Lookout

WHITEPAPER

Lookout Mobile Endpoint Security for App Risks

The emerging risk around leaky and non-compliant mobile apps

As organizations are increasingly embracing mobile devices in the workplace, mobile apps have become the primary way that data is accessed and transmitted on these devices. More and more, organizations are allowing employees to freely download mobile apps without having any visibility into what those apps are actually doing on the device. This is common practice for organizations looking to enable mobile productivity in the workplace, but with it comes new risks that are often not addressed.

Moreover, organizations are now building their own in-house apps for their employees. The development of these apps is often outsourced to independent software vendors who typically assemble these apps from existing code libraries, rather than building them from scratch. These existing code libraries may contain vulnerabilities, risky behaviors, or even malware. These apps do not go through any official app store vetting process and therefore could result in potential data loss or compliance violations if not thoroughly checked before full distribution to employees.

In order for organizations to be able to fully embrace the use of cloud and mobile, enterprises need to apply the appropriate security controls to their mobile fleet. Mobile threats, vulnerabilities, risky behaviors and configurations are now a known enterprise risk and can lead to loss of sensitive corporate data and compliance risk. The same compliance policies applied to fixed endpoints now need to be applied to mobile endpoints.

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:

As more sensitive data is accessed on mobile, attackers are targeting this platform to steal sensitive data. Lookout Mobile Endpoint Security identifies mobile threats as targeting 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:

Some iOS and Android apps are not malicious *threats*, but they can exhibit sensitive behaviors or contain vulnerabilities, violating security or regulatory requirements around data loss of an organization. Lookout provides comprehensive visibility into these app risks within an organization's mobile fleet, enabling admins to monitor and set policies against apps that are at risk of violating internal and regulatory requirements. According to Gartner, Mobile App Reputation Services (MARS) "products evaluate the risk and reputation of individual apps hosted in public stores…"

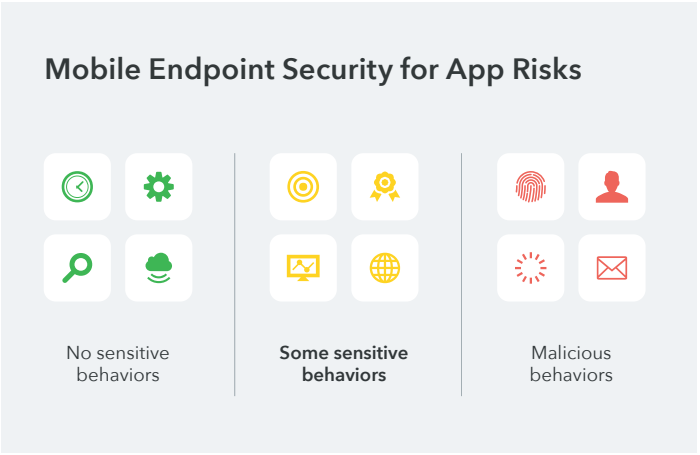
As Gartner recently published,

> "MARS is converging with MTD and will likely not remain a stand-alone market. Technical professionals evaluating MARS products should favor MTD products that include MARS."[1]

[1] Gartner Compare EMM Security Ecosystems to Make a Strategic Selection, Andrew Garver, May 2017

In the spectrum of apps, there are harmless apps on one end and malicious apps on the other. However, there is a grey area of apps in the middle of this spectrum that are not outright malware, but violate the security posture of the organization or specific industry/regional regulations like GDPR.

With the prevalence of free mobile apps, we see now more than ever that user data has become the new currency. Developers are selling any data they've collected via these "grey area" apps to data brokers, ad networks, and other third party vendors - leaving your employees and possibly your organization's data at risk.



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

How does Lookout mitigate these risks?

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

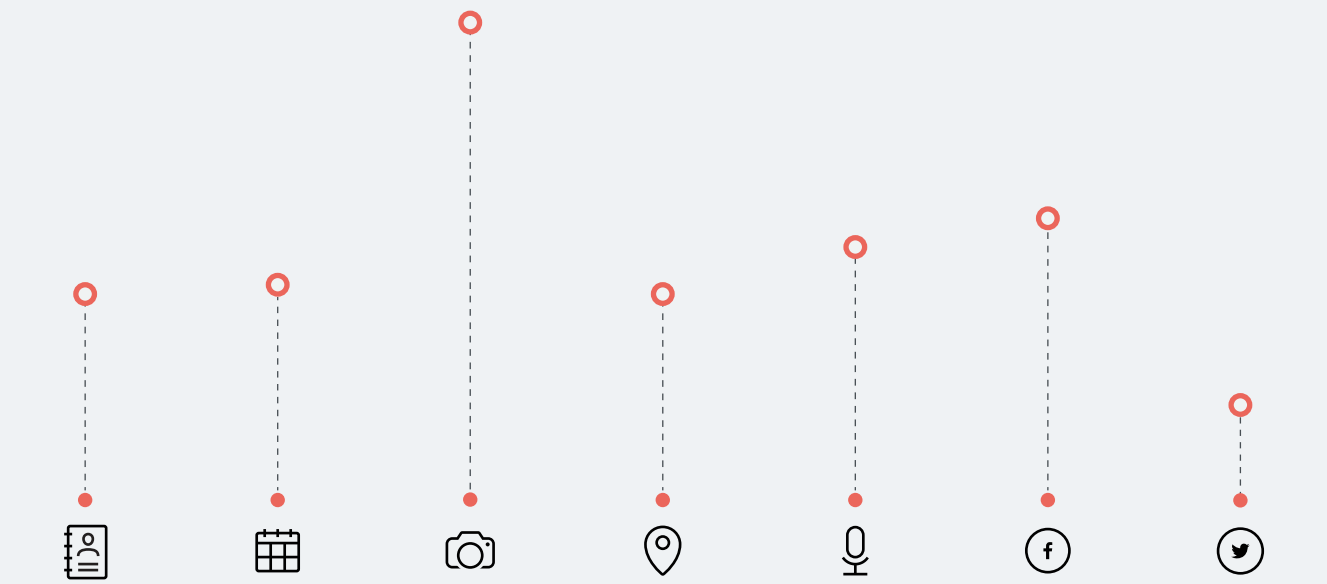
As such, we do not provide subjective risk scores to each app (e.g., "this flashlight app is 86/100 risk"). Rather, we provide visibility into the app capabilities in the context of an organization's overall fleet of applications, allowing the admin to make simple, actionable decisions about the apps on employees' mobile devices.

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

Custom policies to manage app risk at scale

With this in mind, Lookout enables admins to blacklist app behaviors by setting custom policies, with flexible remediation actions using your MDM. This effectively reduces the need to manually vet each application while still preventing data leakage. Organizations can set custom policies to protect enterprise data from malicious threats and data leakage, strengthening their ability to meet internal and regulatory compliance requirements for their mobile endpoints. Lookout's natively developed MTD + MARS solution called Lookout Mobile Endpoint Security provides security professionals with a single dashboard view across their spectrum of mobile risk, allowing enterprises to quickly identify any areas of concern.

App access on iOS enterprise devices:



30% of apps access the address book

31% of apps access the calendar

75% of apps access the camera

30% of apps access the GPS

39% of apps access the microphone

43% of apps connected to Facebook

14% of apps connected to Twitter

Features of Lookout Mobile Endpoint Security for 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 an admin to quickly hone in on risky app capabilities across all the 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 those filters as policies and assign a risk level 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:** Once I identify that an app should not exist on my network, I can place that app in a blacklist and use my MDM to remove the app from the network.
  Example: I've identified a flashlight app on a small number of iOS devices that is too aggressive with data collection, and I want to blacklist that from my network.
- **Enterprise app review:** For custom apps that I build, I can upload that app 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.

A comprehensive MTD + MARS solution

Mobile security technologies of today should integrate with existing mobile management solutions. Lookout integrates with MDM/EMM solutions, as well as SIEM solutions, to allow enterprises to easily set up policies and protect their mobile fleet. Lookout Mobile Endpoint Security for App Risks seamlessly integrates with Lookout's existing threat protection capabilities, enabling admins to both monitor and set actionable policies against apps at risk of violating internal or regulatory requirements. Our massive dataset of over 40 million apps provides the visibility that admins need in order to set policies that protect corporate data against leakage in the most scalable and effective manner. Lookout empowers your organization to adopt secure mobility without compromising productivity.