Lookout®

WHITEPAPER

Understanding Mobile App Risks

Contents

Apps empower greater productivity, but with risks

As organizations embrace smartphones and tablets in the workplace, mobile apps have become a primary way for their workers to access data. Every cloud service has a mobile app, from email communications to customer relationship management, which means everybody is empowered to work the way they want. But with greater flexibly also means greater risks. And what's worse is that the risk on mobile is hard to see. It's difficult for IT administrators to see what other apps or configurations are on their employees' devices,

For organizations to fully leverage the productivity potential of the cloud, they need to deploy the appropriate mobile security measures.

Understanding app risks for mobile

Organizations have three main categories of risk they need to be aware of and take steps to manage.

1. External threats that come from criminals, competitors, and countries.
2. Vulnerabilities within apps and devices. These glitches, flaws or weaknesses in software can be exploited by malicious actors.
3. User behaviors and the way the configure their devices, which allow apps to access sensitive information about users and organizations.

Mobile threats, app vulnerabilities, user behaviors and configurations all create risks, such as loss of sensitive data, leading to breaches of regulations and compliance rules. Any of which could harm your users, organization and your brand.

CASE STUDY

A Lookout customer used Lookout to discover that their mobile app, which was developed by an independent software vendor (ISV), enabled location data. This was a privacy concern for their employees. After running the app through Lookout, they contacted the ISV to remove that feature.

How are app risks different from mobile threats?

Mobile Threats

Attackers are now targeting mobile devices because your workers are now accessing sensitive data on them all the time. Lookout Mobile Endpoint Security identifies mobile threats as these primary attack vectors: app-based threats, network-based threats, and device-based threats. Gartner defines Mobile Threat Defense (MTD) as being "composed of the following features: application scanning and risk, network security and protection, behavioral anomaly and configuration detection and vulnerability assessment and management."

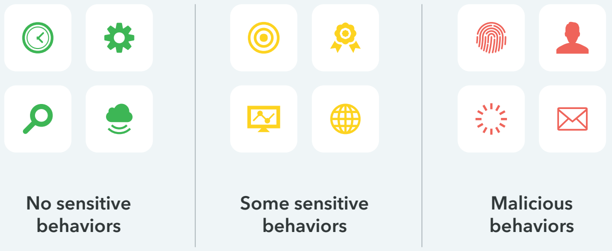
App Risks

Most iOS and Android apps are not malicious but may violate security or regulatory requirements by exhibiting unsafe behaviors or containing vulnerabilities. Lookout provides comprehensive visibility into these app risks within an organization's mobile fleet, enabling admin to monitor and set policies against apps that are at risk of violating internal and regulatory requirements.

If we were to put apps on a spectrum in terms of risk, there would be harmless apps on one end and malicious apps on the other. What remains is a gray area of apps that are not outright malware but violate the security posture of the organization or specific industry/regional regulations like GDPR.

One of the prevailing trends is collecting data in lieu of payment. We're now seeing a proliferation of free apps because user data has become the new currency. Developers are selling data they've collected via these "gray area" apps to data brokers, ad networks, and other third-party vendors – leaving your employees and your organization's data at risk.

Mobile Endpoint Security for App Risks



Sensitive mobile app behaviors

ACCESS TO SENSITIVE DATA
Apps that access sensitive corporate or employee data, including PII

DATA EXFILTRATION
Apps that upload sensitive data to external servers

DATA SOVEREIGNTY VIOLATIONS
Apps that violate data sovereignty regulations or send data to risky geographies

USE OF CLOUD SERVICES
Apps that access cloud storage providers, social networking services, or peer-to-peer networks

INSECURE DATA HANDLING
Apps that don't use proper encryption when storing or sending data

VULNERABILITIES
Applications with known vulnerabilities

Understanding mobile app threats

Mobile app threats manifest in different ways, from an app that asks for one too many permissions, to a surveillanceware with advanced spying capabilities. Most mobile attacks start with phishing, tricking users into installing malicious apps or exploiting software vulnerabilities.

App threats

Malicious mobile apps can harm you in many different ways, including stealing information, physically damaging your device and monitoring a user's or organization's activities. Common ways apps can become unsafe include injecting malicious code into a legitimate app and asking permissions that are beyond what the app needs to function.

Many Organizations think that by having Mobile Device Management (MDM) solution means they're protected from app threats. The reality is that users can easily install apps that are not approved by the App Store or the Google Play Store onto their phone.

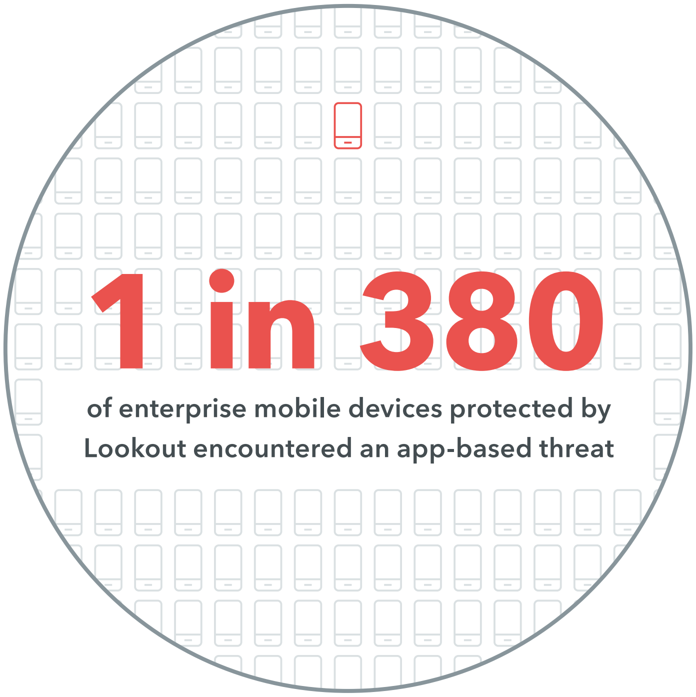
Prevalence of app threats

In the 2nd quarter of 2020, 1 in 380 of enterprise mobile devices protected by Lookout encountered an app-based threat. These app threats include riskware, device hacking tools, spyware, surveillanceware, trojans, adware, and remote code execution.

How do you protect against app threats?

You can protect your organization against app threats by deploying a comprehensive mobile security solution, which should include the following functions:

- **Detect the downloading of malware** such as backdoors, trojans, surveillanceware, and ransomware
- **Block the installation of rootkits**, which provides elevated access to systems and data
- **Detect the installation of riskware**, including adware, spam and Chargeware
- **Prevent the sideloading of apps**, that are not approved by the Google Play Store or the App Store.



1 in 380

of enterprise mobile devices protected by Lookout encountered an app-based threat

Understanding mobile app vulnerabilities

The challenge of securing mobile devices is not limited to blocking apps that have harmful functionalities. Apps and devices themselves have vulnerabilities that can be exploited to harm you.

App vulnerabilities

Mobile apps have vulnerabilities just as PC software does. The difference is that most apps are selected by end-users and are more likely to be built by small teams of developers. PC applications on the other hand, are usually vetted by an organization's IT and developed by large software companies.

Prevalence of app vulnerabilities

Lookout researchers have performed many in-depth analyses on numerous popular Android and iOS productivity and business applications. We identified a diverse range of vulnerabilities with varying in sophistication and impact. On the high-risk, high-sophistication end of the spectrum, we discovered flaws that would allow adversaries to compromise not only the information a user viewed in an app, but also their cloud service account and all data tied to that account.

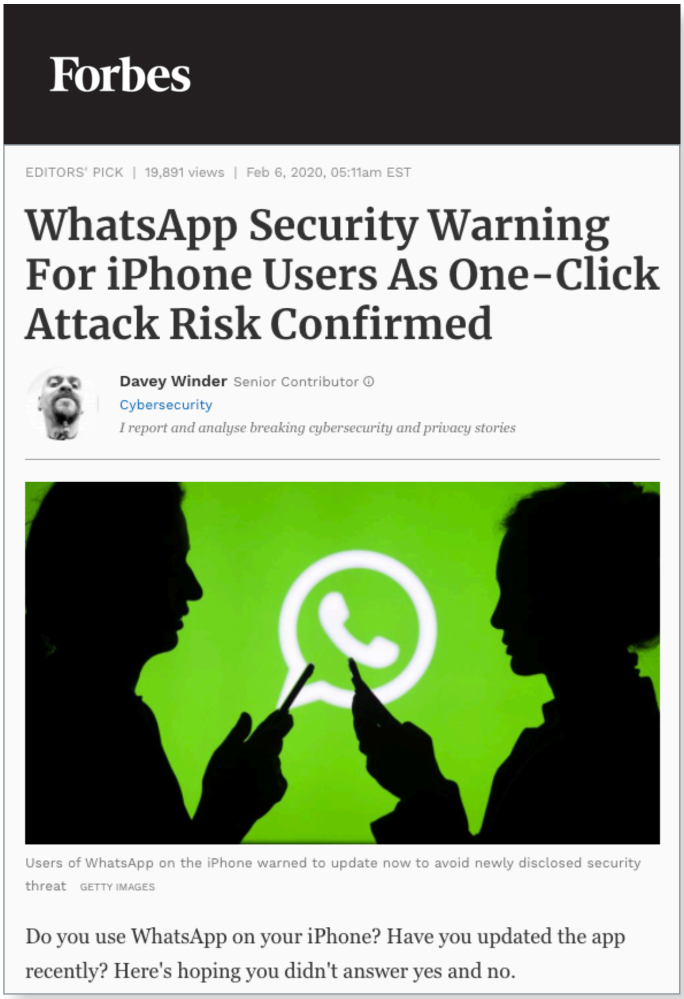
Facebook announced a vulnerability in WhatsApp that it discovered in early May around a bug in the VOIP call feature of the messaging application on both iOS and Android. The vulnerability allowed a caller to install spyware on a device whether the user answered or not. The spyware reportedly being installed was Pegasus - spyware built by NSO Group and originally discovered by Lookout.

How do you protect against app vulnerabilities?

Security controls around data in transit from apps have definitely improved in recent years. But even well-known development companies have released apps with security flaws.

Our App Security Assessments often find apps with inadequate security controls around data in transit, which means they could inadvertently leak sensitive information or providing malicious actors with an opening to attack a victim's device.

As more organizations allow employees to use apps that handle sensitive user and corporate data, we expect an increase in attempts by cybercriminals to compromise apps.



Forbes

EDITORS' PICK | 19,891 views | Feb 6, 2020, 05:11am EST

WhatsApp Security Warning For iPhone Users As One-Click Attack Risk Confirmed

Davey Winder Senior Contributor
Cybersecurity
I report and analyse breaking cybersecurity and privacy stories

Users of WhatsApp on the iPhone warned to update now to avoid newly disclosed security threat GETTY IMAGES

Do you use WhatsApp on your iPhone? Have you updated the app recently? Here's hoping you didn't answer yes and no.

Understanding behaviors and configuration risks

Employees are often of high risk because may decide to use their personal mobile devices for work. And in many cases, they may be configured in ways that conflict with an organization's security policies. Many chief information security officers (CISOs) want to enable a bring-your-own-device (BYOD) policy, but only if they could provide security. Getting visibility into their users' behaviors and their devices' configurations is the first step to enabling secure mobility.

App behaviors and configuration risks

Unsafe app behaviors can lead to the leakage of enterprise data accessed by certain apps.

Examples include:

- Apps that access sensitive enterprise data and public cloud-based storage services not under enterprise control.
- Apps that access data with compliance requirements such as credit card numbers or personally identifiable information, and don't have adequate protection for the use, transmission, and storage of that data.

Prevalence of app behaviors and configuration risks

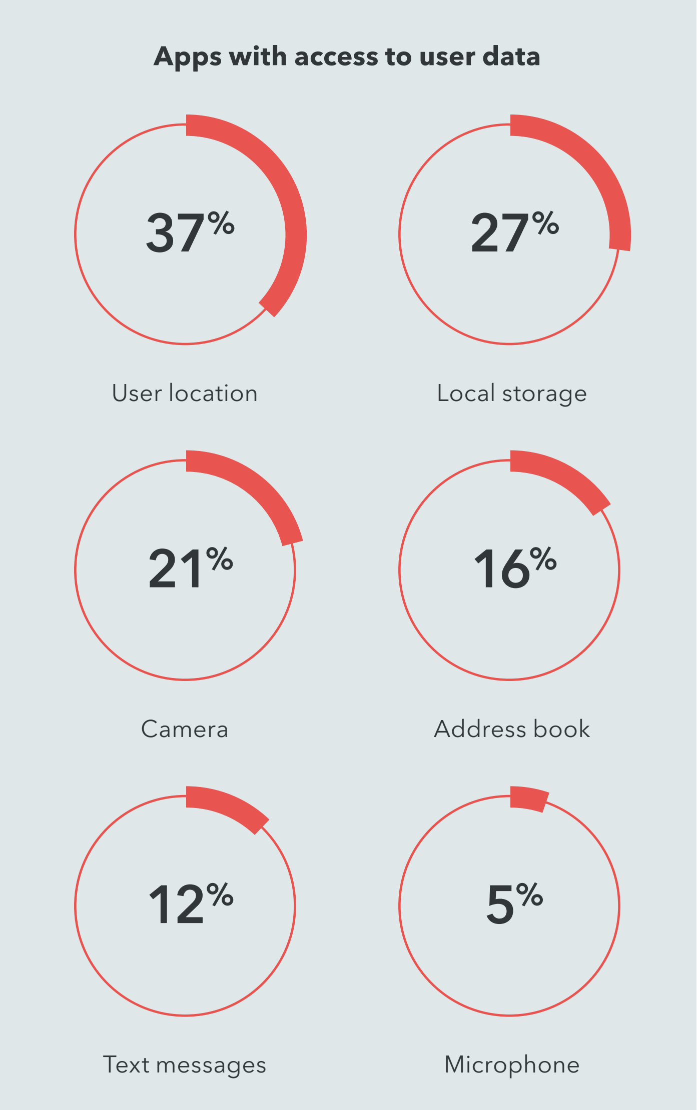
In the first 6 months of 2020, over 30,000 enterprise iOS devices protected by Lookout encountered sideloaded applications.

Across tens of millions of devices with Lookout, 37% of apps access user location, 27% access local storage, 21% access the camera, 16% access the address book, 12% access text messages, and 5% access the microphone.

How to protect against app behaviors and configuration risks

Whether they're corporate or personally owned devices, IT and security teams need visibility into app behaviors to prevent data leakage. Apps can store or share data in ways that conflict with a company's security policies or breach regulatory compliance rules. The challenge is to provide this visibility into app behaviors without impacting employee privacy.

Effective mobile security strategies that include app visibility and remediation can help organizations reduce the risk from risky app behaviors and configurations.



How does Lookout mitigate these risks?

Lookout believes that risk is in the eye of the beholder. An app that is deemed risky for one financial services organization may be perfectly tolerable to a construction firm.

That's why we do not give each apps a risk score. Instead, we show the app's capabilities in the context of an organization's overall fleet of apps, allowing the admin to make simple, actionable decisions about them.

When a risky app is found, the admin has the ability to blocklist that app directly from the console. However, block listing one-off apps each time does not scale, as apps may update to new versions as much as 10 times per year.

Manage app risk at scale with custom policies

We give admins the ability to blocklist individual apps, but that's not a scalable solution when apps may update as much as 10 times a year.

That's why we empower admins to blocklist app behaviors by setting custom policies with flexible remediation actions. This reduces the need to manually vet each application while still prevent data leakage.

With Lookout, organizations can set custom policies to protect enterprise data from malicious apps and data leakage, strengthening their ability to meet internal and regulatory compliance requirements for their mobile endpoints.

We provide the controls and visibility you need to manage app risks

- **Risky apps dashboard:** A central dashboard to view all apps on your network.

  Example: The dashboard tells you that 15% of the apps in your fleet send contact data externally.

- **App risk monitoring at scale:** Apply filters to all the apps in your fleet, allowing your admin to quickly hone in on risky app capabilities across all apps in your mobile fleet.

  Example: Show me all iOS apps that both access contacts AND connect to cloud services like Dropbox.

- **Custom policies for risky apps:** Save filters as policies and assign risk levels to violations of that policy.

  Example: As an admin, I want to prohibit apps that send calendar data overseas and need to notify my employees of these policy violations.

- **App blacklisting:** Flag and remove apps that you don't want to exist on your network.

  Example: I've identified a flashlight app on a small number of iOS devices that is too aggressive with data collection, so I want to blacklist that from my network.

- **Enterprise app review:** Upload custom apps into Lookout to analyze for risky behaviors and malware.

  Example: We've just built an HR app for employees and I want to make sure the developer didn't use any components with malicious code.

Lookout Mobile Endpoint Security for App Risks

Lookout Mobile Endpoint Security for App Risks seamlessly integrates with Lookout's existing threat protection capabilities. Our platform enables admins to both monitor and set actionable policies against apps at risk of violating internal or regulatory requirements. Lookout empowers your organization to adopt secure mobility without compromising productivity.

Learn how Lookout Positioned as a Leader in the IDC MarketScape for Worldwide Mobile App Security Testing.

> "Mobile app security testing software that ingests a high volume and variety of mobile apps as part of its foundation for analysis is a critical success factor for mobile app usage in the workspace."
>
> **Denise Lund**
> Research Director, Enterprise Mobility, IDC

About Lookout

Lookout is the leader in mobile security, protecting the device at the intersection of the personal you and the professional you. Our mission is to secure and empower our digital future in a privacy-focused world where mobile devices are essential to all we do for work and play.

The broad adoption of smartphones and tablets have created new and endless ways for cybercriminals to convince you to willingly use your mobile device for their unlawful gain. The most common start of a cyberattack is a phishing link and mobile devices have enabled new ways to send them to you. Phishing risks no longer simply hide in email, but in messaging, social media, and even dating apps. Because we use these devices for both, protecting against phishing is critical for our personal and professional lives.

Lookout enables consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Our platform uses artificial intelligence to analyze data from nearly 200 million devices and over 100 million apps to protect you from the full spectrum of mobile risk. As a result, Lookout delivers modern endpoint security with the most comprehensive protection from device, network, app and phishing threats without prying into your data.

To learn more, visit lookout.com.