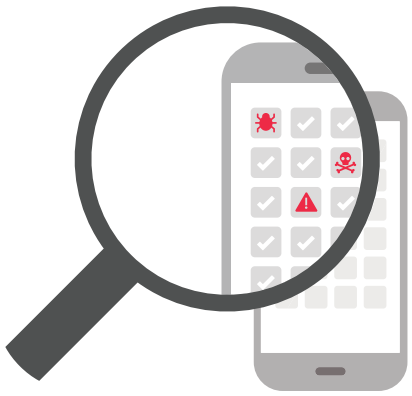
Lookout

Whitepaper

Mobile Security

The 5 Questions Modern Organizations Are Asking



Executive Summary

The modern organization has recognized the need to embrace mobile devices in the workplace. Some have fully implemented a bring-your-own-device (BYOD) program, while some have adopted a hybrid model of corporate-owned and employee-owned devices. Meanwhile, others are now just starting to consider these mobility programs.

Wherever you fall on this spectrum of mobility adoption, the global trend is moving towards BYOD to benefit from enhanced worker productivity, increased revenues, and reduced device and data expenses. In fact, more than 45% of global firms are now introducing or expanding BYOD programs, according to recent survey from Forrester Research.[1]

However, the increase in mobile devices bring with them important security implications. As the CSO's 2015 Mobile Security Survival Guide notes, mobile security risks are growing "because much enterprise data today is created and consumed on mobile devices. This clearly explains why mobile security persistently tops the list of most pressing enterprise security concerns."[2]

Whether you've already embraced enterprise mobility or are just starting to consider it, today's organizations are concerned about the lack of visibility into these five 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

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

[1] Forrester Research, "Building The Business Case For A Bring-Your-Own-Device (BYOD) Program", Michele Pelino, December 2014

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

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 categorize 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 behavior which may be benign in the right context, but may violate your organization's security posture. For example, an app that sends contact data to foreign servers.

Malicious apps

Recently, NSA Director Adm. Michael Rogers warned of increasing cyberattacks on mobile devices as "a coming trend"[3]. But why would an attacker choose a mobile device as the attack surface into your organization among the many options? The answer is nicely summarized 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."[4]

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."[5]

It's for this reason that Gartner recommends you abandon device-centric lockdown security models in favor of app-centric models. Trial data-centric solutions, but be aware of the limitations in terms of maturity and scalability.[5]

Risky apps

At first glance, it might be tempting to consider any app that accesses your employees' contact data to be risky, but would you consider the LinkedIn app risky because it requires access to contacts? Maybe not, but what about the aggressive piece of adware that lives on your CEO's device, which sends contact and browser history data to an unknown server in Russia?

> "Malware is getting better and attackers are targeting mobile more because that's where the data resides."

While some might classify these apps as just "annoying", Craig Shumard, former CISO at Cigna, notes how "if you're an enterprise that supports BYOD, this kind of 'annoying threat' should sound alarms." He goes on to note that "the fact that contacts and personally identifiable information is taken puts your employees and your proprietary secrets, your competitive edge, at risk."

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.

[3] Wall Street Journal, "NSA Director Warns of 'Dramatic' Cyberattack in Next Decade", Siobhan Gorman, November 2014

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

[5] Gartner, "How Digital Business Reshapes Mobile Security", Dionisio Zumerle, Nathan Hill, February 2015

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.[6]

Apps downloaded outside official app marketplaces like 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 apps stores aren't the only source of potentially malicious, sideloaded apps. According to Gartner, another source of malware comes from malicious websites that try to install mobile applications, profiles or certificates on the user's device.[6] It's as simple as clicking a link on a mobile browser, or in an email attachment.

Focus on Visibility

Fortunately, many of these these sideloaded apps can be identified within your organization by examining who signed the app certificates. If they were signed by an entity other than your own organization, 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, "Protecting Mobile Devices Against Malware and Potentially Unwanted Applications", Patrick Hevesi, Mario de Boer, March 2015

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 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 organization 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 organization, as well as the technical risks it presents to sensitive company data.

Prevalence

Estimates on the prevalence of this behavior vary by platform, but recent studies suggest around 8% of iOS devices are jailbroken[7], and upwards of 27% of Android devices.[8]

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.

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

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

Are MDM's sufficient for securing enterprise data on mobile devices?

Modern IT professionals recognize the need for a layered approach to mobile security, and that message has been echoed by leading mobile security analysts such as Forrester Research[9]. In this respect, 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 defense 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

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. As Gartner notes, most MDM/EMM solutions claim to provide jailbreak/root detection, but are not always effective due to the nature of the attack targeting the kernel of the OS.[11]

Advanced malware detection As discussed earlier, malware is getting better and attackers are targeting mobile more because that's where the data resides[10]. 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 organizations, MDMs and containers are important layers in their mobile security stack. However, many CISOs recognize the gaps that need to be filled so the organization can have visibility into advanced mobile malware and jailbroken/rooted devices.

> "Most CISOs I've spoken to conclude that MDM isn't an adequate mobile security answer."

Risks	MDM Protection
Lost device	✔ Locates & remotely wipes lost device
App distribution	✔ Secure distribution of enterprise apps
Policy violations	⚠ Manual blacklisting of apps determined to violate company policy
Data leakage	⚠ Containerizes 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	X None

X No Protection ⚠ Limited Protection ✔ Protected

[9] Forrester Research, "TechRadar™: Enterprise Mobile Security, Q4 2014", Tyler Shields, November 2014

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

[11] Gartner, "How Digital Business Reshapes Mobile Security", Dionisio Zumerle, Nathan Hill, February 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 recent 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."** [12]

> "The most important product attribute in the mobile security market is user experience"

As you look to securely enable your organization's mobile productivity, it is especially important that you also select mobile security solutions that meet the high standards of today's mobile consumer. Forrester Research highlights this in their recent TechRadar report for Enterprise Mobile Security, discussing how "the most important product attribute in the mobile security market is user experience". If user experience suffers, the user is quick to jump to other technologies or options that meet his or her needs.[13]

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. Gartner emphasizes this in their recent Cool Vendors in Security Infrastructure Protection report, recommending that "CISOs and other security decision makers should defend against mobile app threats in the enterprise without encroaching on user data."[14]

Focus on Visibility

Modern organizations recognize 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."[12]

[12] Gartner, "How Digital Business Reshapes Mobile Security", Dionisio Zumerle, Nathan Hill, February 2015

[13] Forrester Research, "TechRadar™: Enterprise Mobile Security, Q4 2014", Tyler Shields, November 2014

[14] Gartner, "Cool Vendors in Security Infrastructure Protection, 2015", Ray Wagner, Joseph Feiman, Avivah Litan, Neil MacDonald, Lawrence Orans, Peter Firstbrook, John Girard, Dionisio Zumerle, April 2015

It Starts With Visibility

As mobile devices are increasingly becoming the primary way that corporate data is accessed, progressive security professionals are recognizing the need to be able to answer these five 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."

Lookout Mobile Threat Protection

Lookout Mobile Threat Protection is a security solution for your mobile workforce, providing visibility into evolving mobile threats so you can protect your sensitive data. Organizations use Lookout to:

- Detect and remediate mobile threats such as surveillanceware, trojans, or data leakers
- View and approve iOS and Android apps that were installed outside of official app stores
- Identify devices that have been rooted or jailbroken, even if they bypass MDM detection
- Connect with leading MDM solutions for simple device provisioning and quarantine
- Deploy a beautiful endpoint app that protects user privacy while securing corporate data

To learn more about these mobile security risks and how Lookout can help address them:

[Visit lookout.com/mobile-threat-protection](lookout.com/mobile-threat-protection)

Or contact us at sales@lookout.com