



Lookout Mobile Endpoint Security

Understanding mobile risk

With the ability to stay connected from anywhere, tablets and smartphones have become indispensable tools that we use everyday. But our reliance on these devices has also introduced new risks, both to our personal privacy as well as enterprise data.

Mobile threats

Your smartphone, just like your laptop, is susceptible to risk. Mobile devices may be more resilient to some threats, but they are just as vulnerable to others, namely phishing, application, network, and device threats.

Apps that you download and install on your mobile device may contain malicious code or present risks to your corporate or personal information through unsecure data handling practices. Every network your mobile device connects to has the potential to be unsafe. And the devices can be compromised by attackers targeting software vulnerabilities. So what's at risk? Your personal data, including texts, calls, contacts, and photos, as well as work data, including sensitive financial and corporate information.

Why do I need Lookout?

Because your mobile device stores so much sensitive information, it's increasingly becoming a target for cyberattacks. Adding Lookout Mobile Endpoint Security to your mobile device will identify and minimize these threats and make it difficult for an attacker to steal your data.

What does Lookout do

Lookout Mobile Endpoint Security identifies potential threats across the device operating system, apps, network connections, and messages. Lookout compares that data against its AI-driven dataset that includes telemetry from hundreds of millions of devices and apps. When a threat is detected, Lookout alerts your company as well as your user with instructions on how to remediate the issue.

What Lookout doesn't do

Lookout firmly believes that your privacy is as important as your security. This is why we want to be completely transparent about the data we collect to help safeguard your device and the security of each employee. Lookout does not collect the following data types: Image, audio, video files, texts, personal information, or data generated using apps. Lookout for Work app won't impact your phone's performance or interfere with data stored on your device.

Mobile risks

Phishing & Executive Impersonation

Threat actors leverage countless channels to deliver socially engineered phishing attacks. They even pretend to be a company executive to further convince targets to fall victim to their attacks.

Malware and risky apps

Any app installed to a mobile device could present a risk to your data, whether it's risky data handling practices or outright malicious behavior.

Malicious networks

Mobile devices can easily connect to any network, whether its at a coffee shop or your home Wi-Fi. This means your data could be exposed to any risk associated with these networks.

Compromised devices

Out of date operating systems or software vulnerabilities can lead to your device being exploited.

© 2024 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design® and the Lookout multi-color/multi-shaded Wingspan Design® are registered trademarks of Lookout, Inc. in the United States and other countries. DAY OF SHECURITY®, LOOKOUT MOBILE SECURITY®, and POWERED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States. Lookout, Inc. maintains common law trademark rights in EVERYTHING IS OK, PROTECTED BY LOOKOUT, CIPHERCLOUD, and the 4 Bar Shield Design.

Lookout Mobile Endpoint Detection and Response (EDR)

Grant security teams
previously unseen visibility
into security threats



Don't let threat actors hide in your mobile blind spot

While many organizations have comprehensive activity monitoring for servers, desktop and laptop computers, they lack the same telemetry for iOS, Android, and Chrome OS endpoints. As employees have increased their use of mobile devices for work, attacks on these devices have increased.

The traditional kill chain is modernizing, and threat actors exploit the mobile edge to compromise organizations since security teams don't have insight into these everyday devices. Without visibility into active threats, exploitable vulnerabilities, and passive risk that mobile devices inherently represent, security teams cannot effectively mitigate the risk of a data breach.

Proactive threat hunting enhances your mobile security strategy

The increase in frequency and cost of cybersecurity breaches has driven an increased need to understand all potential points of risk and how attackers might exploit them. Hunting for these threats and tracking threat actors is a critical piece of keeping your organization safe.

Benefits

- Enable your SOC to analyze and protect the mobile edge
- Integrate mobile data into your SIEM, SOAR, EDR, or XDR
- Gain visibility into vulnerabilities, threats, and risks within your mobile fleet
- Streamline acceptable use policies across all employee endpoints
- Identify cross-platform attacks and contain the incident at the endpoint
- Proactively hunt for threats with the world's largest mobile security dataset

Cyberattacks that result in a data breach rarely occur in a single event. Cyberattackers will work slowly and silently to identify vulnerabilities, steal credentials, insert malicious code like ransomware, or exfiltrate data. Once attackers have identified their plan of action, these attacks can take no more than an hour to execute.

Rapidly analyze real-time telemetry data to stop breaches

To deliver our behavior-based threat protection capabilities, Lookout analyzes thousands of telemetry data points collected from more than 210 million iOS, Android, and Chrome OS endpoints. We are the experts at identifying indicators of compromise necessary to detect and respond to mobile threats both globally and within your organization's mobile fleet.

Key Capabilities

Analyze all endpoints in one place

Integrate security telemetry from the Lookout Mobile Endpoint Security (MES) app running on employee devices into your SIEM, SOAR, XDR, or EDR via our Mobile Intelligence APIs. This enables security teams to analyze mobile exposure, understand data risks, and detect potential exploits in the context of their greater endpoint security strategy.

Detect and respond to threats with ease

Set up rule-based policies to automate rapid responses when malicious activity is detected. By using either Lookout preset policies or custom policies that you define, take immediate action that is in line with your organization's incident response policies.

Correlate activity across your environment

Monthly threat research reports detail the latest threat actor activity providing indicators of compromise (IOCs) in STIX format and Mitre TTPs in JSON. Implement this data into your existing security solutions to identify shared infrastructure and tactics that could indicate threat actor activity on other endpoints.

Investigate incidents

Perform threat and forensic analysis to trace an attack through each phase of the kill chain. Cross-vector search capabilities quickly identify how attackers are moving

laterally through your organization. Answer the big questions about where the attacker went, what they did, and how they did it. This enables you to model the necessary changes to prevent an attack from recurring.

Contain the incident at the endpoint

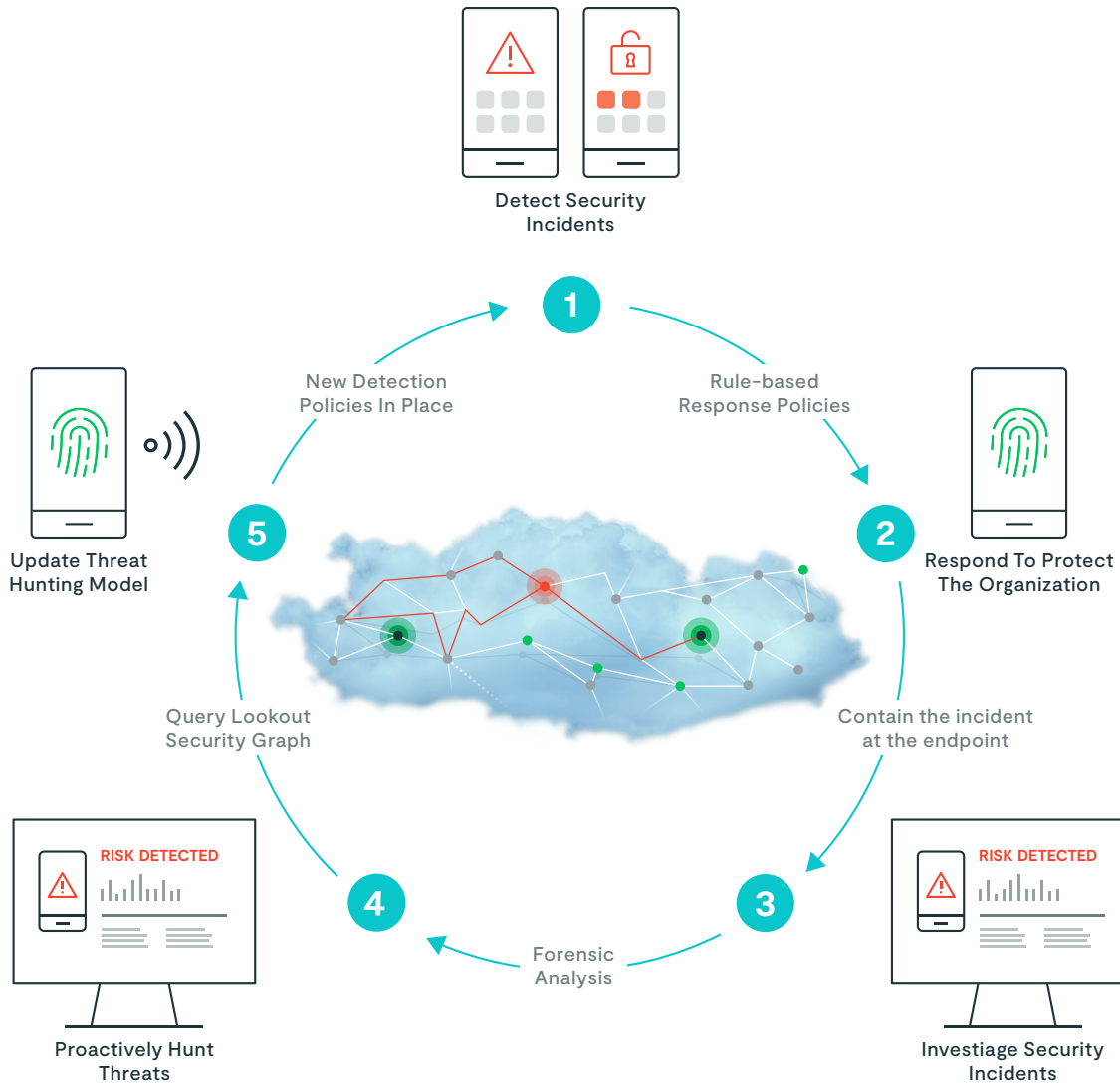
Once a threat is detected on the device, the Lookout platform can immediately quarantine the endpoint, whether managed or unmanaged, stopping connections to the internet or specific domains and apps.

Proactively hunt for threats

With the world's largest dataset of mobile threat telemetry at your fingertips you can analyze global threats and threat actor activity, expanding the reach of your proactive threat hunting. Run queries and perform advanced analytics from our EDR console to unlock deep insights.

Provide remediation guidance

Lookout provides easy-to-follow instructions for users to remediate risks on mobile devices. 95% of threats detected by Lookout are self-remediated by users without involving IT or security operations





About Lookout

Lookout, Inc. is the data-centric cloud security company that uses a defense-in-depth strategy to address the different stages of a modern cybersecurity attack. Data is at the core of every organization, and our approach to cybersecurity is designed to protect that data within today's evolving threat landscape no matter where or how it moves. People — and human behavior — are central to the challenge of protecting data, which is why organizations need total visibility into threats in real time. The Lookout Cloud Security Platform is purpose-built to stop modern breaches as swiftly as they unfold, from the first phishing text to the final cloud data extraction. We are trusted by enterprises and government agencies of all sizes to protect the sensitive data they care about most, enabling them to work and connect freely and securely. To learn more, visit www.lookout.com and follow Lookout on our [blog](#), [LinkedIn](#) and [X](#).

For more information visit
lookout.com

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

© 2025 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design® and the Lookout multi-color/multi-shaded Wingspan Design® are registered trademarks of Lookout, Inc. in the United States and other countries. DAY OF SHECURITY®, LOOKOUT MOBILE SECURITY®, and POWERED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States. Lookout, Inc. maintains common law trademark rights in EVERYTHING IS OK, PROTECTED BY LOOKOUT, CIPHERCLOUD, and the 4 Bar Shield Design.