Lookout Mobile Endpoint Security

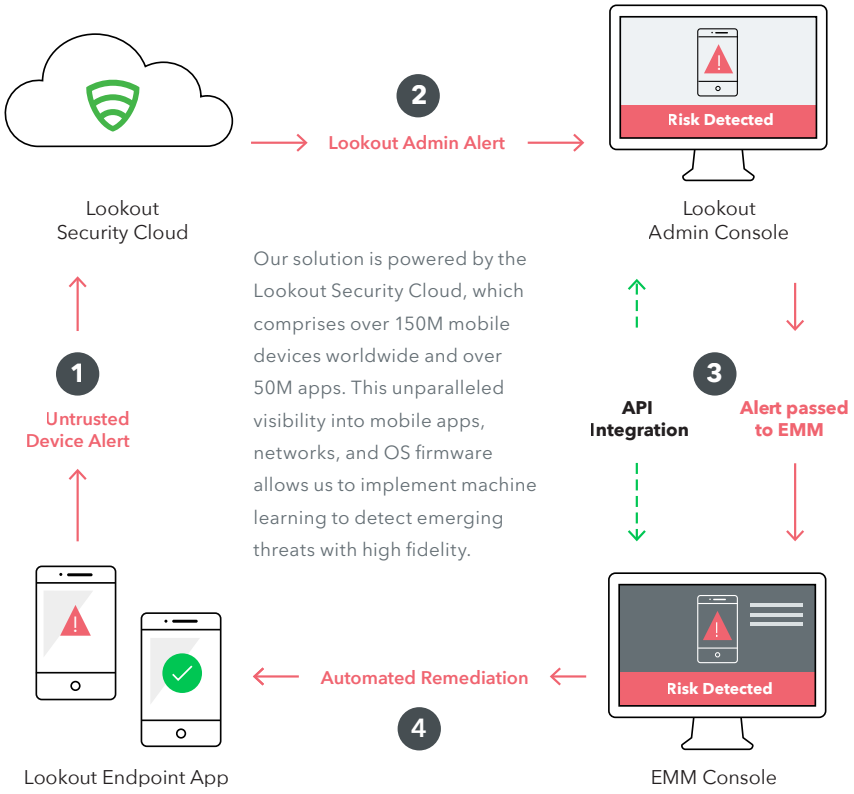
As your data goes mobile, Lookout closes your security gap

Overview

Many organizations are now embracing the use of smartphones and tablets to increase productivity in the workplace, and as more sensitive data goes mobile, your organization's security policies must extend to your mobile endpoint devices. Lookout Mobile Endpoint Security makes it easy to get visibility into the entire spectrum of mobile risk, apply policies to measurably reduce that risk, and integrate into your existing security and mobile management solutions.

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 mobile risk, and integration with leading Enterprise Mobility Management (EMM) solutions.



Benefits

Measurable reduction of risk

Close a large security gap and measure your risk reduction with Lookout's analysis and reporting features

Seamless interoperability

Lookout integrates with all SIEM systems via our Mobile Risk API, including **Splunk, ArcSight, and QRadar**

Visibility into mobile incidents

Get real-time visibility into incidents on mobile devices, so you can respond quickly and effectively

Securely enable mobility

Embrace more flexible mobility programs, including BYOD, to increase employee productivity and stay competitive

Privacy by design

Ensure your data sovereignty and employee privacy policies are upheld using our privacy controls features

Easy to deploy and maintain

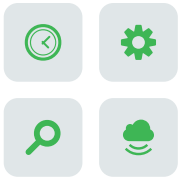
We integrate with any MDM (such as **Intune, AirWatch, MobileIron, MaaS360,** and **BES12**) for simple deployment and management

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:

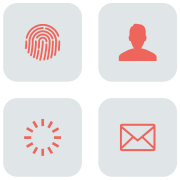
- App-based threats: Malware, rootkits, and spyware
- Network-based threats: Man-in-the-middle attacks
- Device-based threats: Jailbroken/rooted devices, outdated OS, risky device configurations
- Web & Content-based threats: Phishing attacks or malicious websites & files

Mobile Endpoint Security for App Risks



No sensitive behaviors

Some sensitive behaviors



Malicious behaviors

Some iOS and Android apps are not malicious, but they exhibit sensitive behaviors or contain vulnerabilities, 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.

The Lookout Difference

- Lookout has amassed one of the world's largest mobile security datasets due to our global scale and mobile focus. Lookout has collected security data from over 150M devices worldwide and over 50M apps, with up to 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 info@lookout.com.

Lookout Mobile Endpoint Security
Mobile Endpoint Security for Threats
App-based threat protection
Malware
Rootkits
Spyware
Ransomware
Network-based threat protection
Man-in-the-Middle attacks
SSL attacks
Device-based threat protection
Advanced jailbreak/root detection
Operating system vulnerabilities
Risky device configurations
Web & Content-based threat protection
Phishing attacks from any channel
Malicious URLs to risky websites
Custom threat policies
Threat dashboard
Mobile Endpoint Security for App Risks
Data leakage control from apps that:
Access sensitive data, such as calendar
Send sensitive data (PII) externally
Communicate with cloud services
Have insecure data storage/transfer
Risky apps dashboard
Custom policies for risky apps
App blacklisting
Enterprise app review
Management and Support
EMM integration (Intune, AirWatch, MobileIron, MaaS360, BES12)
SIEM integration via Mobile Risk API (Splunk, ArcSight, QRadar)
Exec-level reports showing risk reduction
Role-based access control
Data privacy controls
24/7 Support