THE PRACTICAL GUIDE TO

ENTERPRISE MOBILE SECURITY

What it is, why it matters, and how to implement it in your organization

Lookout

Why you should read this guide

Enterprise mobility started with the Blackberry, a revolutionary messaging device that solved security concerns by giving IT managers the ability to set many restrictions on its functionality. In the following years, employees started using fully-functional, internet-capable smartphones in their personal lives and demanded the same capabilities at work.

With the growth of iOS, Android, and Windows Phone devices, organizations were forced either to allow employees to be productive while assuming an unacceptable level of risk or to satisfy their security needs while restricting productivity.

Today, neither restricting productivity nor accepting tremendous mobile security risk is a viable option. Business processes have migrated to mobile and the level of sensitive data accessible to these devices and increasing sophistication of attackers has made mobile threats a "must-solve" enterprise security risk.

The Practical Guide to Enterprise Mobile Security was created to help IT managers fulfill their dual role of *both* enabling productivity *and* reducing risk through the adoption of modern-enterprise mobile security practices. This guide will help answer questions you might have about implementing mobile security, identify the components that make up a holistic enterprise mobile security strategy, point out key considerations that lead to successful deployments, and provide tips on how to successfully drive adoption of that solution in your global workforce.

I hope this guide will assist you in moving your organization towards the new mobile-first world, securely.

Kevin Mahaffey
Lookout co-founder and chief technology officer

Contents

5 Part 1: What is Mobile Security

14 Part 2: Why Mobile Security Should Be in Your Top Three Priorities

24 Part 3: Six Mobile Security Capabilities You Need

39 Part 4: The Business Case for Mobile Security

58 Part 5: Buying Mobile Security

70 Part 6: Lookout Mobile Endpoint Security

74 Part 7: The Future of Mobile Security

Icons used in this book

Throughout this book, you'll find special call-outs to direct your attention to important information. Here's a key that explains what the icons mean:

The data that you'll see throughout this book is the result of a survey commissioned by Lookout and conducted by Enterprise Strategy Group, an integrated IT research, analyst, strategy, and validation firm.
The survey methodology includes:

- 150 completed online surveys with IT and security practitioners directly involved in the planning, implementation, and/or operations of their organization's mobile endpoint security and threat detection policies, processes, and/or technical safeguards
- Enterprise organizations (2,500 or more employees) in United States and enterprise organizations (1,000 or more employees) in United Kingdom
- Multiple industry verticals including financial, business services, manufacturing, and retail

Ways to learn more:

This icon means you can access another document on the topic.

This icon means you can watch an on-demand webinar on the topic.

This icon means there is a post on the Lookout blog covering the topic.

This icon will link you to more information in another part of this book.

This icon means definitions for technical terms are below.

Craig Shumard, CISO emeritus

As Cigna Corporation's former Chief Information Security Officer, Craig developed and oversaw the implementation of a 21st century, corporate-wide strategy to safeguard information involving more than 65 million Cigna customers. He is currently a trusted advisor on a number of boards for prominent security companies.

Serge Beaulieu, Former Director of IT Security

Serge is a seasoned information security consultant whose experience includes being Director of Technical Security Strategy at Cigna Corporation. Serge is a Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM).

PART ONE

WHAT IS ENTERPRISE MOBILE SECURITY?

PART 1

What is enterprise mobile security?

A frame of reference

Five years ago, most IT and security professionals overlooked mobile devices, thinking that the biggest security challenges were on PCs, where employees did the majority of their work.

Then came enterprise apps.

Box launched its mobile app in 2012. The Salesforce1 app came out in 2013. Employees started using Evernote and other consumer apps for work.

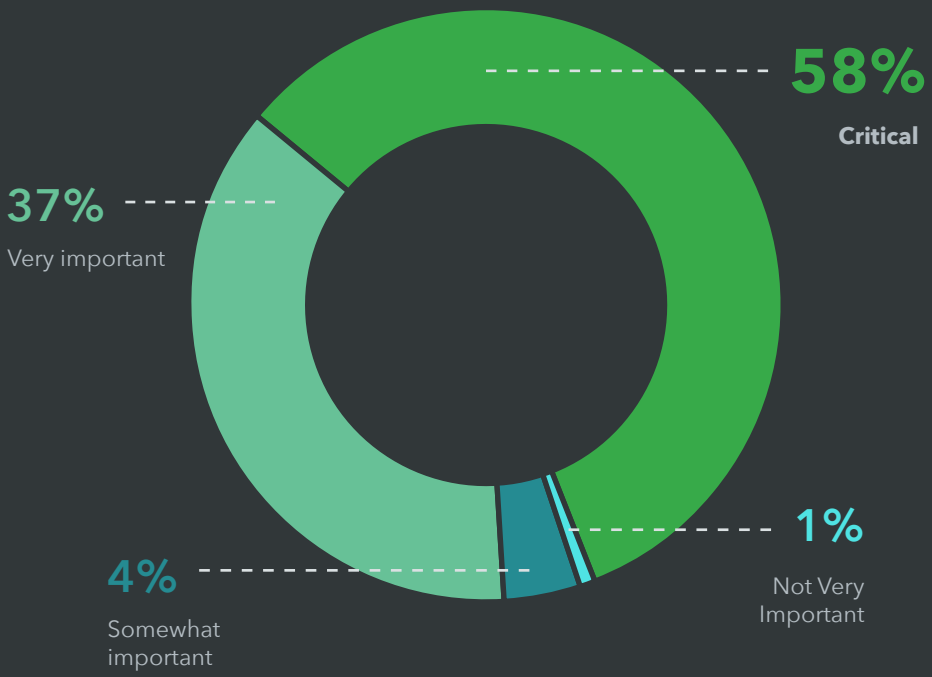
Now, the vast majority of employees rely on mobile apps to be productive, forcing IT departments to rethink device security priorities to include mobile.

THE DATA

Mobile devices are critical productivity tools

The Question: How important would you say the use of mobile devices (i.e., smartphones, tablets) are for employees at your organization in terms of their ability to maximize efficiency and productivity?

The Results:



PART 1

This new, heavy emphasis on mobile devices as a work tool has created a gap between mobile security and Enterprise Mobility Management/ Mobile Device Management (EMM/ MDM) platforms, which enterprises have fallen back on to secure phones and tablets.

EMM/MDM solutions provide great management capabilities, but do not secure mobile endpoints.

To address this gap, a new category of mobile security has emerged that is focused on delivering endpoint security for iOS and Android smartphones and tablets.

Despite the importance of enterprise mobile security, the term has remained ambiguous until now. This is because the technology media – and even security professionals – define "enterprise mobile security" in different ways, often failing to distinguish between the "security" and "management" of mobile devices.

So, what is mobile security?

READ THE BLOG

> **"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 defense (MTD) tools help to fill this void by protecting enterprises from threats on mobile platforms."**

MANJUNATH BHAT AND DIONISIO ZUMERLE, JUNE 2016
"WHEN AND HOW TO GO BEYOND EMM TO ENSURE SECURE ENTERPRISE MOBILITY"

PART 1

Mobile security defined

This guide is focused on mobile security specifically, and its role in securing mobility.

Mobile security is an umbrella term that covers a range of technologies that protect different pieces of the mobile ecosystem from threats. Analysts have several names and categories for mobile security. Gartner uses mobile threat defense, mobile malware protection, app reputation services, and mobile platform health checks. Forrester uses mobile antimalware, mobile device reputation services, and mobile endpoint security; and others just refer to it under the blanket name "enterprise mobile security."

Throughout this eBook, we will call this category "mobile security," because it is an appropriately broad term that encompasses the most relevant technologies for evading latent and targeted attacks.

THE EXPERT

"The biggest priority is being able to understand what the threats are. Mobile, for whatever reason, hasn't had the same focus around threats and threat intelligence as some of the others aspects of security have."

Craig Shumard
CISO EMERITUS

PART 1

The difference between mobile security and securing mobility

You may have heard the terms "mobile security" and "securing mobility" used in a number of different contexts, but they don't actually mean the same thing.

Securing mobility is the umbrella for making sure that company- and employee-data remain safe while being used on mobile devices. There are three elements to securing mobility that every company needs to consider.

Device management

These are technologies, such as Microsoft Intune, VMWare Airwatch, or MobileIron, that allow IT departments to award and revoke access to employee devices, remotely wipe data from the device, and other capabilities.

Identity management

These are technologies like Microsoft Azure Active Directory and Ping Identity that allow IT departments to know who is connecting to their corporate networks and accessing data, and from what devices.

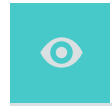
Mobile security

This references technologies and programs that are intended to keep a device and data accessed or stored by that device safe from attacks and threats. This could include malware attacks, risky apps, vulnerabilities, and network attacks.

A note about mobile containers: *Mobile containers protect enterprises from employees mingling work data with their personal data. However, if the device that a container is running on becomes compromised (jailbroken or rooted, for example), container technology fails. For this reason, they aren't a necessary element for securing mobile devices.*

PART 1

Why mobile security is so important:



WATCH WEBINAR HERE

Learn more about the native mobile security features of mobile devices.
"Native Security Measures on iOS and Android: A Security Practitioner's Guide"

Mobile devices have built-in protections, known as "native security," meant to keep the device and data safe. These include application sandboxing, which prevents apps from accessing data between each other on the device; and code-signing, where developers digitally sign their apps and those signatures are used to grant privileges. Apple, in particular, has a remarkable record of preventing malware from entering the App Store, and making it more difficult to jailbreak iPhones.

These native protections are not enough, however, to keep devices or the data on them safe. Malicious actors have developed ways to get around these measures.

This is where mobile security becomes critical to the success of your company's overall security program. Mobile security provides threat detection, analysis, and remediation to protect sensitive company data on mobile devices and the networks to which they connect. It also protects against:

- Network attacks, such as man-in-the-middle attacks
- Malicious apps
- Non-compliant apps, such as apps that may not be inherently malicious, but handle data in a way that is not compliant with enterprise internal- or regulatory-policies
- Vulnerabilities in apps and device operating systems
- Compromised (i.e., rooted, jailbroken) device operating systems

Mobile security matters more than ever because more employees are accessing corporate data via mobile devices everyday, and attackers know there are a number of ways into unprotected mobile devices.

PART 1

According to a report from The Ponemon Institute, 67% of IT and security pros say that their organization has likely already been breached through mobile. Aside from malware attacks, jailbroken devices, sideloaded applications (i.e., applications that are downloaded to the device from a third-party marketplace), and apps that leak data (without being malicious) all make the list.

Mobile security solutions look for signatures and behaviors indicative of:

App-based threats:

Mobile malware – This malicious code is written to access, manipulate, and/or delete sensitive company data on mobile devices. To use a crime metaphor, signatures are akin to digital fingerprints, a distinct set of characters or

THE EXPERT

"When you speak about threats, it's about visibility into the malware, it's visibility into bad applications, and knowing where your data is. It's about protecting your enterprise information, but it's also about respecting and protecting your end-user's private information."

Serge Beaulieu

FORMER DIRECTOR OF IT SECURITY

numbers that, theoretically, identify a developer. In contrast, behaviors are like a modus operandi, which describes the particular manner in which malware operates on mobile devices.

What mobile security can do: Alert admins to the presence of malware, provide educational information about the threat, and a remediation recommendation.

Non-compliant/"risky" apps – There is a wide array of apps that exhibit behavior which may be benign in the right context, but may violate your organization's security compliance requirements (e.g., an app that sends contact data to foreign servers). Apps in this category are not necessarily malicious, but employees who download them may not fully understand how these apps access sensitive company data on their device or on the networks to which their devices connect.

What mobile security can do: Allow admins to determine sensitive data-types and alert admins to the presence of apps that may access this data.

Device-based threats:

Device-based exploitation techniques – Rooting (Android)/jailbreaking (iOS) changes default security or system settings, further opening devices up to attack. Devices in this state do not receive regular patches from carriers and manufacturers and are highly susceptible to running vulnerable software on enterprise networks. Rooting and jailbreaking may occur because of user action to increase the functionality of their device or may be part of a multi-stage malware attack on Android. The six most prevalent families of malware globally are all types of auto-rooting malware[1] that combine adware with exploits that root the device. A Fortune 500 company that recently deployed enterprise mobile security detected a rooted device that was not found by their EMM.

Want more details on app-, device-, and network-based threats, including why they matter to your company?
Go to Part 4: The business case for mobile security

[1] Native Security Measures on iOS and Android, Lookout Webinar, May 2016

What mobile security can do: Investigate the mobile operating system to determine if it has been rooted (Android) or jailbroken (iOS) and provide a warning to admins if a device enters one of these altered states.

Combination app- & device-based threats:

Vulnerabilities – Vulnerabilities can manifest in a number of different ways that impact your organization. Vulnerability detection can look at your in-house developed mobile applications to ensure they are hardened. It can also look for vulnerabilities in apps existing on the same mobile device that is accessing your corporate data, or running an app made by your organization (e.g., employee-facing apps and customer-facing apps). It can also look for vulnerabilities within the mobile operating systems themselves.

What mobile security can do: Detect and alert on software flaws that attackers can exploit to access data and sensitive corporate systems; set policy to define minimum patch levels devices must have.

Network-based threats:

Network-based exploitation techniques – One of the most well-known network attacks is a "man-in-the-middle" attack. A mobile device can be technically tricked to send its data through a fake cellular tower or Wi-Fi router controlled by an adversary. If that data is unencrypted, it can be easily captured and read by the adversary who now "sits" between the mobile device and the broader internet. Even if the mobile device is sending and

DEFINING TERMS

Network-based attacks:

Certificate hijacking: An attacker tricks a victim into accepting a malicious certificate authority, introducing it to the device's root certificate authority store, allowing the attacker to masquerade as a trusted host and view encrypted data.

sslstrip: An attacker rewrites content intercepted through a man-in-the-middle attack, removing HTTPS links, so that they can receive content in plaintext.

TLS Protocol Downgrade: An attacker manipulates a connection in order to push the connection to a lower standard of communication security (i.e., from TLS 1.2 to SSL 3.0)

receiving encrypted sensitive company data, the adversary can use one of several techniques (such as fake root CAs, "sslstrip," and TLS protocol downgrade to trick the mobile device into sending its data without encryption or to weaken the encryption so that the adversary can decrypt it.[2]

What mobile security can do: Detect and stop network attacks in real time.

Mobile security is essential

Mobile security safeguards sensitive company data that even security-minded employees may put at risk, not because they are careless or irresponsible (though that can happen), but simply because they are fallible and doing important, time-sensitive work that does not and should not require them to think constantly about security.

Work increasingly gets done on mobile devices both inside and outside of traditional offices. From a business perspective, mobile-enabled businesses are more adaptive and productive. Like all benefits, however, these come with costs.

> **"Mobility is the single most critical tool to support the top strategic business imperatives. In his role as business enabler, the CIO must deliver high-quality mobile solutions to his organization or risk being replaced."**
>
> FORRESTER®
>
> **DAN BIELER**
> MOBILE BECOMES A KEY SUCCESS IMPERATIVE FOR CIOS, NOVEMBER 2015

[2] See https://blog.lookout.com/blog/2015/10/19/public-wi-fi-csam/ (accessed 5/3/16) and need additional citations.

64% of IT security leaders say it is **very likely that sensitive corporate data is present** on their employees' mobile devices.

ESG

Gone are the days when it was possible to clearly distinguish personal from professional mobile devices.

To continue to get the benefits of these mobile devices as productivity tools, businesses need to move beyond management, and into strong mobile security, so that thousands of mobile devices do not become the weakest link in the corporate security chain.[3]

Why Enterprise Mobility Management / Mobile Device Management is not enough

To recap, EMM/MDM are built primarily as management tools, meant to help IT departments keep track of devices. These tools manage devices and content, and may have some identity access management capabilities, but without mobile security, employees' mobile devices remain low-hanging fruit to attackers.

Using EMM/MDM alone to secure mobile devices leaves a significant gap in your overall security architecture, sometimes negating the large budget put toward securing other areas of the business.

EMM/MDM solutions act as baseline mobile protection – important for curbing crimes of opportunity such as accessing sensitive company data on an unlocked smartphone, but are inadequate for detecting, analyzing, and responding to mobile attacks.

[3] "21% of companies have no plans to implement mobile security." See Webroot's "Survey: Mobile Threats are Real and Costly," 2012

This is because EMM/MDM platforms manage which devices can connect to a business network, what those devices can do when they are on those networks, what settings those devices must have, and what protocols to follow when those devices are lost or stolen. In other words, EMM/MDM platforms are for authentication, permissions, and configuration – not security.

64% of respondents believe **EMM solutions** provide inadequate or limited protection when it comes to **securing data on devices** and they should not be the only protection used.

THE TOP 6 TASKS MOBILE SECURITY ACCOMPLISHES

Enterprises know that "good enough" isn't good enough anymore. EMM/MDM is an important part of managing the devices connecting to your network, but mobile security must be there to cover the threats EMM/MDM do not.

To summarize, here are the top six tasks mobile security should accomplish in order to protect your enterprise data:

1. Detection & remediation of mobile malware
2. Detection & remediation of compromised operating systems
3. Detection & remediation of sideloaded apps
4. Detection & remediation of network-based "man-in-the-middle" attacks
5. Detection & remediation of non-compliant/"risky" apps
6. Ease and depth of integration with your Enterprise Mobility Management (EMM) and Mobile Device Management (MDM) platforms

PART **TWO**

WHY MOBILE SECURITY SHOULD BE IN YOUR TOP THREE PRIORITIES

PART 2

Why mobile security should be in your top three priorities

Mobile devices in the workplace have grown significantly in a very short period of time, and so have the security risks.

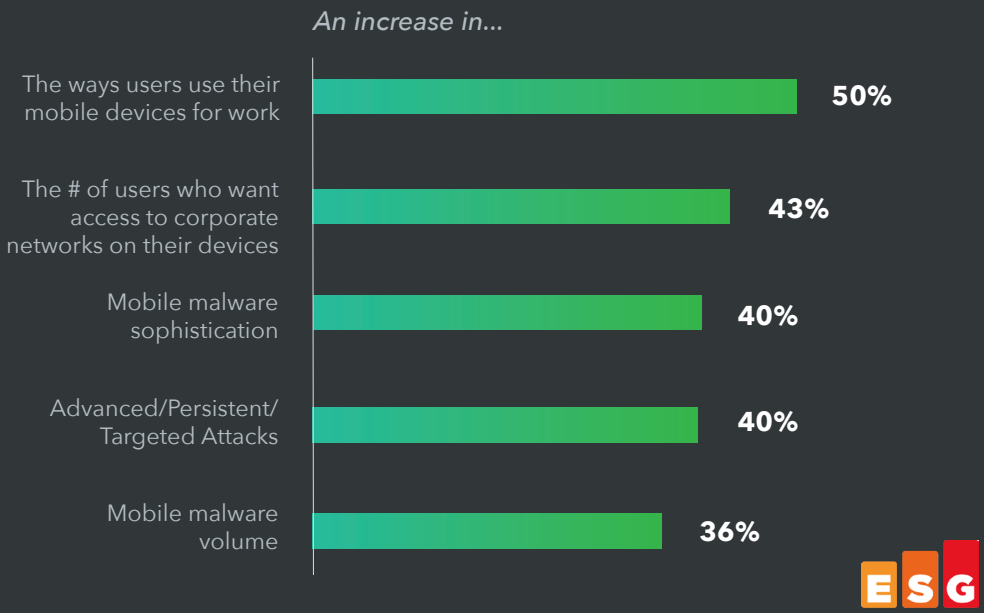
Here's why mobile security is now on the shortlist of priority projects for many technology executives and business leaders: their employees are increasingly working on mobile devices that have access to the enterprise network, corporate email, the device's sensors (e.g., GPS, microphone, camera), and store credentials for all of the above. This "treasure trove" of confidential data has now led malicious actors to turn their attention to mobile platforms, resulting in a significant increase in the sophistication of mobile threats.

Let's level set: companies face many risks. This means security vendors are constantly competing to elevate certain risks to the top of the executive priority list. Not every potential risk can be on top, but sometimes circumstances shift, highlighting risks that need attention now.

THE DATA

Mobile security enables productivity

Respondents (N=129) who indicated that securing mobile devices has become more important over the last two years say the following factors are driving this importance:



This is the case with mobile devices and security today.

The fact is that security risks posed by workplace mobile devices have grown significantly in a very short period of time. Two fast-moving trends, that reinforce each other, are making mobile security necessary now:

1. Employee demand for mobile productivity tools
2. Increasing mobile threats targeting devices with valuable corporate data

PART 2

The reality today is that employees' desire to use mobile devices for work is outpacing their companies' ability to manage and secure them.

The data indicates that companies will continue to move towards mobile productivity, and one of the biggest drivers of this trend is the increasing adoption of cloud-based productivity applications.

Executives and employees are generally in agreement about the benefits of mobile devices in the workplace:

- Increased employee productivity
- Increased employee satisfaction
- Increased access to mobile applications
- Reducing costs[1]

THE EXPERT

"The importance of mobile security has gone from zero to 100. The number of people using their phones at work is increasing the 'quality' of the data on mobile devices, data bad guys want to access. It's skyrocketed over the last couple years, making the value of the device, and the data on that device, critically important to protect."

Craig Shumard
CISO EMERITUS

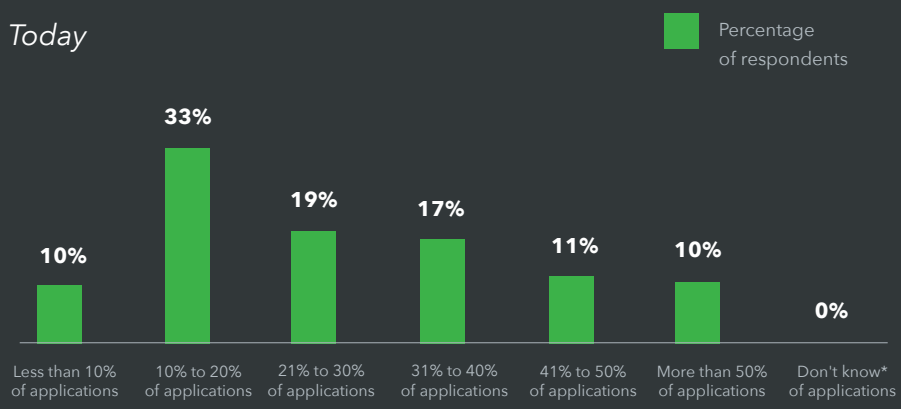
[1] "Comprehensive BYOD Implementation Increases Productivity, Decreases Costs," Cisco, 2013

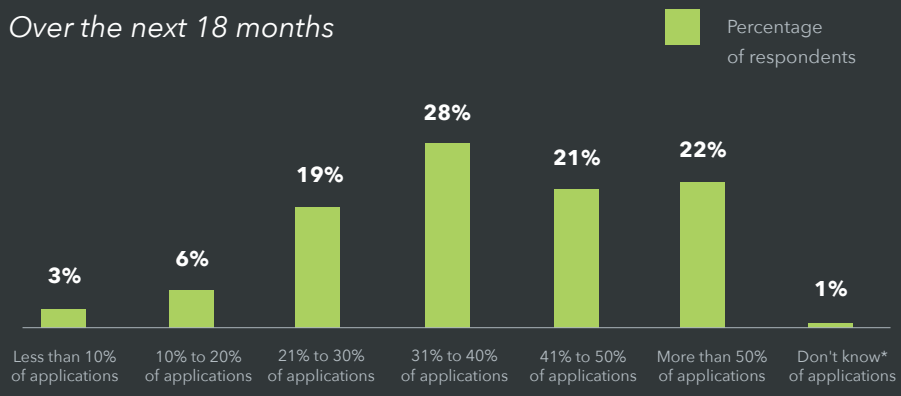
THE DATA

Cloud applications drive demand for mobile access to corporate resources

The Question: Of all the applications used by end-users at your organization, approximately what percentage is currently delivered via the SaaS model? How do you expect this to change - if at all - over the next 18 months?

The Results:





PART 2

Despite its popularity with employees, the implementation of mobility policies is a big challenge for businesses. However, there's no stopping the mobility wave.[2]

Increasing threat and risk ecosystem

The more day-to-day business that occurs on mobile devices, the more that malicious individuals, groups, and states will target them.

THE EXPERT

"The momentum to move data and move functionality to the mobile device is going to significantly increase, for example, cloud. We've seen a tremendous increase of data and companies using cloud, which is also a mobile leverage point."

Craig Shumard

CISO EMERITUS

Here are several telling indicators of what the mobile threat landscape looks like today:

- Approximately three percent of mobile devices in the average Global 2000 enterprise are infected by malware at any given time.[3]
- Sixty-seven percent of the Global 2000 report that their organization has had a data breach as a result of employees using their mobile devices to access the company's sensitive and confidential information.[4]

[2] The Ericsson Mobility report indicates that mobile data traffic grew 60% between 1Q2015 and 1Q2016.
[3] The Economic Risk of Confidential Data on Mobile Devices in the Workplace (2016), jointly produced by Lookout and Ponemon Institute, an independent research company focused on privacy, data protection, and information security.
[4] The Economic Risk of Confidential Data on Mobile Devices in the Workplace (2016)

- For an enterprise, the economic risk of mobile data breaches, including direct operational costs, as well as potential maximum loss from non-compliance and reputational damage, could be as high as $26.4 million.[6]

Mobile threats will continue to grow in complexity and frequency as mobile devices enable increasingly powerful productivity apps used for work.

In this environment, policies and management (enterprise mobility management and mobile device management tools) will certainly help businesses manage their device fleet, but only with mobile security will companies have a strong solution that provides the level of detection, analysis, and response to measurably reduce the mobile risks faced by enterprises today.

For example, devoid of an existing blacklist, mobile security would be able to detect the presence of a piece of malware on a device, alert the end-user to its presence, and provide remediation options while simultaneously alerting the IT admin and providing the same information. An MDM solution, for example, would only block pre-defined blacklisted apps or only allow specifically whitelisted apps onto the device.

The bottom line

Just as the PC radically changed the way we operate as a society, now it's mobile that's transforming our lives and work.

This change from PC to mobile is creating a perfect storm — mobile devices with increasing amounts of sensitive data operating in an ecosystem where malicious code, malicious networks, and compromised operating systems are proliferating wildly.

We already have indications of increased experimentation and sophistication with mobile threats, such as NotCompatible, Shuanet, and XcodeGhost. Current enterprise customers of Lookout are seeing nearly 30 in 1,000 mobile devices encounter threats.

[6] The Economic Risk of Confidential Data on Mobile Devices in the Workplace (2016)

"What we're seeing is the evolution of mobile malware and threats that are only going to increase as more and more gets pushed to the mobile device. So, it's really important that we understand the threat landscape and that we understand that there's more people being attracted to it that don't have our best interests at heart."

Craig Shumard
CISO EMERITUS

The fact that nearly half of enterprise organizations surveyed say they've suffered at least one mobile device-related security breach in the last 12 months is significant. Since malware often gains access to an organization and sits dormant before being put into action, it's very possible that organizations reporting no mobile device breach "to the best of their knowledge," still have one or more end-users with a compromised device, but don't have enough visibility to report the breach.

It's easy to assume there are no threats when you can't see them. Visibility is one of the most important elements of mobile security: you need to know what's there in order to remediate potential breach scenarios.

The rising use of mobile devices combined with the rising prevalence of sophisticated malware adds up to one clear conclusion: it's vital that enterprises get ahead of their mobile risks.

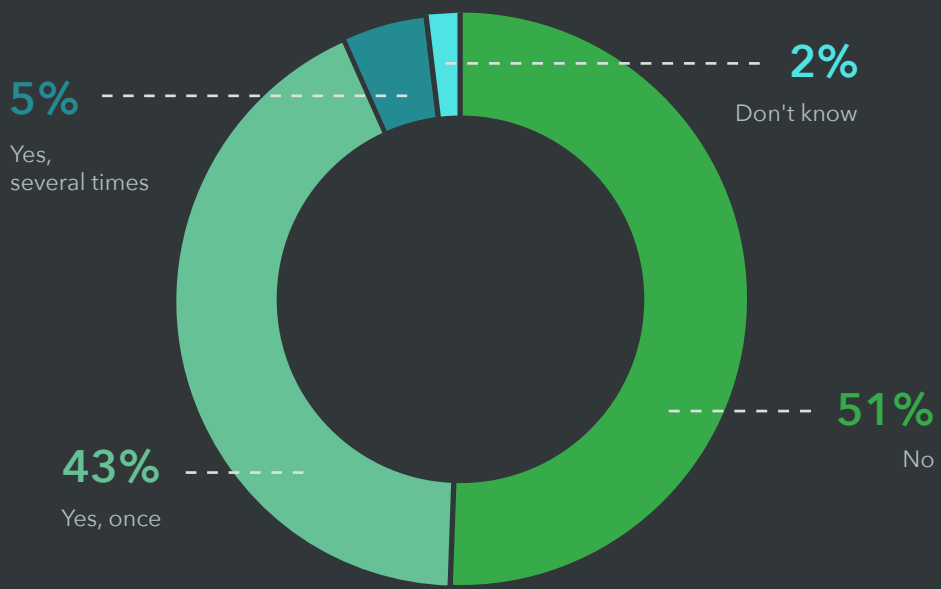
> **"IT spending on mobility-related products, projects, and initiatives will grow from 25 % of IT budgets in 2015 to 40 % of large (>1,000 employees) enterprise IT budgets in 2018."**
>
> IDC
>
> **IDC FUTURESCAPE: WORLDWIDE MOBILITY 2016 PREDICTIONS**

THE DATA

Data breaches are happening via mobile

The Question: To the best of your knowledge, has your organization suffered a security breach as a result of a compromised (e.g., lost, stolen, infected by malware, etc.) mobile device in the last 12 months?

The Results:



PART **THREE**

SIX MOBILE SECURITY CAPABILITIES YOU NEED

PART 3

Six mobile security capabilities you need

Mobile security features overview

The early 2000s was a unique time in the history of computer security. From 2000 - 2003, major enterprises played whack-a-mole with significant viruses with names like Slammer, Blaster, Code Red, and Nimba. The entire industry quickly learned its lesson as businesses everywhere began cleaning up the mess.

That period spawned the creation of the cybersecurity industry we know today, and caused many large companies to course correct and create security strategies. We swore we wouldn't let it happen again, and we didn't. Enterprise malware infection rates are in the fractions of a percentage point per year.

On PCs, anyway.

In the mobile world, we have a very similar ecosystem – small, but powerful computers in our pockets – but we're headed toward a repeat of history if the security technology doesn't also follow.

PART 3

To evaluate mobile security solutions you should focus on these capabilities:

- Detection & remediation of mobile malware
- Detection & remediation of compromised operating systems
- Detection & remediation of sideloaded apps
- Detection & remediation of network-based "man-in-the-middle" attacks
- Detection & remediation of non-compliant/"risky" apps
- Ease and depth of integration with your Enterprise Mobility Management (EMM) and Mobile Device Management (MDM) platforms

By providing visibility into mobile malware, compromised operating systems, network attacks, and non-compliant/"risky" apps, mobile security gives you a holistic view of the overall threat ecosystem in which your business operates.

THE EXPERT

"I think too often technology folks have taken the attitude that mobile is just another platform, and that whatever they're doing on enterprise desktop machines just automatically applies to mobile. The rules on mobile are different. In fact, many companies already have a specialized mobility team. Those have sprung up because mobile is really a different type of a platform, and with that comes a different set of things to think about from a threat and security standpoint."

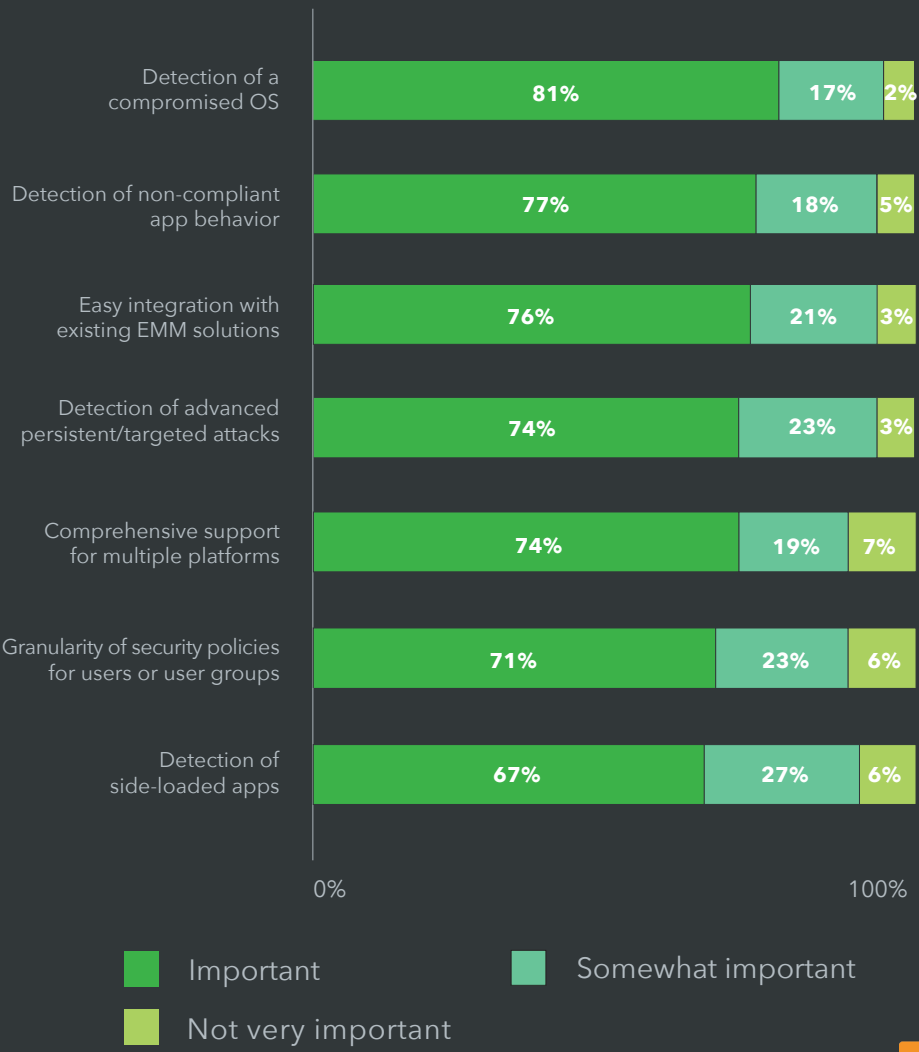
Craig Shumard
CISO EMERITUS

THE DATA

Mobile security capabilities to care about

The Question: How would you characterize the importance of the following mobile security capabilities if you were evaulating a new mobile security solution for purchase at your organization?

The Results:



This is part of the foundation for a successful mobility program, yet many large corporations don't know how many mobile endpoints are part of their network, let alone what risk these devices may pose to sensitive company data.

How to evaluate the 6 key capabilities of a mobile security solution

CAPABILITY: Detection and remediation of mobile malware

The challenge

Traditionally, mobile malware detection solutions use signature- and behavioral-based technology.

Signatures can effectively block simplistic, static malware, but are unable to adapt to malicious software development and routinely miss advanced attacks. Like their counterparts in the legitimate software industry, adversaries tinker with their malware, iteratively improving it to thwart security measures. Adversaries will also deploy customized malware – zero-day malware – which cannot be identified by signatures because they have not been previously seen or analyzed.

DID YOU KNOW? Protection from mobile malware can also help protect from vulnerability exploitation on an employee's device. For example, mobile threat protection would be able to detect if an app attempts to exploit the Stagefright Android vulnerability, alerting to both the presence of malware and the exploit.

Mobile security detects and responds to mobile malware through several mutually reinforcing approaches, such as signature- and behavioral-based techniques as well as big data analysis and machine learning.

What a winning solution looks like

To overcome the limitations of signature- and behavioral-based advanced threat detection and response, you want a mobile security solution that captures real-time security telemetry from a largest possible network of mobile devices, that act like sensors, providing telemetry on new and evolving threats.

PART 3

Next, you want to select a solution that uses big data analysis and machine learning (sometimes called predictive) algorithms to identify risk correlations and zero-day malware that would otherwise evade human analysis and behavioral detection by performing analysis in the cloud, not on individual devices. This approach is the only one that makes it possible to detect threats for which no prior signatures exist before they exhibit malicious behavior – and won't aggressively drain the battery of your employees' devices.

CAPABILITY: Detection & remediation of jailbroken or rooted operating systems

The challenge

Adversaries want to root mobile operating systems because it gives them heightened control over the compromised device and its operating system. Auto-rooting malware that combines adware with exploits that root the device has been a major rising trend over the past year, with a very high prevalence globally.

THE EXPERT

"Detection and response capabilities are critical. The challenges of mobile computing, security threats, and risk are fundamentally different than what we we've seen in the closed loop world of the enterprise computing environment. I think that a vendor that has experience and expertise in the mobile world is very, very important."

Serge Beaulieu

FORMER DIRECTOR OF IT SECURITY

PART 3

In the Android world, rooting specifically involves getting privileged administrative-level access (root) on the device. Rooting effectively gives users or adversaries permission to alter or replace system applications or settings as well as run specialized apps that use operating system capabilities not normally granted to ordinary apps.[1]

READ THIS BLOG POST

Read "Lookout discovers new trojanized adware; 20K popular apps caught in the crossfire," to learn more about auto-rooting malware that masquerading as legitimate applications, including Okta, NYTimes, Twitter, Candy Crush, Facebook, GoogleNow, Snapchat, WhatsApp, and many others.

Jailbreaking on iOS is a broader concept that both involves rooting (gaining administrative-level permissions) and bypassing several types of system-level restrictions, including modifying the operating system and more easily installing unofficial apps via sideloading.[2]

What a winning solution looks like

To protect the underlying security of mobile devices from rooting and jailbroken, the mobile security solution you select should collect a range of device information, including OS/firmware fingerprints,[3] configuration, and other data.

After collecting this data, the solutions should be able to assemble it to form a device fingerprint. Next, it should correlate the various data points of this fingerprint against a reference dataset to identify when a device is compromised by a known attack or user jailbreak/root technique as well as identify anomalous changes in a device's fingerprint, a tactic unique to mobile security solutions.

When a compromised device is detected, your mobile security solution should respond itself or via an integrated MDM client to limit the functionality of that device and its access to your network.

[1] See https://en.wikipedia.org/wiki/Rooting_(Android_OS) (Accessed 5/9/16)
[2] See https://en.wikipedia.org/wiki/Rooting_(Android_OS) (Accessed 5/9/16)
[3] "Firmware" is semi-permanent software that provides instructions for how a mobile device communicates with its hardware components.

PART 3

CAPABILITY: Detection and remediation of sideloaded apps on your network

The challenge

Apps that employee end-users download outside of official app stores – sideloading – create a complex set of problems for businesses.

Sideloading is more common for Android devices because these devices allow users to check "unknown sources" in the device settings to allow app downloads from unofficial app stores without having to alter the state of the device or trust a developer certificate, as on iOS.

Thanks to this setting, employees can download apps that look legitimate, but may in fact contain malware. Without an analysis of the underlying app code, employees have no way to know whether the newest downloads to their mobile devices are actually threatening. Even worse, employees may be tricked into sideloading malicious apps through adversaries' use of phishing or other social engineering techniques, which may innocuously arrive via email or SMS from a"trusted colleague" or your company's CEO.

A MOBILE PHISHING SCENARIO THWARTED

An adversary pretending to be your company's CEO emails your employees with a message that contains links to an app to download. Some employees may download and install the app after accepting the device's standard security notifications.

However, before the app can execute, your mobile security solution has analyzed the app's source and signing certificate and alerted the employees that it is not approved.

Finally, in the case of malicious apps, your mobile security solution will provide employees with an immediate alert to remove the app and will keep a record of all such apps, to protect other employees from the same risk.

What a winning solution looks like

Mobile security safeguards businesses from risks associated with sideloading by analyzing apps downloaded from outside official app stores to determine whether or not that app should be permitted to run on employees' mobile devices. If an app is determined to be out of compliance, a mobile security solution should flag it and alert the user to uninstall it.

With a bird's-eye view of all sideloaded apps on the corporate network, IT professionals can approve apps that may be permitted under their security policy or, more importantly, reject apps that are threatening or not permitted before employees are able to run these apps on their mobile devices. In iOS 9, Apple also introduced a new feature that allows an enterprise to restrict the downloading of sideloaded apps via the enterprise's MDM solution.

CAPABILITY: Detection and remediation of network-based man-in-the-middle attacks

The challenge

Data in transit is increasingly becoming an enterprise risk. This is because employees tend to be careless about connecting to public Wi-Fi, sometimes installing certificates that can decrypt data in order to connect to "free" Wi-Fi at an airport or hotel. Encrypted traffic mitigates many of the threats associated with connecting to the internet through untrusted access points or proxies, but does not solve all problems. This is in part because users are being trained to install configuration profiles with a root CA (Certificate Authority), which gives attackers the ability to decrypt encrypted traffic originating from the device. These methods can allow an attacker to view encrypted enterprise data, such as corporate login credentials (watch a video threat simulation of a man-in-the-middle attack here).

There are a variety of ways for an attacker to get into the network traffic, including:

- Setting up a fake base station or cell tower

- Invoking a VPN to tunnel traffic through their network
- Implementing a proxy to redirect traffic in their network path
- Spoofing Address Resolution Protocol (ARP) to advertise their own hardware address in place of a gateway

While it's important to detect these activities as signals of network compromise, the critical capability is alerting on attacks that attempt to decrypt sensitive enterprise data that is intercepted.

The are three ways this typically occurs:

- Fake Root CA – An attacker introduces a malicious certificate authority under attacker control into the trusted root certificate authority store of the victim's device, allowing the attacker to masquerade as a trusted host that can view encrypted data.
- sslstrip – An attacker effectively removes the "S" in HTTPS connections, allowing normally encrypted data to be viewed in plaintext.
- TLS Protocol Downgrade – An attacker manipulates the negotiated connection to downgrade the protocol or cipher suites and lower the security guarantees of the connection.

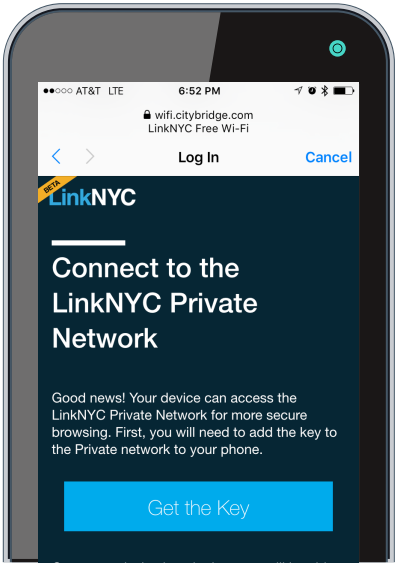
DEFINING TERMS

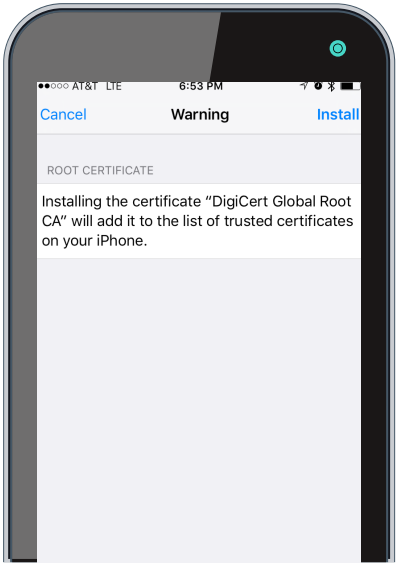
Root CA:
A root certificate authority is responsible for ensuring that the chain of trust used in secure communications can be trusted and is verifiable. The chain of trust allows an end-user to be sure that, for example, the website they are connecting to is, in fact, the site they want and their traffic is encrypted end-to-end to that server. For example, a root CA should ensure that only Google can request certificates for Google-owned properties.

In theory this is how it should work, but there have been many known and public failures with the issuance of certificates that question the chain of trust.

LinkNYC

New York City requires users to install configuration profiles with root CA's as part of the connection process for its free Wi-Fi program "LinkNYC."





What a winning solution looks like

Whenever a device connects to a new network, the mobile security solution you select should probe reference servers with known certificate properties and a known TLS configuration. This allows it to compare expected network configuration properties with the established network properties of the new connection. By analyzing whether these established connections meet expected properties, it can determine whether connections are being tampered with by utilizing any of the methods described above.

Look for an approach that focuses on the risky types of connections that put encrypted data at risk and thus are not reasonable for employee use. Consider a

!

BEWARE FALSE POSITIVES

Most progressive mobility programs do not restrict an employee's ability to connect to cafe, hotel, or airport Wi-Fi networks as that would hinder productivity, yet some approaches to man-in-the-middle detection will surface admin alerts for this everyday activity. These approaches lead to an abundance of false positives that are not actionable.

solution that uses an endpoint agent on the device, rather than requiring VPN to analyze network traffic. This approach provides higher performance and fewer privacy concerns for the end-user. The solution should detect when attacks are happening in real time and then allow an admin to cut off that device's access to corporate data.

CAPABILITY: Detection and remediation of non-compliant, non-malicious apps

The challenge

Not all applications are wholly good or bad. Some fall into a grey area that can be referenced as "non-compliant," or risky. The way non-compliant apps are defined really depends on the team or enterprise defining them. A non-compliant app could be an otherwise benign app that accesses or sends data that your enterprise specifically wants to protect. For example, an IT department may not want their VP of Sales using apps that take contact information off of the device. A non-compliant app could also be one that sends or stores customer data in a country that would violate the organization's data storage policy. Another form of non-compliant app could be one that gathers data that is prohibited by regulation.

The scenarios are endless as, really, a non-compliant app depends on what the organization cares about or is mandated to protect or refrain from distributing.

DOWNLOAD THIS GUIDE

Technical Evaluation Best Practices Guide: There are four stages to technical evaluation of a mobile threat defense solution in your environment: deployment, security monitoring, threat protection, and support testing.

Get this Technical Evaluation Best Practices Guide to use as a framework for evaluating your shortlisted solutions.

What a winning solution looks like

You will want to identify what types of data are sensitive to your organization, what app behaviors are concerning, and what regulations to which you must adhere.

The solution selected should allow you or your IT team to set policies against that sensitivity. The solution if triggered by a violated policy, should allow admins to remediate, such as revoking corporate network access to that device. Look for solutions that understand the difference between malware and apps that may look good, but cause an enterprise headaches down the road.

CAPABILITY: Easy integration with EMM/MDM solutions

The challenge

Most mobile security providers integrate their various offerings with the leading EMM/MDM platforms, including Microsoft Intune, VMWare AirWatch, and MobileIron.

The main benefits of integration with EMM/MDM platforms are:

- Device Provisioning – Using your EMM/MDM solution, the mobile security endpoint app can be easily distributed across your mobile devices, allowing for rapid and scalable device provisioning.
- Threat Remediation – When a threat or non-compliance is detected, the offending device can be remotely locked, wiped, quarantined, or blocked from accessing your corporate network according to your remediation policies.

- Containerization – If you choose to employ a container, this can help separate enterprise and personal data, keeping you one layer safer if an end-user encounters a threat. This will only work if the end-user's device is not jailbroken or rooted. Mobile security solutions will be able to alert you, if that is the case.

Once deployed, mobile security can detect new or emerging threats and then work with EMM/MDM solutions to remediate them. This integration provides businesses with significant policy flexibility by enabling a more precise matching of the risks posed by certain threats to particular remediation strategies.

For example, using a mobile security solution, IT admins can set a unique risk level for different types of malware threats, such as Trojans. Then, depending upon the level of risk assigned to a particular threat, IT professionals can use their EMM/MDM solutions to execute corresponding levels of device remediation, such as quarantine or app disabling.

DOWNLOAD REPORT HERE

> **"Mobile security tools complement an EMM by detecting malware or identifying suspicious behavior and potentially leaky applications. EMM then applies suitable policies to respond to the threat by either uninstalling the app, blocking access or selectively wiping the device."**

Gartner

WHEN AND HOW TO GO BEYOND EMM TO ENSURE SECURE ENTERPRISE MOBILITY MANJUNATH BHAT AND DIONISIO ZUMERLE, JUNE 2016

PART 3

What a winning solution looks like

In order to reduce the time to value for your investment in mobile security, choose the solution that most easily and fully integrates with the EMM/MDM you may already have.

This will enable you to get visibility into mobile threats and non-compliant apps with the ability respond to them, overcoming the limitations commonly found among security vendors who sometimes provide deep technical analysis of threats but no business- and user-friendly mechanism for remediation.

PART **FOUR**

THE BUSINESS CASE FOR MOBILE SECURITY

PART 4

The business case for mobile security

The foundation of your business case: Reducing mobile risks

To successfully make a business case for mobile security, focus your attention on how it will measurably reduce the the risks facing your organization from mobile devices.

A few of the risks could include:

- Damaged brand reputation
- Revenue loss[1]
- Fines
- Potential job loss

Breaches reach beyond technology damage, and wind up impacting serious business metrics.

A compelling business case for mobile security requires clearly communicating that protecting against mobile threats enables you to reduce business risks.

[1] "Target Profit Falls 46% On Credit Card Breach And The Hits Could Keep On Coming" Forbes, 2014

PART 4

The final step is tailoring your message to specific security, technology, and business leaders:

For security leaders risk usually means: malware, device vulnerabilities, app vulnerabilities, data leakage, non-compliant apps, network attacks, and social engineering attacks.

For IT leaders risk usually means: data leakage, "non-compliant"[2] apps, and driving user adoption of a new security solution.

For mobility leaders risk usually means: a roadblock that prevents them from enabling workers to be more productive.

The reason that every company has some element of mobile risk is that mobile devices – the computers that live in our pockets – have become critical enterprise productivity tools.

Employees start responding to emails on the commute to work. They quickly pull up documents in an offsite meeting. They take pictures of a strategy they just "white-boarded" and send it to themselves. They submit expenses, update customer information, respond to support queries, review presentations, finalize budgets, and some even make phone calls.

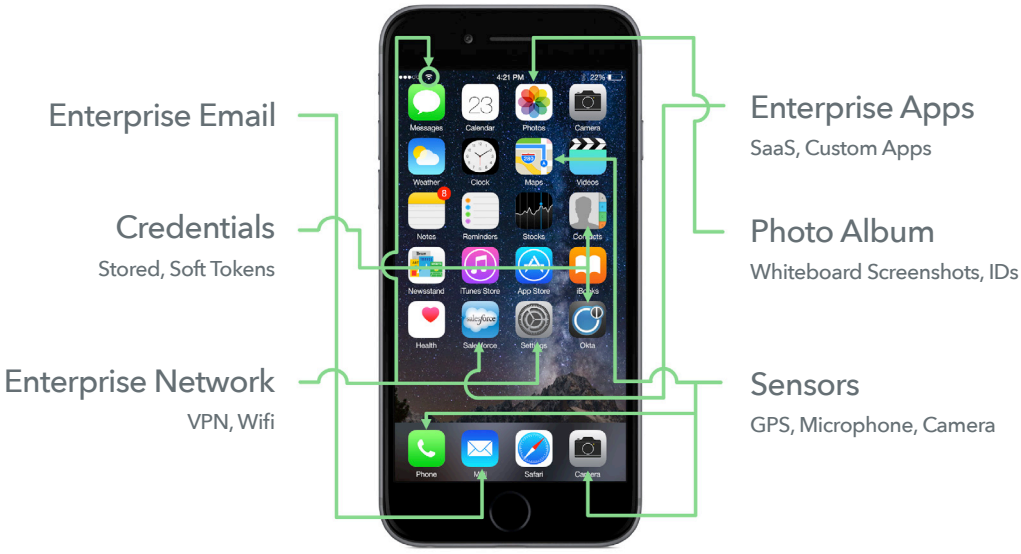
All of this mobile data introduces potential risk, exactly what mobile security solutions are created to mitigate.

DID YOU KNOW? Seventy-four percent of IT and security pros report employee access to data on mobile devices has increased significantly in the last two years.[3]

[2] Non-compliant apps: a wide array of apps that exhibit behavior which may be benign in the right context, but may violate your organization's security posture (e.g. an app that sends contact data to foreign servers).
[3] https://www.lookout.com/enterprise-mobile-risk

Here's a bird's eye view of what you can find on the device:

Your data is mobile



Enterprise mobile threat vectors today

Many organizations have zero visibility into the mobile risks they face. Depending on your security posture, that lack of visibility may be enough to bring on a mobile security solution.

For the majority of organizations, you'll want to start by educating your broader team on what enterprise mobile threat vectors look like today.

Helping your leadership team understand the most significant mobile risks is the first step towards making a business case for a mobile security solution. The risk to your organization's sensitive data from mobile devices, however, may not look like what you expect.

App-based threats

Malware can be installed from a number of sources including being sideloaded from the web, via infected websites, in-app ads, push notification ads, emails & SMS messages such as fake system updates, and pirated versions of legitimate apps.

Non-compliant apps, or those apps that may violate a company's policies based on the data it accesses or collects, can also pose a threat. Vulnerabilities within apps can also be exploited to collect data.

Device-based threats

iOS and Android, like their PC counterparts, contain vulnerabilities in their operating systems that can be exploited locally or remotely. If exploitation of an OS vulnerability leads to root or kernel-level privilege escalation, an attacker can then compromise any application on the device, including those that encrypt data at rest, such as enterprise containers.

A note: Not all jailbreaking/rooting is malicious. Sometimes users opt to jailbreak or root their device in order to gain deeper control over the system.

Network-based threats

Attackers can use malware or socially engineer users to configure a device to route all network traffic through a malicious proxy or VPN connection. Active man-in-the-middle attacks can be used to exploit OS or app vulnerabilities. Man-in-the-middle attacks can also leverage these types of vulnerabilities to steal data.

POTENTIAL DAMAGE

When installed on a device, malware can use multiple techniques to cause damage:

Abuse of legitimate APIs to steal data, monitor the device's sensors, access protected Wi-Fi/VPN networks, or perform other malicious actions. OS vulnerability exploitation to gain full access to the device.

If an enterprise includes an app as part of its product offering, malicious applications could also compromise brand reputation. (Marchcaban, for example, places an invisible overlay on top of Paypal's application to steal user data).

Depending on the data collected, non-compliant apps could violate an enterprise's compliance obligations or otherwise jeopardize sensitive information. App vulnerabilities can be exploited to cause similar damage.

EXAMPLES: Mobile malware, such as Not-Compatible, Malapp.d, and many others.

Rooting and jailbreaking breaks the trust model of a device, exposing enterprise containers and other apps to data theft from any app that runs under elevated privileges.

EXAMPLES: OS vulnerabilities such as "Stagefright" let attackers exploit the native Android media player to remotely steal data.

While most iOS and Android mobile apps and websites use SSL to encrypt data in motion, an attacker who is able to become a man-in-the-middle can use multiple techniques to exploit improper SSL configurations and decrypt and steal data.

EXAMPLES: Fake Root CA attacks occur when an attacker introduces a malicious certificate authority into the trusted root certificate authority store of the victim device. sslstrip is a tactic that effectively strips out the "S" in HTTPS connections, allowing normally encrypted data to be viewed in plaintext. TLS Protocol Downgrade occurs when an attacker manipulates the negotiated connection to downgrade the protocol or cipher suites.

SOLUTIONS

A technology that detects mobile threats using signature-, behavioral-, and machine learning technology. This solution will alert both users and IT admins and provide education on the threat, as well as remediation options.

The technology should be powered by an encompassing dataset of the world's mobile code as obtained from millions of devices that report device state and application data into that data set. The technology should run in the cloud, automatically scaling with the size of the dataset to ensure that it is powerful, but lightweight on the end-user device.

A technology or service that can detect vulnerabilities in apps and OSes. The solution may also be able to test the environment in which a corporate app lives to check for existing vulnerabilities or vulnerable apps. It should then provide education and remediation options.

The technology should be powered by a large, crowdsourced dataset of mobile code as obtained from millions of devices that report device state and application data into that data set. The technology should run in the cloud, automatically scaling with the size of the dataset to ensure that it is powerful, but lightweight on the end-user device.

A technology that automatically detects device connections to various networks and either tests those networks to determine if they are secure or detects attacks in real time. The solution should alert users and IT admins to the presence of a threat, and offer remediation options.

PART 4

WATCH THIS VIDEO

Here's what that risk can look like in the following scenario about Patricia, your company's HR Director.

Mobile Risk Assessment

It's natural to want to understand your mobile risk exposure before investing in a security solution. You may have data on your managed devices in the MDM, but likely can't use this data to determine if the mobile devices with access to corporate data are at risk or not.

One of the ways you can advance the conversation about the specific mobile risks facing your company is to request a Mobile Risk Assessment (MRA) from Lookout.

The MRA pulls data from Lookout's global sensor network of over 100 million mobile devices in order to determine what mobile threats may already exist on a company's network.

When examining threats on your network, your MRA will look at three different barometers of concern:

- The prevalence of the threat, or how widespread it is
- The severity of the threat, or how much damage it could impose if on a corporate mobile device
- The complexity of the threat, or how sophisticated its technology is

Example Mobile Risk Assessment

SHUANET

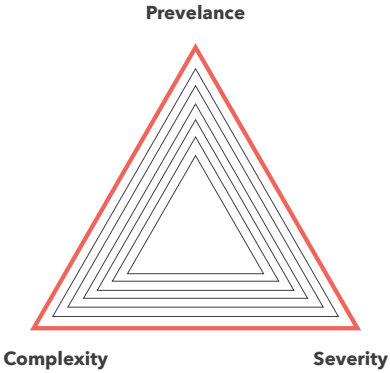
Shuanet is a type of mobile malware classified as "trojanized adware." This is a type of adware that can silently root a victim's device and install further applications that may be malicious to it. Shuanet is an example of this kind of malware, which we consider to be a fairly sophisticated threat.

Mobile malware sophistication has come into the limelight in the past two-to-three years as we've seen a number of families start maturing. This could be in its obfuscation, or the way it hides itself; the way it persists on a device; or in what it does once it is on the device. In Shuanet's case, the malicious app installs itself on the phone's system partition to avoid being removed.

The **complexity** of a threat

Adware like Shuanet

PREVELANCE: High
SEVERITY: High
COMPLEXITY: High



The **complexity** of a threat

A typical piece of Adware

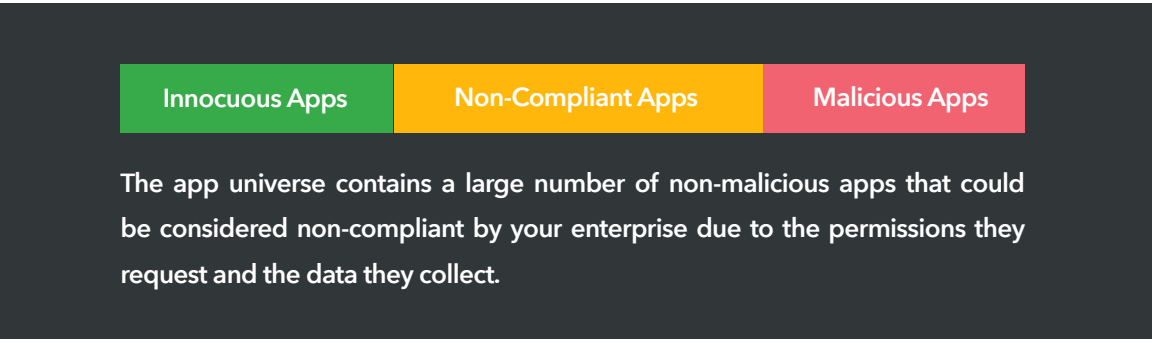
PREVELANCE: High
SEVERITY: Low
COMPLEXITY: Low

GET YOUR MOBILE RISK ASSESSMENT: To learn more about your company's specific risk profile, request a Mobile Risk Assessment (MRA) from Lookout to analyze and measure your company's mobile risks. Request your custom Mobile Risk Assessment.

PART 4

Preventing data leakage: non-compliant versus malicious apps

Once you've established a baseline of potential malicious threats facing your organization, the next step is to make a case for mitigating potential threats from apps that are not intended to do harm, but still are a potential risk for data leakage because of the types of data they collect.



The app universe contains a large number of non-malicious apps that could be considered non-compliant by your enterprise due to the permissions they request and the data they collect.

Let's take a deeper look at non-compliant apps.

Non-compliant apps aren't classified according to a binary "good" or "bad," but an enterprise may deem apps to be non-compliant based on their specific security posture and regulatory requirements.

For example, apps that collect location data may pose great risk to an enterprise or government organization deploying employees to sensitive locations. A doctor working for a healthcare organization might store patient contact information in her phone's contacts and will want to restrict apps that access contact information in order to maintain HIPAA compliance.

Which apps your enterprise deems non-compliant is highly dependent on your industry and the kinds of data your mobile devices – both managed and unmanaged – have access to.

A big part of the business case for mobile security is that it allows IT and security teams to establish security policies to prevent data leakage to which end-user devices must adhere.

These teams also no longer have to maintain manual black/whitelists, as the solution will detect apps that fall into the non-compliant as well as malicious ranges and automatically convict them as they appear on employees' devices.

The ability to replace manual blacklisted and whitelisted apps will enable enterprise IT and security teams work more efficiently, a benefit that tends to pique the interest of decision-makers on both sides of the aisle.

Enabling mobile productivity

Many enterprises now have projects underway to improve productivity and respond to employee requests for using mobile devices at work through a bring-your-own-device (BYOD), corporate-owned-personally-enabled (COPE), or another mobility program.

One of the major challenges facing these programs is that all employees are also consumers, and their approach to mobile technology is, "If I like it, I'll use it. If I don't, I won't." If they don't trust the security technology or they feel that it inhibits their usage of the device, they will try to work around the technology or they won't use it altogether.

THE EXPERT

"If you're an enterprise that supports BYOD, this kind of 'annoying threat' should sound alarms. The fact that contacts and personally identifiable information are taken puts your employees and your proprietary secrets – your competitive edge – at risk."

Craig Shumard
CISO EMERITUS

THE DATA

The business initiatives that drive mobile security requirements

The Question: Which of the following business initiatives are underway at your organization that are directly increasing mobile risk or driving the need for greater mobile security?

The Results:

This is why it's important to evaluate the user experience of the endpoint app of any solution you're considering. The simplest way to do this is to check the ratings and user review in the Google Play Store or Apple App Store.

A mobile security app should build trust between IT and employees. Communicate to your company's mobility team that this solution is intended to protect employees' devices and data just as much as it is intended to protect enterprise data. The bottom line they want to hear is that end-users are free to go about their business, using apps that make them more productive.

*The Lookout for Work Android app benefits from the nine years of continuous improvements to the Lookout Personal app.**

This is the beauty of mobile devices: everyone has incentives to protect them. Many people's work phone or tablet is also their home phone or tablet. A mobile security product will protect any data, regardless of whether it's enterprise or personal, incentivizing the employee to use it.

Selling mobile security internally

You may already recognize the need for a mobile security solution in your organization, but tailoring your case to other key stakeholders is a critical part of getting sign-off on a mobile security project.

For mobile security you need to make a case to your:

- CISO
- CIO
- CEO
- CFO
- Head of HR
- Head of Sales
- Other line of business stakeholders

Understand how to speak to each of these stakeholders and the value they can expect from making secure mobile devices a reality in your organization.

> **"As an S&R [security and risk] professional, failure to establish a strong and comprehensive mobile security program today is as egregious as failing to secure your entire network."**
>
> FORRESTER®
>
> **DAN BIELER**
> MOBILE BECOMES A KEY SUCCESS IMPERATIVE FOR CIOS, NOVEMBER 2015

Making a case to your CISO

CISOs care about the overall security health and risk posture of an organization and have likely invested a significant amount of money keeping the business – and its data – safe. They often think in terms of managing risk that has a high degree of uncertainty, where traditional risk management calculations don't work. CISOs rarely have accurate estimates for the chances of security-related events happening or the damage caused by these events. However, before allocating budget to a mobile security solution your CISO may want to create a mobile threat model to quantify the risk to your business.

Key considerations:

- Mobile threats are becoming increasingly sophisticated across Android and iOS platforms. Malware like Shuanet can have devastating consequences if they make it onto a mobile device that has access to corporate data.
- The impact and likelihood of these mobile threats is growing as the organization continues to embrace mobility.

- The risk of business data leaking is increasingly likely as more employees access corporate resources from their personal mobile devices and/or to use their company-provided mobile devices for both personal and business use.
- The organization lacks the ability to detect these mobile threats and risks today.

READ THIS CASE STUDY

See the mobile risks this Fortune 500 company found.

Learn how one of the world's largest investment management firms closed its mobile security gap by getting visibility into over 300 iOS and Android threats across 10,000 mobile devices, including serious threats such as the iOS malware YiSpecter.

Focus areas for your CISO:

A mobile security solution...

- Would enable the organization to securely allow mobile devices access to the corporate network, promoting enhanced workforce productivity.
- Aligns with any potential BYOD goals and objectives.
- Provides proactive incident response capabilities if a malware outbreak were to occur.
- Would ensure consistent level of security defenses across all types of endpoints.
- Would maintain and strengthen regulatory and audit compliance posture.
- Would provide a necessary security infrastructure to defend against the growing mobile threat landscape.

Making a case to your CIO

Your CIO owns the IT budget and is the primary decision maker for technology purchases.

PART 4

From her perspective, mobile devices are a potential source of headaches and she'll want to ensure they are protected. CIOs care about making sure the company keeps humming along from a digital perspective – downtime is unacceptable.

Key considerations:

- Enable the business and adopt technology that enables productivity gains – an overall win for any business
- Technologies should be easily implemented and managed
- Ensure IT systems adhere to applicable laws and regulations
- Ensure the protection of all proprietary organization data and information systems
- Establish and uphold written policies and procedures regarding all computer operations
- An attack could have major impact on the organization, such as a leaked email server or lengthy downtime, which could result in job loss.

Focus areas for your CIO:

- Proposal should outline a clear business case and value add for technology investments.
- If the organization has already purchased MDM, note that MDM is a very worthy investment from a management perspective, but is not security and will not offer protection from threats.
- Clear implementation plans.
- Proposed vendor should have deep understanding in security compliance and risk management.

THE EXPERT

"Total cost of ownership, especially with security products, has to be viewed in the context of risk mitigation and business enablement. People always want to see a cost justification, but it really has to be looked at terms of your brand reputation, how well you deliver secure services to your employees, other stakeholders, and your consumers."

Serge Beaulieu
FORMER DIRECTOR OF IT SECURITY

- Proposed vendor should also have a proven track record of successfully enabling end-user adoption and usage, resulting in lower helpdesk tickets.
- A vendor with a track record of success, in similar lines of business, with similarly-sized clients.
- Thought leadership and guidance on data management, governance, security, architecture.
- 24/7 global support capabilities.

Making a case to your CEO

CEOs will look at everything from the business growth perspective. This includes ensuring customer and employee data is safe to build and retain brand trust. Focus on the showing the business advantages to protecting your organization's mobile devices.

PART 4

Key considerations:

- Protecting brand reputation from a mobile breach that makes headlines.
- Knowing that mobile device usage is continuously increasing, a CEO will want to ensure that critical infrastructure is protected.
- CEOs accept that the risk of a breach needs to be managed, but will want to confirm that the company has a prepared strategy to get back up and running quickly following an attack.
- CEOs may also have to deliver on client expectations that they are protecting mobile devices used by employees connecting to a client's corporate network.
- Overall operational efficiency, which ties closely to productivity, is one of the CEO's main concerns

Focus areas for your CEO:

- Be able to show the board of directors that there is a plan in place to protect critical infrastructure and remediate mobile threats.
- Mobile security includes protecting employee mobile devices, but also securing your company's own apps from a breach that damages the brand reputation, especially if customer information is involved. In regulated industries, litigation can be brought by affected customers.[4]
- Establish a relationship with a mobile security vendor that can help the company to move quickly in response to an attack to minimize damage.
- Mobile security will give necessary visibility to attacks actively happening to employees' mobile devices.
- Mobile security can help employees around the world to safely, and frictionlessly, connect to the corporate network.

[4] http://www.reuters.com/article/us-home-depot-breach-settlement-idUSKCN0WA24Z

PART 4

Making a case to your CFO

Your CFO naturally wants to ensure that they are getting the biggest bang for their buck in every aspect of the business. Financial loss, however, can come in a number of forms, one of which being diminished brand reputation or client loss from a data breach.

Similar to the CIO's concerns, it also costs a significant amount to triage a breach – the Ponemon Institute quotes the total potential cost of a data breach via a mobile device at $26 million. This figure takes into account a number of factors including "direct costs," such as device replacement, threat investigation, forensics, and diminished employee productivity; as well as "indirect costs" such as costs of non-compliance and diminished reputation.

Key considerations:

- Cash flow, income statements, and balance sheets can all be affected by a public, or even a "small," private breach that results in data loss.
- Productivity loss: a mobile breach may cause the loss of important information or systems, and needs to be cleaned up.
- Similar productivity loss is felt in the sales and marketing operations around a breach, assuaging customer fears, and maintaining client relations.
- The CFO understands where all the data in your organization may live, including Human Resources apps like Oracle or Workday; procurement apps like Coupa; financial apps like Netsuite; and customer data like Salesforce. Help your CFO to see how a mobile security solution protects this data, and reduces the risk of breach through a cloud application.

Focus areas for your CFO:

- Modern mobile security should be a cloud product that does not require a capital expense that needs to be depreciated.

- The endpoint apps that protect individual mobile devices can be deployed quickly to employees globally, delivering value in a short amount of time compared to other IT projects.
- Mobile security is a productivity enabler for every line of business.
- CFOs will push CIOs and CISOs to look for a solution that addresses threat detection, compliance management, and vulnerability management in order to minimize vendors and get maximum value.
- Confidential data, including financial data, that lives outside company walls is significantly safer when the employees who access that data have a mobile security app on their smartphone and/or tablet.

PART 4

Making a case to other executives:

THE CMO: Chief Marketing Officers may be even more sensitive than a CEO to a damaged brand reputation, as it will lead to a suboptimal environment for customer engagement. Marketing leaders want to drive positive customer experiences. Mobile security helps protect the experiences that lead to positive brand sentiment.

HEAD OF HR: Organizations are under pressure to have robust support for mobile devices in order to recruit new employees. The Head of HR will also need to communicate the benefits of a mobile security product to existing employees. This is a great opportunity to use mobile security as an added employee benefit: employees get top-of-line protection for the corporate information they access, and their personal information.

HEAD OF SALES: Sales representatives are often traveling, pulling up customer information on the go, looking at sensitive documents, connecting to whatever Wi-Fi they can to get the information they need to cinch the deal. The Head of Sales will want to make sure that customer and prospect data is secure, while not stifling the salesperson's ability to access what they need whenever they need it.

Focusing on the messaging that each stakeholder cares about will expedite your procurement cycle — and enable you to deliver the measurable reduction in mobile risk that everyone needs.

Read More: Buying Mobile Security > Employee education > Encouraging adoption

PART **FIVE**

HOW TO BUY A MOBILE SECURITY SOLUTION

PART 5

How to buy a mobile security solution

The purchase process

This guide is a practical plan that will help you get an enterprise mobile security solution into your organization, deploy it, and overcome employee privacy concerns to encourage adoption.

THE EXPERT

"First and foremost, ask yourself, 'does this mobile security solution solve the business problem I have?' You're not out there looking to buy security solutions to check-off a check box on some compliance list. There are real business issues associated with securing data on mobile devices."

Craig Shumard
CISO EMERITUS

Before you reach out to vendors:

Phase 1: Document your goals

Your existing business goals will drive your mobile security decisions, and make the case for launching this program.

They may include:

- Adopting more cloud applications
- Implementing a BYOD program or protecting your existing one
- Protecting brand reputation

USE THIS SPREADSHEET

Know your mobile inventory:
As part of your goal setting, it's helpful to document your mobile inventory. This includes: number of iOS devices, number of Android devices, what EMM/MDM you have, and if container technology is being used.

Use this simple Mobile Inventory Spreadsheet to document your devices and environment.

Phase 2: Establish your timeline

The question to answer is: When should these solutions be deployed?

Then work backwards to determine when each step needs to be complete:

1. Vendor demos
2. Your security team's technical evaluation of shortlisted solutions
3. Final decision from the buying committee
4. Your IT or Operations teams' integration of the solution with existing technologies
5. The roll-out together with HR, to ensure product adoption and that privacy concerns are quelled
6. Tracking to determine which employees have or have not enrolled

7. Initial analysis of threats found in your mobile fleet
8. Feedback on the product roll-out and how employees are reacting to its presence on their devices

Phase 3: Document requirements

The requirements your organization will need to meet depends wholly on the industry you service and the kinds of compliance standards you need to maintain. These standards may include PCI, HIPAA, or data transfer/storage laws in your country.

Make sure to assess capabilities beyond security, as the survey results show, ease of deployment and end-user support are among the most important evaluation criteria.

Phase 4: Identify who will buy and manage the solution

You'll want two teams, that may have overlapping members, as part of the mobile security vetting process. The first team should be the key decision stakeholders, who are likely to be the IT and security leaders up to the CIO and CISO level.

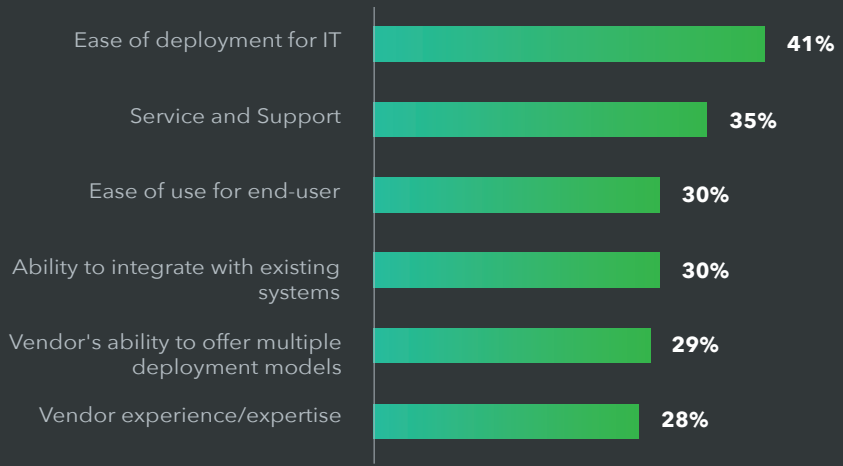
You'll also want to assemble a team of individuals who will eventually manage the solution. This might be made up of individuals on your IT, security, or operations teams. This team will be able to confirm that the mobile security solution being vetted can integrate with the existing security stack. The solution at hand should integrate easily with current solutions to reduce the cost of integration that IT, security, and ops teams naturally incur. These folks will need to be part of any technical evaluation, and will be a critical part of the enterprise-wide deployment.

THE DATA

Ease of deployment and support are key for buyers

The Question: If you were evaluating a new mobile security solution for your organization, which of the following criteria would be the most important?

The Results:



Phase 5: Assess vendors against your actual scenarios

To get the mobile security solution that's right for your company, the key thing is to get specific with each potential vendor about how they measurably reduce the specific mobile risks facing your company and industry.

Make sure you also assess:

- That the solution can integrate with your existing EMM/MDM if you have one
- The availability of support and training for your global locations
- That the endpoint app isn't a burden for end-users to adopt
- The level of effort required to deploy and manage the solution
- That the vendor can actually deliver the capabilities they promote

Focus on how each solution maps back to the business goals you documented. Try to avoid comparing checklists of features, since that could lead your evaluation away from what really matters to your company.

Phase 6: Talk with other customers

Just like a job interview, ask for customer references who can tell you how the vendor has helped them, how deployment went, and any cautionary tales.

If references aren't immediately available, ask for case studies that can educate you on real-world situations in which this technology has worked.

Here are some sample questions to ask on the call:

- What was your deployment experience like?
- If applicable: How easy was it to connect the mobile security solution with your EMM/MDM solution?
- Is the solution easy to manage on an ongoing basis?
- What is the threat detection experience like for end-users and admins?
- What is the remediation experience like for end-users and admins?
- What is your average dwell time (the time between the device encountering a threat and the moment the IT admin receives an alert)?

- What has your support experience been like?
- What feedback have you heard from your end-users?

All of these will help you confirm the solution you really need in your organization.

DOWNLOAD THIS GUIDE

Technical Evaluation Best Practices Guide: There are four stages to technical evaluation of a mobile security solution in your environment: deployment, security monitoring, threat protection, and support testing.

Get this Technical Evaluation Best Practices Guide to use as a framework for evaluating your shortlisted solutions.

Phase 7: Run a technical evaluation

There's no better way to do a technical evaluation than to deploy the solution that your team has rated the highest to a segment of your end-users – or even just your IT and security teams – to experience the solution from both the admin and user perspectives.

THE EXPERT

"People want to put an ROI to security, and I don't know that you can. What you should do is forecast the total cost of ownership over the years of the contract. Know what it costs to administer, and how that is going to be impacted by potential changes in your organization."

Craig Shumard

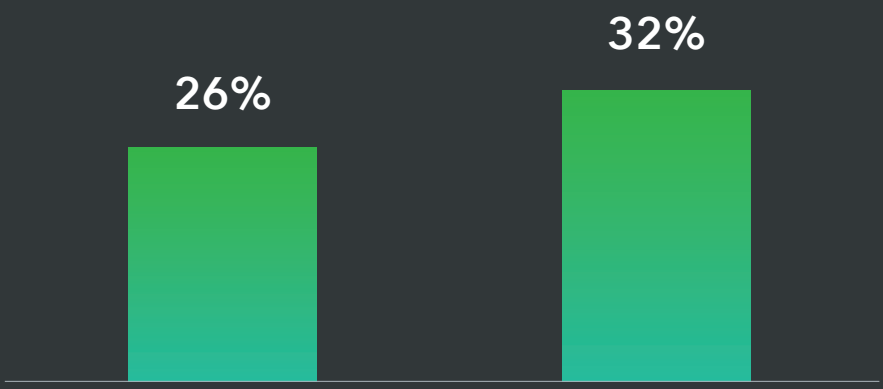
CISO EMERITUS

THE DATA

The desire for higher mobile security budget allocation

The Question: Approximately what percent of your organization's overall security budget for 2017 is, or do you expect will be, earmaked for mobile-specific security product or services? Based on how you view mobile security risk as it compares to other risk vectors (desktop security, network security, etc.) how much of the overall security budget for 2017 do you feel should be allocated to mobile-specific security products or services?

The Results:



% of overall security budget allocated, or which will be allocated, to mobile-specific products/services in 2017

% of overall security budget you feel should be allocated to mobile-specific products/services in 2017

Responses from this survey indicate that IT & security leaders think mobile security should be an even larger part of the overall budget.

PART 5

Phase 8: Cost considerations

Several recent surveys indicate that mobile security is growing as a percentage of the overall security budget.

Another recent survey by the Ponemon Institute indicates that mobile security budgets could be expected to rise 37%[1] to in the next year.

Regardless of your budget, there will be a variety of factors specific to your organization that will drive the cost of your purchase. Consider the following when you're negotiating with a mobile security provider:

1. How many employees do I have? Many times you'll need to consider pricing by the number of "users" for whom you may be purchasing licenses as each employee could be using more than one mobile device to access corporate assets. This style of pricing is most relevant to companies with a bring-your-own-device policy.

2. How many devices do I manage? Some mobile security vendors may sell licenses based on the number of devices. This is most relevant to organizations with a corporate-owned-personally-enabled policy.

3. A mix. Many large organizations have a mix of corporate-owned and, BYOD devices, some of which are managed via an MDM and others that are not. If this is the case for your company, use the Mobile Inventory Spreadsheet to make sure you get the precise number of licenses you need.

Phase 9: Make a decision

Now is the time to assemble your buying committee, make your final business case, confirm that the solution works, is easy from an IT administrative perspective, and the finance team approves the costs and contract terms.

[1] https://info.lookout.com/ponemon-report.html

PART 5

Phase 10: Deployment

There are two main ways to deploy a mobile security solution. The first, and most common is to use an MDM solution, such as Microsoft Intune, VMware AirWatch, or MobileIron as the deployment mechanism for the mobile security endpoint app.

If your company hasn't invested in EMM/MDM because you have a BYOD policy (or any other reason), then deployment will come in the form of an email to employees that includes a download button and a unique code to access and activate the endpoint app.

However, before you physically deploy a mobile security solution to a global workforce that can number in the tens of thousands, you have to plan for two things:

1. Your mobility policies
2. Employee education & internal communication

Your mobile security policies

Your organization will need to have policies based on your risk tolerance and the types of data you collect and store. This could include data from your product, data from your customers, and data from your employees. All three should be taken into account when setting up policies.

Mobile security policies may include "if, then" statements, such as:

- If a malicious or non-compliant app is present on the device, then block device from accessing corporate applications or services, such as email
- If an app accesses "contact information," then flag it as a "non-compliant app" to the end-user and admin – do not block access, unless other remediation instructions are set by the admin
- If a device connects to a malicious Wi-Fi connection, then block traffic from the device to corporate servers

In addition, take time to understand what really makes your company nervous. Are you uncomfortable with employee information being sent to servers outside your country? What defines a "non-compliant" app for you?

Employee education: encouraging adoption

Internal communication is very important during a global roll out, especially if your company primarily relies on employees using their own devices at work.

Employees will want to know:

- Are you watching what apps I download?
- Are you monitoring my browsing?
- How are you protecting my privacy?
- Do I need this security app on my phone?

Communicate to your employees that this solution is intended to protect their device and data just as much as it is intended to protect enterprise data.

THE EXPERT

"If it's not adopted by your users, it just won't work, and the only way it's going to get adopted is if you respect the individual's device and their data. You have to respect your end-users' privacy and communicate that to them."

Serge Beaulieu

FORMER DIRECTOR OF IT SECURITY

PART 5

As far as privacy is concerned, your internal communication should clearly state that the security app is just for threats on the device, not YouTube habits. For example, the solution will be used to determine if the phone was compromised during a trip abroad to a "high-risk" country, or, more generally, if it connected to unsafe Wi-Fi.

The solution will warn them just as quickly as it will warn the admin to make sure everyone stays safe.

Finally, the bottom line is that, yes, they will need it on their phone. If they want to conduct business on their device, it's important that they are not an easy target that compromises your overall security posture.

PART **SIX**

LOOKOUT MOBILE ENDPOINT SECURITY

PART 6

Lookout Mobile Endpoint Security

Why Lookout

- Lookout has amassed one of the world's largest mobile security datasets due to the success of our consumer product. This has created a global sensor network of over 100 million sensors and 30 millions apps, with 90 thousand new apps added daily.
- This global sensor network enables our platform to be predictive by letting machine intelligence identify complex patterns that indicate risk. These patterns would otherwise escape human analysts.
- Mobile is a new era of computing and requires security solutions designed exclusively for this platform. Lookout has been focused on mobile security since 2007 and has expertise in this space.
- Lookout empowers your organization to adopt secure mobility without compromising productivity by providing the visibility IT and security teams need.

The Lookout Difference

Productivity without compromise

Empower your organization to fully adopt secure mobility across personal and corporate productivity, employee privacy, or user experience.

Data leakage control

Lookout enables you to set policies against non-compliant mobile apps that pose a data leakage risk.

Threat protection

Lookout protects your organization from mobile threats across apps, network connections, and devices.

Proven risk reduction

Forward-thinking security organizations have achieved measurable risk reduction with Lookout Mobile Endpoint Security powered by the predictive technology of the Lookout Security Cloud.

Low total cost of ownership

Integrates with your existing EMM solution to seamlessly deploy the Lookout app, with a 95% self-remediation rate to limit helpdesk tickets.

User privacy

Lookout collects the minimum amount of personal information to protect both personally-owned and corporate-owned devices, and provides administrative privacy controls to comply with internal or regulatory privacy requirements.

DOWNLOAD WHITEPAPER

How lookout's predictive security unmasked a mobile threat: the malapp.d case study

Predictive security spots even the most hidden malware – bad stuff that looks innocent on the surface, but whose code, at the binary level, reveals its true malevolence. Lookout used predictive security to uncover Malapp.d, a piece of malware pretending to be the VoIP app "FireTalk" that snuck its way into the Google Play Store.

Learn more about how Lookout found this threat using its "fuzzy code similarity" technology that connected this seemingly innocuous app to two major families of malware.

DEFINING TERMS

The Lookout Security Cloud is powered by a worldwide network of 100 million mobile sensors. These sensors provide threat data that enables us to deliver predictive security that gets more precise as sensors are added and the world becomes more connected.

PART 6

READ THIS CASE STUDY

Lookout performed an anonymous case study of one of our customers – a major Fortune 500 financial institution – that revealed just how real risks are. After realizing that its EMM solution was not enough to protect the organization against mobile attack, this institution brought Lookout on to assess its mobile risk and determine what mobile threats were active.

Within this organization, there were 110 sideloaded applications on iOS devices, or apps that were downloaded outside of the official Apple App Store. There was one detection of a major iOS threat called YiSpecter. YiSpecter is a trojan that can install and execute arbitrary iOS apps and steal data from affected devices.

Further reading:

1) The Lookout Security Platform: Predictive Security in Action

Get a deep dive into Lookout's security platform, how it works and how it will protect your business.

2) Mobile Endpoint Security data sheet

Get a quick take on our Mobile Endpoint Security product, and how it can protect you from network attacks, mobile malware, and more.

3) Mobile Defense in Depth: Lookout and Enterprise Mobility Management

Get a better understanding of how Lookout and your EMM/MDM solution work together to keep your data and devices safe.

PART **SEVEN**

THE FUTURE OF MOBILE SECURITY

PART 7

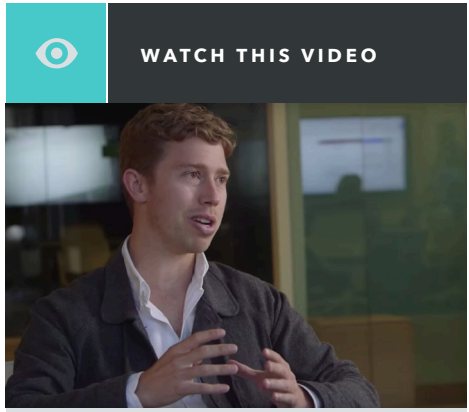
The Future of Mobile Security

Forecast 1: The enterprise network perimeter will die and be reborn

While many major breaches involve an attacker bypassing a firewall to get at valuable data behind it, most organizations still use the perimeter as a cornerstone of their security architecture.

Even when moving to the cloud, enterprises often extend their perimeter to virtual systems. Because business needs dictate having many exceptions to perimeter access controls (e.g., open ports for web services, partners and contractors needing access, VPNs and Wi-Fi granting access to unmanaged devices), IT no longer effectively controls what can get behind the firewall.

We foresee "re-perimeterization," where instead of monolithic internal networks, enterprises will build micro-perimeters that protect individual applications and data stores, each enforcing its own security policy.



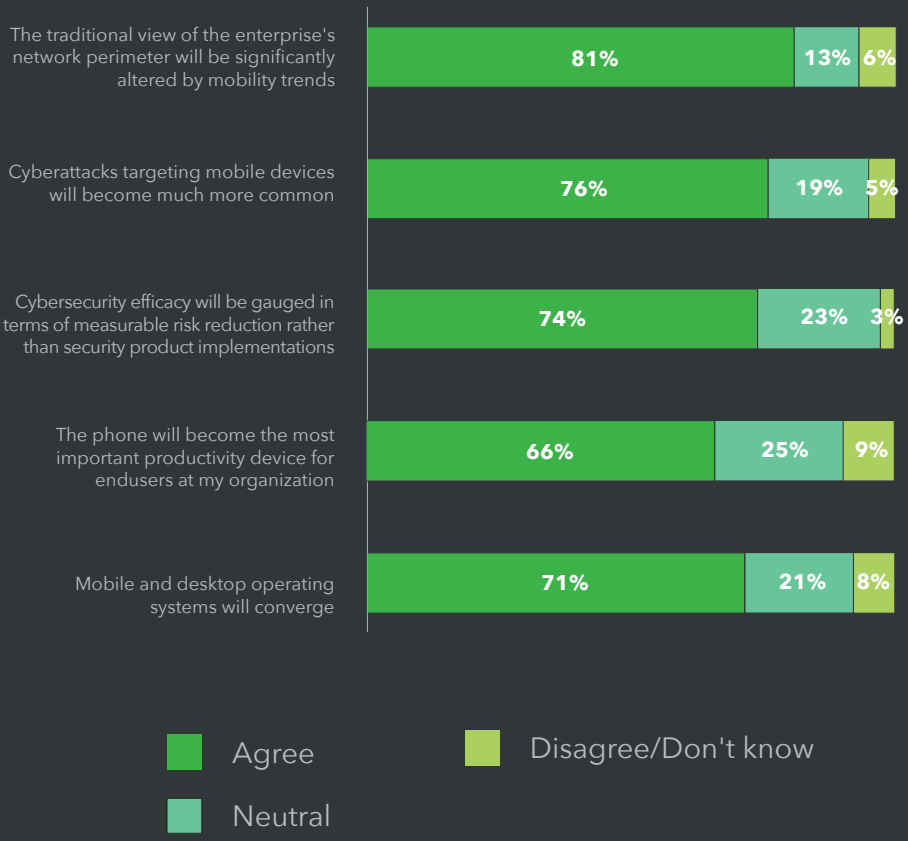
Watch a video of Lookout co-founder Kevin Mahaffey discussing the spawning perimeter.

THE DATA

Targeted attacks on mobile will increase

The Question: Please rate your agreements with the following statements as they relate to mobility trends over the next 24 months.

The Results:



PART 7

Forecast 2: Cybersecurity effectiveness will be measured by risk reduction, not technology deployment

In the past, increasing focus on cybersecurity meant buying "yet another box." Deploying solutions without understanding the problems to solve and a strategy to solve them has proven ineffective and mega-breaches have proliferated over the past few years. Real progress, however, will come by measuring *actual* risk reduction, instead of aiming for the hollow victory of solution deployment. Cybersecurity professionals will need to show how their technical solutions have reduced risk across an organization and the companies behind those technical solutions will need to measure success based on their effectiveness. This is a significant shift from the current paradigm that often highlights implementation over efficacy, and a lot of security vendors won't be happy.

WATCH THIS VIDEO

Watch a video of Lookout co-founder Kevin Mahaffey discussing cybersecurity effectiveness.

This is because it marks a change in the way security vendors report success. As it comes to mobile security, there are a few important metrics a vendor should consider. Dwell time, for example, is the length of time it takes for the security technology to detect and report the presence malware. A good enterprise mobile security solution should have a very short dwell time. Unknown threats is another. Today there are many tests to see how well vendors catch known malware, but the novel, unknown threats are just as important, if not more so in some targeted cases. Is this technology able to detect more than just the known threats in the wild?

CISOs and CIOs will start to be measured against these questions as opposed to whether they were able to deploy a solution.

Forecast 3: A smartphone will be the most important device you own

WATCH THIS VIDEO

Watch a video of Lookout co-founder Kevin Mahaffey discussing the changing importance of mobile devices

A smartphone contains your email, your work projects, your bank, your map, your camera, your health tracker, and the primary way you connect to the internet. It's also now going to become the device through which you authenticate yourself – it's becoming your password. Yahoo, for example, offers its users the option to sign into its email through a push notification sent to their phone. The idea is, if you have your phone, you can verify that you are who you say you are with the click of a button.

Going forward, we foresee a world where practically everyone uses their smartphone as a multi-factor authentication element. In this world, the smartphone becomes your most valuable asset: both something that enables you to unlock your life online and a target for attackers seeking to access your services.

Forecast 4: Operating systems and form factors will converge

Most people define mobile devices – smartphones and tablets – as those running a mobile-optimized operating system (for example, iOS, Android, Windows Phone). There's a trend emerging, however, in which traditional mobile devices are gaining functionality typically associated with PCs.

At the same time, PCs are being architected more like mobile devices – an interbreeding of species, if you will. The iPad Pro, for example, has a keyboard. With Windows 10, phones and tablets can run "universal" apps that also run on PCs. Windows 10 also has application-layer sandboxing, code-signing, and an app store with apps pre-vetted by Microsoft.

WATCH THIS VIDEO

Watch a video of Lookout co-founder Kevin Mahaffey discussing the convergance of operating systems

In certain configurations (such as enterprise-managed devices), a laptop running Windows 10 has a security architecture that looks strikingly similar to a smartphone or tablet.

We expect the blending of species to continue and cause the classic differentiators between mobile devices and PCs to (eventually) disintegrate into a difference in nothing more than screen size.

THE EXPERT

"I would probably cry more about losing my phone than losing my wallet. And I would certainly lose a lot more functionality, and personal information. The idea that in the future we'll be leveraging the biometric data of this device, or some other functionality to do two-factor authentication, means you need to protect the device more than ever to ensure your data and your applications are protected."

Serge Beaulieu

FORMER DIRECTOR OF IT SECURITY

CONCLUSION

Mobile threat protection is a new security layer that has become an acute need in a very short amount of time. Here are the five other key takeaways from the original research in this guide:

1. The employee productivity stakes are incredibly high. In the research we conducted with ESG, 95 percent of respondents reported that the use of mobile devices is critical or very important to maximizing efficiency and productivity

2. Data is at risk. The research also showed that 64 percent of respondents report it is very likely that sensitive data is present on employees' mobile devices.

3. Protecting that data is the top objective. Fifty-four percent of respondents included protecting customer information, 49 percent included protecting employee information, and 45 percent included protecting proprietary company information as among their top goals for mobile security (the three most-frequently mentioned responses).

4. EMM solutions alone are not seen as up to the task. Sixty-four percent of respondents believe EMM solutions should not be the only protection for data on mobile devices.

5. Protecting mobile devices is not optional. An overwhelming majority, 86 percent, of security practitioners reported that the importance associated with protecting and detecting threats on mobile devices is increasing.

The threats and technologies powering enterprise mobile security evolve rapidly. To continue staying on top of the latest developments, visit the insights page of our website (www.lookout.com/insights) and our blog at https://blog.lookout.com/.

If you'd like to speak with a representative from Lookout, call (888)-988-5795 or email info@lookout.com today.

Contact us

Website: www.lookout.com
Blog: blog.lookout.com
Twitter: @lookout

About Lookout:

Lookout is a cybersecurity company that makes it possible for individuals and enterprises to be both mobile and secure. With 100 million mobile sensors fueling a dataset of virtually all the mobile code in the world, the Lookout Security Cloud can identify connections that would otherwise go unseen - predicting and stopping mobile attacks before they do harm. The world's leading mobile network operators, including AT&T, Deutsche Telekom, EE, KDDI, Orange, Sprint, T-Mobile and Telstra, have selected Lookout as its preferred mobile security solution. Lookout is also partnered with such enterprise leaders as Microsoft AirWatch, Ingram Micro and MobileIron. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.

www.lookout.com