MobileIron Access

Secure cloud access for mobile apps

The mobile-cloud world requires you to rethink security

As the era of the locked-down, corporate-owned PC comes to a close, organizations are increasingly moving their data to the cloud to help lower IT costs and deliver a more productive experience to mobile employees wherever they work. Today, mobile apps are the primary way employees access enterprise content. While mobile cloud access gives business users tremendous flexibility on any device, it also introduces a whole new security challenge: the mobile app-to-cloud risk.

As enterprises shift from PC-centric to mobile environments, security requirements are changing as well. This is because accessing data through mobile apps is fundamentally different than launching a browser on a PC:

- **Browser on corporate-owned PC:** Users access content through a web browser on a PC, which is completely secured and controlled by IT. Browser sessions are only temporary and no data is stored offline, so content can't be easily shared with other apps.

- **Mobile apps:** Mobile apps can be accessed on personal or corporate-owned devices. App sessions are persistent and data can be stored on the device, which makes it easier to share data with other apps and cloud services.

As a result, businesses that are transitioning from PC environments to mobile apps and cloud services have to rethink their security approach. Traditional, PC-based security solutions that rely primarily on user ID and password can't sufficiently protect cloud data from falling into the wrong hands through unsecured mobile apps. Mobile app-to-cloud security requires a solution that enforces policy based on both user identity and the security posture of the mobile device and app.

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

415 East Middlefield Road,
Mountain View, CA 94043

info@mobileiron.com
www.mobileiron.com

Tel: +1.877.819.3451
Fax :+1.650.919.8006

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 or shared with unauthorized 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.

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

- **Family iPad:** An employee wants to look up some information on Salesforce, but left her company iPad at work. With traditional security, the employee could just grab her personal iPad, enter her credentials in the Salesforce app, and access and store corporate content on the unsecured device. With MobileIron Access, the employee is instead prompted to register her device and can access data once the device is secured by MobileIron.

- **Sloppy App:** An employee accidentally downloads an app, such as Office 365, from 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 unsecured version of Office 365 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. MobileIron Access easily prevents the risk of data loss by prompting the user to download the secure Office 365 app from the enterprise app store.

- **Parasite App:** An employee discovers a new productivity app and connects it to his corporate Box account using only his user ID and password. Unfortunately, the app contains malware and uses publically available Box APIs to copy sensitive company files to an unauthorized cloud service. MobileIron Access eliminates the security risk of unapproved cloud services connecting to enterprise cloud services and exfiltrating sensitive data.

The Solution: MobileIron Access

- Protect cloud data from mobile app-to-cloud security threats.
- Leverage a standards-based approach that secures enterprise cloud services such as Office 365, Salesforce, and Box.
- Enforce conditional access and refine policies based on app and device posture, OS type and version, app state, geographic location, user identity, and more.
- Prevent data loss with granular policy enforcement.
- Automate comprehensive visibility and reporting.
- Ensure a seamlessly secure user experience and workflow.

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 the mobile app-to-cloud security challenge at mobileiron.com/access.