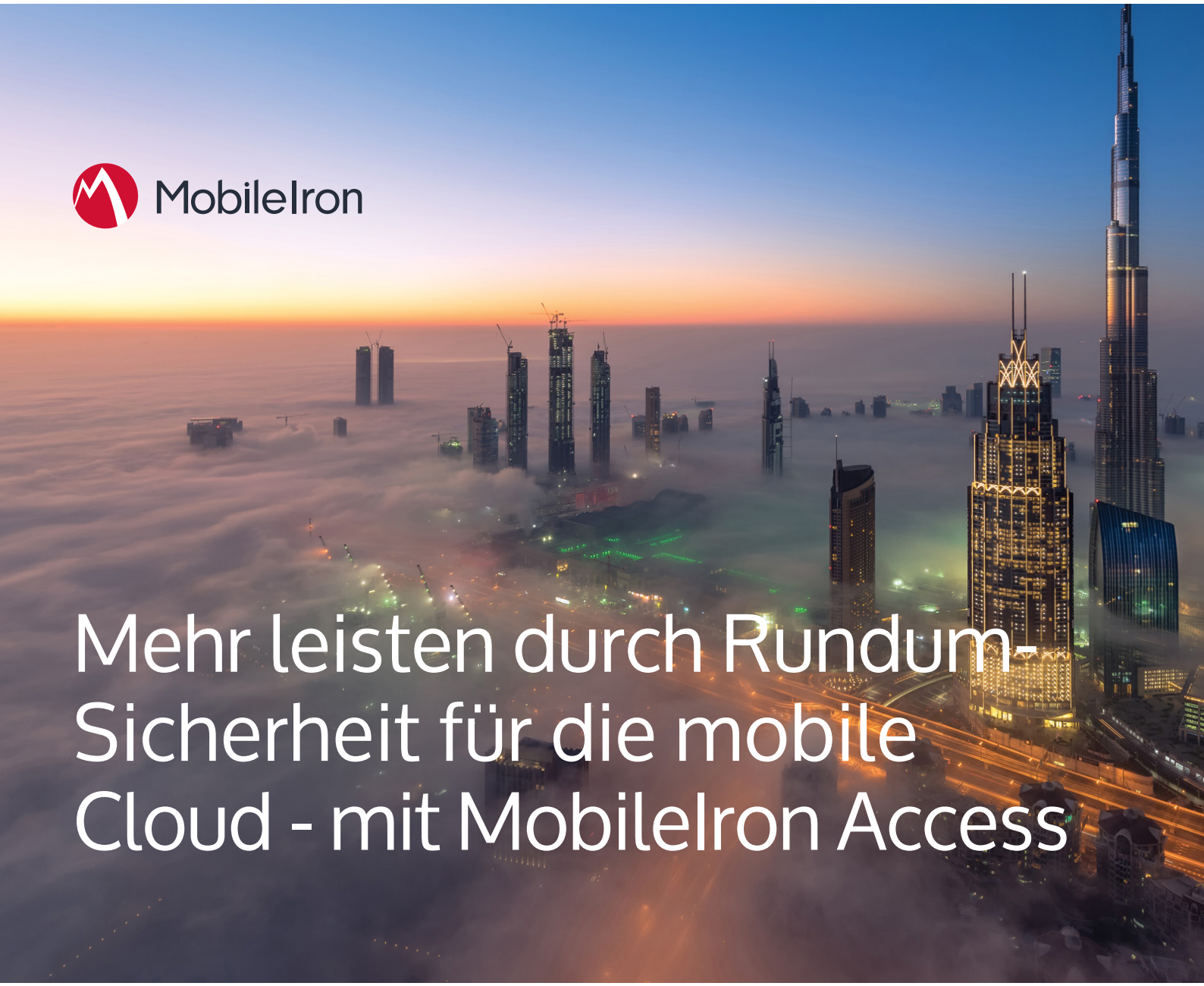


Mehr leisten durch Rundum-Sicherheit für die mobile Cloud - mit MobileIron Access

MobileIron Access: Komplette Cloud-Sicherheit

Umfassende Sicherheit
MobileIron Access wertet das Risikoprofil von Geräten und Apps, Benutzeridentität, Standort und vieles mehr aus, damit nur vertrauenswürdige Geräte, Apps und Benutzer auf die Unternehmens-Cloud-Dienste zugreifen können.

Einheitliche Plattform
MobileIron Access ist eine einheitliche, schnell installierte Plattform zur Absicherung von Unternehmens-Apps und Unternehmens-Daten in der mobilen Cloud.

Auf Standards aufbauende Sicherheit
MobileIron Access integriert problemlos die jeweils besten Identitätsanbieter und kann jeden Cloud-Dienst absichern, der den Standard SAML 2.0 unterstützt. Kundenseitige Integrationsarbeiten sind nicht erforderlich.

Die Herausforderung: Absicherung der mobilen Cloud

In aller Welt führen Unternehmen Cloud-Dienste und mobile Endgeräte in nie dagewesenem Tempo ein. Die Umstellung auf moderne, mobile Cloud-Technologien zwingt die Unternehmen, ihre Konzepte von der Architektur des Rechenzentrums bis zur Endgeräte-Sicherheit komplett zu überdenken, weil konventionelle Sicherheitsmodelle wie bei Desktops nicht mehr ausreichen.

Als die IT noch die Desktop-PCs kontrollierte, brauchten die Unternehmen nur Benutzernamen und Passwörter zu vergeben, um den Zugriff auf Informationen abzusichern. In der Welt der mobilen Cloud reicht eine Sicherheitsprüfung der Identität nicht aus, weil damit weder ein Mechanismus zur Überprüfung des App- oder Gerätestatus zur Verfügung steht noch unsicheres Verhalten erkannt werden kann. Zudem kompliziert dieses konventionelle Konzept das Benutzererlebnis. Wenn sich die Sicherheitskontrollen beispielsweise nur auf die Identitätsprüfung beschränken, wird nicht erkennbar, ob ein Benutzer auf Unternehmens-Apps mit einem nicht konformen Mobilgerät zugreift und dadurch Unternehmensdaten gefährdet. Benutzer erstellen auch gern schwache Passwörter, die leicht zu merken sind, oder speichern Passwörter an bequem zugänglichen, aber unsicheren Orten, beispielsweise in einer privaten Google-Textdatei. Zudem kann die Eingabe komplizierter Passwörter auf den kleinen Displays von Mobilgeräten eine echte Frustquelle für Unternehmensbenutzer sein, die mit ihren Mobilgeräten auf Unternehmensdokumenten und Unternehmensdaten zugreifen wollen. Wenn die Benutzer falsche Anmeldeinformationen eintippen, kann dies dazu führen, dass die Benutzer nach zu vielen Fehlversuchen ihre Konten blockieren.

Dieses Whitepaper erläutert einige der kritischen Sicherheitslücken, die Unternehmen beseitigen müssen, die mit der mobilen Cloud arbeiten:

- **Unsichere Geräte** Unsichere Geräte ermöglichen es den Benutzern, mit mobilen Apps oder Cloud-Diensten auf Unternehmensdaten zuzugreifen, indem sie ihre Anmeldeinformationen in eine App oder den Browser auf dem Gerät eingeben. Sobald sich die Daten auf dem Gerät befinden, sind sie gefährdet und können mit nicht genehmigten externen Quellen geteilt werden. Ein unsicheres Gerät ist beispielsweise ein Gerät mit einem modernen Betriebssystem wie iOS, Android oder Windows 10, das aber nicht auf einer mobilen Geräte-Verwaltungsplattform (MDM-Plattform) registriert ist. Ein Gerät mit Windows 7, das nicht bei einer Domain angemeldet ist, ist ebenfalls anfällig für Sicherheitslücken.
- **Nicht verwaltete Apps** Dazu gehören beispielsweise Produktivitäts-Apps wie Office 365, die der Benutzer aus einem privaten App Store statt aus dem Unternehmens-App-Store heruntergeladen hat. Infolgedessen hat die IT-Abteilung über diese Apps keine Kontrolle. Trotzdem kann der Benutzer mit diesen Apps auf Unternehmens-Content zugreifen, wenn er seine Anmeldeinformationen eingibt. Diese Daten können dann mit anderen Geräten und Apps geteilt werden, weil die IT nicht verwaltete, mobile Apps weder sieht noch kontrollieren kann.
- **Nicht genehmigte Cloud-Dienste** Die meisten Unternehmens-Cloud-Dienste verfügen über entsprechende App-Ökosysteme und Dienste, die über APIs integriert werden. Auch wenn der Unternehmens-Cloud-Dienst selbst genehmigt ist, trifft dies nicht unbedingt auch auf die Apps und Dienste aus seinem Ökosystem zu. Benutzer können daher mit ihren Anmeldeinformationen eine genehmigte Verbindung zu Unternehmens-Cloud-Diensten für nicht genehmigten Dienste von Drittanbietern herstellen. Unternehmensdaten können somit durch einen nicht genehmigten Cloud-Dienst abgerufen oder geteilt werden, ohne dass die IT-Abteilung davon weiß oder es kontrollieren kann.

Bewährte Verfahren zur Absicherung der mobilen Cloud

Die Minimierung der Sicherheitslücken in der Infrastruktur der mobilen Cloud erfordert bestimmte bewährte Verfahren, damit die IT-Abteilung Kontrolle und Transparenz behält, Leistung und Produktivität aber nicht beeinträchtigt werden. Unternehmen sollten nach einer umfassenden Sicherheitslösung für die mobile Cloud suchen, die solche bewährten Verfahren problemlos in die Plattform integriert.

Durchsetzung von Kontextrichtlinien für jeden Cloud-Dienst und jedes mobile Betriebssystem aktivieren

Da Unternehmensanwender zunehmend mit Mobilgeräten auf Unternehmens-Apps und Cloud-Dienste zugreifen, reicht eine Identitätsprüfung nicht aus, um den Zugriff durch ungesicherte Geräte, nicht verwaltete Apps und nicht genehmigte Cloud-Dienste zu verhindern. Die Sicherheit der mobilen Cloud erfordert eine moderne Plattform für mehrere Betriebssysteme, mit der die IT die Bedingungen für die Zugriffs-Kontrollrichtlinien definieren und durchsetzen sowie Geräte-Art und Geräte-Risiko, Status der mobilen App, Art des Cloud-Dienstes und Benutzeridentität berücksichtigt kann.

Vereinfachung der Benutzerauthentifizierung durch problemloses SSO

Die Steigerung der Produktivität der Mitarbeiter ist einer der Hauptgründe, weshalb Unternehmen Geschäftsabläufe in die Cloud verlagern. Wenn Benutzer jedesmal ein Passwort eingeben sollen, wenn sie auf einen Cloud-Dienst zugreifen, wird der Zugang zu den Ressourcen, die sie für ihre Tätigkeit brauchen, nur behindert. Benutzer vergessen nicht nur oft ihre Passwörter, sondern tippen auf den kleinen Displays von Mobilgeräten ihre Benutzerdaten auch öfter falsch ein und sperren sich nach zu vielen Fehlversuchen selbst aus, sodass das Helpdesk eingreifen muss. Dadurch sinkt die Produktivität der Mitarbeiter sowie die Effizienz und es steigen die Supportkosten. Unternehmen müssen daher den sicheren Zugriff mit Technologien vereinfachen, beispielsweise mit Single Sign On.

Compliance-Reports verwalten und verfolgen

Die IT-Abteilung muss nicht nur allgemein sichere Cloud-Dienste, Apps und Geräte einführen, sondern auch Sicherheitsrichtlinien skalierbar und zentral durchsetzen sowie die Compliance verfolgen, überwachen und melden. Konventionelle Lösungen können die nötige Transparenz zum Risiko und zum Status der Geräte oder Apps, welche die Mitarbeiter zur Verbindung mit Unternehmens-Cloud-Diensten verwenden, nicht zuverlässig gewährleisten. In solchen Fällen muss die IT außerdem in der Regel Protokolle jedes einzelnen Cloud-Dienstes erstellen und manuell mit den Protokollen anderer Quellen zusammenführen, um nicht-konforme Geräte und Apps zu identifizieren. Dieses Konzept ist zu fragmentiert und nicht wirklich skalierbar. Aufgrund strengerer Compliance-Forderungen - beispielsweise durch die neuen Bestimmungen zum globalen Datenschutz (GDPR) - benötigen Unternehmen eine konsolidierte Berichtsplattform, welche Berichterstellung, Audits und Risikominimierung erleichtert.

Konventionelle Konzepte reichen nicht aus

Es gibt heute auf dem Markt eine Vielzahl von Lösungen, mit denen Unternehmen einzelne Sicherheitsprobleme der mobilen Cloud lösen können. Diese Lösungen unterstützen jedoch nicht die oben erwähnten umfassenden Best Practices.

- **Identitäts-Zugriffsverwaltung (IAM)**
  IAM konzentriert sich vor allem auf Identitätsverwaltung und Zugangskontrolle. IAM-Lösungen ermöglichen eine identitätsabhängige Zugriffskontrolle für die Cloud-Dienste, können den Zugriff aber nicht unter Berücksichtigung des Geräte-Risiko oder App-Risikos erlauben oder verweigern.

- **Verwaltung von Mobilgeräten (MDM)**
  MDM konzentriert sich auf die Absicherung von Mobilgeräten. Es sei darauf hingewiesen, dass nicht alle MDM-Anbieter die Cloud-Sicherheit angemessen berücksichtigen und viele Anbieter die oben beschriebenen Probleme durch nicht verwaltete Apps und nicht genehmigte Clouds nicht beseitigen können.
- **Cloud-Zugriffssicherheits-Broker (CASBs)**
  CASBs bieten Transparenz und eine granulare Kontrolle des Zugriffs auf Dateiebene sowie Sicherheit für Cloud-Dienste. Die Funktionalität zur Bestimmung der Profile von Geräten, zur Ermittlung des Geräte-Risikos und zur Sperrung des Zugriffs nicht konformer Geräte oder nicht genehmigter Apps auf Unternehmens-Cloud-Dienste ist jedoch sehr eingeschränkt.

Zwar sind bei diesen Lösungen allgemein die jeweiligen Einzelfunktionen gut implementiert, jedoch lassen sich diese isolierten Lösungen schwer integrieren, sodass Sicherheitslücken entstehen und die Unternehmensdaten weiter gefährdet bleiben.

MobileIron Access ermöglicht konsistente Sicherheit für die mobile Cloud

Unternehmen, die Unternehmens-Cloud-Dienste wie Box, G Suite, Office 365 und Salesforce nutzen, müssen eine bedingte Zugangskontrolle für all diese Dienste anbieten. MobileIron Access bietet sicheres, problemloses SSO und eine umfassende Transparenz, so dass Unternehmensdaten aus der Cloud nur für abgesicherte Geräte, verwaltete Apps und genehmigte Cloud-Dienste verfügbar sind.

Im Gegensatz zu Konkurrenzangeboten bietet MobileIron Access eine aus Standards aufbauende, einheitliche Plattform, welche die Cloud-Dienste absichert und den Benutzern zugleich die Möglichkeit gibt, mit dem Gerät unabhängig vom Ort produktiv zu bleiben. Unternehmensdaten sind daher auch bei der Übertragung in die und von der Cloud gesichert.

Vermeidung von Datenverlust

Eine wichtige Rolle spielt die Vermeidung von Datenverlusten durch bewusste oder unbewusste Handlungen der Mitarbeiter. Wie kann die IT-Abteilung beispielsweise verhindern, dass ein Benutzer Dateien aus Salesforce herunterlädt und in seinen privaten Dropbox-Ordner kopiert? Kann die IT den Zugriff auf Salesforce-Daten mit einem Webbrowser aus dem Cydia Store auf einem jailbroken iOS-Gerät blockieren?

MobileIron Access reduziert das Risiko solcher Datenverluste mit bedingten Zugriffsrichtlinien, die den Zugriff auf Unternehmens-Cloud-Dienste und Unternehmensdaten nur vertrauenswürdigen Benutzern, konformen Geräten, verwalteten Apps und genehmigten Cloud-Diensten erlauben. Das heißt, ein Mitarbeiter kann weder Dateien noch Daten aus einem verwalteten Cloud-Dienst wie Office 365 mit einer nicht verwalteten App, beispielsweise einem privaten Google Drive, teilen.

Vorrang für das Benutzererlebnis

MobileIron Access verbessert das Benutzererlebnis und bietet dazu problemloses, sicheres SSO für die Unternehmens-Cloud-Dienste, damit die Benutzer sofort auf Unternehmensdaten zugreifen können und nicht ständig spezifische Benutzernamen-Passwort-Kombinationen für jede einzelne mobile App und jeden Cloud-Dienst eingeben müssen. Im Gegensatz zu einfachem SSO arbeitet MobileIron Access problemlos mit jeder mobilen App zusammen und bietet damit eine zusätzliche Sicherheitsebene, weil Anmeldungen ungesicherter Apps verhindert werden.

Da Benutzerdaten nur noch selten eingegeben werden müssen, sinkt mit MobileIron Access SSO die Anzahl der Kontosperrungen aufgrund falsch eingegebener Anmeldeinformationen. Unternehmen können die Produktivität auch dadurch erhöhen, dass sie intuitive Workflows zur Risikominimierung nutzen und den Benutzern die Möglichkeit geben, ohne Einschaltung des Helpdesks Probleme selbst zu lösen.

Vereinfachung der Compliance-Berichte

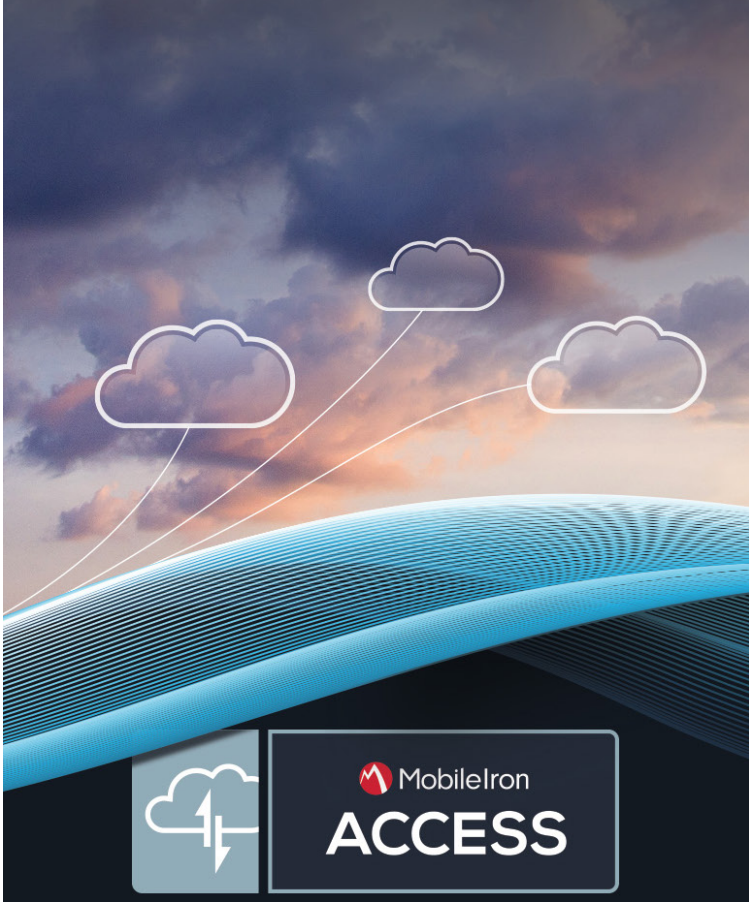
MobileIron Access fördert die Compliance durch umfassende Transparenz und Auditfähigkeit dank eines modernen Report-Generators, der alle Geräte, Apps, Dienste, Standorte und Benutzer verfolgt, die sich mit den Unternehmens-Cloud-Diensten verbinden. Diese sehr umfassende Transparenz macht es für Unternehmen einfacher, nicht-konforme Benutzer und Geräte zu identifizieren und Maßnahmen zur Wiederherstellung der Compliance einzuleiten. Genauso wichtig ist die Vereinfachung der Audits und der Compliance-Überwachung durch detaillierte Protokoll- und Berichtsfunktionen mit MobileIron Access.

MobileIron Access: Absicherung der Unternehmenstransformation in der Cloud

Die Einführung von Mobil- und Cloud-Technologien fördert massive Veränderungen in Unternehmen in aller Welt. Mit diesen neuen Technologien können Unternehmen Geschäftsprozesse rationalisieren, Kosten senken und den Mitarbeitern erlauben, unabhängig vom Ort produktiver zu arbeiten. Die Absicherung der mobilen Apps und der Cloud-Dienste erfordert jedoch mehr als die konventionellen, bei PCs üblichen Sicherheitskonzepte, die nicht für die mobile Cloud entwickelt wurden.

Das moderne Unternehmen benötigt heute eine umfassende, einheitliche Plattform wie MobileIron Access, die von Grund auf zur Absicherung von mobilen Apps, Geräten und Cloud-Diensten konzipiert wurde. MobileIron vereinfacht die Umgestaltung der Geschäftsabläufe durch Absicherung kritischer Unternehmensressourcen, beispielsweise der Desktop-PCs, Mobilgeräte, modernen Apps und Cloud-Dienste von einer zentralen Stelle aus.

Informieren Sie sich über MobileIron Access unter mobileiron.com/access



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