Five steps to executing a mobile threat defense strategy

Protecting your business against mobile threats is a race against time. Are you doing everything you can to defend against an attack?

Do your employees ever use free airport, hotel, or coffee shop Wi-Fi networks? What about USB ports? How do you know if their devices are safe from a man-in-the-middle (MITM) attack or a hacker attempting to steal their corporate credentials? Do you have a strategy in place to recognize and block these types of attacks?

This five-step guide can help you design a best-practice strategy that delivers actionable intelligence and immediate protection against advanced mobile threats that target your mobile workforce. Learn how on-device mobile threat defense can protect your devices, apps, and data from the latest security risks.

MobileIron

An effective mobile threat defense (MTD) strategy is a race against time because attacks on mobile devices are rapidly escalating and increasing in severity. The organizations behind these exploits are driven by a huge profit motive, so they are extremely determined and very good at what they do. A 2017 Ponemon Institute security report found that companies have an estimated 28% chance of experiencing a recurring data breach that involves the loss of at least 1,000 records containing personal information about consumers or customers — information that is highly valuable to cybercriminals.[1] The consequences of this kind of attack can be staggering: In addition to lost or compromised data, a well-publicized data breach can hurt customer relationships, damage your corporate reputation, result in lost revenue, run up excessive fines and legal costs, and siphon valuable time and resources to clean up the mess.

If you aren't doing everything you can to insure your business against this level of risk, now is the time to start. These five best-practice steps can help you identify your security blind spots and deliver complete protection to all the mobile devices accessing corporate apps and data wherever employees work, on any network.

The current mobile threat landscape

75% OF ATTACKS
ARE PERPETRATED BY OUTSIDE HACKERS

81% OF HACKING-RELATED BREACHES
LEVERAGE STOLEN PASSWORDS

73% OF BREACHES
ARE FINANCIALLY MOTIVATED [2]

ICT Security Magazine, "2017 Data Breach Investigations Report, 10th Edition"

[1] https://www.ponemon.org/blog/2017-cost-of-data-breach-study-united-states

[2] https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

Step 1:
Activate seamless and invisible threat defense

Some mobile security solutions rely on end users to secure their mobile devices, which is an unreasonable and ineffective approach to MTD. These "user-based security" solutions require a mobile employee to go to the company's app store, download the client, and follow multiple steps to install, activate, and keep the app consistently updated. What's worse, after the client is installed, IT has very little enforcement control because users can simply delete the app or deactivate it (swipe off) — putting corporate data at risk. In fact, one study found that over one-third of companies fail to adequately secure mobile devices due to the lack of budget and resources needed to consistently deploy advanced security across their organization.[3]

IT organizations often depend on users to activate the latest security apps on their devices. However, if users fail to update their devices, the company may be vulnerable to attacks if not all endpoints are in compliance with security policies. It's therefore no surprise that a 2017 Dimensional Research report found that "two-thirds of the survey's participants stated they are doubtful that their organizations can defend against a mobile cyberattack, while nearly all security professionals believe the number of mobile attacks will increase rapidly."[4]

To ensure immediate, 100% security coverage on every mobile device that accesses corporate resources, organizations must stop relying on users to install the latest updates. To seamlessly deploy advanced mobile security, Gartner recommends that organizations "integrate the MTD solution with the enterprise mobility management (EMM) tool."[5] With this approach, IT admins deploy security protection and updates directly to the device through EMM. This means no user action is required to download and activate the latest security updates, and privacy policies are upheld. A solution that integrates EMM with MTD also allows IT to focus on more strategic priorities and reduce operational overhead by eliminating the need for admins to chase down users to make sure their devices are in compliance.

> *"Two-thirds of the survey's participants stated they are doubtful that their organizations can defend against a mobile cyberattack, while nearly all security professionals believe the number of mobile attacks will increase rapidly."*
>
> *Dimensional Research, "The Growing Threat of Mobile Security Breaches: A Global Survey of Security Professionals"*

[3] https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf
[4] https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf
[5] https://www.gartner.com/doc/3789664/market-guide-mobile-threat-defense

Step 2:
See all types of cyberattacks

The lack of visibility into mobile threats is one of the greatest mobile security challenges businesses face today. In fact, more than half (51%) of surveyed companies said they had no idea if malware had ever been downloaded on the mobile devices employees use for work.[6] Some mobile security solutions actually contribute to the lack of visibility because they focus only on app-level threats. However, not all cyberattacks are created equal. There are several types of attack vectors that can bypass this narrow approach through other means. As a result, organizations can't just focus on a single layer; they have to provide fully integrated and comprehensive mobile security to prevent device, network, and application (DNA) attacks.

- **Device-level attacks:** These include some of the most serious threats because successful exploits can give hackers complete control of the device and allow them to remove encrypted content. Device-level attacks are often launched through free app downloads or an SMS message that launches malware as soon as the user opens it.
- **Network-level attacks:** Public networks, while useful and convenient, can also provide the on-ramp that lead exploits directly to mobile devices. For instance, a rogue access point coming from free Wi-Fi in a hotel or coffee shop can launch an MITM attack and intercept communications between the device and the corporate network. The attacker can quickly scan the device for known vulnerabilities that can be used to compromise the device, collect usernames, passwords, and confidential corporate data that can be used later to gain access to corporate resources.
- **App-level attacks:** These attacks usually happen when unsuspecting users install an app from a third-party app store. The app contains malware that can access permissions, execute a device exploit, and penetrate internal networks to steal corporate data.

Solutions that leverage sophisticated machine-learning algorithms and behavior-based detection on the mobile device can help organizations block these types of known and unknown (zero-day) attacks. Instead of narrowly focusing on a single app-based threat vector, machine-learning tools can instantly recognize and block all types of abnormal activity, such as an unauthorized VPN configuration or free app download.

> *"More than half (51%) of surveyed companies said they had no idea if malware had ever been downloaded on mobile devices employees use for work."*
>
> *Zimperium, "Mobile Security 2017 Spotlight Report"*

[6] http://go.zimperium.com/2017-mobile-security-report

Step 3:
Deliver actionable threat intelligence

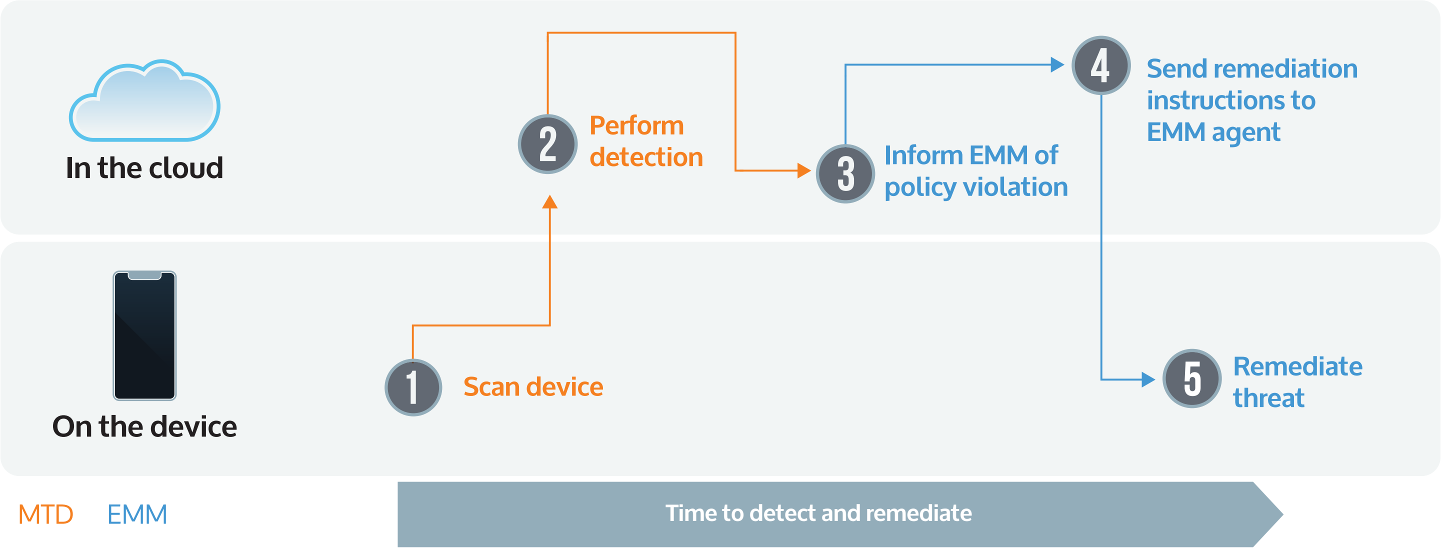
Just as the lack of visibility can create security blind spots, so can a constant barrage of alerts that assign all threats the same level of priority. As a result, "alert fatigue" can set in and make it difficult for mobile security admins to make informed decisions quickly.

To deliver actionable threat intelligence, MTD solutions should include an analytics engine that leverages machine-learning algorithms to distinguish normal from malicious behavior on the device itself. By analyzing slight deviations to the mobile device's OS statistics, memory, CPU, and other system parameters, machine learning can accurately identify not only the specific type of malicious attack, but also provide detailed forensics associated with the who, what, where, when, and how of an attack.

On-device, machine learning-based solutions detect attacks even when users are not connected to the network or when confronted with unknown malware, new threats, or zero-day attacks. This type of solution also works faster than cloud-based solutions because there's no need to tunnel traffic through the cloud. Mobile security experts can quickly identify imminent threats, assign them a priority, and take immediate action to prevent a serious attack from accessing corporate resources.

Detection and remediation

Other MTD and EMM solutions


In the cloud
On the device
1 Scan device
2 Perform detection
3 Inform EMM of policy violation
4 Send remediation instructions to EMM agent
5 Remediate threat
MTD
EMM
Time to detect and remediate

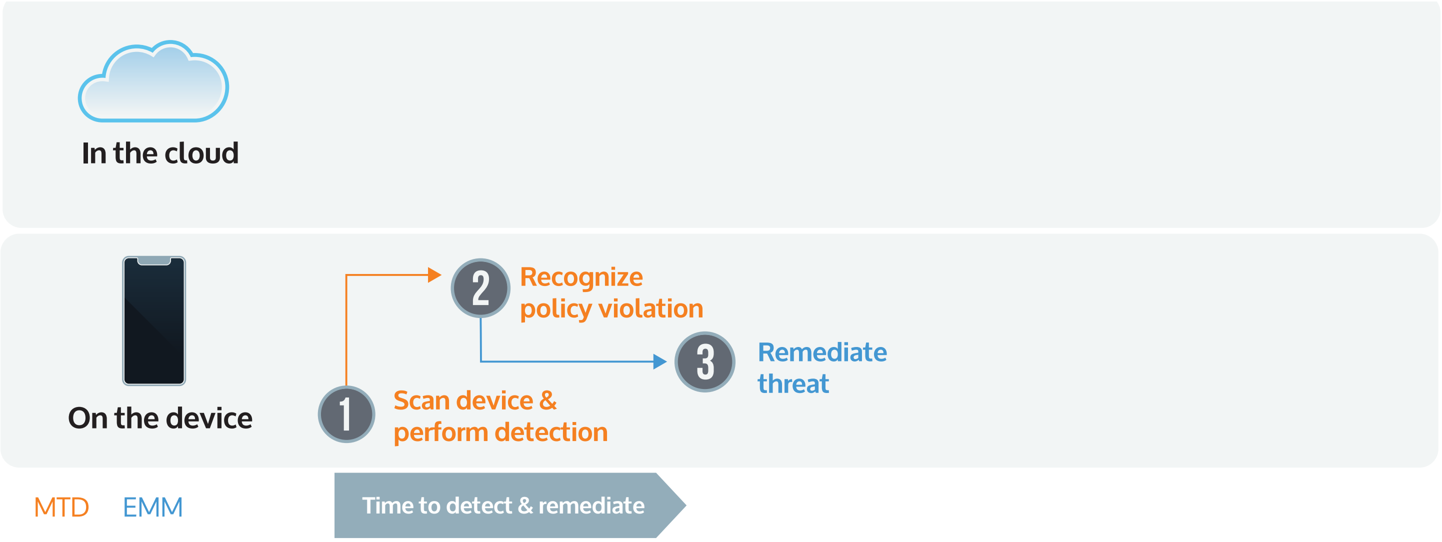
Step 4:
Remediate device threats at machine speed

Attacks occur at machine speed, so on-device security must respond at machine speed also. Cloud-only MTD solutions can actually delay the detection and remediation of on-device mobile threats because first they must scan the device and then send alerts through the cloud before notifying EMM about a security violation. This can result in the loss of critical response time to counter a potentially devastating attack, such as MITM, which can target a device through free Wi-Fi access. In this type of attack, the hacker delivers an exploit that compromises the mobile device and gives the hacker greater control over the device than the user. For instance, the hacker can download all the user's contacts, steal email messages, and log in as the user to send a phishing email to the CEO — which could set off a massive security breach across the entire company.

An on-device MTD solution responds to threats at machine speed because it does not require extra steps to detect and remediate threats. Because the intelligence resides on the device, it can instantly detect a policy violation and block the threat, including MITM, on the device. In a race against time, this gives you the decisive edge against hackers, and prevents a lot of major headaches down the road.

Detection and remediation

The MobileIron Threat Defense Solution


In the cloud
On the device
1 Scan device & perform detection
2 Recognize policy violation
3 Remediate threat
MTD
EMM
Time to detect & remediate

Step 5:
In-depth reporting simplifies compliance requirements

In any global enterprise, the ability to meet compliance regulations requires organizations to have clear auditing and reporting processes to comply with regulations such as the General Data Protection Regulation (GDPR), PCI Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and the Notifiable Data Breaches (NDB), to name a few.

In mobile enterprise organizations, this has become far more challenging because users are no longer tethered to IT-controlled desktops; they are accessing business apps and data from a variety of personal and corporate-owned mobile devices across multiple networks. As one report found: "One of the challenges of achieving GDPR compliance will be securing personally identifiable information (PII) held on laptops and other mobile devices. It is harder to track and at a greater risk of being compromised because it is not behind the company firewall."[7]

The ability to track and manage all devices and apps is critical to meeting compliance requirements by maintaining a clear picture of the overall mobile threat and risk posture. With the ability to quickly generate audit reports, view threat logs, and track detailed access and usage histories, admins can quickly identify potential vulnerabilities and ensure all users, devices, and apps are in compliance. This helps organizations ensure they are meeting compliance guidelines and doing everything possible to insure the business against mobile risks.

> *"One of the challenges of achieving GDPR compliance will be securing personally identifiable information (PII) held on laptops and other mobile devices. It is harder to track and at a greater risk of being compromised because it is not behind the company firewall."*
>
> *GDPR: Report,*
> *"GDPR Compliance for Mobile Workers," October 2017*

[7] https://gdpr.report/news/2017/10/13/gdpr-compliance-mobile-workers

MobileIron THREAT DEFENSE

MobileIron Threat Defense: The solution for easy, insightful, on-device mobile security

MobileIron knows that cybercriminals are continuously generating more advanced ways to steal your data by any means necessary. That's why we are committed to continually innovating and delivering new solutions that help our customers win the race against time to get ahead of the latest mobile security threats. As part of that commitment, MobileIron Threat Defense supports the five critical steps to deploying advanced, on-device mobile security. Our solution provides a single, integrated app that delivers several key advantages:

- A single app of threat protection is fully integrated with EMM.
- No user action is required to activate or update on-device security.
- Advanced mobile security blocks known and zero-day threats across iOS and Android devices with no Internet connectivity required.
- Machine-learning algorithms instantly detect and remediate on-device DNA threats.

The result is easy, insightful, on-device security that delivers actionable intelligence and immediate protection from DNA threats across your entire mobile workforce. This helps you execute a modern mobile security strategy that builds on the already strong foundation of EMM to provide these additional protections against mobile threats. This means you can focus on what matters most to your business: Keeping mobile employees productive and ensuring your organization maintains an innovative, competitive edge.

To learn more about our fully integrated solution for mobile threat detection and remediation, visit us at www.mobileiron.com/threatdefense.

MobileIron

401 East Middlefield Road
Mountain View, CA 94043
globalsales@mobileiron.com
www.mobileiron.com
Tel: +1.877.819.3451
Fax :+1.650.919.8006