In recent years, the market for mobile and cloud technologies has completely shifted the behavior of enterprise users. People can now work anywhere, on any device, to access business apps and data from mobile apps and cloud services. Static, perimeter-based security can no longer keep up with all of the endpoints, users, apps, and data that travel far beyond the corporate firewall. Relying on old security approaches like password-only access control is no longer enough to secure this vast mobile-cloud infrastructure — especially since stolen user credentials were the top cause of data breaches in 2017.

In the era of the locked-down, IT-controlled PC, passwords alone could provide sufficient authentication to back-end resources. In the mobile-cloud world, passwords are inadequate because:

Passwords are not secure. 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.

Passwords are not user-friendly. 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 of course requires a call to the help desk to restore access, which results in even more downtime.

Passwords aren’t intelligent or aware of the user’s environment. From an IT perspective, passwords don’t offer any information about the endpoint, app, or network being used to access business data. Passwords can’t tell if the device is jailbroken or running malicious apps over compromised wireless networks. This lack of visibility and control puts enterprise data at risk.

Secure cloud access requires more than passwords

To protect access to cloud-based apps and data, organizations need a solution that is simple for the user and smart enough to adapt to complex environments. To meet these requirements, a true cloud security solution should provide:

- **Multifactor authentication (MFA):** Because passwords are easily hacked, lost, or stolen, MFA ensures that only verified users can access business apps and data.

- **Passwordless single sign-on (SSO):** Passwords are cumbersome. Replace passwords with a secure sign-on process that makes authentication as easy and seamless as possible for the user.

- **Powerful trust engine:** IT needs a trust engine that leverages device and app posture, user identity, location, and more to ensure only trusted users, endpoints, and apps can access enterprise cloud services.
Why traditional approaches fall short

There are a variety of solutions on the market today that help organizations solve separate pieces of the mobile-cloud security challenge, but they don’t provide the comprehensive platform required.

<table>
<thead>
<tr>
<th>Identity access management (IAM)</th>
<th>Mobile device management (MDM)</th>
<th>Cloud access security brokers (CASBs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM solutions primarily focus on identity management and access control. While they provide identity-based access control for cloud services, they have limited ability to allow or deny access based on the device or app posture.</td>
<td>MDM focuses on securing mobile devices. It’s important to note that not all MDM vendors adequately address cloud security. Many also lack adequate controls to block unauthorized access to enterprise cloud services, such as Office 365 and Salesforce.</td>
<td>CASBs provide visibility and granular file-level access control and data security for cloud services. However, they have very limited capabilities when it comes to profiling devices, assessing device posture, and preventing non-compliant devices or unsanctioned apps from accessing enterprise cloud services.</td>
</tr>
</tbody>
</table>

While each of these solutions generally perform their individual functions well, they are siloed solutions that are challenging to integrate, resulting in security gaps that leave business data vulnerable.
MobileIron Access: A simple and smart solution for mobile-cloud security

Organizations that use enterprise cloud services such as Box, G Suite, Office 365, and Salesforce need to provide conditional access control for all of these services. MobileIron Access helps establish baseline trust in the user’s environment based on a variety of factors including device, app, network, location, and user context. This allows IT to then apply the right policy to match the present risk with the sensitivity of the data they are accessing. In other words, Access can enable passwordless SSO if the risk is relatively low, or require MFA if the risk is higher. So if the CMO wants to access confidential product launch documents over an airport Wi-Fi connection, Access could require MFA as part of the security response to the user’s request.

The following capabilities enable organizations to confidently adopt mobile-cloud technologies and reduce the risk of data breaches.

Easy-to-use MFA app

MobileIron Authenticator is a simple MFA app that replaces cumbersome and expensive hard tokens with a secure mobile MFA solution that’s easy to use and cost-efficient. It also helps prevent the misuse of an employee’s corporate credentials in case they are stolen.

One-touch setup

Authenticator is extremely easy to set up through the MobileIron platform, which eliminates confusing setup guides and QR codes. The user only has to launch the Authenticator app for one-touch activation. Once activation is complete, the user is ready to verify login attempts on their configured smartphone.

Push notifications

MobileIron Authenticator sends instant notifications to users on their managed mobile phone, which gives them a quick and easy method to start approving login attempts.

Adaptive authentication

MobileIron Authenticator provides intelligent authentication flows that can adapt to a variety of feeds including endpoint posture, app, network, and user location.
### Native sign-on experience for modern endpoints

MobileIron Access provides sign-on capabilities that allow users to authenticate without having to enter passwords when an authorized app and endpoint is being used.

<table>
<thead>
<tr>
<th>Native mobile SSO experience</th>
<th>Posture checks and intelligent sign-on</th>
<th>Seamless SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access allows users to securely connect to business services via native mobile apps instead of first authenticating through a different SSO app or portal.</td>
<td>Access includes context-aware posture checks that traditional SSO solutions do not. These SSO checks verify the user’s identity as well as the state and posture of the endpoint and app. If the login request is made from an unauthorized endpoint or app, the user is provided with an easy-to-follow remediation workflow.</td>
<td>Adaptive policies provide users with passwordless authentication when users connect via authorized apps and endpoints.</td>
</tr>
</tbody>
</table>

### Trust engine for smart policies

Access also provides a context-aware policy engine that allows IT to make smart access control decisions that go beyond user identity and include device, app, service, user location, network, and more.

<table>
<thead>
<tr>
<th>Adaptive policies</th>
<th>Intuitive remediation workflows</th>
<th>Standards-based security</th>
<th>Advanced reporting engine</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT can correlate data based on various signals and then apply adaptive, risk-based policies that match the user’s environment.</td>
<td>The policy engine provides remediation workflows that help users quickly resolve problems on their own so they can stay productive wherever they work.</td>
<td>Any cloud service can be secured using a standards-based approach, which helps businesses choose the mobile-cloud technologies they need to meet growing business needs.</td>
<td>IT can track all the endpoints, apps, and users that connect to enterprise cloud services so they can identify and take corrective action toward non-compliant users and devices.</td>
</tr>
</tbody>
</table>
MobileIron Access: Securing cloud-based business transformation

The adoption of mobile and cloud technologies is driving massive change in organizations around the world. These new technologies enable organizations to streamline business processes, lower costs, and help employees work productively anywhere. However, securing mobile apps and cloud services requires more than passwords and legacy security approaches that aren’t designed for the mobile-cloud world.

Today’s modern enterprise requires a comprehensive, unified platform like MobileIron Access, which is designed from the ground up to secure mobile apps, endpoints, and cloud services — all from a single point of control.

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