MobileIron Access: Zero trust security for the enterprise cloud

The solution for modern cloud security challenges

The shift toward mobile-cloud technologies is forcing organizations to completely rethink their approach to endpoint security — and that means eliminating the need for passwords for three main reasons:

1. **Identity alone is not enough.**
   Users often adopt unsafe password habits to make them easy to remember. For instance, they create weak passwords, write their passwords on sticky notes, or inadvertently fall victim to phishing scams.

2. **Passwords are a pain.**
   Typing credentials on small device screens multiple times per day is a productivity killer. Not only is it time-consuming, users often forget or mis-type their credentials often enough to get locked out of their accounts. This requires a call to the help desk to restore access, which results in even more downtime.

3. **Context is important for security.**
   Passwords don't offer any intelligence about the endpoint, app, or network being used to access business data. IT can't tell if the device is jailbroken or running malicious apps over compromised wireless networks. This lack of IT visibility and control puts enterprise data at risk.

Key benefits of MobileIron Access

Reduce the risk of data breaches
By eliminating passwords, ZSO reduces the risk of data breaches that result from stolen credentials.

Provide frictionless access
Access eliminates the need to memorize, enter, or reset complex passwords, which also reduces password-related help-desk costs.

Deploy zero trust mobile-cloud security
Conditional access ensuring that only authorized users, devices, and apps that are free of threats, can connect with business resources over authorized networks.

MobileIron Access drives mobile productivity while reducing the risk of data loss

MobileIron Access provides adaptive, context-aware policies that can quickly verify the user's identity as well as the security posture of the endpoint and the user's environment. This ensures only trusted users, endpoints, and apps can access enteprise cloud services such as Box, G Suite, Office 365, and Salesforce.

- **Reduce data loss by eliminating passwords.**
  MobileIron Access supports adaptive security that reduces the risk of data breaches from two main sources: identity theft and access through unauthorized endpoints, apps, and services. Access provides a smart policy engine that combines zero sign-on (ZSO), multi-factor authentication (MFA), and zero trust IT conditional access policies. Passwordless ZSO authentication allows users to quickly and securely gain access through authorized and compliant endpoints and apps. If threats are detected, adaptive access policies can require MFA for an added layer of security.

- **Enhance the user experience.**
  Capabilities such as ZSO or passwordless access, MFA with mobile push notifications, and intuitive remediation workflows simplify the user experience. These combined capabilities give IT the right tools and assurance needed to adopt mobile-cloud technologies while users benefit from easy and secure access to business data.

- **Simplify compliance reporting.**
  MobileIron Access helps drive compliance with in-depth visibility and audit capabilities through an advanced reporting engine that tracks all the endpoints, apps, services, locations, and users that connect to enterprise cloud services. This highly detailed level of visibility makes it easier for organizations to identify non-compliant users and endpoints and take steps to bring them back into compliance.

Our unique approach

MobileIron Access enables zero sign-on by replacing passwords with secure mobile devices as the user ID. The combination of Access, unified endpoint management (UEM) as the foundation, and mobile threat detection (MTD) as an added layer of security, forms our mobile-centric, zero trust platform. Together these capabilities ensure that only verified users, devices, apps, and networks can access business resources — without the need for passwords.

MobileIron Access: Complete cloud-based security

- **Zero sign-on.**
  Enable passwordless authentication by using mobile devices as the user ID and primary factor for authentication. ZSO provides adaptive authentication, including multi-factor authentication (MFA), based on risk. ZSO also works on any device — whether it's managed or not.

- **Zero trust policy engine.**
  Enforce smart, risk-based policies to prevent unauthorized users, endpoints, apps, or services from connecting to enterprise cloud services such as Office 365, Salesforce, G Suite, and Box. These policies can be enforced across any device running iOS, Android, Windows 10, or macOS.

- **Advanced reporting and analytics.**
  Access provides a single dashboard to monitor authentications, violations, and failed login attempts. It also enables easy-to-follow workflows that empower users to remediate device or compliance issues.

- **Standards-based security.**
  Access easily integrates with best-of-breed identity providers including Okta, Ping, and others to secure any cloud service that supports the SAML 2.0 and WS-FED standards — no custom integration work required.

Why MobileIron

Organizations need to provide easy, adaptive security that eliminates the need for passwords. Find out why a comprehensive, unified platform like MobileIron Access is the right choice for securing mobile apps, endpoints, and cloud services.

Learn more about MobileIron Access at www.mobileiron.com/access

MKT EN-0819-US