MobileIron Access

Secure cloud services on mobile

Rethinking security in a mobile-cloud world

The consumerization of IT has led to more employees using their personal mobile devices and apps for work. At the same time, companies around the world are shifting business processes to cloud apps and services like Box, G Suite, Microsoft Office 365, and Salesforce. As a result, more users are accessing these enterprise cloud resources simply by entering their company username and password on their personal devices or apps — putting enterprise data at risk.

While the username/password approach was adequate for securing cloud services on corporate PCs, it's not enough to protect enterprise data in the mobile-cloud world. In addition to verifying user identity, mobile app-to-cloud security requires a framework that includes the ability to check device posture and app authorization status to ensure only trusted users, devices, and apps can access corporate resources from the cloud.

The Challenge

- Mobile apps have become the primary way for business users to access cloud services.
- Traditional, PC-based security solutions are not enough to protect your data in the cloud.

MobileIron Access: The solution for mobile app-to-cloud security

MobileIron Access is a cloud security solution that provides conditional access to cloud services from mobile apps and browsers. Unlike traditional security approaches, MobileIron Access correlates user identity with unique information feeds such as device posture and app state. MobileIron ensures that business data stays within IT bounds so it can't be stored on unsecured devices, connect to unmanaged apps, or share information with unsanctioned cloud services. With MobileIron Access, organizations benefit from a standards-based approach that can secure any cloud service, including Office 365, without requiring any proprietary integrations.

Secure business data with MobileIron Access

MobileIron Access helps eliminate the mobile app-to-cloud risk in these common scenarios:

1. **Unmanaged device:** An employee wants to look up some information on Salesforce, but left her company iPad at work. With a username/password-only approach, the employee can enter her credentials in the Salesforce app on her personal iPad and access and store corporate content on the unsecured device. With MobileIron Access, the employee can't access data until she has registered and secured her device through MobileIron.

MobileIron

401 East Middlefield Road,
Mountain View, CA 94043

info@mobileiron.com
www.mobileiron.com

Tel: +1.877.819.3451
Fax :+1.650.919.8006

2. **Unmanaged app:** An employee accidentally downloads PowerPoint from the Office 365 suite using a third-party app store instead of the secure enterprise app store. With a traditional identity-based security solution in place, the employee can use the unmanaged version of PowerPoint to access corporate data. This data can also be shared with other insecure apps as well as unauthorized cloud services. Additionally, app data can't be wiped if the device is lost or stolen. MobileIron Access easily prevents the risk of data loss by prompting the user to download the managed version of PowerPoint from the enterprise app store.

3. **Unsanctioned cloud services:** An employee discovers a new productivity app and connects it to his corporate Box account using his user ID and password. Unfortunately, the app is malicious and uses publically available Box APIs to copy sensitive company files to an unauthorized cloud service. With MobileIron Access, unsanctioned cloud services can't connect to enterprise cloud services, which eliminates the security risk of data exfiltration.

Why MobileIron Access:

- Protect data with conditional authorization based on device, app, and cloud posture
- Simplify authentication with seamless SSO
- Accelerate remediation workflows to ensure continuous productivity
- Maintain detailed logs for audit and compliance reporting
- Use a standards-based approach to support a scalable, best-of-breed cloud security deployment
- Leverage an end-to-end platform for mobile-cloud security

Drive user adoption with seamless, SSO cloud access

The need to constantly remember and re-enter passwords is an ongoing frustration for users, especially since they rely on more mobile and cloud apps for work. Entering passwords on small mobile screens is no easy task, and users often mistype their credentials which can result in account lockouts, increase help desk calls, and diminish employee productivity.

MobileIron Access supports secure single sign-on (SSO) for cloud-based and in-house mobile apps. The best part is, it doesn't require any special integrations or modifications to the app itself. With MobileIron Access, users not only get the benefits of SSO, IT can ensure user privacy, simplify access to mobile business apps and data, and provide seamless security that keeps corporate data safe without creating obstacles to mobile productivity.

MobileIron Access gives you better visibility

As enterprises increasingly adopt a mix of cloud services, apps, and devices, IT needs a scalable, centralized way to apply policies and track, monitor, and report on compliance.

MobileIron Access offers detailed reporting and logging capabilities that allow IT to see how many users connect to cloud services, view the types of mobile devices and apps being used, and ensure that they are secured. Admins can easily drill down into the reports to identify users with outdated apps and so on.

Protecting data in the cloud is easier than you think

MobileIron Access combines unique device and app posture feeds with a standards-based framework to provide seamless and secure access to any cloud service from any mobile device. Learn how easy it is to solve mobile and cloud app security challenges at mobileiron.com/access.