Lookout®

# LOOKOUT MOBILE RISK & COMPLIANCE

**IDENTIFY THE APPS YOUR EMPLOYEES USE THAT ACCESS CORPORATE AND PERSONAL DATA**

## Visibility into mobile apps is necessary

Mobile apps are a key part of our everyday work and personal lives. Some of these apps appear to be innocuous, but certain permissions may create unintentional yet serious risks for your organization. This includes the other apps to which it has access, the data on your device that it's accessing and the geolocation of the IP address to which it sends that data.

Mobile apps have become the next frontier of shadow IT. The average employee may not think it's a problem, but your organization has explicit policies on how data is shared and stored. Because a mobile device sits at the intersection of the employee's personal and professional life, these apps may pose a hidden violation of the governance, risk and compliance policies of your organization.

Mobile devices and apps are extensions of ourselves as we've made them keys part of our everyday lives. However, some mobile apps have permissions and capabilities that do not align with regulations and privacy policies.

### BENEFITS

- Analyze any app to understand potential policy violations before deployment
- Gain visibility into all data access and app permissions
- Understand how business and personal data is used, transferred and stored by apps
- Implement policies to limit risk of out-of-policy apps
- Use data privacy controls to comply with regulations like GDPR, CCPA and HIPAA

Mobile users can have hundreds of apps on their devices. To be certain that apps don't violate internal or external policies, you need visibility into an app's permissions, communication lines, and potential privacy risks. With this information, you can implement policies across your mobile fleet that protect user data and reduce leakage of corporate data.

## Compliance and privacy standards apply to mobile

Most organizations have visibility into the data transfer and storage practices of laptop and desktop apps, but lack parallel capabilities on mobile. Without insight into mobile apps, security and compliance teams have a massive gap in protecting corporate data used on mobile endpoints. Today's risk management strategies must now include mobile apps and devices. Visibility into mobile app risks is necessary to protect your organization from the risks of data loss and maintain compliance with regulations.

Without the right tools, your security team can't analyze the capabilities, permissions and data access controls of apps used by your employees. Even when using mobile device management (MDM) or mobile application management (MAM) solutions, these approaches don't provide visibility into all the risks and vulnerabilities of native and third-party apps used by employees.

## Build data and compliance policies backed by industry-leading intelligence

Lookout Mobile Risk and Compliance provides your team with the visibility into the capabilities of mobile apps. This enables you to apply organization-wide governance, risk and compliance  policies to mobile endpoints.

Lookout provides unmatched insight into mobile apps. We have analyzed nearly every version of every mobile app in existence. With security telemetry from more than 120 million apps, Lookout analyzes more than a hundred thousand new app binaries every day. At the same time, we use machine learning to auto convict more than 10,000 apps a day. This approach enables Lookout to block risky apps and enables app risk scoring by checking if an app:

- Has access to sensitive data such as contacts or the calendar.
- Communicates with cloud services.
- Sends data to servers in foreign countries.
- Has any risky or malicious SDKs.
- Insecurely transfers or stores data.

You can also implement data-protection controls that will ensure alignment with compliance and privacy standards. Doing so includes being able to:

- Implement mobile data privacy controls, limiting risk of corporate data leakage.
- Create customizable policies that permit or block app use by specific risks .
- Add specific apps and app versions to deny lists.
- Run a risk analysis report for any app or IPA/APK file.

Preserving employee privacy is at the core of Lookout Mobile Risk and Compliance capabilities. If a user has an app that violates policy, Lookout provides guidance to the employee on their device about how to remediate the issue on their own. They will appreciate the discretion in the case that the app may indicate aspects of private life that they may not want to share. While an admin may be alerted in the Lookout console that a device is out of compliance, it won't share the specifics such as the name of the app. This discreet and individual communication and remediation process will greatly increase the likelihood of employees resolving compliance issues on their devices with peace of mind that aspects of their personal lives are not exposed at work.

## 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. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust.

For more information visit
**lookout.com**

Request a demo at
**lookout.com/request-a-demo**

A platform built for mobile from the ground up

Explore the Lookout Platform at **lookout.com/platform**