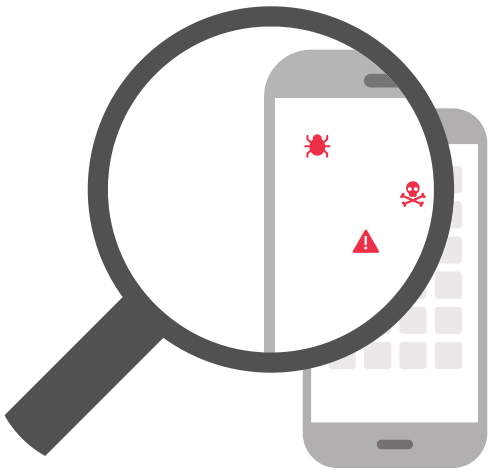
Lookout

WHITEPAPER

Mobile Security

The 6 Questions Modern Organisations Are Asking



Executive Summary

The modern organisation has recognised the need to embrace mobile devices in the workplace. Some have fully implemented a bring-your-own-device (BYOD) programme, while some have adopted a hybrid model of corporate-owned and personally-enabled (COPE) devices. Many companies then choose to deploy an Enterprise Mobility Management (EMM) or Mobile Device Management (MDM) solution to enable some control of the mobile devices that access corporate data. For companies at this stage of mobility, security is the next critical layer. As Gartner states, "It is becoming increasingly important that security leaders look at the anti-malware, mobile threat defense solutions market, the products available and how they should be used.[1]"

Sophisticated mobile threats with the ability to target valuable enterprise data and devices are a reality. To achieve the highest level of protection for critical mobile infrastructure, integrate your EMM/MDM solution with Lookout Mobile Endpoint Security for mobile threat defence, app risk mitigation and compliance.

Today's organisations are concerned about the lack of visibility into these six areas:

Are the mobile apps on our employees' devices a security threat? As more sensitive data is accessed on mobile devices, malware is becoming significantly more sophisticated, and non-malicious risky apps are creating a compliance challenge for companies in regulated industries.

Do our employees install iOS and Android apps from unknown sources? It is now easier to acquire iOS and Android apps from sources outside of official app stores, introducing new risks.

How many iOS and Android devices on our network have been jailbroken or rooted? An estimated 8% of iOS devices are jailbroken, while user tools like xCon render traditional jailbreak detection ineffective.

Are MDMs sufficient for securing enterprise data on mobile devices? MDM and container solutions can be an important part of a mobile security stack, but they do not protect against advanced mobile malware and compromised operating systems.

Are employees using their own mobile tools, putting sensitive data at risk? Employees expect a great user experience on mobile devices, and if mobile productivity and security solutions are not adopted, enterprise data is put at risk.

Can employees' mobile devices be compromised by man-in-the-middle attacks by connecting to Wi-Fi networks even if they use a mobile VPN? Attackers use a number of techniques to intercept network traffic to and from a mobile device, commonly called a man-in-the-middle attack. Since there's some time between when a user connects to a new Wi-Fi connection and the VPN is established, there is still a window of attack opportunity. Moreover, as an admin you would want to know if your users are connecting to these malicious networks, despite having a VPN installed.

[1] ©2016 Gartner, Inc., Market Guide for Mobile Threat Defense Solutions, John Girard, Dionisio Zumerle, 28 July 2016.

Are the mobile apps on our employees' devices a security threat?

To answer this question, you first need to understand the categories of app-based threats that exist today. We can broadly categorise them as:

Malicious apps Mobile apps that exploit a vulnerability to create a security risk for the device or data.

Risky apps Mobile apps that exhibit behaviour which may be benign in the right context, but may violate your organisation's security posture. For example, an app that sends contact data to foreign servers.

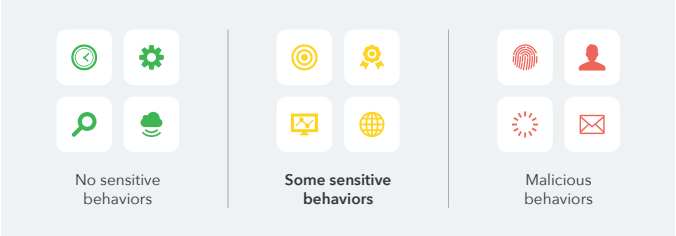
Malicious apps

Why would an attacker choose a mobile device as the attack surface into your organisation among the many options? The answer is nicely summarised in CSO's 2015 Mobile Security Survival Guide: "malware is getting better and attackers are targeting mobile more because that's where the data resides."[2]

We also know that mobile platforms are inherently application-centric; to access the data you need to open an app. Gartner notes that, similarly, "for attackers to get hold of files, they need to attack mobile apps, which makes it necessary to protect apps so that the enterprise data is protected." [3]

Gartner recommends you "abandon device-centric lockdown security models in favor of app-centric models." [4] Trial data-centric solutions, but be aware of the limitations in terms of maturity and scalability.

The spectrum of risky apps



As organisations increasingly embrace mobile devices in the workplace, mobile apps are the primary way that data is accessed and transmitted on these devices.[5] Organisations often allow employees to freely download mobile apps without having any visibility into what those apps are actually doing on the device. This is common practice for organisations looking to enable mobile productivity in the workplace, but with it comes new risks that are often not addressed.

In the image above, yellow represents risky apps, apps with behaviours that are not malicious in that they do not have malicious intent, but they may violate an organisation's security policy. For regulated industries, this is especially important because industry regulations and guidance may lead an organisation to restrict app behaviours that might put them out of compliance.

Focus on Visibility

A "risky app" is in the eye of the beholder, but at the very least you need visibility into the apps on your network and their capabilities. This enables you to make an informed decision about balancing the need to empower mobile productivity with the need to protect company data.

[2] CSO Online, "CSO's 2015 Mobile Security Survival Guide", George V. Hulme, January 2015

[3] Gartner, "How Digital Business Reshapes Mobile Security", Dionisio Zumerle, Nathan Hill, February 2015, Foundational, June 2016

[4] Gartner, "How Digital Business Reshapes Mobile Security", Dionisio Zumerle, Nathan Hill, February 2015, Foundational, June 2016

[5] Andreessen Horowitz, Mobile Is Eating the World (2016), Slide 55

Do our employees install iOS and Android apps from unknown sources?

In Gartner's recent report on mobile malware, they reveal one of the main sources for today's attacks are nonstandard application stores, "One common practice for malicious actors is to acquire 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."[6]

Apps downloaded outside official app marketplaces such as the Play Store and App Store are considered sideloaded apps and are inherently risky due to the simple fact that they bypass the review and controls present in official app marketplaces.

> "Sideloaded apps: Apps loaded onto the device via third-party app stores, webpages or email attachments."

Apple in particular has a great reputation for keeping the App Store free of malware, but there's an emerging threat vector for sideloaded apps on iOS that does not require jailbreak: apps that abuse enterprise provisioning profiles.

Companies increasingly build and distribute custom iOS apps directly to employee devices using enterprise provisioning profiles. Apple created them to enable corporate mobility and these provisioning profiles contain Apple-signed certificates that enable app distribution without Apple's app review.

While employees will see a security notice on their device the first time they download an enterprise-provisioned app from a new developer, employees today are conditioned to clicking the "trust" button as custom enterprise apps have become ubiquitous.

As a result, attackers that obtain valid, Apple-signed certificates can take advantage of this changing enterprise dynamic to target users with apps that were never vetted by Apple.

On Android, the barriers to installing sideloaded apps is much lower: Android users can easily enable sideloaded apps by changing their settings to allow the installation of apps from sources other than the Play Store.

Third-party app stores aren't the only source of potentially malicious, sideloaded apps. According to Gartner, "another source of malware is malicious websites that try to install mobile applications, profiles or certificates on the user's device."[7] It's as simple as clicking a link on a mobile browser, or in an email attachment.

Focus on Visibility

Fortunately, many of these sideloaded apps can be identified within your organisation by examining who signed the app certificates. If they were signed by an entity other than your own organisation, you may want to investigate further or block those apps entirely.

How an Attacker abuses Apple enterprise provisioning profiles:

Step 1 Attacker acquires enterprise certificate and signs app

Step 2 Attacker distributes app via email attachment or webpage

Step 3 Employee installs the app, which may exfiltrate sensitive data

[6] Gartner, "Comparing Approaches to Mobile Security Strategies," Patrick Hevesi, September 2016

[7] Gartner, "Comparing Approaches to Mobile Security Strategies," Patrick Hevesi, September 2016

How many iOS and Android devices on our network have been jailbroken or rooted?

It is generally well understood by security professionals that if a device's underlying operating system is compromised, then it's game over. Any software-based attempts to protect the data on the device can be rendered useless, including data containers and anti-malware solutions.

A couple of quick definitions:

iOS jailbreaking: The process of removing hardware restrictions on the operating system (breaking the device out of its "jail") by modifying iOS system kernels to allow file system read and write access.

Android rooting: Obtaining administrator or privileged access to the Android OS, enabling the user to alter, remove or replace the OS.

Why Jailbreak or Root?

Many users intentionally jailbreak or root their devices for non-malicious purposes. Common reasons include:

- Downloading apps from third party app sources
- Blocking advertisements or removing pre-installed "bloatware"
- Enhancing device functions, such as creating mobile hotspots without paying extra
- Unlocking the phone to use the device internationally
- Accessing pirated apps from app repositories

Should your organisation be concerned about this? As with any security decision, you need to weigh the risk of the threat against the cost of protecting against it. So to better understand the risk, you need to understand jailbreak/root prevalence in your organisation, as well as the technical risks it presents to sensitive company data.

Prevalence

Estimates on the prevalence of this behaviour vary by platform, but recent studies suggest around 8% of iOS devices are jailbroken[8], and upwards of 27% of Android devices.[9]

Technical Risks

- Some jailbreaking methods leave SSH enabled with a well-known default password (e.g. alpine) that attackers can use for Command & Control.
- The entire file system of a jailbroken/rooted device is vulnerable to a malicious user inserting or extracting files. This vulnerability is exploited by many malware programs, including the recent Xsser mRAT trojan.
- Credentials to sensitive applications, such as banking or corporate applications, can be stolen using key logging, sniffing or other malicious software.

> Estimates suggest upwards of 8% of global iOS devices are jailbroken

Focus on Visibility

Protection against this emerging threat starts by knowing what's on your network. Yet jailbroken and rooted devices can be difficult to detect. While MDM solutions may offer basic jailbreak detection, they are constantly battling against users who try to evade this detection. In the next section, we'll discuss this further.

[8] Daily Tech, "WireLurker Malware May Have Infected 100,000+ iPhones, No Jailbreak Required", Jason Mick, November 2014

[9] Know Your Mobile, "How To Root Your Android Phone", Richard Goodwin, February 2015

Are Enterprise Mobility Management solutions sufficient for securing enterprise data on mobile devices?

Modern IT professionals recognise the need for a layered approach to mobile security, and Enterprise Mobility Management (EMM) and Mobile Device Management (MDM) solutions can be an important component of a progressive enterprise mobile strategy.

As the author of the CSO's 2015 Mobile Security Survival Guide notes, MDM solutions are currently an important part of the mobile defence toolkit. However, he goes on to say "most CISOs, CIOs and security analysts I've spoken to conclude that MDM isn't an adequate mobile security answer."[10]

Critical Gaps

EMM solutions have some critical gaps in protecting mobile endpoints. As Gartner states in the research report, When and How to Go Beyond EMM to Ensure Secure Enterprise Mobility, "EMM solutions have limitations in that they are unable to detect platform and app vulnerabilities. They are also limited in their capacity to detect malware threats on their own. Mobile threat defence (MTD) tools help to fill this void by protecting enterprises from threats on mobile platforms." [11]

Specific gaps include:

Jailbreak/Root Detection As we discussed in the last section, if a device has been jailbroken or rooted then your existing security investments can be rendered ineffective. While most MDM/EMM solutions claim to provide jailbreak/root detection, they are not always effective due to the nature of the attack targeting the kernel of the OS.

Advanced malware detection As discussed earlier, malware is getting better and attackers are targeting mobile more because that's where the data resides[12]. As malware evolves, you can't rely on basic app reputation solutions to protect against modern mobile malware. Containers provide basic separation of personal and corporate data, but do not prevent malicious applications from getting on the device in the first place.

Focus on Visibility

For many organisations, MDMs and containers are important layers in their mobile security stack. However, many CISOs recognise the gaps that need to be filled so the organisation can have visibility into advanced mobile malware and jailbroken/rooted devices.

Risk	MDM Protection
Lost device	Locates & remotely wipes lost
App distribution	Secure distribution of enterprise apps
Policy violations	Manual blacklisting of apps determined to violate company policy
Data leakage	Containerises enterprise data such as emails or content, which remains vulnerable to compromise from sophisticated attacks
Jailbreaking and rooting	Not always effective due to the nature of the attack targeting the kernel of the OS
Malicious apps	None

Protected No Limited

[10] CSO Online, "CSO's 2015 Mobile Security Survival Guide", George V. Hulme, January 2015

[11] Gartner, "When and How to Go Beyond EMM to Ensure Secure Enterprise Mobility", Manjunath Bhat, Dionisio Zumerle, June 2016.

[12] CSO Online, "CSO's 2015 Mobile Security Survival Guide", George V. Hulme, January 2015

Are employees using their own mobile tools, putting sensitive data at risk?

As many IT professionals are well-aware, enterprise cloud solutions have enabled employees to adopt their own work productivity tools. This is often done when the IT-provided solutions are too hard to use or too obtrusive on user privacy. Yet the need to provide this consumer-friendly experience on mobile devices is especially important for securing enterprise data and preventing "Shadow IT".

This is because users have come to expect a great experience on mobile devices. As Gartner notes in a February 2015 report, "[mobile] solutions with a suboptimal user experience lead to users adopting privately owned devices and sometimes privately managed apps to work with enterprise data. This second practice is directly responsible for enterprise leaks." [13]

As you look to securely enable your organisation's mobile productivity, it is especially important that you also select mobile security solutions that meet the high standards of today's mobile consumer. If user experience suffers, the user is quick to jump to other technologies or options that meet his or her needs.

More than just good design

User acceptance of mobile security technologies goes beyond just a user-friendly experience. Data privacy is top of mind for today's knowledge workers, and security solutions that are perceived to be too aggressive with accessing user data are often rejected. This is especially true in a BYOD environment.

Focus on Visibility

Modern organisations recognise that user experience is especially critical for driving employee acceptance of mobile IT solutions. But visibility into employee adoption of these solutions starts by selecting mobile-first solutions. As Gartner recommends, "focus your efforts on providing solutions that are tailored for mobile use and, therefore, obviate shadow IT practices, rather than forcing legacy toolsets to deliver functionality on mobile platforms that they were never designed for." [14]

It Starts With Visibility

As mobile devices are increasingly becoming the primary way that corporate data is accessed, progressive security professionals are recognising the need to be able to answer these six questions. With this in mind, Craig Shumard, who spent 11 years as the CISO of a Fortune 500 company, discusses how "mobile is an issue, we can't ignore it, and enterprises need visibility and control now" into those endpoints.

Here's another way to think about it. If your local bank only invested in securing the main doors, it might protect against the robbers that use predictable entry points. But what if access to the bank vault was becoming easier via air ducts and pipes? At the very least you'd want that bank to install surveillance cameras to keep an eye on those attack points.

Similarly, the modern workforce requires modern security solutions to protect against this new way of accessing company data. As Craig concludes, "[mobile] security is not an 'if' game, it's a 'when' game. An enterprise's visibility into their mobile stack will only strengthen their security suit of armor. Without insight into mobile there can be no effective action when the attack comes."

[13] Gartner, "How Digital Business Reshapes Mobile Security", Dionisio Zumerle, Nathan Hill, February 2015, Foundational, June 2016

[14] Gartner, "How Digital Business Reshapes Mobile Security", Dionisio Zumerle, Nathan Hill, February 2015, Foundational, June 2016

Can employees' mobile devices be compromised by man-in-the-middle attacks by connecting to Wi-Fi networks even if they use a mobile VPN?

In general terms what has become known as a man-in-the-middle attack is executed by a person or computer who sits on a network connection and eavesdrops on the information being transferred. They may collect this information and may also be able to decrypt it, despite strong encryption used by many companies, such as email providers. On mobile devices, these attacks aim to get in the middle of data transferred over cellular and Wi-Fi networks, and use exploits to view encrypted information.

Man-in-the-middle attacks can take place in several different ways and typically require two steps. The first step is to get into the network traffic. If an attacker is physically nearby a target device, they can establish a fake Wi-Fi or cellular network to gain access to network traffic. Another tactic used is Address Resolution Protocol (ARP) spoofing to advertise their own hardware address in place of a gateway.

If not nearby, an attacker can use either malware or social engineering to convince an end-user to configure their device to route all network traffic through a malicious proxy or VPN connection.

After getting into the network path, the attacker then has to manipulate the connection or user to view encrypted data. Here are a couple of ways this can happen:

1. Host Certificate Hijacking – An attacker introduces a malicious certificate authority under attacker control into the trusted root certificate authority store of the victim device, allowing the attacker to masquerade as a trusted host that can view encrypted data.

2. SSL Strip – An attacker effectively strips out the "S" in HTTPS connections, allowing normally encrypted data to be viewed in plaintext.

3. TLS Protocol Downgrade – An attacker manipulates the negotiated connection to downgrade the protocol or cipher suites and lower the security guarantees of the connection.

Lookout Mobile Threat Protection has man-in-the-middle detection that identifies these activities as signals of network activity, but focuses alerts on attacks that attempt to decrypt sensitive enterprise data. This is because enterprise data is almost always encrypted, so simply getting in the middle of traffic is not likely to result in data theft. The result is a reduction in false positives for admins by filtering out many of the legitimate reasons that a third party would get in the middle of network traffic, such as an airport Wi-Fi portal.

How might my employees or end-users encounter a man-in-the-middle attack?

Man-in-the-middle attacks on enterprise devices are more likely to come via Wi-Fi networks. The attacker may trick a victim to connect to a Wi-Fi network that has been spoofed, or made to look like a legitimate hotel, airport, or corporate Wi-Fi network.

A spoofed hotel Wi-Fi network is a another approach to man-in-the-middle attacks. Many hotels use an interstitial landing page that requires things like a room number and accepting the hotel's terms and condition in order to access the Wi-Fi. The page is usually branded with the hotel's name and looks trustworthy.

This little set-up process makes it easier for an attacker to trick an unsuspecting hotel guest into connecting to a spoofed network and entering their credentials. Since mobile devices have a different web experience from PCs, some individuals may not realise when potentially unnecessary instructions are being thrown in. For example, an attacker may create a network to look exactly like the hotel network – same name and all – but then ask the victim to install a configuration profile that contains a malicious certificate. From there the attacker not only has access to all the data being transferred over the network, but they can also decrypt the traffic and see everything that was once protected. This could include emails, information flowing to and from apps, text messages, or more.

What is an example of a man-in-the-middle attack?

On 60 Minutes, Lookout co-founder John Hering shows what one of these attacks could do. He set up the same attack we describe above and easily convinced one of the CBS News producers, who had no knowledge of the rogue Wi-Fi connection at the time, to connect. Not long after, John was able to access the reporter's email history, phone history and payment information.

Lookout Mobile Endpoint Security

Lookout Mobile Endpoint Security is a mobile security solution that mitigates the risks of unprotected data accessed via mobile devices, provides visibility into mobile threats across apps, devices and the network, seamlessly integrates with and enhances existing mobile investments while minimising help desk tickets and being embraced by employees because of a mobile-optimised design.

Unlike PC/web era providers that don't account for the new requirements introduced by the mobile/app era, our solution has amassed a global sensor network of over 100 million sensors thanks to the success of our consumer product. This network enables our platform to be predictive by letting machine intelligence identify complex patterns that indicate risk, patterns that would otherwise escape human analysts. No other vendor provides an enterprise security solution that ensures strong employee adoption across corporate and personally owned mobile devices.

Lookout Mobile Endpoint Security secures your enterprise from mobile threats, and risky non-compliant mobile apps that pose a data leakage risk. With a seamless integration to your EMM solution, Lookout empowers your organisation to adopt secure mobility across personal and corporate owned devices without compromising productivity.

To learn more about these mobile security risks and how Lookout can help address them: https://www.lookout.com/products/mobile-endpoint-security or contact us at sales@lookout.com