Cyber Talk

THE COMPLETE GUIDE TO

ENTERPRISE MOBILE SECURITY

Securing Mobile Devices, Building Trust

Many businesses have addressed the need to enable workers to access business resources and data from their mobile devices. Allowing access from these portable, often untrusted computing devices, typically owned by the employee (i.e. BYOD), compelled many businesses to put in place a mobile device management (MDM) solution, or its more capable successors enterprise mobility management (EMM) and unified endpoint management (UEM).

But even with an EMM/UEM solution in place, attackers quickly identified the mobile device as an easy target. They found mobile users to be more distracted and less discerning when using their devices, which makes them easy to fool into doing careless and downright reckless things. The mobile device itself provides multiple new vectors of attack that can be exploited to gain unauthorized access to data on the device, or as an entry point to remote resources and data.

As most EMMs/UEMs do not actively scan for mobile-related threats like malicious apps, vulnerable operating systems, network-based attacks, or protect users against phishing and other social engineering attacks, businesses are rolling mobile security solutions to provide this missing layer of protection.

This guide discusses the full breadth of considerations when evaluating a mobile security solution for your business.

Why Businesses Need a Mobile Security Solution

MOBILE DEVICES AND THEIR USERS ARE VULNERABLE TO MULTIPLE ATTACK VECTORS, WHICH PUTS BUSINESSES AT RISK WHENEVER EMPLOYEES ACCESS BUSINESS RESOURCES AND DATA FROM THEIR DEVICES.

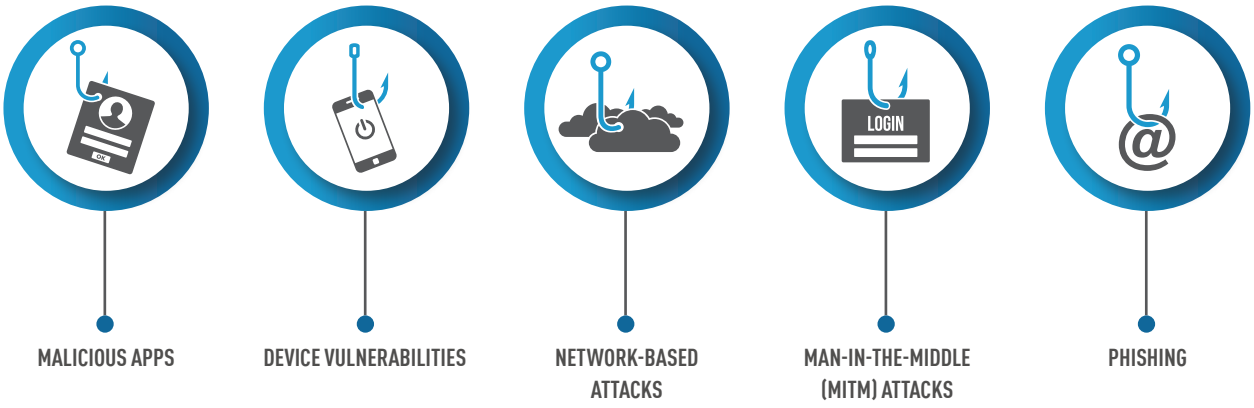
Attackers attempt to gain unauthorized access to sensitive data and applications on mobile devices, or use devices as an entry point to access remotely hosted data and applications. Sensitive data can include anything from access credentials to sensitive patient or customer data, and even intellectual property. Unauthorized access to applications can result in the execution of fraudulent transactions or as a means to access sensitive data hosted on some backend service.

While sometimes perceived as more secure than personal computers, the fact is that mobile devices are vulnerable in many ways, and open-up multiple attack vectors that can compromise the device or steal a credential. According to a recent Check Point Research report, 100% of all businesses analyzed experienced a mobile malware attack (with an average of 54 attacks per business during a 12-month period); and 89% experienced a man-in-the-middle (MitM) attack over Wi-Fi.

It is therefore a foregone conclusion that mobile devices are no different than laptops — they are used to access business resources and data, and they are vulnerable, which means they require the same standard of protection applied to laptops.

Mobile attack vectors

Common attack vectors on mobile devices and users include:



MALICIOUS APPS.

Installing malicious apps can result in a host of rogue activities from exfiltration of sensitive data to remotely seizing control of sensors like the camera and microphone to spy on users. For attackers mobile malware offers an easy and effective way to launch sophisticated, targeted attacks because most users implicitly trust the apps they install no matter where they came from. As a result, devices are easily infected with malware such as credential stealers, keyloggers, remote-access trojans, and root kits. Making matters worse, most users don't understand or read the permissions they grant applications during installation, which enables attackers to wreak havoc on the device once their malicious apps are installed.

DEVICE VULNERABILITIES.

Operating system vulnerabilities and "promiscuous" configurations open the door to compromise. Running a properly patched operating environment and limiting its attack surface via proper configuration settings significantly improves protection. Most successful attacks don't need sophisticated tools that exploit zero-day vulnerabilities—they simply exploit known vulnerabilities that businesses neglected to patch. Therefore, neglecting to identify and remediate vulnerabilities in the device's operating environment is equivalent to not patching a vulnerable laptop or server against a known vulnerability.

NETWORK-BASED ATTACKS.

Understanding the connections to and from a mobile device is critically important for the prevention of attacks, as most mobile malware needs to communicate with a command-and-control server for instructions, and eventually to exfiltrate data. Detecting these rogue communication channels and blocking them has proven to be a very effective means for preventing multiple types of attack.

MAN-IN-THE-MIDDLE (MITM) ATTACKS.

To intercept and eavesdrop on communications between a device and remote servers, threat actors frequently employ man-in-the-middle attacks. A successful MitM attack allows the attacker to intercept sensitive data, including passwords, authorization tokens, and sensitive personal data. It also allows the attack to tamper with the communication session to carry out fraud. For example, a man-in-the-middle attack on an online banking session allows the attacker to modify a funds transfer initiated by the account holder to divert funds to the attacker's account.

PHISHING.

Ninety percent of all cyberattacks begin with a phishing campaign. So it's no surprise that threat actors exploit the many messaging apps available on mobile devices to try to link a user to a phishing site. Typical apps used include private and corporate email, SMS, and a host of messaging apps like Slack, Facebook Messenger, WhatsApp, etc. Credential phishing can also be accomplished using malicious apps and man-in-the-middle attacks.

Unauthorized access of a mobile device or an application can infringe on a user's privacy by stealing sensitive pictures, eavesdropping on private communications, or using the device's sensors to spy on the user. For businesses, the same infringements can quickly result in a damaging data breach, which inevitably leads to a compliance violation and substantial penalties.

ATTACKS CAN HURT BOTH USERS AND THE BUSINESSES THEY WORK FOR.

Fraud is another common motivator for attackers, which hurts both users and businesses. Most commonly, fraudsters target financial applications to execute fraudulent money transfers for the benefit of the attacker. Fraud itself can take on many forms, from an account takeover enabled by credential theft to a man-in-the-middle attack that tampers with transactions originated by an authenticated account holder.

Finally, for the vast majority of businesses, a successful attack can inflict severe damage to its brand and reputation — damage that requires a lot of time and resources to undo.

A Prescription for a Mobile Security Solution

Common use-cases that need to be considered when evaluating a mobile security solution include:

ENDPOINT SECURITY. Mobile devices are no different than other endpoints, therefore they require the same standard of protection. An endpoint security solution for mobile needs to provide protection against known attack vectors, including malware, network-based attacks and phishing, and also prevent attacks that are not yet known (i.e. zero-days). As a result, businesses are increasingly expanding the scope of their endpoint security strategy to also include mobile endpoints.

BRING YOUR OWN DEVICE (BYOD), and unmanaged devices in general, are particularly challenging for businesses. Ordinarily, businesses strive to provide employees with the flexibility to access email and other business applications required to get their jobs done from their personal mobile devices. But on the other hand, users often do careless and foolish things on their mobile devices, which can put the business at risk. Deploying a mobile security solution turns an untrusted mobile device into a trusted one, and therefore offers a responsible way to provide mobile users with the access they need, while preventing risks that a mobile channel creates.

SECURING MOBILITY SOLUTIONS. Mobile security is increasingly used as an add-on to enterprise mobility management (EMM) / unified endpoint management (UEM) solutions. While some businesses wrongfully perceive their EMM/UEM solutions as providing adequate protections, better informed businesses realize that they fall short of protecting against significant security threats, including scanning and identifying misbehaving or malicious apps, preventing network-based attacks, and completely ignoring phishing and social engineering attacks that lead to credential theft. Deploying a mobile security solution to secure an EMM/UEM is considered best practice and becoming the norm for many businesses.

PHISHING and social engineering attacks on mobile users are often overlooked for all businesses. Mobile users are routinely targeted with phishing links sent over any one of the many messaging apps available on mobile devices, and their stolen credentials are putting not only their personal accounts at risk, but also their employer's business. Protecting mobile email, SMS, and chat/messaging apps from malicious web links is therefore critically important for the security of the business.

COMPLIANCE. As more regulations are put in place to protect customer data, businesses are compelled to also deploy an endpoint protection solution on mobile devices that have access to business resources and data, to ensure that those devices are not used as the entry point for a data breach. GDPR, HIPAA, PSD2 and other regulations are cracking down on practices that put customer data and privacy at risk, or fueling the rampant payment fraud problem. Some regulations are specifically calling out threats to mobile devices and users.

Develop a Strategy for Protection

When a business owns the mobile device, it can choose to protect the entire device and apply similar protection standards to those applied to other mobile endpoints (i.e. laptops). But in many situations, the device belongs to the employee (i.e. BYOD), in which case security policies need to be mindful of what the employee will allow.

PROTECTING THE MOBILE ENDPOINT. Practically all businesses have an endpoint security solution deployed on their PCs. Without a security solution, those endpoints expose the business to potentially devastating attacks. As mobile phones and tablets become a common and often preferred endpoint from which employees get their work done, the same level of protection needs to be extended to those devices. A comprehensive mobile security solution should be a non-negotiable pre-requisite for granting access to business applications and data from a mobile device. When devices are owned by the business, then it is often accepted without question. In situations where the device is owned by the employee (i.e. BYOD), achieving the same standard of protection is contingent upon the employee's consent.

WHENEVER DEPLOYING A SECURITY SOLUTION, IT'S IMPORTANT TO UNDERSTAND WHAT YOU CAN AND NEED TO PROTECT.

SECURING A MOBILITY SOLUTION. Deploying an enterprise mobility solution, such as EMM or UEM, does not mean the device is secured. Mobility solutions deploy a secured container to segregate sensitive data and applications from the rest of the device. They perform rudimentary policy checks to make sure the device is configured with password protection, and running an up-to-date OS version. But mobility solutions do very little to actually prevent compromise of the device itself and its user. Adding a mobile security solution protects against threats that are not in scope for the mobility solution, including credential theft attacks, vulnerable device configurations, malicious applications, rogue Wi-Fi access point, and more.

PROTECTING A MOBILE APPLICATION. Sensitive mobile applications require protection because running them on a compromised device exposes the app and its users to numerous attacks, including from other (malicious) apps on the device that can steal the protected app's credentials, eavesdrop on its communications, tamper with its transactions, and steal its data. A compromised device operating system, whether through malicious configurations or privilege escalation enabled by jailbreaking or rooting, also puts the application at risk.

Securing a mobile application typically requires integrating protection into the app itself. When the only foothold the business has on a user device is an app — for example a financial institution with banking app — then protection has to be integrated via an SDK, and deployed as an integral part of the app.

Correctly Balancing Privacy and Performance

Privacy and trust are probably the most sensitive issues with employees, especially when deploying a security app on their personal devices. And while concerns are natural and understandable, when it comes to mobile security the dilemma is a very simple one — don't install a mobile security solution and let the attackers wreak havoc on your privacy, or install a mobile security solution from a reputable vendor that is subject to third party scrutiny (e.g. a publically traded security company) and let this vendor protect your privacy.

Also factoring into the privacy and performance question is the architecture of the solution.

PRIVACY AND PERFORMANCE CONSIDERATIONS WILL INEVITABLY WEIGH INTO THE DECISION PROCESS, AND OFTEN HAVE A DECISIVE INFLUENCE ON WHETHER MOBILE SECURITY IS DEPLOYED.

Mobile security solutions that work **on-device**, using device resources to carry out their security functions, help maintain user privacy, and in many cases also user experience, as no data is sent from the device, including private data. On-device architectures also help ensure that there are no latencies associated with transporting data and waiting for responses. That said, security analytics can draw a lot of processing and memory resources from the device, which can impact the device's performance and drain its battery.

Secure **mobile gateways**, or proxy-based security solutions, offer an alternative to on-device security, as they leave the processing and memory resources of the device relatively untouched. But mobile gateways come with privacy as well as latency issues, as all network traffic is routed through the proxy for inspection. This inspection can infringe on user privacy and also introduce latencies that negatively impact user experience if it is not managed well. In situations where the device is not a corporate-owned-business-only device, users might object to having their personal activities routed through and scrutinized by their employer's mobile gateway.

On-device, **cloud-assisted** architectures offer a hybrid approach that balances performance and privacy considerations, and also adds capabilities that are not available when relying solely on the device itself. Hybrid solutions can perform sensitive analytics on the device itself to preserve user privacy, and offload to the cloud only analysis that is not privacy-sensitive. A hybrid approach also enables an enforcement point on the device itself, which is often required to prevent certain compromises that are not preventable with a gateway solution. And with supporting compute resources off the device, the security solution can perform powerful analyses, based on the latest and greatest algorithms and intelligence, to detect and prevent zero-day threats.

In summary, to effectively address all attack vectors on the mobile device and user, and also to maintain a good balance between performance and user privacy, a hybrid approach is often the only approach that truly works. And when it comes to user concerns about infringements on their privacy, mobile security solutions actually provide more privacy than they may take away by preventing malicious actors from stealing and spying on users and their surroundings.

Don't be Confused: MDM, EMM and UEM are not Security Solutions

Much like traditional endpoint security, mobile security solutions are designed to protect the device and its user from various forms of compromise, most notably malware, man-in-the-middle attacks, and phishing.

Mobility solutions are a different animal. They are designed to help businesses create a segregated, managed workspace on unmanaged mobile devices, to allow a mobile workforce to access business applications and data from their devices. This often translates into creating an encrypted and protected area on the mobile device—often called a container—that can be remotely locked or wiped if needed. Applications can be deployed to this protected area and establish a secure communication channel to their backend. In order to ensure that the workspace is not easily compromised, basic security controls and checks are performed. Security controls include enforcement of an access control policy, remote locking, remote wiping, etc.

Many companies rely on the basic mobile hygiene policies enforced by their EMM/UEM. Basic checks performed are typically limited to jailbreak and root detection, to prevent the container from installing on a device with broken access controls. Some augment these capabilities with a hodgepodge of point solutions that may help detect things like known threats, but are unable to detect recently created malware or new vulnerabilities in networks, operating systems, and apps. For example, gaining root access to a mobile device (also called "rooting" on Android or "jailbreaking" on iOS) enables cybercriminals to make a broad range of customizations and configurations to serve their objectives. EMM/UEM systems can detect the existence of certain files in a system directory that enable root access by employing several methods, including static root indicators. However, free tools for avoiding this type of detection are widely available for both Android and iOS. By changing root access indicators continually, cybercriminals can evade detection, and even deny root check requests from the EMM/UEM system, disabling detection entirely.

Mobile security solutions focus on securing the mobile device and its user from multiple vectors of attack that may compromise sensitive access credentials, data stored on the device or use the device as an entry point to access sensitive business resources and data hosted remotely. They provide a level of protection that is out of scope for EMM/UEM solutions, and therefore commonly used together with EMM/UEM. While messaging might sometimes confuse customers, recent partner relationships established between EMM/UEM vendors and EMM/UEM vendors proves the point that the two solutions are complementary rather than competing.

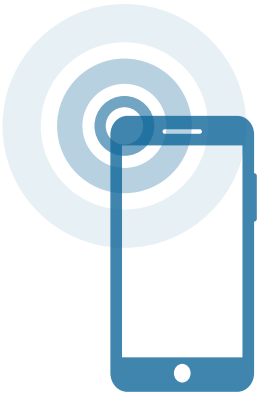
MOBILITY SOLUTIONS—MOBILE DEVICE MANAGEMENT, AND THEIR SUCCESSORS ENTERPRISE MOBILITY MANAGEMENT AND UNIFIED ENDPOINT MANAGEMENT, ARE OFTEN CONFUSED WITH MOBILE SECURITY (I.E. MOBILE THREAT DEFENSE / MOBILE THREAT MANAGEMENT.

Mobile Security is a Journey

While it is tempting to think about security as another product feature, implementing security properly requires highly specialized skills, a profound understanding of the platform to be protected and in-depth familiarity with relevant attack vectors and how to effectively prevent them. It is rarely the case that a mobile app developer or a mobility solution vendor will bring to the table sufficient security expertise to adequately protect the business and its employees from all mobile threats, known and unknown.

Protecting from known threats is relatively straightforward for a security expert. It is being able to identify and prevent unknown threats that requires extensive intelligence gathering, ongoing threat research, and advanced technology that can incorporate the intelligence and research to effectively detect zero-day threats.

Lastly, security requires specific technologies, especially when it comes to detecting the stealthier attacks or zero-day exploits. Inspecting unknown code, analyzing its execution flows and behavior patterns, at scale and with minimal impact on user experience, requires nothing less than "rocket science." This is not something you can expect to get from a mobile developer, or as a feature that is part of a larger offering. This is something that requires 100% focus and many dedicated resources.



MOBILE SECURITY REQUIRES SPECIALIZED EXPERTISE, PERSISTENCE, AND SOPHISTICATED TECHNOLOGY.

ENTERPRISE MOBILE SECURITY CHECKLIST:

1. **What are you protecting against?** Consider relevant attack vectors on your mobile devices and users — malicious apps, device vulnerabilities, network-based attacks, man-in-the-middle attacks, and phishing.
2. **What are the outcomes that you would like to achieve?** Identify the mobility use-cases that require protection — securing the endpoint, allowing BYOD to access business data and apps, securing mobility solutions (MDM/EMM/UEM), preventing credential theft, and achieving compliance.
3. **How do different mobile security solution architectures impact user privacy and device performance?** Security controls can be deployed on-device, using a mobile gateway, or with a hybrid approach where some things are done on-device and some in a supporting cloud service.
4. **Do you need a mobile security solution if you are have an MDM solution deployed?** Mobile security and MDM are a different animal, each solving a different problem. MDMs focuse on managing and protecting business data. Mobile security focuses on preventing threats to the device and user.
5. **How is your mobile security solution maintained over time to ensure that it remains effective against current and zero-day threats?** Mobile security solutions need to be backed by security experts, ongoing threat intelligence and dedicated technology.

Conclusion

Mobile endpoints such as phones and tablets are as vulnerable as laptops and PCs, so there is no reason to require different security standards when allowing them to access business resources and datamobile devices should be a part of any endpoint security strategy. Like other endpoint security solutions, mobile security needs to provide protection against known attack vectors, including malware, network-based attacks and phishing, and also prevent attacks that are not yet known, i.e. zero-day attacks.

Learn how SandBlast Mobile can help protect your business from mobile threats.
Visit www.checkpoint.com/mobilesecurity