# The perimeter's gone. Can your security handle it?

Protect the modern enterprise with
a mobile-centric, zero trust framework

MobileIron

MobileIron

# INTRODUCTION

## Security in a perimeter-less world

It's safe to say that mobile dominates the enterprise. In addition to changing the way we work, mobile and cloud technologies have dissolved the enterprise security perimeter. This has introduced new threat vectors that traditional security frameworks are simply not designed to defend against. Organizations need to shift their security strategy to secure the new ways work gets done. That takes a "never trust, always verify" approach that starts with devices and goes further than other zero trust security methods.

In this eBook, we'll explore the industry's first mobile-centric, zero trust framework, and how a strategy using this approach can help the modern enterprise stay agile and secure in a perimeter-less world.

MobileIron

# THE NEED

### With freedom comes risk

No one doubts the impact mobile devices have on our lives—or the enterprise. The latest statistics speak for themselves.

Productivity and business innovation have benefited immensely as data flows freely across a wide information fabric of devices, apps, networks, and cloud services. This freedom of anytime, anywhere access has effectively dissolved the traditional security perimeter. This has created a massive attack surface and a host of new risks and threats that traditional security approaches weren't designed to address.

### Data's getting around

As desktops are replaced by mobile endpoints, and data centers move workloads to the cloud, data no longer stays inside a tidy enterprise perimeter. It's on devices and clouds you own and those you don't, crossing networks other than yours—many with less than robust security.

### Hackers follow the opportunity

Attacks that we've seen on the desktop are quickly making their way toward mobile because of simple economics. Hackers follow the data, which is their jackpot. It's more efficient for bad actors to try new doors instead of breaking through old ones with layers of PC protection. With so many devices and so little security, it's a no brainer.

### Mobile vulnerabilities

Hackers can easily exploit mobile vulnerabilities and user behavior to gain an alarming level of control over your entire company. As mobile attacks become more sophisticated, organizations need a mobile-centric security approach to keep their data secure.

**It's clear that traditional security models built for the PC and data-center world don't translate to the mobile-cloud world.**

**It's time to take a hard look at your security strategy.**

**WE CHECK OUR PHONES 80X A DAY.[1]**

**77% OF ENTERPRISES USE CLOUD SERVICES.[2]**

**52% OF WEBSITE TRAFFIC IS FROM PHONES.[3]**

**AN AVERAGE ENTERPRISE USES ~1,000 APPS.[4]**

# THE ZERO TRUST APPROACH

### Never trust, always verify

Introduced by Forrester in 2014, the zero trust approach recommends that while building a security strategy, you should start from the assumption that your network is already compromised. Secure access should be determined by a "never trust, always verify" approach that requires you to verify the device, user, apps, networks, and presence of threats before granting access—with constant enforcement.


There are multiple approaches to zero trust, but the main ones are focused on identity, gateway, and the device. But only a mobile-centric approach addresses the security challenges of the perimeter-less modern enterprise while allowing the agility and anytime access business needs.

### Raising the security bar

A mobile-centric, zero trust framework goes beyond traditional identity management and gateway point solutions by raising the security bar. It demands more answers from a comprehensive set of attributes before granting access. It validates the device, establishes user context, checks app authorization, verifies the network, and detects and remediates threats—all before granting secure access to any device or user. And it all happens instantaneously.

# THE MOBILEIRON SOLUTION

### Mobile-centric, zero trust security

MobileIron has always believed that mobile is the center of the enterprise. So we created a security platform that starts from the device and goes beyond other zero trust approaches.

### Your device is your ID

By making your mobile device your secure ID, we are eliminating passwords and making access to business information more secure and much easier. This allows organizations to give mobile users the freedom and flexibility they need to be productive wherever they work. And to protect data wherever it lives.

**WE'VE MADE YOUR MOBILE DEVICE YOUR SECURE ID AND ACCESS TO THE ENTERPRISE.**

### How we do it

MobileIron is redefining enterprise security with the first mobile-centric, zero trust platform built on our award-winning, unified endpoint management (UEM) foundation to secure access across the perimeter-less enterprise.

Our approach significantly reduces risk by taking more signals into account before granting access. It validates the device, establishes user context, checks app authorization, verifies the network, and detects and mitigates threats—all before green-lighting access to a device or user. This gives you complete control over your business data as it flows across devices, apps, networks, and cloud services.

The diagram below outlines the four-step process to implement a mobile-centric, zero trust approach—one that's both embraced by users for its seamless experience, and by IT for its easy implementation and dramatic reduction in help-ticket requests.

## MOBILE-CENTRIC, ZERO TRUST APPROACH

**1. PROVISION** any device for a user with the appropriate apps, profiles, and policies. UEM (Unified Endpoint Management) is the foundation—the first step in achieving mobile-centric, zero trust security.

**4. ENFORCE SECURITY POLICIES** with ongoing monitoring; any change in signals will trigger adaptive policies to mitigate threats, quarantine devices, and maintain compliance.


**2. GRANT ACCESS** based on full context: verify the user, posture of the device, app authorization, network type, presence of threats, and a variety of other signals. This adaptive access control check is the basis of the zero trust model.

**3. PROTECT DATA** at rest and in motion with state-of–the-art encryption and threat monitoring to detect device, network, and app-level attacks.

MobileIron

# THE MOBILEIRON SOLUTION

## What powers mobile-centric, zero trust security

**MOBILEIRON UEM** Our award-winning unified endpoint management (UEM) product provides the visibility and IT controls needed to secure, manage, and monitor any corporate or employee-owned mobile device or desktop that accesses business-critical data. It allows you to secure a vast range of employee devices coming into the enterprise and manage their entire lifecycle.

**MOBILE THREAT DEFENSE** We provide zero trust security using built-in threat detection and remediation across devices, apps, and networks — without the need for Internet connectivity or concerns about user adoption. This is critical as hackers continue to target and develop sophisticated attacks for mobile devices and apps.

**MOBILEIRON ACCESS** Seamless, conditional access is achieved through password-less single sign-on (SSO) and multi-factor authentication (MFA). This supports a zero trust framework by ensuring only authorized resources can access and share corporate data from any device, OS, or location to any service.

## Seamless security for the ways work gets done today

Not only are employees unaware of all the checks going on in the background, but we've created an enhanced experience that makes life easier for both IT and end users:

- **Easy device on-boarding and automatic configuration – no lengthy employee set up guides to struggle through.**
- **Zero password for instant access – no more fumbling, retyping, or remembering passwords – ever.**
- **Continuous on-device threat detection – no user action required.**
- **Intuitive remediation workflows – non-compliant devices can be easily fixed without helpdesk involvement.**

MobileIron

# THE TAKEAWAYS

## The security strategy for a perimeter-less world

Mobile and cloud have both transformed business and complicated security by creating a perimeter-less environment that traditional security solutions weren't designed to address. Many organizations are adopting a zero trust security model, which assumes the threat is already inside the network. Gateway- and identity-centric approaches are two variations on zero trust, but both fall short in several key areas. As more organizations shift their workloads to the cloud, it's clear that today's security strategies need to start with mobile at the center.

MobileIron has redefined enterprise security with the first mobile-centric, zero trust platform that turns the mobile device into a user's secure ID for enterprise access. Built on an award-winning UEM foundation, this approach provides the enterprise with a modern security strategy that allows it to:

- **Drive business innovation by confidently adopting mobile and cloud technologies**
- **Provide users with the best experience to drive productivity**
- **Provide the right level of security from all points of access**

If you'd like to learn how MobileIron can help your organization benefit from a mobile-centric, zero trust security strategy, let's talk.

LEARN MORE

[1] "Americans check their phones 80 times a day: study." Newyorkpost.com, November 8, 2017, https://nypost.com/2017/11/08/americans-check-their-phones-80-times-a-day-study/

[2] "State of Enterprise Cloud Computing, 2018." Forbes.com, August 30, 2018, https://www.forbes.com/sites/louiscolumbus/2018/08/30/state-of-enterprise-cloud-computing-2018/#446d48e0265e

[3] "Percentage of all global web pages served to mobile phones from 2009 to 2018." Statista, 2019, https://www.statista.com/statistics/241462/global-mobile-phone-website-traffic-share/

[4] "Enterprises on average use up to 1000 cloud apps but their CIOs think it's just 30 or 40 apps." ETCIO.com, April 28, 2017, https://cio.economictimes.indiatimes.com/news/strategy-and-management/enterprises-on-average-use-up-to-1000-cloud-apps-but-their-cios-think-its-just-30-or-40-apps/58410934