

# Lookout Mobile Endpoint Security

Visibility into mobile threats & data leakage

## Overview

Many organizations are now embracing the use of smartphones and tablets to increase productivity in the workplace. However, this era of mobility introduces new risks to enterprise data. Lookout Mobile Endpoint Security enables secure mobility by providing comprehensive risk management across iOS and Android devices to protect against app, network, and device-based threats while providing visibility and control over data leakage.

## How It Works

Lookout Mobile Endpoint Security leverages a lightweight endpoint app on employee devices, a cloud-based admin console that provides real-time visibility into threats and data leakage, and integration with leading Enterprise Mobility Management (EMM) solutions.

## Benefits

### Productivity without compromise

We empower your organization to fully adopt secure mobility across personal and corporate owned devices without compromising productivity, employee privacy, or user experience

### Data leakage control

Lookout allows 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, and device

### Proven risk reduction

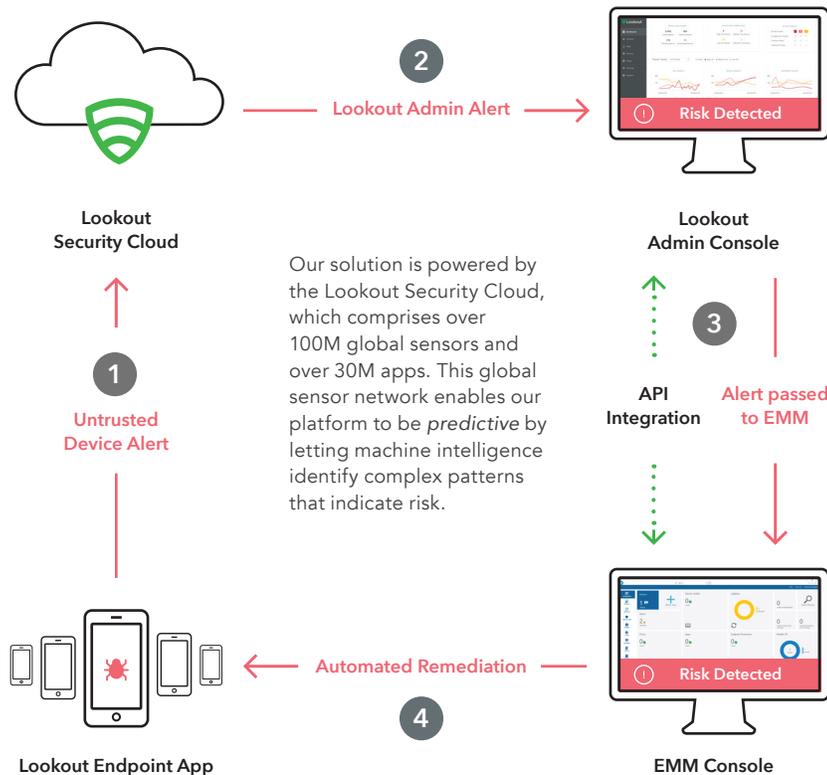
Forward-thinking organizations have achieved measurable risk reduction with Lookout Mobile Endpoint Security

### Low TCO

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

### Respects user privacy

Lookout collects the minimum amount of personal information to protect both personally owned and corporate-owned devices



## Mobile Endpoint Security for Threats

As more sensitive data is accessed by mobile devices, they are increasingly becoming a target for attackers. Lookout Mobile Endpoint Security identifies mobile threats targeting these primary attack vectors:

- App-based threats: Malware, rootkits, and sideloaded apps
- Network-based threats: Man-in-the-middle
- Device-based threats: Jailbroken/rooted mobile devices

## Mobile Endpoint Security for App Risks



Apps that exhibit no sensitive behaviors



Apps that exhibit some sensitive behaviors



Apps that exhibit malicious behaviors

Some iOS and Android apps are not malicious, but they exhibit sensitive behaviors that may leak data, contravening the security policy of an organization or even violate regulatory requirements around data loss. Lookout provides comprehensive visibility into these app risks within your mobile fleet, enabling admins to both monitor and set actionable policies against apps at risk of violating internal or regulatory requirements.

Lookout Mobile Endpoint Security	
<b>Mobile Endpoint Security for Threats</b>	
App-based threat protection	
Malware	
Rootkits	
Spyware	
Sideloaded apps	
Network-based threat protection	
Man-in-the-Middle attacks	
SSL attacks	
Device-based threat protection	
Jailbreak detection	
Root detection	
Custom threat policies	
Threat dashboard	
<b>Mobile Endpoint Security for App Risks</b>	
Data leakage control from apps that:	
Access sensitive data such as calendar or location	
Send sensitive data, such as PII, over the network	
Communicate with cloud services	
Risky apps dashboard	
App risk monitoring	
Custom policies for risky apps	
One-click app blacklisting	
App upload and analysis	
<b>Management and Support</b>	
EMM integration (Intune, AirWatch, MobileIron)	
Exec-level reports showing risk reduction	
Role based access control	
Data Privacy Controls	
24/7 Support	

## The Lookout Difference

- Lookout has amassed one of the world’s largest mobile security datasets due our global scale and mobile focus. This has created a global sensor network of over 100M mobile sensors and 30M apps, with 90K 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 a new era of security solution designed exclusively for this platform. Lookout has been securing mobility 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. To learn how you can secure your mobile fleet today, contact us at [sales@lookout.com](mailto:sales@lookout.com)