Advance and Improve Your Mobile Security Strategy

Published 19 November 2019 - ID G00463436 - 42 min read

By Analysts Patrick Hevesi

Initiatives:Security Technology and Infrastructure for Technical Professionals

Threats to mobile applications and devices pose security risks to global enterprises. Security and risk management technical professionals responsible for IT security, especially in organizations with high security or compliance needs, must have an in-depth strategy to defend mobile devices.

Overview

Key Findings

- Mobile attacks are leveraging vectors that focus on consumers and enterprise alike, such as mobile application stores and network-based proximity attacks.
- Android has been the largest target for mobile malware and unwanted applications, but Apple iOS mobile attacks continue to surface, and new jailbreaks that affect numerous versions of iOS, like checkm8, are starting to change things.
- Mobile security products are becoming increasingly important as the rate of mobile attacks continues to grow, though the frequency of these attacks are several orders of magnitude lower than traditional endpoint attacks.

Recommendations

Technical professionals responsible for mobile security should:

- Track the mobile threat landscape from mobile security vendors. Be aware of new types of attacks.
- Build a mobile security strategy based on a mobile device data model. Offer a menu of options for employees, while providing the appropriate levels of security for the enterprise.
- Set minimum and recommended OS and hardware versions, use multifactor authentication (MFA), and manage and monitor device configurations and security patch levels. Install applications only from trusted sources.

- Use application wrapping and shielding techniques for mobile devices on corporate applications and data when needing additional assurances on highly classified or regulatory data.
- Plan for mobile threat defense products if needing more advanced levels of protection for iOS and Android devices.
- Drive user awareness of the primary attack vectors: mobile applications that request permission to install additional applications, profiles, VPN and certificate installs, email and SMS phishing URLs that can sideload applications, downloading APKs, and use of Wi-Fi and location services.

Problem Statement

The mobile attack landscape has continued to grow and change with the increase of smartphone and tablet sales, and with the proliferation of bring your own device (BYOD) in the enterprise. Every year, we see new statistics claiming hundreds of percentage points of growth in mobile malware.

But what does that mean to the consumer in general and the enterprise IT staff in particular? With the constant increase in consumer devices as enterprise tools, IT has an opportunity to train users to protect both personal and professional data from these threats by invoking the impact on their personal lives. They may not listen to IT when it comes to corporate data protection, but words like “identity theft,” “surveillance software,” “financial attack” and “privacy violations” will wake them up. These can be translated into the risks that the organization faces each day.

Below are some of the top questions Gartner clients have about mobile security that will be answered in this report:

- Is mobile malware a real risk to the enterprise?
- What are potentially unwanted or “leaky” applications and their impact to my enterprise?
- Applications aside, what are the main threats to mobile devices and mobile device use?
- How can I protect my mobile devices, workforce and enterprise applications?
- Do I need a mobile security solution to defend my organization?
- Which of the mobile security solutions really work?
- Do I need a mobile threat detection (MTD) product on all my mobile devices?
- Is a unified endpoint management/enterprise mobile management (UEM/EMM) product enough to protect my mobile devices?

Mobile malware, network-based attacks and potentially unwanted applications pose a risk to the enterprise. Mobile malware and attacks need to be addressed by enterprise mobile security strategies for both BYOD and corporate-managed deployments.

Numerous solutions can help address these new threats. IT organizations should evaluate the right approach based on their use cases. This research discusses the protection capabilities of all the mobile security solutions and will help you build a defense-in-depth strategy based on mobile device data requirements.

The Gartner Approach

To protect your enterprise mobile devices against attack and deal with the challenges of mobile operating system, begin with the following guiding principles:

- **Monitor** the risks and new tactics being leveraged on mobile devices by malware, applications, websites and so on. Leverage the MTD vendors' mobile threat intelligence reports for quarterly and yearly mobile risk profile updates.
- **Set** minimum and recommended mobile OS and device standards on all devices regardless of device ownership (i.e., personal or business-owned). For a list of Gartner recommendations, see "Mobile OSs and Device Security: A Comparison of Platforms."
- **Enforce** rules that applications be installed only from trusted sources (Google Play, Apple App Store, Microsoft Store or enterprise apps stores) with EMM or MTD solutions.
- **Plan** for MTD solutions with cloud-based application reputation services in stand-alone or UEM/EMM integrated mode.
- **Enforce** conditional access to corporate email and data, based on the security posture checking of the device. There are a few ways to accomplish this:
  - Through an MTD device risk check and then a manual process to disconnect users.
  - By integrating an MTD with a UEM/EMM to automate conditional access.
  - Through enterprise digital rights management (EDRM) solutions like Microsoft's Azure Information Protection, which can perform conditional access through Azure Active Directory (AD).
  - Some cloud access security brokers (CASBs) have forms of conditional access called adaptive access control.
- **Use** mobile app security solutions to harden and encrypt corporate applications and the application data when needing additional assurances on higher classified data or as required by industry regulations.

- **Train** users to drive awareness about which permissions mobile applications are requesting. This approach can help reduce unwanted applications from being installed.

As we go through the principles above, you have already started to build a high-level mobile security strategy. As we continue in this document, you will begin to fill in the details on different mobile security products, standards, and best practices to complete your mobile security strategy. At the end of this guidance framework, we will show you how to build a menu of recommendations on all of the key features of mobile security defense in depth. You will accomplish this by filling out the **worksheet.xlsx** in the Downloads section (in the icons column to the left of this document) and populating options for your enterprise complete mobile security strategy.

The Guidance Framework

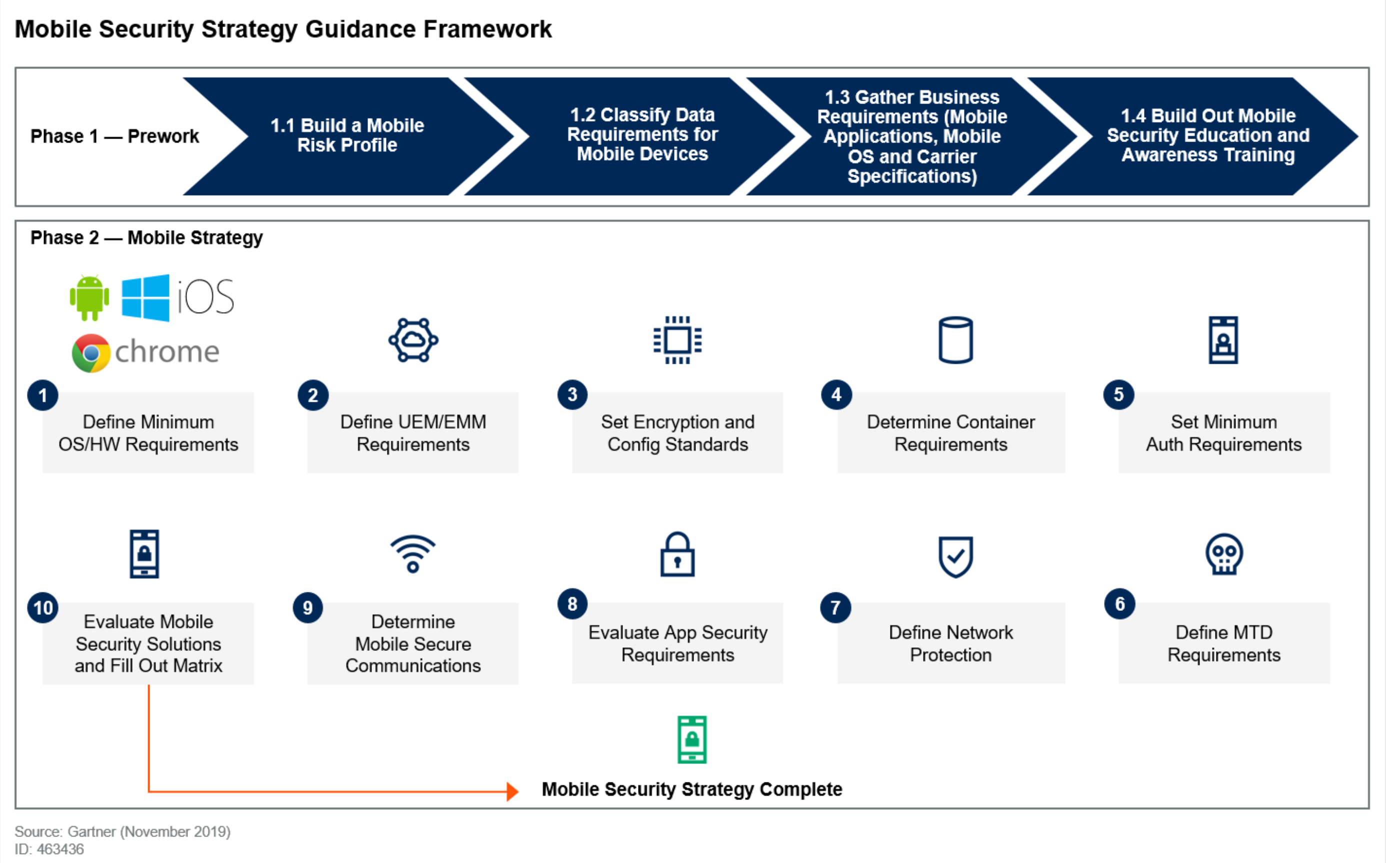
Gartner Welcomes Your Feedback

We strive to continuously improve the quality and relevance of our research. If you would like to provide feedback on this document, please visit Gartner GTP Paper to fill out a short survey. Your valuable input will help us deliver better content and service in the future.

This mobile security strategy guidance framework (see Figure 1 below) will take IT technical professionals dealing with security through the steps to build a mobile defense-in-depth strategy. The prework entails gathering the mobile business requirements, determining the types of data being used on the mobile devices, gathering any mobile carrier requirements and building a mobile-specific training for end users. Then, we will go through the different mobile solutions and configurations required, based upon the type of data required on the mobile devices. In the end, you will have a complete mobile security strategy with guidance on the following feature areas:

- Mobile operating system/hardware requirements
- UEM/EMM requirements
- Use of software/hardware mobile containers
- Network-based protections
- MTD requirements
- Mobile application security options
- Device authentication requirements
- Container/mobile application authentication requirements
- Device and removable storage encryption requirements
- Secure communications options

Figure 1. Mobile Security Strategy


Mobile Security Strategy Guidance Framework
Phase 1 — Prework
1.1 Build a Mobile Risk Profile
1.2 Classify Data Requirements for Mobile Devices
1.3 Gather Business Requirements (Mobile Applications, Mobile OS and Carrier Specifications)
1.4 Build Out Mobile Security Education and Awareness Training
Phase 2 — Mobile Strategy
iOS
chrome
1 Define Minimum OS/HW Requirements
2 Define UEM/EMM Requirements
3 Set Encryption and Config Standards
4 Determine Container Requirements
5 Set Minimum Auth Requirements
6 Define MTD Requirements
7 Define Network Protection
8 Evaluate App Security Requirements
9 Determine Mobile Secure Communications
10 Evaluate Mobile Security Solutions and Fill Out Matrix
Mobile Security Strategy Complete

Source: Gartner (November 2019)
ID: 463436

Prework

In the prework phase, it is important to identify all the key stakeholders in the organization that have mobile device requirements. Key stakeholders should include the security, identity, mobile, operations and enterprise architecture teams. Build a working team to review and manage the end-to-end, strategy-building process.

Many organizations have begun building mobile centers of excellence. Two of the key pillars to building an effective mobile strategy are security and identity. These teams should be represented in your working group, and they should leverage the guidance framework below to build the mobile security strategy.

Step 1.1: Build a Mobile Risk Profile

Understanding what the risks are for your mobile devices have aspects of different mobile OSs, hardware versions, application and data requirements, networks the devices join and finally the attack vectors that malicious actors are leveraging. You will need to start tracking mobile attacks and vulnerabilities for your mobile OSs, hardware devices and applications that your employees will install on the devices.

New and Expanded Attack Vectors

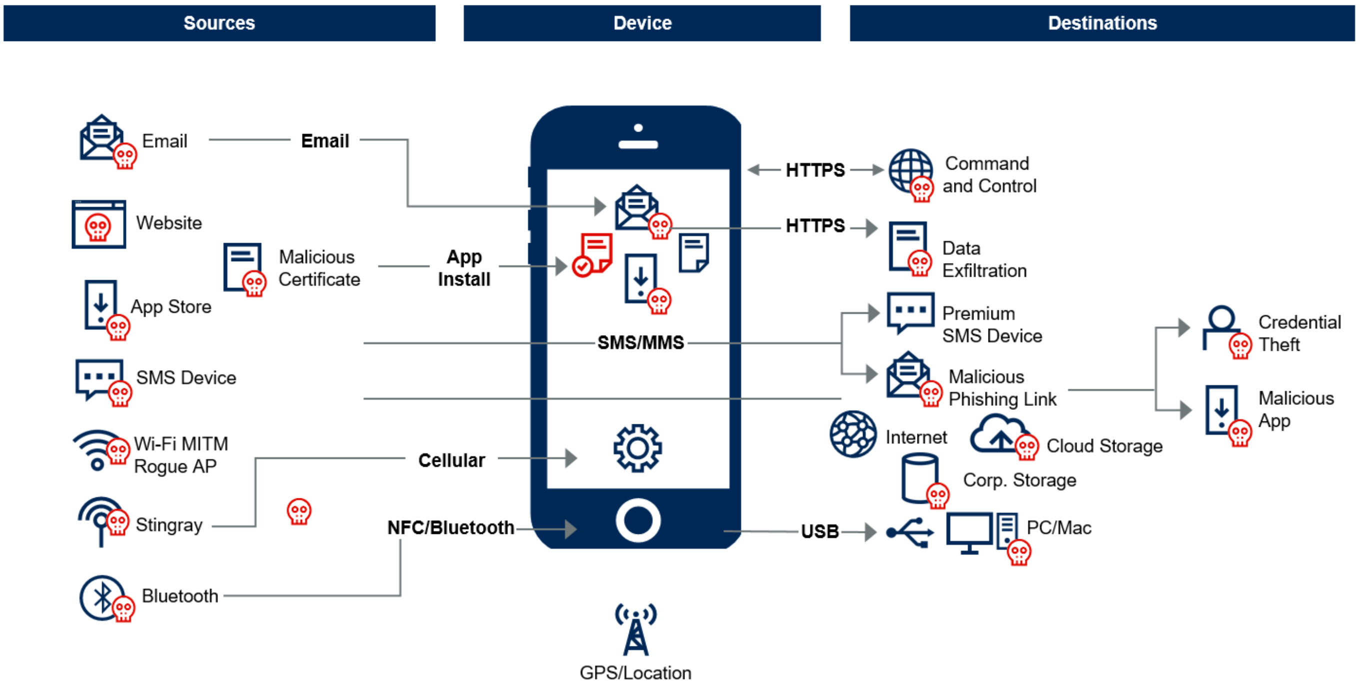
In recent mobile threat reports from Lookout, Symantec, Zimperium and Verizon Mobile Security Index 2019, there have been increases across the board for Android and iOS mobile threats. The latest generation of attacks has begun to implement new attack vectors that IT organizations need to be aware of to defend the enterprise. Figure 2 shows a few of the most prevalent sources and paths for mobile malware to attempt to gain access to the enterprise.

Let us start by defining some key terms. Mobile threats can be loosely categorized into the following categories:

- **Mobile malware:** A program or piece of code that exploits a vulnerability or executes something malicious that imposes a security risk to a user's mobile device and/or information. Categories of malware include viruses, ransomware, rootkits, worms, botnets, spyware and trojans. Another tactic is to leverage stolen or malicious certificates as payload of malware to sideload surveillance or command and control software.
- **Potentially unwanted applications (PUAs) or leaky applications:** Programs that have been installed on mobile devices, usually with the user's consent, but with unclear intentions that can have negative consequences to privacy or to the performance of the device.
- **Data exfiltration:** Another tactic of malicious actors is sending data from the device or from cloud-based storage once the device has been infected.
- **Configuration-based attacks:** These change profiles or install some form of malicious certificates or VPNs that direct traffic to malicious sites.
- **Network-based attacks:** These intercept wireless or other mobile network channels (Bluetooth, LTE, NFC) and perform man in the middle (MITM)-based attacks. There has been a rise of SMS-based phishing attacks that started with redirecting to premium SMS numbers to make money, and which are now sending tiny URLs to phish users to malicious websites or installing malicious applications.
- **Physical loss or theft of device:** These can lead to data exfiltration of both personal and corporate data if the device can be unlocked through attack or if there is no lock screen passcode.
- **Malicious or careless end users:** Users that either intentionally or unintentionally install malware/PUA that leads to data theft.
- **Compromised cryptographic systems:** Increasingly, mobile devices (and many other IT systems) rely on cryptography for security, trust and privacy. However, cryptographic systems can at any moment become vulnerable. Security leaders must ensure that they understand their dependencies on cryptography when it comes to mobile devices, and when cryptography, such as X.509 device certificates, becomes vulnerable (see "Better Safe Than Sorry: Preparing for Crypto-Agility").

Figure 2. Mobile Attack Vectors

Mobile Attack Vectors



Source: Gartner (November 2019)
ID: 463436

Nonstandard Application Stores

One of the main sources for today's attacks is nonstandard application stores. These are third-party, private or hacker-run application stores, potentially filled with malicious or unwanted applications. Both Android and iOS are vulnerable to these sources. Android allows applications to be installed from multiple application stores or sideloaded. This is a simple configuration setting, though it can be controlled via mobile device management (MDM) configuration. iOS devices do not have to be jailbroken to leverage third-party stores. They can be installed with enterprise or root certificates that will have to be trusted to sideload applications.

One common practice for malicious actors is to get popular applications, repackage them with malicious code and submit them to third-party app stores, or to steal enterprise developer certificates so their apps appear to be legitimately signed. This was evidenced by the Pokémon GO application, which was repackaged within a few days of release with some variants containing remote access toolkits. These were loaded to third-party mobile application stores, where they promoted themselves as the official app in numerous regions around the world that were not supported countries.

Malicious Actors

Another source of mobile attacks are malicious websites that try to execute malicious code and install mobile applications, profiles or certificates on the user's device. Once an iOS user installs a malicious profile with an attached root certificate and a VPN profile or malicious software that can control the device, all traffic (encrypted or unencrypted) can be sniffed by the malicious author. In 2019, we saw Google Project Zero discover five iOS attack chains that were able to execute low-level attacks and install surveillance software onto iOS devices. For more details, see "A Very Deep Dive Into iOS Exploit Chains Found in the Wild" (Google Project Zero).

Network-Based Attacks

Network-based attacks can come from unsecured public Wi-Fi networks or rogue access points. These are malicious attackers broadcasting known Wi-Fi names to trick end users into connecting their mobile devices and then being compromised by MITM attacks.

There are also network-based attacks against the mobile carrier networks called “stingray” (cell tower masquerading) devices that can intercept cellular data and voice from mobile devices. These attacks allow for unencrypted IP traffic for the Wi-Fi and voice traffic for the stingray device to be sniffed. They can be combined with other forms of malware, like creating fake Secure Sockets Layer (SSL) certificates and roots of trusts that allow for decryption of traffic. Email, SMS and multimedia messaging service (MMS) are other attack vectors that can have embedded links to malicious content.

Once infected with malicious code, the next step is not always targeting the mobile device, but possibly targeting the users’ other devices through USB connections, over the carrier network, through Wi-Fi to cloud storage, or via corporate resources. For example, there were Android games that would create an infected PDF, HTML or other file type and sync it up to a cloud file store. When the user opened the file on an Apple Mac or PC, it had code targeting the desktop OS.

The Challenge of Protecting Mobile OSs

Mobile OSs, such as Android, Chrome OS, iOS and Microsoft Windows 10 in S mode, have been designed to be more resilient against some of the traditional attacks, but this makes it difficult for security vendors to build mobile security solutions. There is no concept of “kernel mode access” for the security solutions to plug into for low-level security scanning access like on traditional endpoints. This makes it challenging to protect against malicious attacks and has driven development of alternate methods for mobile security solutions to secure devices.

Furthermore, not all methods of protection are available for all mobile OSs because of their different approaches to architecture. For example, Android allows for more access to configuration, policy settings and other device resources, whereas iOS limits solutions to rely on less-granular indicators, such as system changes and active network scanning, to determine possible risk. More recently, there is some movement by Apple to create iOS network extension APIs for third parties to scan network traffic.

A common misconception is that attacks and threats are the same on mobile devices as in the traditional desktop world. In reality, mobile architecture is built to prevent some of the attacks that succeed on the desktop. Mobile operating systems do not allow direct access to the kernel. They have application-level containerization, secure boot for the system, secure browsers without add-ons and other security features that prevent common desktop malware from being effective.

Apple and Google have built-in security features to reduce the attack footprint of the mobile device. While Microsoft tablets can run full versions of Windows 10, there are many built-in security solutions that can be managed by UEM/EMM like other mobile devices. The risks are more based upon the traditional desktop model. Microsoft also has released Windows 10 in S mode that only allows modern applications to run, therefore hardening the device and enforcing apps from the Microsoft Store. A new version of Windows, Windows 10X, with a more modular, Linux-like architecture, will allow different UIs and subsystems to be loaded on a secure kernel. For a deeper dive into the latest security features, see "Mobile OSs and Device Security: A Comparison of Platforms."

In most cases, but not for Windows, traditional anti-malware agents installed on mobile devices cannot prevent malicious software from being installed because they do not have access to the system. They do not have visibility into what is being installed until after the fact.

Responding to the Threat

All these issues are why vendors are looking to alternative ways to protect mobile devices. Many vendors have built, for example, application reputation services to inventory, categorize and assess the risk of applications installed on mobile devices. These often can be integrated with UEM or EMM solutions to help the enterprise manage the applications installed on their mobile devices. IT organizations can then set policies and actions based on the risk level of the applications.

The other options for detecting malicious actions include monitoring the network stack or forcing all traffic through a VPN or secure web gateway. This allows the security solution to understand where the applications are connecting and leverage an IP reputation service to compare against known malicious sites.

According to mobile malware security reports from the past few years, most malicious attacks continue to fall into the trojan category, although the number of incidents is dramatically lower than malware on the desktop and with servers. Part of the issue is that the ability to report on the numbers of infections is based on the number of mobile endpoints reporting incidents.

As the MTD vendors continue to deploy new agents, our ability to gain better insight in the spread of mobile threats grows. Some examples of trojan behavior on mobile devices include SMS sending, file or app downloading, location tracking, bank fraud, data theft and fee charging, just to name a few.

Most mobile attacks on individuals are motivated by profit. Mobile security vendors have seen possible trends of attackers that are looking to steal personal information for possible "spear phishing" attempts. Once infected, the mobile device can be leveraged as a new attack vector to infiltrate enterprise PCs and networks. As for the scale of attacks, there may be many variants, but spreading attacks is much harder than in the desktop space. So, the number of infections for each mobile malware variant may be extremely low compared to traditional endpoint malware.

Now that we understand the mobile threats, we will discuss building your mobile security strategy.

Step 1.2: Classify Data Requirements for Mobile Devices

In this step, it is important to map out the different types of data that will be required to be stored or processed through mobile phones, tablets or other mobile devices (e.g., kiosks, payment terminals). Take into consideration the mobile applications like email, file synchronization, collaboration and any line of business (LOB) applications, and what types of data will be in each application. If you have a current data classification strategy, those levels can be used for this mapping. If not, you can start with a basic high, medium and low types of data requirements. Below are some examples of types of data that might fit into those classes.

- **Defense grade:** These are military-level, highly classified type of files that could impact public safety, state secrets or confidentiality if the data has been leaked.
- **High + restricted:** This is highly regulated data with strict regulatory requirements or stricter internal compliance mandates, which may have another level above the data rated as high business impact below. Examples are Health Insurance Portability and Accountability Act (HIPAA) data, PCI data, and EU citizen data under the General Data Protection Regulation (GDPR).
- **High:** Personally identifiable information (PII), legal, intellectual property, merger and acquisition information, corporate confidential emails/documents, passwords or other secret types of data.
- **Medium:** Internally sensitive data that should be for the organization only, internal projects, organizational information.
- **Low:** Public information, standard contacts, low-priority emails, generic company information.

Once you have determined what types of data will be required on the devices by the different business units and grouped them into buckets, look to gather the additional requirements in Step 1.3.

For more information on data governance, see "Building a Comprehensive Data Governance Program."

Step 1.3: Gather Business Requirements From Key Stakeholders (Mobile Applications, Mobile OS and Carrier Specifications)

Start with identifying all the key stakeholders involved with the overall mobile strategy for the organization: teams like IT (groups that provision and or run UEM tools), security, mobile contract owners and possibly mobile development.

This step continues to gather specific LOB applications, both internal or externally developed, that may be required by the business. Determine which mobile OS and versions are required to run and support the applications. These applications should be vetted through a mobile security development life cycle process if developed in-house.

If they are purchased applications, use some form of mobile application risk scanning and verification to ensure that all the applications are secure. This is where MTD can help. See Step 2.6 below for more information on MTD products.

Finally, determine if there are any mobile carrier requirements due to business contracts, to understand what types of mobile OSs and devices will be available to build your mobile security strategy.

Step 1.4: Build Out Mobile Security Education and Awareness Training

Today, many organizations offer user security training for traditional endpoint attacks and email phishing types of attacks. But most organizations do not do any specific training on mobile devices, and this needs to change.

Users are critical agents for detecting any type of security breach, potentially unwanted applications and mobile malware. Users often are the detection agent of last resort, but awareness and education can transform users into a detection agent of first resort. With mobile, it becomes critical to educate users to the risk to themselves and the separate risk to the company from their actions on their mobile devices. For example, if a user installs a highly rated flashlight application that has every possible access on the mobile device, what is the risk to his or her personal information? And what then is the possible impact if the user brings that device into the enterprise? A basic flashlight application should only have access to turning the flash on and off.

Awareness and education should teach users three things:

- **What not to do:** Even in managed environments, users of mobile devices have various ways to evade or disable security technology. Users may try to change (corporate) proxy settings, install new (potentially malicious) security profiles, remove corporate security profiles, sideload applications, or even jailbreak or root a device. Users should be made aware of the individual and corporate risks for their actions. There are many ways to accomplish this, from helping employees protect themselves to recommending remediation actions or mandating policy on enterprise access.

- **What events to watch for:** Educate users to detect events that may indicate malware or unwanted applications, such as requests for excessive permissions, unexpected pop-ups and messages with suspicious links. Users should also understand the approved sources for applications, such as an enterprise repository or the main vendor’s application store.

- **How to respond to events:** A concise, documented and tested process for incident management and response must be part of any user education process. Help desk contacts should be at the fingertips of all users on each of their devices. Help desks also need to build trust with the employee community. Incident response greatly depends on the mobile platforms: Some will only allow for user notification (“please deinstall that malicious app”), while others allow for full remote management of the mobile device (“sit back and wait while we fix the issues”). In general, more and more users are technically savvy on mobile devices. IT and help desks need to understand and consider self-service support tools as an option.

Mobile awareness and security training should show the personal effect on the employee (like stealing personal banking data) and the effect on the enterprise if the employee’s device is infected (like possible leakage of confidential corporate data or stealing the employee's data from the enterprise).

Phase 2: Build Mobile Security Strategy

In Phase 2, we begin to build the mobile security strategy and fill out the matrix of requirements, standards and products for each key technology area. This is where you will need to download the "mobile_sec_worksheet.xlsx" from the download menu of the document. As you go through all the steps, keep in mind there will be choices for each of the mobile data levels you have defined in Step 1.2. The choices can range from required to optional, and in some cases, like Step 2.1, setting minimum OS/HW requirements may apply to all the data levels. Once you make your decisions, fill in your worksheet. For an example of how it can be filled out or some recommendations, see the Sample tab.

Step 2.1: Define Minimum OS/HW Requirements

Modern mobile platforms, including iOS and Android, have strong native controls that protect against initial infection and limit the impact of malware on the device. Many organizations are using full versions of Windows 10 on tablets and beginning to manage these devices with UEM/EMM solutions. For more details on native security controls for the most popular mobile platforms, see "Mobile OSs and Device Security: A Comparison of Platforms."

Older hardware can also impose problems, especially when vulnerabilities are discovered that cannot be mitigated. Older versions of devices were susceptible to attacks like Spectre and Meltdown, which initially had some software patches but were fixed with newer hardware in subsequent devices. There are also examples like checkm8, which exposes hardware flaws in Apple iPhones from the 4s to the X that cannot be patched because it attacks the read-only bootrom (see the Ars Technica article, "Developer of Checkm8 Explains Why iDevice Jailbreak Exploit Is a Game Changer"). This is why setting minimum hardware versions becomes critical.

Native security controls in some modern mobile devices have been successful in mitigating some malware risk. Native controls help harden the mobile devices to prevent some of the attacks, while more hardened devices from Samsung Electronics (Knox), Google (Pixel), Android Enterprise Recommended and Microsoft (Surface Pro) add additional layers of security. It also becomes key to keep Android, Chrome OS, iOS and Windows up to date and set minimums and recommended versions for the operating systems. On Android and Windows, maintain security patch levels to protect the enterprise from new threats. Use the current minimum and recommended versions of both the OS and hardware device versions in the "Mobile OSs and Device Security: A Comparison of Platforms" for your corporate standards.

These are evolving faster than we can refresh our research, and enterprises should be ready to move forward in case new major vulnerabilities are discovered. You can also schedule an inquiry with a Gartner mobile security analyst to review any changes that may affect the yearly published recommendations.

Step 2.2: Define UEM/EMM Requirements

Even though UEM/EMM solutions do not include anti-malware controls themselves, their use is key in the detection and remediation of mobile threats. First, EMM agents may include rootkit detection functionality that can determine whether the mobile device was compromised using a known rooting or jailbreak technique.

Note that detecting unknown privileged malware is as difficult on a mobile device as detecting rootkits on a desktop PC. Most EMM agents will be limited in their protection capabilities. Any rooted or jailbroken device could be denied access to corporate resources or the corporate container, or its data could be remotely wiped through the EMM platform.

Other critical capabilities of EMM are the control and management of applications, and control over profile installation to help prevent malicious profile and VPN-based attacks. EMM may also provide inventories of all installed mobile applications and integrate with a mobile app risk management solution to determine the risk level for a specific device.

The capability of EMM to manage applications beyond inventories (that is, the installation and deinstallation of applications) greatly differs between mobile platforms. Often, application control is limited to managed applications — applications that are installed through EMM — which are often of limited use for detecting and removing malware. On supported platforms, EMM may be used to deinstall malicious or potentially unwanted programs. For details on the capabilities of app monitoring and controls per mobile platform, see "Mobile OSs and Device Security: A Comparison of Platforms."

Organizations that want more advanced control on managed iOS devices can use supervised mode. This will enable greater control, including silent update of apps, filtering websites and additional device control.

For more information on selecting a UEM/EMM, see "Evaluation Criteria for Enterprise Mobility Management Suites."

Step 2.3: Set Encryption and Configuration Standards

In this step, you can use the UEM/EMM or Microsoft Exchange ActiveSync to set encryption standards and common enterprise configuration settings.

Base Configuration Standards

Some common baselines for enterprises to set are:

- Password lengths (six-digit or alphanumeric minimum to more complex for higher-security organizations)
- Password types like biometrics
- Container password types different than the device passwords
- Password lockouts (for example, the phone locks after three to five attempts)
- Automatic wipe after password lockout

- Device encryption on
- Minimum OS versions
- Block jailbroken or rooted devices

Device Encryption

All modern mobile OSs (iOS, Android and Windows) support native, full disk/device encryption. Newer versions automatically enable this encryption, but there are some older and OEM devices that can have these options turned off. This is where mobile security solutions can be leveraged to ensure that full device encryption is turned on before the device accesses corporate resources. This policy should be set for all levels and types of mobile devices supported in the organization. Also, set “enable storage encryption” for removable storage on devices that support Secure Digital (SD) cards.

File-Level Protection

For file-level protection, leverage the data grouping prework to determine which level may require additional protection. If there are high-security or secret data requirements on devices, look for file-level-encryption-type solutions. These include Windows Information Protection, or the more advanced, identity-based Microsoft Azure Rights Management (Azure RMS), Android 7.0 file-based encryption, iOS 11 Apple File System (APFS) or third-party app/file encryption products. This will add a secondary encryption layer in case the device encryption/passcode has been breached. Another benefit can be to isolate data in the context of a user or app so that no app can access another app’s unencrypted data without authorization. The keys used to encrypt files should be different than the device-level keys.

Other Configurations

UEMs can also be used to manage and monitor additional or malicious profiles, DNS settings, SWG as a service, proxy settings, VPN profiles, certificates, and modes like device admin on older Android and supervised mode on iOS. These are all settings that an attacker could change to compromise the device and exfiltrate data.

Mobile Application Stores

Managing and monitoring which application stores are enabled on mobile devices becomes critical to reducing the unwanted and malicious apps installed and possibly propagated into the enterprise. UEM/EMM solutions typically support the management of app deployment channels to a corporate application store by using mobile application management (MAM) tools.

Apple, Google and Microsoft have programs and procedures in place to curate the applications in their stores. These vendor sites may still contain malicious applications, but the time to remove them is generally faster than the smaller third-party application stores. If your corporation uses enterprise application stores for internal mobile application development, it is important to establish mobile app security verification procedures.

Third-party vendors such as Veracode, Micro Focus and IBM security offer tools and services that can be used to scan enterprise mobile applications for possible threats and vulnerabilities before release to the enterprise application store. Most of the benefit of using application security testing (AST) vendors to assess the security of mobile apps comes from manual testing (if they offer it), which usually comes at a premium. You can quickly get into the realm of two to four weeks, especially with multiple mobile platforms, with costs of $20,000 or more depending on the scope of testing.

For more information on mobile app security testing, see "How to Integrate Application Security Testing Into a Software Development Life Cycle."

Step 2.4: Determine Container Requirements

Another option to evaluate is the use of a container or workspace isolation solution to separate corporate data from personal data. This can help when employees want access to corporate data but do not want their personal data monitored or possibly wiped as part of the device being stolen or compromised. Containers also can be encrypted or remotely wiped, and some can enforce container-level VPNs for protecting corporate traffic.

Android has a built-in container called Android Enterprise, which will create a work profile separate from the consumer side. Samsung Galaxy devices enabled with Knox have an advanced, hardware-protected container called Knox Workspace. This container has a hardwired e-fuse that will short out if the workspace is tampered with. Once triggered, the keys are lost and the container is locked forever. Some of the UEM/EMMs provide software-level versions of containers like VMware's Workspace ONE and MobileIron that can be created and managed separately from the personal side of the device.

Containers help IT maintain control of where data and applications are stored on the device as well as setting encryption and network protection for the corporate side. Using containers is recommended for BYOD use cases where separation of corporate and consumer data is needed and also as a defense-in-depth feature for high-security or highly regulated organizations.

Step 2.5: Set Minimum Device Authentication Requirements

Identity and authentication (or IAM) is another key component for your mobile security strategy. Without the proper authentication, there is possible impact to encryption at the device, file and container layers. This shows up often when employees turn off passcodes or possibly register multiple family members' fingerprints to make corporate or personal tablets multiuse home devices.

Depending on the type of organization, there will be different minimum levels of authentication at the device, container or application layers. For example, defense organizations will have strict government authentication methods like Common Access Card (CAC)/smart cards (physical/virtual), advanced biometrics, use of X.509 certificates and other multifactor authentication methods. On the other hand, a retail organization may prioritize easy access for the sales floor employee and use simple passcodes, biometrics or even patterns to unlock mobile devices.

Regardless of what minimums you set for your organization, look to enforce different types of authentication at the device level versus the container or corporate application level, with higher levels of complexity and more sensitive data requirements. This will create multiple barriers for attackers if they try and exfiltrate or compromise data. At the same time, this will limit the number of devices you can use. Not all can work with CAC cards, for example.

For more information on biometrics, see “Technology Insight for Biometric Authentication.”

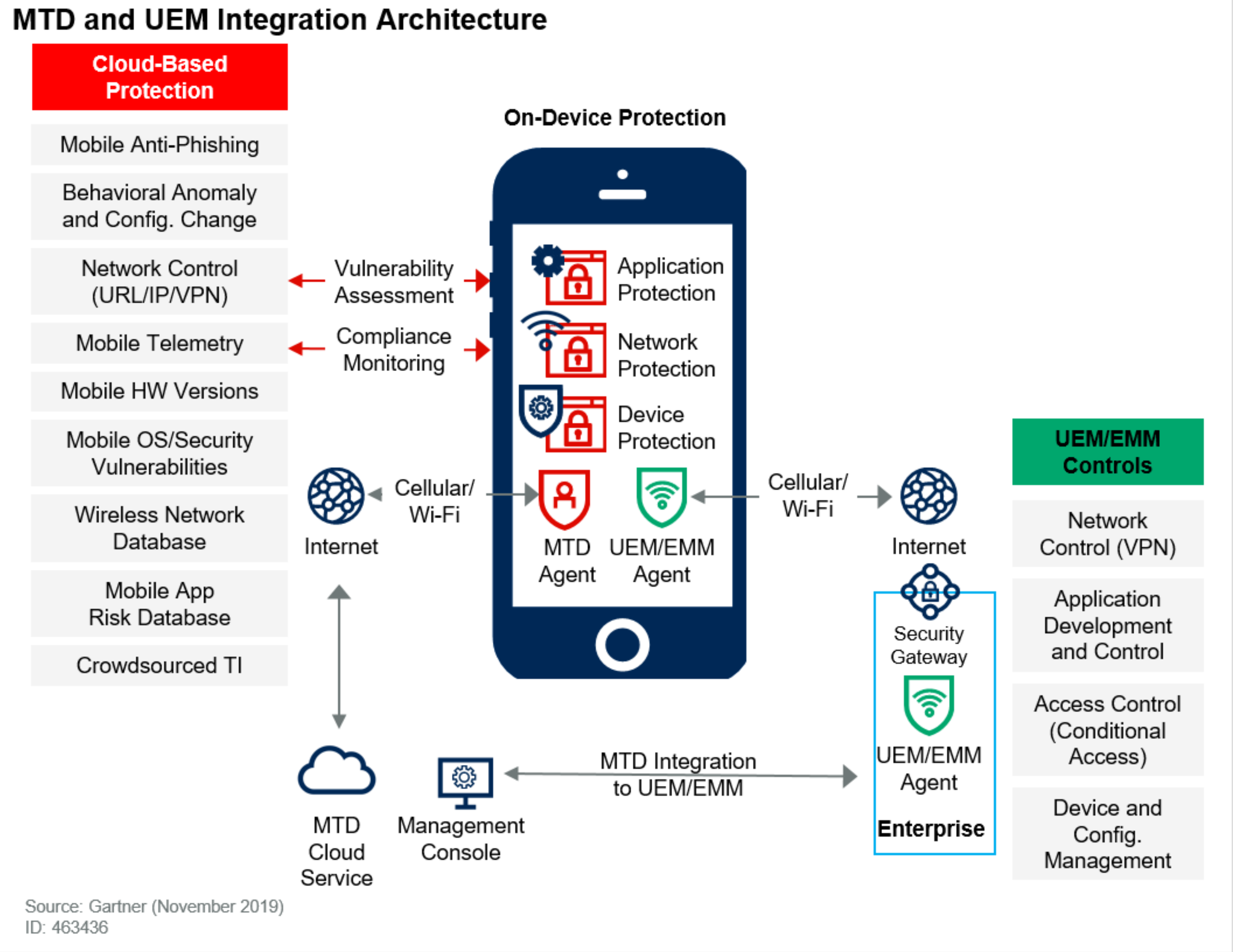
Step 2.6: Define MTD Requirements

This market segment consists of vendors leveraging some combination of the following mobile protection methods for Android and iOS:

- Behavioral anomaly and configuration detection
- Protection for device attacks, network attacks and malicious and leaky apps
- Mobile anti-phishing protection
- OS-, hardware- and application-based vulnerability assessment, monitoring and compliance
- Crowdsourced threat intelligence

See Figure 3 for MTD and UEM integration architecture.

Figure 3. MTD and UEM Integration Architecture



Source: Gartner (November 2019)
ID: 463436

Behavioral Anomaly Detection

This type of protection focuses on detecting abnormal behavior or configuration changes of the device and applications. Some examples of the most important indicators of possible compromise include:

- Jailbreaking and rooting of the device
- Third-party application stores
- Unknown sources and sideloaded applications
- Applications being granted elevation of privilege (EOP) or device administrator access on Android

The ability to monitor the device and understand when there is an event or configuration change is critical. We are seeing malware that starts off as valid to get past the app store curation process and then triggers malicious activities (other application installs, configuration changes, certificate installations, or VPN configurations) at a later date.

Network Protection

One of the key features of modern mobile OSs is the ability to find Wi-Fi and automatically switch over to it to improve performance and reduce network traffic on the carrier's data networks. In doing so, mobile devices make network-based attacks easier. As the device detects public Wi-Fi, it automatically starts directing traffic over that channel. Some of the newer versions of mobile OSs are looking at putting warnings to help protect users when joining unsecure public Wi-Fi networks. This is where malicious users with rogue access points can begin their probes and attacks. The applications on the mobile devices are in separate containers, but the apps all share the same network stack.

Hackers can bring up MITM proxy servers or a VPN profile and then leverage a fake SSL certificate to intercept traffic from the device through the following steps:

1. Generate a root certificate authority (CA) and get the user to accept and trust it (e.g., a malicious profile attack).
2. Set up an intercepting proxy, rogue AP or malicious VPN.
3. Modify the network connection to route traffic through the proxy, AP or VPN profile. This is done through modification of IP tables, Wi-Fi connection properties or Access Point Name (APN).

At that point, attackers have MITM of the traffic and can decrypt any SSL/Transport Layer Security (TLS) requests or responses. Data exfiltration, credential theft, session hijacking and so forth are then all feasible.

To protect against these types of attacks, it becomes important to detect the following:

- Rogue access points
- Fake SSL certificates
- Address Resolution Protocol (ARP) and Domain Name System (DNS) poisoning
- Any traffic being sent to malicious address
- Reconnaissance scanning
- Web-based content manipulation

If the network is deemed suspicious or previously discovered to be malicious by other users, some form of alert, blocking of the malicious network connection or establishing a VPN connection to the organization is needed to protect the corporate traffic. These forms of protection rely on crowdsourcing databases, active probes of the networks and detection of known types of network spoofing attacks.

Once they've detected that a location could be compromised, some solutions will leverage the location information on the device to tag the site as risky. Then, when other users are in the vicinity, they can be warned of the possibility of attack. There is some risk to having a reliance on a network service to check for these types of attacks. The more advanced malware authors could start blocking traffic to the back-end data stores. This could make some of the solutions less effective, so it will be critical to have both on-device and cloud-based protection to secure the device.

Vulnerability Management

In the scope of mobile devices, vulnerability management is defined as both assessment and management of OS and security vulnerabilities. Mobile OS vendors track vulnerabilities by common vulnerabilities and exposures (CVEs) tied to mobile OS versions, and now in monthly security patches for Android.

This area is the least developed out of the four features that compose MTD solutions. Most solutions will track OS versions, but none have yet implemented tracking the monthly security patches on Android. The other thing that makes this more complicated on mobile devices is the lack of capability to force OS updates and security patches. This makes the current features more assessment than management. The one exception is on iOS if the devices are in Apple School Manager (education) or Apple Deployment Programs (business). With these settings, OS updates can be pushed to the devices and be required to be installed.

The final complexity here is to understand which OS versions can be installed on the different hardware devices. This is obviously more difficult to track on the Android platform due to the numerous OEMs and different supported versions and time frames for the updates.

Application Risk Scanning

Understanding what applications are installed on mobile devices and how risky they are is a key feature for MTD solutions.

The basic premise is to provide a mixture of static and dynamic code analysis based on a binary analysis of the mobile applications for malicious behavior or embedded malware. This feature relies on a cloud-based database of applications that have been scanned out of band. The app database also often includes reputation information (prevalence, age, risk score, privacy score). Once the application ID is determined (by analyzing the binary, using an agent on the device, or integrating with an EMM application inventory feature), the app is compared to the cloud-based service list for a risk score.

If the application is new to the service, then the application is typically installed on a virtual instance of a mobile device and OS in the cloud and analyzed for security issues. Based on the analysis, a new risk score is assigned and sent back to the management console. Then the MTD solution can alert IT and the user that a malicious app is installed and take action. This action could include an end-user action of uninstall. For the IT admin, it could be some kind of conditional access workflow like sending an alert with specific instructions or time frames and then blocking the device or stopping email.

As mobile attacks become more advanced and the MTD vendors continue to mature, now is the time to start planning for MTD adoption for both iOS and Android devices. Most MTDs do not support Windows 10 app scanning at this time. Stand-alone MTDs can be used for more BYOD protection and integrated with UEM/EMMs for fully managed scenarios.

For more information on MTD products, see "Comparison of Mobile Threat Defense Solutions."

If you are running Windows tablets in a more mobile mode (leveraging UEM/EMMs for management of Windows 10 devices), you may need to look to advanced malware solutions, endpoint protection platforms (EPPs), or endpoint detection and response (EDR)-type solutions.

Step 2.7: Define Network Protection

In many organizations, a constant challenge is corporate-owned devices versus BYOD. As malicious attackers target corporations, there is a real threat from outside mobile devices coming on to the enterprise network. An additional layer of defense to help mitigate some of the new mobile attacks can entail network segregation by creating mobile-only wireless networks connected directly to the internet, and not allowing access to the corporate virtual LANs (VLANs).

Secure web gateways (SWGs) or enterprise firewalls have expanded their support for mobile devices. Organizations can set up device-, app- or container-level VPNs to direct the traffic back through the enterprise to help defend against network-based attacks. Then, the gateways can identify mobile apps based on the observed traffic or the download of applications. This allows filtering on bad IP addresses, adding risk scores to these apps, and blocking specific functionality for apps (for example, to allow the use of a file sync solution but block the upload of files).

For the detection of malware in unknown applications, some solutions include network sandboxes that can detonate unknown mobile apps. Both when on-premises and off the corporate network, managed mobile devices can have their traffic redirected to cloud-based SWGs, such as Symantec-Blue Coat, Cisco, Forcepoint, McAfee or Zscaler. But directing all mobile traffic through SWGs as a service can cause performance, latency and application issues, especially if certificate pinning is being used.

For more information on SWG and mobile, see "Assessing Secure Web Gateway Technologies."

Step 2.8: Evaluate Mobile Application Security Requirements

In some cases, organizations want or need to protect specific apps on a device, rather than the whole device, or they need additional protection in addition to device protection. Even in the case of BYOD or corporate-owned, personally enabled (COPE) devices, the device controls may be insufficiently deployable or not strong enough for highly sensitive apps. Securing the individual apps, in essence increasing their protection from attacks that originate elsewhere on the device, can be done using three techniques:

- Mobile application shielding, which adds threat-protection capabilities, such as jailbreak detection and debugger detection, to the app. It then applies obfuscation and encryption techniques that make the app resistant to tampering and reverse engineering. It does not provide ironclad protection, but it makes such attacks much more difficult or "good enough."

- Mobile application wrapping, which adds security capabilities, such as authentication, encryption, threat protection and sometimes EMM linkage, into the app. Wrapping overlaps with shielding, mostly in the area of encryption and some threat protection like rooting detection, but does not provide the same level of protection.

- When building homegrown applications, require that your mobile app suppliers sufficiently harden the app as they build it and not just rely on app shielding or app wrapping. These techniques are secure design, secure coding practices and defensive coding.

Representative vendors include Appdome, Arxan Technologies, Intertrust (whiteCryption), Guardsquare and Verimatrix. For more information, see "Market Guide for In-App Protection."

Step 2.9: Determine Mobile Secure Communication Requirements

Some organizations will have requirements or industry regulations to secure all mobile data, voice and SMS messaging with full, end-to-end encryption solutions. The secure mobile communication or instant communications market can be broken down in two parts:

- The first segment requires encryption solutions for particular use cases. Hacktivism, fraud, advanced threats and simple enterprise data loss are all examples of the risks that need to be mitigated. A typical example is a top executive traveling to a country that is considered high risk for industrial espionage. Organizations want to ensure that their executives can speak about sensitive enterprise matters without the risk of interception of these communications. There are multiple solutions that can cover mobile secure communications from software, hardware and service-based vendors.

- The second option is to leverage existing unified communication solutions like Teams, Whatsapp, Slack, etc. Unified communications can also provide a service-based secure channel for your enterprise users.

For more information, see "Market Guide for Instant Communications Security and Compliance."

Step 2.10: Select Mobile Security Solutions and Fill Out Matrix

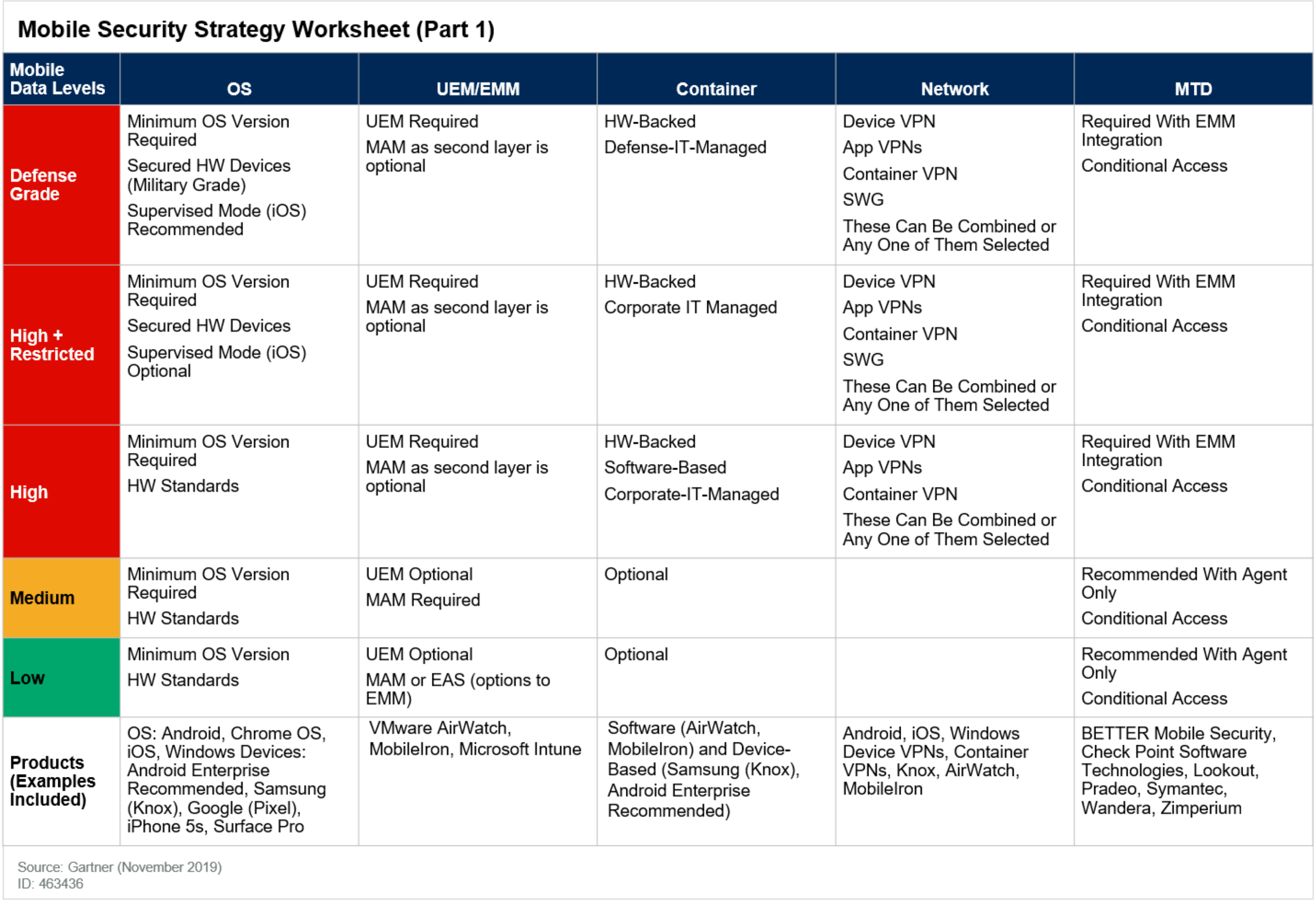
As you build your mobile security strategy, it can be leveraged for both personally and corporate-owned devices because it abstracts the ownership model and pivots controls on the type of data access needed (see Figures 4 and 5 below). For example, if employees need access for high or high-and-restricted data on their mobile devices, they would have to meet the requirements defined in each category. That requirement may be a certain mobile device or a hardened one (e.g., one with Samsung [Knox], a Google [Pixel] or Android Enterprise Recommended device). It, as well as the other requirements that you define for your data levels, would need to be managed by an EMM.

Since this model is ownership-agnostic, you can either buy one of those devices and allow it to be managed, or, if the company provides devices, select it from them. On the other hand, employees may only want access to email, calendar, and contacts or low-classified data. In this case, they could bring a device or select a corporate device with a minimum OS level, leverage Exchange ActiveSync with basic management capabilities, and look to file-level encryption, a secure email client or mobile application security to protect higher-sensitivity data.

This menu approach can be adapted to your different data classification levels based on the different ownership models, and legal and cultural requirements. As higher levels of access are required, there may be reasons why fully managing or using supervisor mode on iOS would not be allowed on personally owned devices, thus requiring the corporation to provide the device.

These are things to consider when building your corporate menu. They can be achieved by building a separate menu for BYOD versus corporate-owned devices. Download the mobile security strategy worksheet in the downloadable attachment folder of this document, and use Figures 4 and 5 below as a starting point for your mobile security strategy. The figures contain recommendations for different mobile data levels and provide some example vendors that provide the security tools to implement the options.

Figure 4. Mobile Security Strategy Worksheet (Part 1)

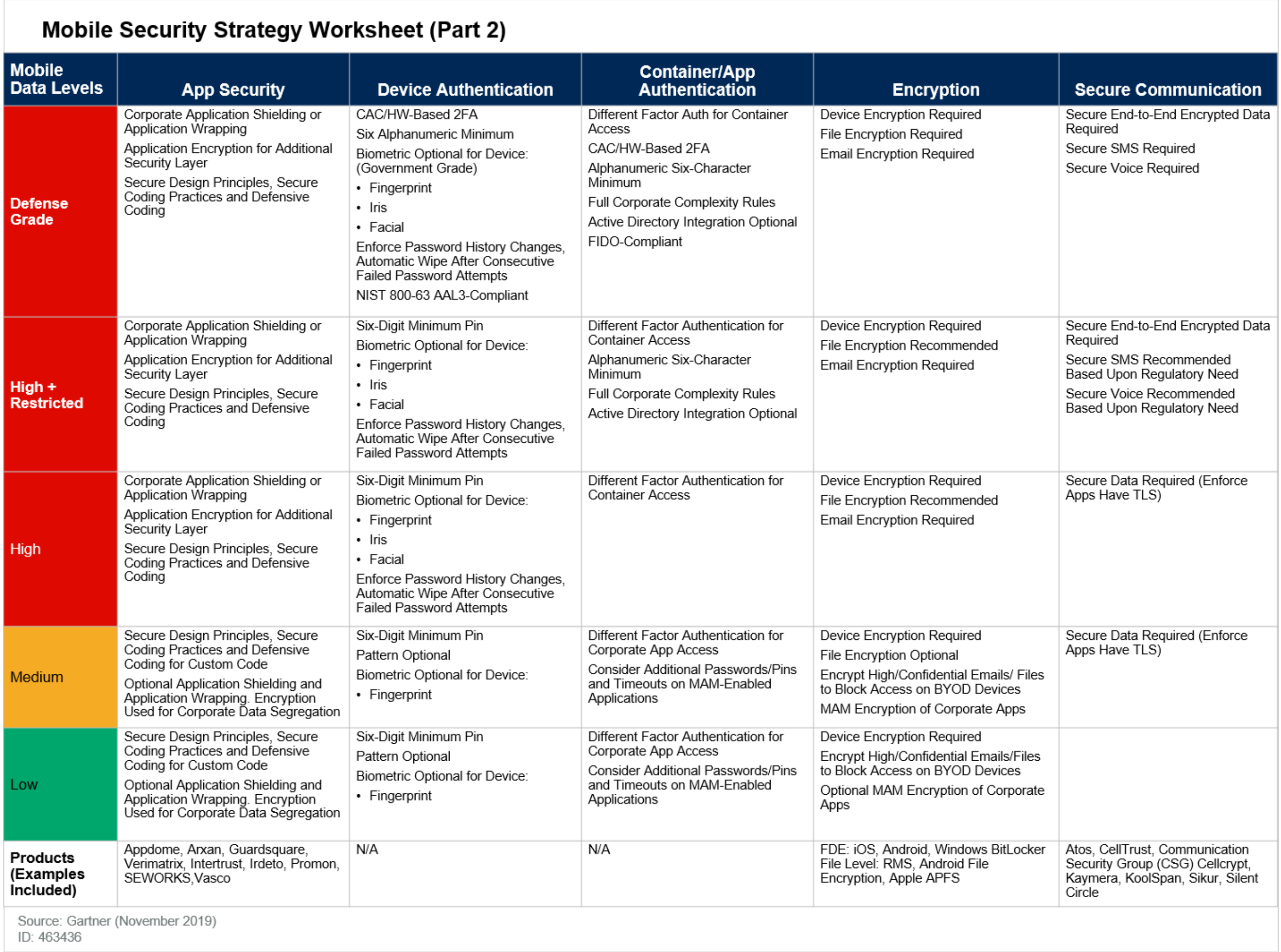


Mobile Security Strategy Worksheet (Part 1)

Mobile Data Levels	OS	UEM/EMM	Container	Network	MTD
Defense Grade	Minimum OS Version Required Secured HW Devices (Military Grade) Supervised Mode (iOS) Recommended	UEM Required MAM as second layer is optional	HW-Backed Defense-IT-Managed	Device VPN App VPNs Container VPN SWG These Can Be Combined or Any One of Them Selected	Required With EMM Integration Conditional Access
High + Restricted	Minimum OS Version Required Secured HW Devices Supervised Mode (iOS) Optional	UEM Required MAM as second layer is optional	HW-Backed Corporate IT Managed	Device VPN App VPNs Container VPN SWG These Can Be Combined or Any One of Them Selected	Required With EMM Integration Conditional Access
High	Minimum OS Version Required HW Standards	UEM Required MAM as second layer is optional	HW-Backed Software-Based Corporate-IT-Managed	Device VPN App VPNs Container VPN These Can Be Combined or Any One of Them Selected	Required With EMM Integration Conditional Access
Medium	Minimum OS Version Required HW Standards	UEM Optional MAM Required	Optional		Recommended With Agent Only Conditional Access
Low	Minimum OS Version HW Standards	UEM Optional MAM or EAS (options to EMM)	Optional		Recommended With Agent Only Conditional Access
Products (Examples Included)	OS: Android, Chrome OS, iOS, Windows Devices: Android Enterprise Recommended, Samsung (Knox), Google (Pixel), iPhone 5s, Surface Pro	VMware AirWatch, MobileIron, Microsoft Intune	Software (AirWatch, MobileIron) and Device-Based (Samsung (Knox), Android Enterprise Recommended)	Android, iOS, Windows Device VPNs, Container VPNs, Knox, AirWatch, MobileIron	BETTER Mobile Security, Check Point Software Technologies, Lookout, Pradeo, Symantec, Wandera, Zimperium

Source: Gartner (November 2019)
ID: 463436

Figure 5. Mobile Security Strategy (Part 2)



Mobile Security Strategy Worksheet (Part 2)

Mobile Data Levels	App Security	Device Authentication	Container/App Authentication	Encryption	Secure Communication
Defense Grade	Corporate Application Shielding or Application Wrapping Application Encryption for Additional Security Layer Secure Design Principles, Secure Coding Practices and Defensive Coding	CAC/HW-Based 2FA Six Alphanumeric Minimum Biometric Optional for Device: (Government Grade) • Fingerprint • Iris • Facial Enforce Password History Changes, Automatic Wipe After Consecutive Failed Password Attempts NIST 800-63 AAL3-Compliant	Different Factor Auth for Container Access CAC/HW-Based 2FA Alphanumeric Six-Character Minimum Full Corporate Complexity Rules Active Directory Integration Optional FIDO-Compliant	Device Encryption Required File Encryption Required Email Encryption Required	Secure End-to-End Encrypted Data Required Secure SMS Required Secure Voice Required
High + Restricted	Corporate Application Shielding or Application Wrapping Application Encryption for Additional Security Layer Secure Design Principles, Secure Coding Practices and Defensive Coding	Six-Digit Minimum Pin Biometric Optional for Device: • Fingerprint • Iris • Facial Enforce Password History Changes, Automatic Wipe After Consecutive Failed Password Attempts	Different Factor Authentication for Container Access Alphanumeric Six-Character Minimum Full Corporate Complexity Rules Active Directory Integration Optional	Device Encryption Required File Encryption Recommended Email Encryption Required	Secure End-to-End Encrypted Data Required Secure SMS Recommended Based Upon Regulatory Need Secure Voice Recommended Based Upon Regulatory Need
High	Corporate Application Shielding or Application Wrapping Application Encryption for Additional Security Layer Secure Design Principles, Secure Coding Practices and Defensive Coding	Six-Digit Minimum Pin Biometric Optional for Device: • Fingerprint • Iris • Facial Enforce Password History Changes, Automatic Wipe After Consecutive Failed Password Attempts	Different Factor Authentication for Container Access	Device Encryption Required File Encryption Recommended Email Encryption Required	Secure Data Required (Enforce Apps Have TLS)
Medium	Secure Design Principles, Secure Coding Practices and Defensive Coding for Custom Code Optional Application Shielding and Application Wrapping. Encryption Used for Corporate Data Segregation	Six-Digit Minimum Pin Pattern Optional Biometric Optional for Device: • Fingerprint	Different Factor Authentication for Corporate App Access Consider Additional Passwords/Pins and Timeouts on MAM-Enabled Applications	Device Encryption Required File Encryption Optional Encrypt High/Confidential Emails/ Files to Block Access on BYOD Devices MAM Encryption of Corporate Apps	Secure Data Required (Enforce Apps Have TLS)
Low	Secure Design Principles, Secure Coding Practices and Defensive Coding for Custom Code Optional Application Shielding and Application Wrapping. Encryption Used for Corporate Data Segregation	Six-Digit Minimum Pin Pattern Optional Biometric Optional for Device: • Fingerprint	Different Factor Authentication for Corporate App Access Consider Additional Passwords/Pins and Timeouts on MAM-Enabled Applications	Device Encryption Required Encrypt High/Confidential Emails/Files to Block Access on BYOD Devices Optional MAM Encryption of Corporate Apps	
Products (Examples Included)	Appdome, Arxan, Guardsquare, Verimatrix, Intertrust, Irdeto, Promon, SEWORKS,Vasco	N/A	N/A	FDE: iOS, Android, Windows BitLocker File Level: RMS, Android File Encryption, Apple APFS	Atos, CellTrust, Communication Security Group (CSG) Cellcrypt, Kaymera, KoolSpan, Sikur, Silent Circle

Source: Gartner (November 2019)
ID: 463436

Follow-Up

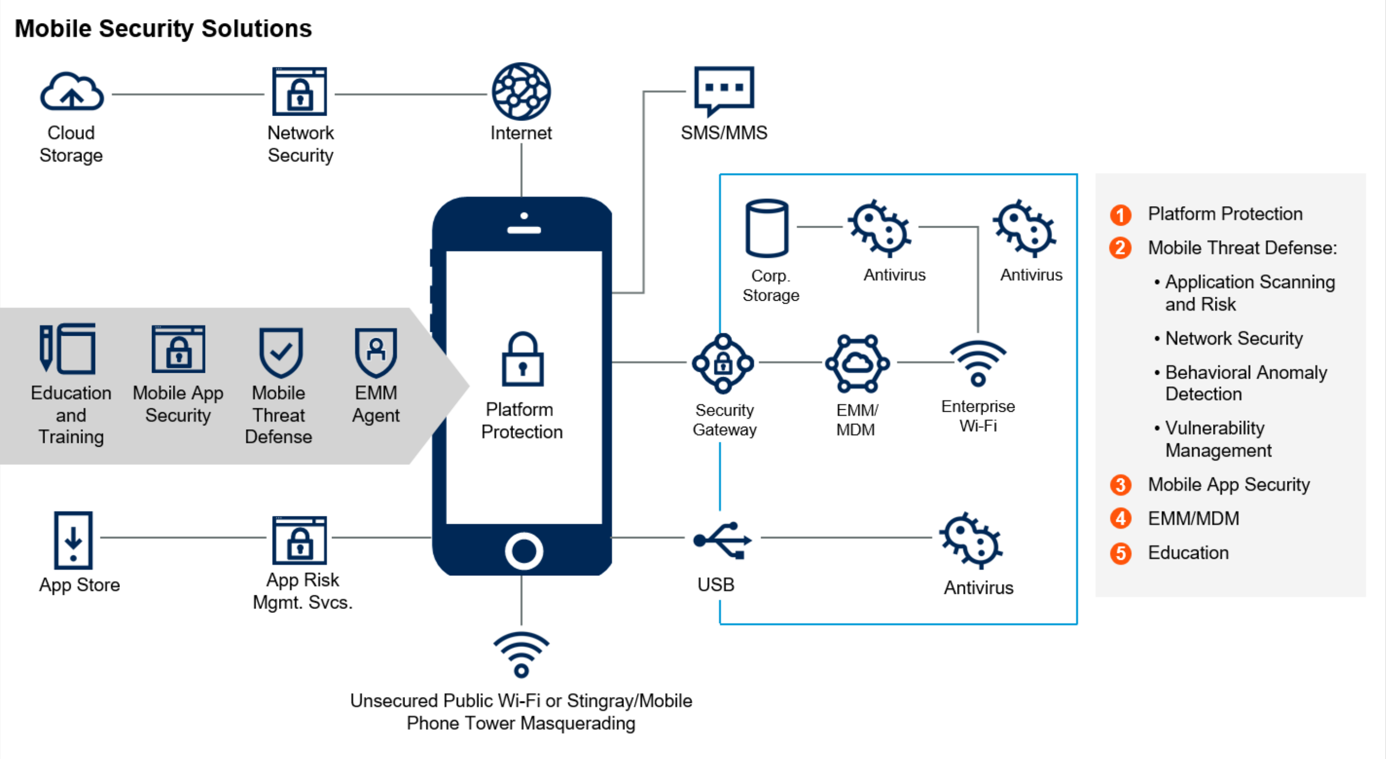
After you have built your organization's mobile security strategy and selected the products to meet your use cases, you will need to:

- Periodically, especially at the beginning of the year, verify the selected standards and solutions (this timing relates to OS and device releases in the fall from Apple, Google and Microsoft as well as the publication cadence of the Gartner Mobile OS and Device Comparison).
- Keep up with mobile threat research from mobile security vendors, in particular the MTD and Verizon Mobile Security report.
- Factor in the mobile device support life cycle for hardware support, OS updates and security updates to ensure that corporate and personal devices continue to meet your mobile device minimum standards.
- Update the employee mobile education and awareness training that was created as part of the prework phase as new types of attacks and mobile incidents are discovered.

Risks and Pitfalls

The biggest risk to building your mobile security strategy is to assume that there is one solution that will protect all your mobile devices from all types of attacks. Another common misconception is that UEM and EMM are enough protection for your mobile infrastructure. This is not the case. Those types of solutions focus on configuration and management first, with some minor security capabilities. Therefore, you will have to invest in multiple products and build your mobile security strategy to protect your mobile devices. Figure 6 below shows how the different mobile security products, standards and education work together to build your mobile defense in depth solution.

Figure 6. Mobile Security Solutions



Source: Gartner (November 2019)
ID: 463436

Another common misconception is that certain devices are secure enough for the enterprise, and therefore mobile security solutions are not required. Even if you leverage the Gartner minimum mobile OS and hardware requirements, new attacks on Android, Chrome OS, iOS and Windows will continue to surface.

Document Revision History

Advance and Improve Your Mobile Security Strategy in 2018 - 29 November 2017

Comparing Approaches to Mobile Security Strategies - 12 September 2016

Protecting Mobile Devices Against Malware and Potentially Unwanted Applications - 4 March 2015

Recommended by the Author

Mobile OSs and Device Security: A Comparison of Platforms

Comparison of Mobile Threat Defense Solutions

Recommended For You

Mobile OSs and Device Security: A Comparison of Platforms

Solution Path for Forming an API Security Strategy

5 Core Security Patterns to Protect Against Highly Evasive Attacks

Decision Point for Postmodern Security Zones

Achieving Data Security Through Privacy-Enhanced Computation Techniques