esper

How Strong is Your MDM Security?

6 Layer MDM Cybersecurity Self-Assessment

How Strong is Your MDM Security?

66% of organizations admit a mobile cybersecurity issue has spiraled into a “significant organizational calamity” in the past, according to the 2020 Verizon Mobile Security Index (MSI). Your chances of experiencing a mobile cybersecurity incident in the next two years are 28%. So, how strong is your MDM security? It’s officially time to examine whether your mobile device management supports a secure, lifecycle approach to deploying and managing devices.

Mobile security risks vary according to device type, industry, and use case. Single-purpose enterprise devices like kiosks, mobile point-of-sale (mPoS), and employee tablets face a unique set of threats compared to BYOD smartphones. But, all smart, connected devices are vulnerable to external and internal threat actors.

An MDM’s security is defined by how well it deploys and manages devices for different use cases. An MDM needs to lock devices to the dedicated purpose without hindering the user experience, and it needs to provide real-time insights into security risks.

6 Signs Your MDM Security is a Risk

Globally, the average cybersecurity breach costs $3.92 million. If your company is victimized by hackers, your customers won't exactly care to hear that your MDM features were inadequate.

Regulatory agencies also won't buy the MDM security excuse.

If your firm is subject to HIPAA, the CCPA, the GDPR or other frameworks, security incidents could be costly. 29% of firms surveyed in the MSI paid a regulatory penalty due to a mobile security breach.

2

The following 6 questions are a litmus test to determine whether your MDM security is risky.

Sign 1: Unauthorized Use

Are your employees or customers able to use your kiosks, tablets, smartphones or other devices to access unauthorized websites, apps, or device settings?

Sign 2: Downtime

Are you losing money, productivity, or customers due to device or app performance issues?

Sign 3: Manual Provisioning

Is your IT team or mobile technicians tasked with manually configuring and deploying each enterprise device?

Sign 4: Device Compatibility

Does your MDM provide enough features to deploy and manage the security of all your different device hardware and operating system (OS) versions?

Sign 5: Device Lock-Down

Are you able to view the security of devices against mobile threats, including insider abuse, tampering, theft, network security issues, and malware?

Sign 6: Updates

Are you up-to-date on patching, or within 30 days of the latest patch release date via firmware over-the-air (FOTA) updates?

3

How Secure is Your MDM? An EMM Cybersecurity Checklist

MDM security and safe mobility is a concept that involves multiple layers. Each layer needs to be aligned with the use case and risks to avoid cybersecurity issues.

A full MDM cybersecurity assessment should involve a look at each 6 layers to understand the greater picture of risk and vulnerabilities. Within these 6 layers, we've identified 42 separate MDM security criteria.

The 6 Layers of MDM Cybersecurity

Layer 1: Cloud MDM Platform Security

Layer 2: Device Hardware Security

Layer 3: Network Security

Layer 4: App Security

Layer 5: Alerts & Remediation

Layer 6: User Experience

Layer 1: Cloud MDM Platform

Your cloud MDM console is ground zero for effective mobile security. Your MDM admin portal should make it easy to provision, deploy, and manage devices according to policy and determine which users can read and write device policies.

Usability is a key factor for cloud MDM security, and so is data integrity. You need to be able to trust that your MDM will deliver timely alerts and a complete audit trail.

Cloud Platform Security | Does Your MDM Offer		
☐	1.1	Ease-of-Use
☐	1.2	Secure Cloud Gateway
☐	1.3	MDM User Access Permissions
☐	1.4	Data Integrity
☐	1.5	Easily-Accessible Info on Devices, Policies & more
☐	1.6	Intelligent Event Feeds

Learn more: *Role-based access control is crucial to device health and security. Check out our blog to learn what it is and how it optimizes role management: The Benefits of RBAC.*

Layer 2: Device Hardware Security

Device hardware security matters, especially for today's enterprise Android fleets. Most MDM are built to accommodate smartphones and tablets, but far fewer offer compatibility with mPoS, kiosks, ruggedized devices, smart fitness equipment, and telehealth devices.

A smart approach to hardware procurement is key to mobile security, and this process should involve learning whether devices are compatible with your MDM. Device interoperability and updates aren't the whole scope of hardware security, but they're important measures of MDM strength.

Device Hardware Security | Does Your MDM Offer		
☐	2.1	Support Current & Future Fleet Device Types
☐	2.2	Support Current & Future Device Use Cases
☐	2.3	Offer Interoperability with Your Devices
☐	2.4	Simplify Device Updates
☐	2.5	Offers Validated Hardware

Learn more: *Struggling to protect your devices in the field? Check out our device-specific security guides for tips on how to keep them safe: mPOS security, POS security, and Kiosk security.*

Layer 3: Network Security

A secure mobile device on a compromised Wi-Fi network can leak sensitive data. Network security matters, even for single-purpose devices not intended for public Wi-Fi.

Corporate mobile devices rely on Wi-Fi 300% more than cellular data, with 25% exposed to corrupt networks and 4% exposed to man-in-the-middle attacks.

Wi-Fi security is crucial for dedicated devices that travel with employees or customers. Network security policies should safeguard against worst-case scenarios, such as stolen devices connected to compromised Wi-Fi outside the premises

Network Security | Does Your MDM Offer		
☐	3.1	Limiting Wi-Fi Connectivity To Trusted Networks
☐	3.2	Detecting Wi-Fi Network Changes
☐	3.3	Locking Mobile Devices if They Leave the Network
☐	3.4	Wiping Lost or Stolen Mobile Devices
☐	3.5	Blocking User Access to Wi-Fi/Data Setting
☐	3.6	Detecting Unusual Data Usage Patterns

Learn more: *See how our customer Spire Health used Esper to proactively address their network security issues: Read the case study.*

Layer 4: App Security

Over 11% of mobile apps downloaded from Google Play Store contain hidden cybersecurity risks, according to a recent academic study of 150,000 apps. Researchers found that 12,706 Play Store apps had signs of a mobile backdoor, such as secret access keys or master passwords. On pre-installed bloatware apps, the percent compromised is closer to 16%.

Mobile Apps from Official Play Stores or unauthorized web sources may also contain riskware, defined as extensive permission requirements that compromise user policy. Riskware apps are typically free and perform as promised, while secretly sharing the user's private data with a remote server. Mobile apps can also introduce risk if they're laden with mobile ad malware, which run continuously in the background and lead to issues like a drained battery or slow performance. Juniper Research projects mobile malware ads will cost over $100 billion each year by 2023 in productivity loss and damage.

So, you can't trust most end users to carefully read app permissions before downloading. You also can't trust Play Store apps by default. An MDM should support top-down app management for the use case, including restricting app and user permissions.

Layer 4: App Security

App Security | Does Your MDM Offer		
☐	4.1	Install and Uninstall Apps
☐	4.2	Manage App Versions
☐	4.3	Update Apps
☐	4.4	Support Single or Multi-App Kiosk Mode
☐	4.5	Monitor App Behavior
☐	4.6	Offer Restricted Access to Google Play or Play for Work
☐	4.7	Limit User to Downloading Authorised Apps Only

Learn more: *Kiosk mode can help you lock down your devices to specific apps and restrict user behavior. Learn more about how to use it on our blog: What is kiosk mode?*

Layer 5: Alerts & Remediation

At least 4.5% of Android devices contain known malware, according to a MobileIron survey. Regular updates matter, but they're not enough — 7% of Android devices are unpatched for at least 6 months or more after the patch release date.

Mobile security is dynamic. A secure kiosk or mPoS can quickly become a liability when any single factor changes. The key to avoid threats is visibility, so you can see which negative changes create risk.

Intelligent alerts are critically-important, but so is the ability to remotely respond to cybersecurity threats before a situation turns into a data breach. An MDM should offer automated response, such as device lockdown when geofencing data indicates it's been lost or stolen.

Layer 5: Alerts & Remediation

		Alerts & Remediation | Does Your MDM Offer
☐	5.1	Custom Alerts
☐	5.2	Intelligent Notifications
☐	5.3	Automated Security Alert Responses
☐	5.4	Geofencing
☐	5.5	Device Lock Down
☐	5.6	Remote View & Control
☐	5.7	Remote Debugging & Wipe
☐	5.8	Device Tracking
☐	5.9	Offline Device Actions

Learn more: *Esper offers a full suite of security features to keep your devices safe, including geofencing, kiosk mode, and remote control. Click the links to learn more!*

Layer 6: Secure User Experience

72% of organizations worry about device abuse or misuse, according to the Verizon MSI. 44% of organizations lack a device compliance policy entirely, despite their fears of employees or customers acting outside of bounds. Countless organizations also struggle to enforce basic mobile cyber hygiene measures. 42% of organizations have at least one mobile device without lock screen security, per Wandera. The majority of these devices with lockscreen security have a simple 4-digit code, instead of alphabetic or alphanumeric codes that are harder to crack.

The user experience should protect your enterprise from authorized and unauthorized users — including unacceptable activities among employees, customers, device thieves, and hackers. An MDM should support a customized user interface that's built according to the principle of least privilege. This is the least amount of user access possible to fit a use case without cutting into user productivity or happiness.

Layer 6: Secure User Experience

		User Experience | Does Your MDM Offer
☐	6.1	Load Kiosk Mode Apps When Powered On
☐	6.2	Restrict Calls & SMS Messages
☐	6.3	Block Settings Access
☐	6.4	Hide Notifications
☐	6.5	Hide Status Bar
☐	6.6	Restrict Camera & Screenshots
☐	6.7	Block local App Installs
☐	6.8	Block Browser Access
☐	6.9	Block Google Voice Assistant

Learn more: *Want to fully customize your user experience? Learn more about the endless possibilities with Esper Foundation for Android.*

4

The Future of MDM is Dynamic Mobile Security

Your mobile security risks vary depending by device type, industry, and most importantly, use case. MDM originated as a tool to protect enterprise data from users in BYOD and COPE use cases. Today, it's evolved to mean much more. Looking to the future of MDM is the only way to protect your fleet against the changing mobile threat landscape.

Modern MDM security must be dynamic. You need the flexibility to deploy and manage single-purpose Android devices according to use cases. MDM should offer features to completely wipe and re-provision devices at any given point during the device lifecycle. Most importantly, MDM security should allow real-time or automated response based on insights into devices, apps, and user behaviors.

Esper is the first-ever complete toolchain with MDM for single-purpose Android enterprise devices. To learn more, request a demo.

MDM Cybersecurity Checklist

Download Complete Checklist