# State of App Security

Recent attacks targeting mobile apps and operating systems have put an unprecedented amount of mobile business data at risk. Many enterprises are unprepared to combat the latest mobile threats:

- One in 10 enterprises have at least one compromised device.
- More than 53% have at least one device that is not in compliance with corporate security policies.

This white paper outlines how to protect enterprise data while realizing the transformative benefits of mobility.

For more information about protecting corporate data against mobile threats, listen to MobileIron's on-demand webinar.

415 East Middlefield Road
Mountain View, CA 94043 USA
Tel. +1.650.919.8100
Fax +1.650.919.8006
info@mobileiron.com

MobileIron

## Apps drive business

The transformative power of mobility can only be realized by mobilizing core business processes. Both custom-developed and third-party apps are at the heart of this transformation.

*We are tech savvy consumers that have come to expect consumer-grade experiences from our work tools.*

MobileIron customers have deployed more than

**300,000 apps**

that were custom built for employee use.

**Top third-party apps deployed:**

1. Salesforce
2. Goodreader
3. Microsoft Office Suite
4. Cisco AnyConnect
5. Box
6. Cisco Webex
7. Skype for Business
8. Google Docs
9. Evernote
10. Xora Mobile Worker

## But they need to be properly secured

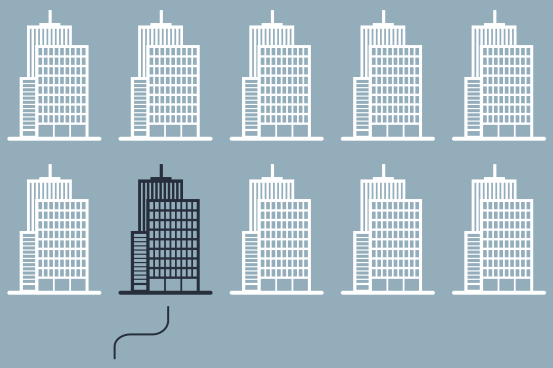
As the future of work evolves toward mobility, the future of data breaches and cybercrime lies in mobile apps and operating systems.

Recent attacks, such as XcodeGhost, Stagefright, Key Raider, and YiSpecter, for the first time are targeting mobile apps and operating systems to exfiltrate sensitive data. Many enterprises are unprepared.

For example, iOS apps infected with XcodeGhost malware can collect information about devices and then encrypt and upload that data to command and control (CnC) servers run by attackers through the HTTP protocol. Malware detection company FireEye identified more than 4,000 infected apps on the App Store and mobile app risk management company Appthority found that almost every organization with at least 100 iOS devices had at least one infected device.

*Attackers are starting to capitalize on enterprises' inability to prevent and detect mobile malware.*

The KeyRaider malware was used to steal information from 225,000 jailbroken iPhones. ActiveSync/O365 and anti-virus tools are ill-equipped to protect against today's mobile threats because they have no visibility into jailbroken or rooted devices.



**1 in 10 enterprises** has at least one compromised device

Malware is becoming more sophisticated and a recent approach is to infiltrate corporate networks over the VPN to steal data. Anti-virus is not effective in this situation because mobile operating systems sandbox applications, preventing anti-virus from removing threats. When employees use a VPN to access the corporate network, organizations are unknowingly allowing all apps to possibly access the network, including malicious apps.

Companies need to make sure they are using **anti-malware**

Enterprises must also consider data loss from rogue access points and Man in the Middle (MitM) attacks. In the mobile world, devices that the company may or may not own are crossing networks the company doesn't own. For example, an employee traveling on business may connect to an open Wi-Fi hotspot that may or may not be legitimate. Traditional Network Access Control (NAC) has very limited visibility into the security posture of a mobile device.

More than 53% of enterprises have at least one device that is **not in compliance** with corporate security policies

Today's organizations have many disparate security technologies that are rarely fully integrated. Even when they are, they seldom include information about mobile devices and apps. As more work gets done on mobile devices and more enterprise data moves in apps and clouds, organizations need to ensure that they are protecting themselves against internal and external threats.

## Time to rethink app security

MobileIron secures corporate data in a world of mixed-use devices by separating the corporate data and apps from the personal data and apps, and by authenticating users, apps, and devices before granting access to network resources. Based on the identity of the user and the security context of the user, app, device, network, and cloud, MobileIron allows the enterprise to make dynamic decisions about what services to provide to whom and when.

*To protect sensitive data against the threats of tomorrow, enterprises need to rethink their security approach for a fundamentally different mobile architecture.*

## Proactive Defenses

Most current security technologies lack mobile awareness and the ability to prevent data loss. MobileIron embraces the new features found in mobile to create innovative ways of protecting mobile enterprise data in apps, in the cloud, on the network, and on the device using containerization, encryption, and app-level data loss prevention (DLP) controls.

- MobileIron AppConnect secures app data-at-rest.
- MobileIron Tunnel secures app data-in-motion.
- MobileIron's Content Security Service provides document-level security to protect enterprise content across personal cloud services.
- MobileIron Sentry, MobileIron's intelligent gateway, manages, encrypts, and secures traffic between the mobile device and back-end enterprise systems.

## Automated response to threats

Current response mechanisms are failing to detect and respond to mobile threats. MobileIron does both online and offline detection of malware/compromise and initiates automated, real-time responses such as wiping corporate data and apps or blocking network access. For example:

- A compromised or out of compliance device can be quarantined and the enterprise data removed.
- Network access can be limited or totally blocked in response to the device being rooted or jailbroken.

## App data-at-rest and app data-in-motion security

Mobile computing puts enterprise data in apps, therefore data must be secured at the app level. MobileIron's AppConnect protects data-at-rest within the app and provides DLP controls in order to ensure that enterprise data is shared only with corporate sanctioned apps and cloud services. AppConnect deletes corporate data

when a threat is detected. Data-in-motion is secured using MobileIron Tunnel for per-App VPN.

MobileIron Docs@Work provides data loss prevention (DLP) controls to protect these documents from unauthorized distribution and secure access to enterprise storage services like SharePoint, Office 365, OneDrive Pro, and Box. In conjunction with MobileIron Sentry, Docs@Work secures email attachments so that they are encrypted and can only be viewed using authorized applications that are managed by MobileIron.

## Integrations to make the existing enterprise security stack mobile-aware

MobileIron provides in-depth defense with an ecosystem of best-of-breed partners which integrate with MobileIron to make enterprise infrastructure mobile-aware. MobileIron has integrated with leading Threat Management vendors including FireEye, Veracode, CheckPoint, and Proofpoint for malware detection and mitigation, and top Network Access Control vendors Aruba, Cisco and Forescout. MobileIron has also integrated with Splunk to allow IT to intercept security threats by correlating mobile device data with Splunk's common information model to diagnose problems.

## MobileIron AppConnect: an ecosystem of secure mobile apps

MobileIron's partnerships with leading Enterprise File Sync and Sharing (EFSS) vendors lets IT give users access to the consumer apps they want to use while ensuring that corporate data can be protected. With MobileIron, companies can put controls on EFSS apps including:

- Requiring that users login to apps such as Box only on trusted devices
- Whitelisting specific 3rd-party apps to ensure content can only be opened into other managed applications
- Restricting the ability for users to cut, copy, or paste content

In addition to EFSS partners, MobileIron has more than 70 AppConnect partners with more than 80 integrated solutions in market.

## Conclusion

Mobile has introduced a new operating system architecture and application model. User expectations and threat landscapes have changed so that traditional information security technologies are no longer effective.

MobileIron incorporates identity, security context, and privacy enforcement to set the appropriate level of access to enterprise data and services. This prevents the loss of enterprise data from mobile devices, apps, internal networks, or cloud.

With MobileIron, only trusted users on trusted devices with trusted apps over trusted sessions can access enterprise data. That's modern enterprise security.