Secure cloud access without passwords

Your MobileIron UEM holds the key

mobileiron

SECURING CLOUD SERVICES

As your business moves to the cloud, providing secure access that doesn't impede productivity is critical—and extremely challenging. Because password-only security is no longer up to the task, relying on it presents a tremendous risk.

The good news is that you already hold the key to protecting your mobile and cloud resources. By leveraging your existing MobileIron UEM, you can achieve mobile-centric, zero trust security. Adding MobileIron Access allows you to eliminate passwords and strengthen your company's entire security posture—anywhere.

This ebook explores how you can better secure access to your enterprise cloud services by taking your security requirements anywhere your digital infrastructure takes you. Learn how MobileIron's mobile-centric, zero trust security enables your organization to confidently adopt mobile-cloud technologies to drive greater business efficiency while reducing the risk of data breaches.

CLOUD-BOUND AND SECURITY-CHALLENGED

Cloud-based technologies are becoming the default choice for more and more companies. From Office 365 to Salesforce and Dropbox, most organizations are either aggressively adopting cloud services or are being forced to as users bring them in. They introduce significant business efficiencies—and a large gap in your security.

The adoption of mobile and cloud technologies is where business is headed, but for many organizations, their security hasn't kept up. Protecting mobile and cloud resources from unauthorized or malicious access is one of the toughest challenges facing organizations today.

Securing them takes a different approach—a mobile-centric, zero trust security approach that eliminates passwords and strengthens your entire security posture.

60% OF ENTERPRISES RELY ON THE CLOUD – UP 5X FROM 5 YEARS AGO.[1]

71% WILL INCREASE CLOUD SPEND >20%.[2]

[1] Predictions 2019: Cloud Computing Comes of Age as the Foundation for Enterprise Digital Transformation. Dave Bartoletti, Forrester. Nov 8, 2018.

[2] RightScale 2018 State of the Cloud Report.

WHY PASSWORDS FAIL

They aren't secure

Users have their own way of managing passwords, often with cringe-worthy work-arounds like password sticky-notes and files named "Password". Many use the same password across multiple accounts. Add this to the relative ease with which hackers can steal passwords, and it's little wonder passwords are the number one cause of breaches.[3]

They aren't smart enough

Passwords only give you one piece of an intricate security puzzle: verifying user identity before granting access to cloud services. But you're no longer on tethered computers in a tidy, defined enterprise network. Access is now from anywhere, often on questionable Wi-Fi, on a variety of mobile devices, across a variety of apps. Passwords don't give any security context, such as the state of the device requesting access, the application, the network and possible threats on the device. Insight into each of these factors helps make the right access decisions.

Users can't stand them

Ask anyone their opinion of passwords and the eye-roll is similar. The complex combination of caps, numbers, symbols and unrepeatability creates a frustrating cycle of forgetting, resetting and lockouts. And as the number of apps your company uses grows, so too does the password memory challenge and hassle.

They're expensive

The major issue with passwords is forgetting them. The cost of supporting password systems, including staffing and infrastructure can be significant. As more work is done in the cloud on more systems with multiple log-in details, the chances for problems to arise and workflow to be interrupted grows. In the enterprise, every minute wasted affects productivity, which in turn, directly affects revenue. IDG research estimates they cost an employer around $1/minute—more if the help desk gets involved.[4] You can do the rest of the math.

There's a better way

The productivity benefits of your mobile and cloud resources need not be diminished by using frustrating and ineffective passwords to secure access. You can eliminate the pain of passwords and strengthen your security by building upon your existing MobileIron UEM to create a mobile-centric, zero trust security approach that supports your mobile-cloud technologies. Let's take a look at how that's achieved by adding **MobileIron Access** and **Threat Defense**.

81% OF BREACHES ARE FROM WEAK, STOLEN OR REUSED PASSWORDS.

PASSWORDS COST EMPLOYERS $1/MINUTE.

[3] Verizon Data Breach Investigations Report (DBIR).

[4] Hidden costs of passwords. M.E. Kabay, Network World. October 18, 2007.

mobileiron

SMARTER SECURE ACCESS TO THE CLOUD

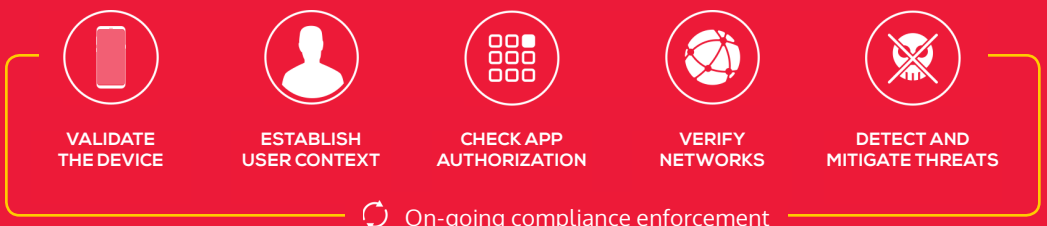
The power of mobile-centric, zero trust security

For companies who rely on cloud platforms and apps to move their business forward, our mobile-centric, zero trust approach security is ideal.

It allows you to grant access to your cloud services only after receiving far greater security context than mere passwords can provide.

The Zero Trust Approach
Assume bad actors are already on your network

Never trust, always verify.



mobileiron

Mobile-Centric, Zero Trust Security

Built upon the UEM foundation you already have

ACCESS
Eliminate passwords with secure frictionless authentication
Zero Sign-On

THREAT DEFENSE
Block any threat on any device

YOUR UEM
Turn your device into your secure enterprise ID

MobileIron Access: stronger security without passwords

Your existing MobileIron UEM gives you the foundation to redefine your security strategy and achieve mobile-centric, zero trust security—by turning your device into your secure ID to the enterprise.

By adding MobileIron Access you'll have a more complete security snapshot before granting access to any cloud service or app. Zero Sign-on verifies critical signals for greater security context before granting access—without a single password.

SMARTER SECURE ACCESS TO THE CLOUD

MobileIron Access: more context, security and freedom

Ensure that business information is only available to verified users on authorized endpoints, apps, and cloud services—all without a single password. Consider the advantages:

PASSWORD-FREE EXPERIENCE Many vendors have talked about it, but only MobileIron did it with Zero Sign-On—eliminating the password once and for all.

We turned the mobile device into your ID and secure access, for a seamless authentication experience from anywhere. Users can securely access any business app, device, or resource with a glance or a tap of their finger. No passwords or single sign-on (SSO). Just simple password-free access from anywhere.

SECURE ACCESS FROM ANY DEVICE – WHETHER YOU MANAGE IT OR NOT
Whether Android, iOS, macOS, or Windows 10 devices, our standards-based platform is device agnostic to give you and users secure password-less access from any device—even those not managed by your organization. That means not a single unauthorized device, app or network can connect to your business systems.

CLOUD SERVICE FREEDOM WITH STANDARDS-BASED SECURITY Our mobile-centric, zero trust security is built on a standards-based platform that allows you to deploy a common security framework across all of your cloud services. Whether it's Office 365 or Salesforce or an internally developed app—MobileIron Access can protect any enterprise app and will continue to meet your evolving business needs. Some other vendors are not as generous, locking you into either their own SaaS solutions or only securing Office 365.

FINALLY, NO MORE PASSWORDS.

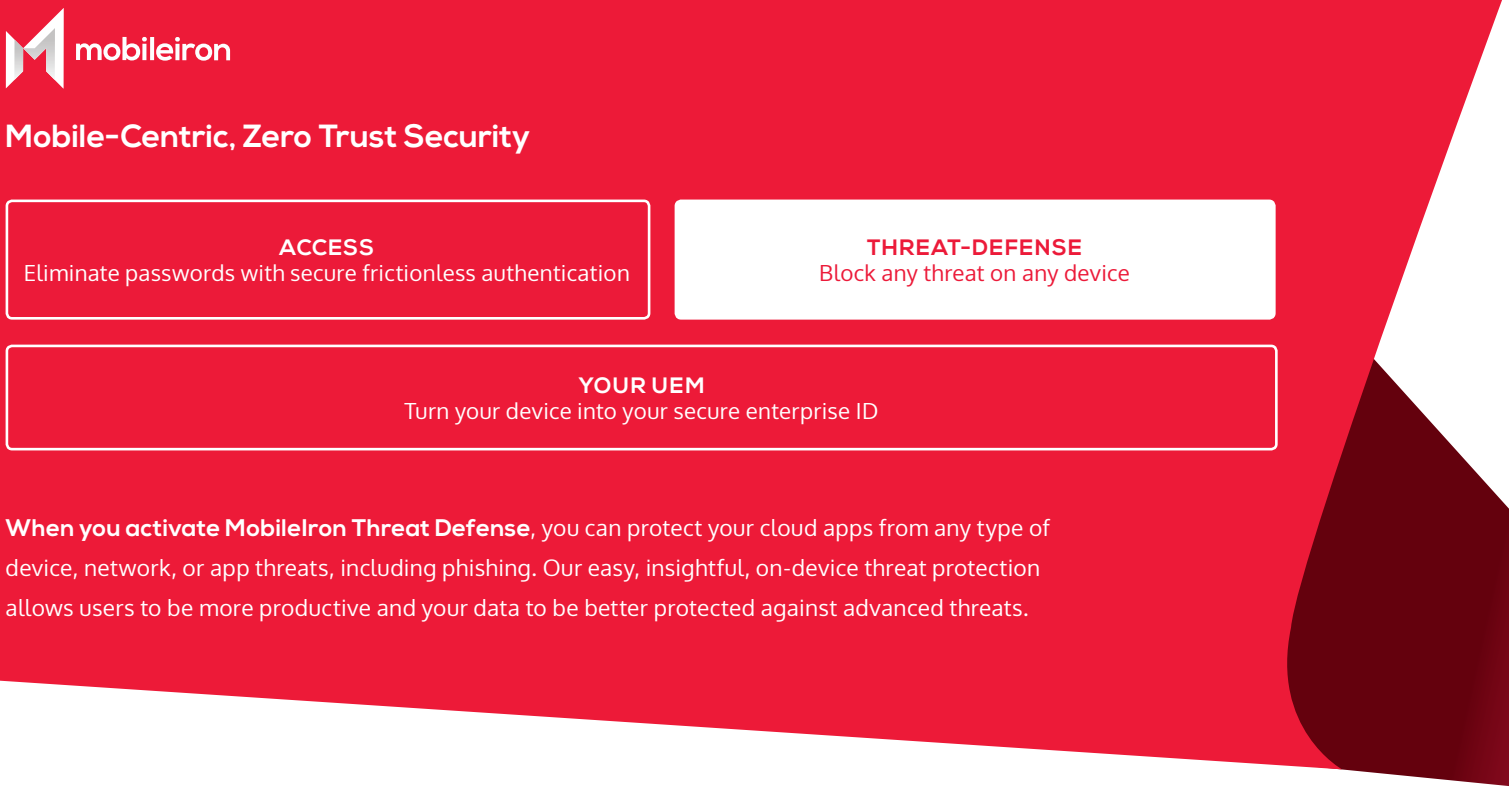
SECURE ANY DEVICE. USE ANY APP.

DATA PROTECTION WHEREVER IT LIVES

MobileIron Threat Defense

We've shown how MobileIron Access can protect access to all of your critical productivity apps and cloud services. Information from your existing MobileIron UEM, which establishes device, app and posture compliance, makes that possible.

The third leg of our mobile-centric, zero trust security approach is **Threat Defense**.



When you activate MobileIron Threat Defense, you can protect your cloud apps from any type of device, network, or app threats, including phishing. Our easy, insightful, on-device threat protection allows users to be more productive and your data to be better protected against advanced threats.

Immediate, on-device threat protection

Protect against device, app, network, and phishing attacks even when the device is offline. Receive unmatched detection of known and zero-day mobile threats with machine-learning algorithms on-device and local remediation actions with local user notification, across iOS and Android devices.

100% user adoption

A single app makes it easy to deploy and manage for every user because threat protection is built into the MobileIron UEM client. As a result, IT can activate threat detection and remediation capabilities without requiring any user action.

Detailed threat forensics

Gain immediate and ongoing visibility into malicious threats across all mobile devices and receive detailed analyses of risky apps.

HEAD TO THE CLOUD SECURELY WITH MOBILEIRON

As your company embraces more cloud resources, make sure you have the right security to protect them from unauthorized or malicious access. Passwords are no longer up to the task—from the breach risk they represent to their widespread unpopularity with IT and end-users alike.

Your existing MobileIron UEM is the key to achieving mobile-centric, zero trust security. By adding standards-based security with MobileIron Access, you can ensure that access is only granted after users, endpoints, apps and cloud services are verified—without a single password. And MobileIron Threat Defense blocks any type of threat—around the clock.

Maximum security. Minimum hoops.

The cloud is where your business is headed. MobileIron can take your security where it needs to be too.

- **End-users** can access their cloud business tools on any device they choose with a seamless access experience.
- **IT** can interact with one scalable platform and one screen into your mobile and cloud security. Goodbye lock-outs, you've got better things to do.

With the UEM you already have, you're already on your way to achieving mobile-centric, zero trust security. Head to the cloud with your security and productivity held high by adding MobileIron Access and Threat Defense today.

CONTACT YOUR REP TODAY

To learn more, go to: info.mobileiron.com/ContactUs