GUIDELINES FOR MANAGING AND SECURING

MOBILE DEVICES IN THE ENTERPRISE

As mobility has transformed the way business is done, it's also increased demands on enterprise IT departments.

Barcoding

8 KEY SECURITY PRACTICES WITHIN ENTERPRISE MOBILITY MANAGEMENT

The portability, size, and convenient use of mobile devices both on and off enterprise networks make data more accessible than ever for workers. But those same features, along with the complexity of enterprise mobile ecosystems, also create new opportunities for threats from malicious actors.

That's why it's more important than ever for enterprise organizations to get ahead and stay ahead of rapidly evolving threats. By implementing an **enterprise mobility management (EMM) system that incorporates mobile device security controls**, IT departments can more effectively protect against threats:

- Device loss or theft
- Exploitation of software vulnerabilities
- Connection by improperly configured or insecure devices
- Malicious or unauthorized certificates
- Use of untrusted devices (such as employees' personal devices)
- Wireless eavesdropping via WiFi, Bluetooth, and cellular networks
- Mobile malware
- Data synchronization risks
- Shadow IT usage

Along with the use of mobile threat defense tools and various on-device technologies (such as biometrics, encryption, VPN support, data isolation, APIs, etc.), EMM is a key weapon in an enterprise's arsenal against mobile security threats.

EFFECTIVE EMM STARTS WITH AN

ENTERPRISE IMPLEMENTATION PLAN

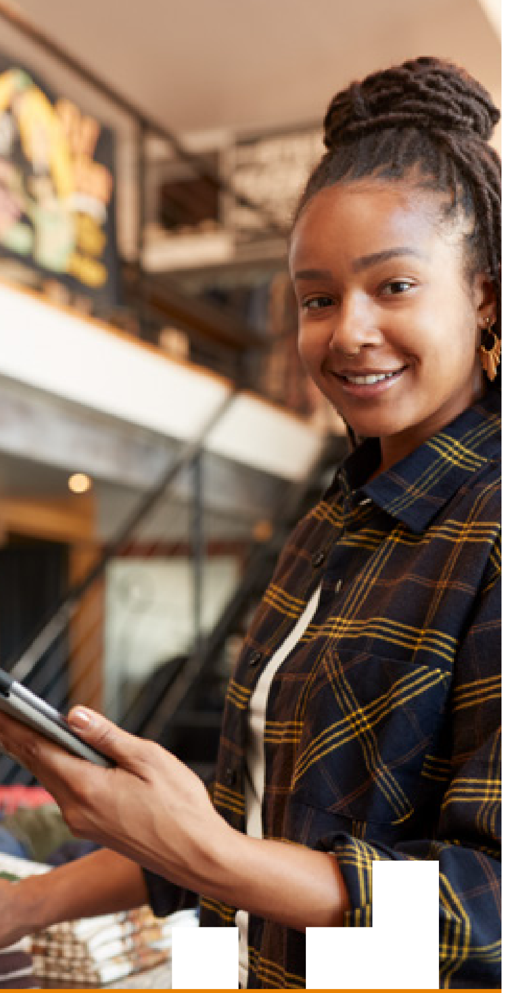
Enterprise mobility management is a continuous process that uses mobile device management (MDM) tools and covers all aspects of device deployment, configuration, and active management down to the individual device level to ensure consistent access, operation, and security of mobile devices. An EMM solution makes it possible to:

- Control and manage user access
- Push security updates when they become available or on the timeline you determine
- Perform ongoing monitoring to detect potential issues
- Remotely lock and wipe devices of their data (including passwords) in the case of lost or stolen devices
- Ensure adherence to security standards like GDPR (general data protection regulations, which help protect data) and provide legal protection to the organization in case of a mishap
- Prevent transfer of data
- Encrypt data

An enterprise implementation plan is key to ensuring that investments in mobility management are selected for their effectiveness, implemented successfully, and managed for optimal ROI.

While a trusted EMM partner will ask the right questions to ensure your chosen solutions are best suited to your enterprise applications, networks, integration, and security needs, a carefully planned, strategic approach is needed to fully protect against attacks or unplanned downtime within your enterprise.

Look for a partner that plans your EMM strategy to address these key security guidelines.



1 CREATE AND ENFORCE AN ENTERPRISE MOBILITY POLICY

Developing and communicating a comprehensive policy helps device users understand and avoid certain threats, including:

- Use of network radios such as WiFi, Bluetooth, near-field communication, GPS, etc.
- Access to cameras, removable storage, copy and paste, and other features or hardware
- Approved security configurations
- Limits to enterprise services access based on operating system, device model, etc.

User education is and should always remain integral to enterprise mobility, and an EMM system can disseminate educational content directly to users. An EMM system also helps enforce policies by monitoring, detecting, and reporting violations. Plus, automations can enable the solution to take immediate and appropriate action when certain critical violations are detected.

2 SELECT FOR SECURITY AND RUN PILOT TESTING BEFORE IMPLEMENTING ACROSS AN ENTERPRISE

An experienced EMM partner can show the way by proving out devices and solutions in advance, and designing pilot plans with select enterprise users. Security should always factor into ROI considerations on investments in hardware, software, and mobility management.

3 NEW DEVICES SHOULD ALWAYS BE ENROLLED AND CONFIGURED IN THE EMM

Protecting against shadow IT practices means making it absolutely clear, enterprise-wide, that any and all devices and networks must be accounted for within the EMM system. That means new devices and connected assets need to be properly enrolled, configured, and installed by IT-authorized agents.

4 REQUIRE DEVICE AND USER AUTHENTICATION

Devices should default to a locked state, and they should lock automatically after a specified idle period. To unlock, they should require an authenticator—whether a password, face, fingerprint, voice, or other unique identifier. Networks should also require token-based authentication, digital certificate, or another authentication mechanism to control and manage device and user access to enterprise resources.

An EMM system can remotely lock devices and/or wipe them after too many incorrect authentication attempts to protect enterprise networks and resources against intrusions.

5 PROTECT DATA ON DEVICES AND IN COMMUNICATIONS

Ensuring adherence to security standards like GDPR (general data protection regulations) helps protect data and user privacy, and compliance provides legal protection to an enterprise in the case of a mishap.

Strong data encryption can be achieved using a VPN, encryption and decryption of media storage, proper device lifecycle management including wiping devices between users and at device disposition, and remote wiping any device suspected lost, stolen, or accessed by the wrong user—including credential theft by phishing.

6 KEEP MOBILE DEVICES UPDATED— BOTH OPERATING SYSTEMS AND APPLICATIONS

An EMM solution can push updates directly to devices when they become available, or on a timeline determined by IT. Mobile application management can help ensure that only acceptable apps are deployed, and that apps only have access to necessary device features, hardware, and data, by implementing the following:

- Restricting or allowing app store access
- Including or excluding specific apps
- Restricting app access to cameras, microphones, location, etc.
- Restricting the use of sharing services and other data transfer
- Directly distributing specified apps

7 INTEGRATE A MOBILE THREAT DEFENSE (MTD) SYSTEM

Also known as end-point protection and mobile threat protection, MTD systems detect threats that can attack using networks, applications, and more to extract enterprise data. An MTD can also detect misconfigured devices that can pose a security risk.

When integrated, an EMM and MTD can detect threats, remove malicious apps, notify a user to apply a patch, alert an administrator, remotely wipe a device, and more.

WHAT ABOUT OTHER SECURITY TOOLS?

Relatively low-cost, “light” EMM tools may be effective at what they can do, but it’s often a case of getting what you pay for. Capabilities are often quite limited, and they may be OS-dependent. For a more complex, robust enterprise environment, they’re not the best answer.

8 LEVERAGE EMM THROUGHOUT DEVICE LIFECYCLE MANAGEMENT —AND VICE VERSA

Lifecycle management that supports enterprise security requires ongoing consideration of all your business processes, people, and technologies involved. It starts with an accurate inventory of all devices and requires a holistic approach, from new device selection and rollout to ongoing support and maintenance, through to final device disposition.

EMM supports lifecycle management by delivering comprehensive visibility into device inventory, usage, policy compliance, and more. And active device lifecycle management provides data, insights, and opportunities to support improved security within EMM.

START OFF RIGHT

WITH A TRUSTED PARTNER

Achieving enterprise mobile device management and security is a complex undertaking, and one that enterprises simply can't afford to get wrong. When you partner with Barcoding, you get the benefit of more than just our expertise and 24/7 service; you gain access to a robust ecosystem of thoroughly vetted, proven, and trusted OEMs and technology partners.

Put our experience to work integrating security into your enterprise mobility management system, so you can focus on business.

Reach out to Barcoding today. We're ready to show you how the security benefits of EMM can help drive enterprise growth.

LET'S TALK EMM

Barcoding

1.888.412.SCAN (7226) | info@barcoding.com

barcoding.com