Lookout

MOBILE ENDPOINT DETECTION AND RESPONSE (EDR)

HUNT FOR THE LATEST THREATS IN YOUR MOBILE FLEET WITH LOOKOUT MOBILE ENDPOINT SECURITY

Add threat hunting and incident response to your mobile security strategy

Cyberattacks that lead to data breaches are rarely composed of a single event. Cyberattackers will work methodically and silently to conduct recon, identify vulnerabilities, steal credentials, move laterally, and exfiltrate data or insert malicious code like ransomware. These steps take place across multiple endpoints, and over many weeks or months.

To combat these sophisticated threat campaigns, security teams have adopted endpoint detection and response (EDR) solutions to maintain situational awareness by continuously monitoring endpoint telemetry. This enables proactive threat hunting and kill chain reconstruction in the event of an incident. However, traditional EDR products typically only provide coverage for fixed endpoints like desktops and laptops. As enterprises rapidly adopt mobility initiatives and bring-your-own-device (BYOD) programs, security teams are left with gaps in the visibility that feeds their EDR strategies.

Mobile has opened new opportunities for cybercriminals

While many organizations have comprehensive monitoring for servers, desktops and laptops, they lack the same visibility for iOS, Android and Chrome OS endpoints.

BENEFITS

- Stop breaches that exploit mobile devices.
- Provide comprehensive mobile threat protection.
- Rapidly detect and respond to mobile threats.
- Investigate mobile app security incident forensics.
- Hunt for mobile app threats and unwanted risks.
- Take proactive action to protect your users.
- Provide guidance for remediation.

As employees use mobile devices to access and share sensitive data more frequently, those devices are becoming attractive targets for threat actors. For instance, 20% of enterprise mobile devices were exposed to a mobile phishing attack in 2021. This is nearly double the rate from 2020.

To empower security teams to stop data breaches, organizations need the same comprehensive monitoring for mobile endpoints that they have for traditional endpoints. Without filling this mobile endpoint visibility gap, security teams are left with blind spots when it comes to incident response, kill chain reconstruction, and proactive threat hunting.

Rapidly analyze real-time telemetry data to stop breaches

To enable SOCs to detect and respond to mobile incidents, Lookout analyzes thousands of data points collected from over 200 million iOS, Android and Chrome OS devices. We provide comprehensive protection against mobile phishing and malicious web content, risky iOS and Android apps, untrustworthy network connections, and device compromise.

Our mobile EDR solution leverages a streaming detection engine to analyze telemetry and detect anomalous behavior based on a set of policies that administrators can configure. The resulting detections drive response and remediation actions through both the Lookout agent and a collection of available integrations.

When an incident occurs, the Lookout console provides analysts with tools to conduct incident response investigations. For mobile app incidents, this includes the ability to write complex queries over Lookout's unmatched mobile security graph that has analyzed over 165 million apps. This ability to turn data into intelligence enables security teams to understand the extent and impact of an incident and determine if there is a larger campaign or adjacent threats. Answering these questions empowers them to contain the incident, stop a data breach and make proactive changes to prevent the attack from happening again.

Capabilities of Lookout Mobile EDR

Detect and respond to threats with ease

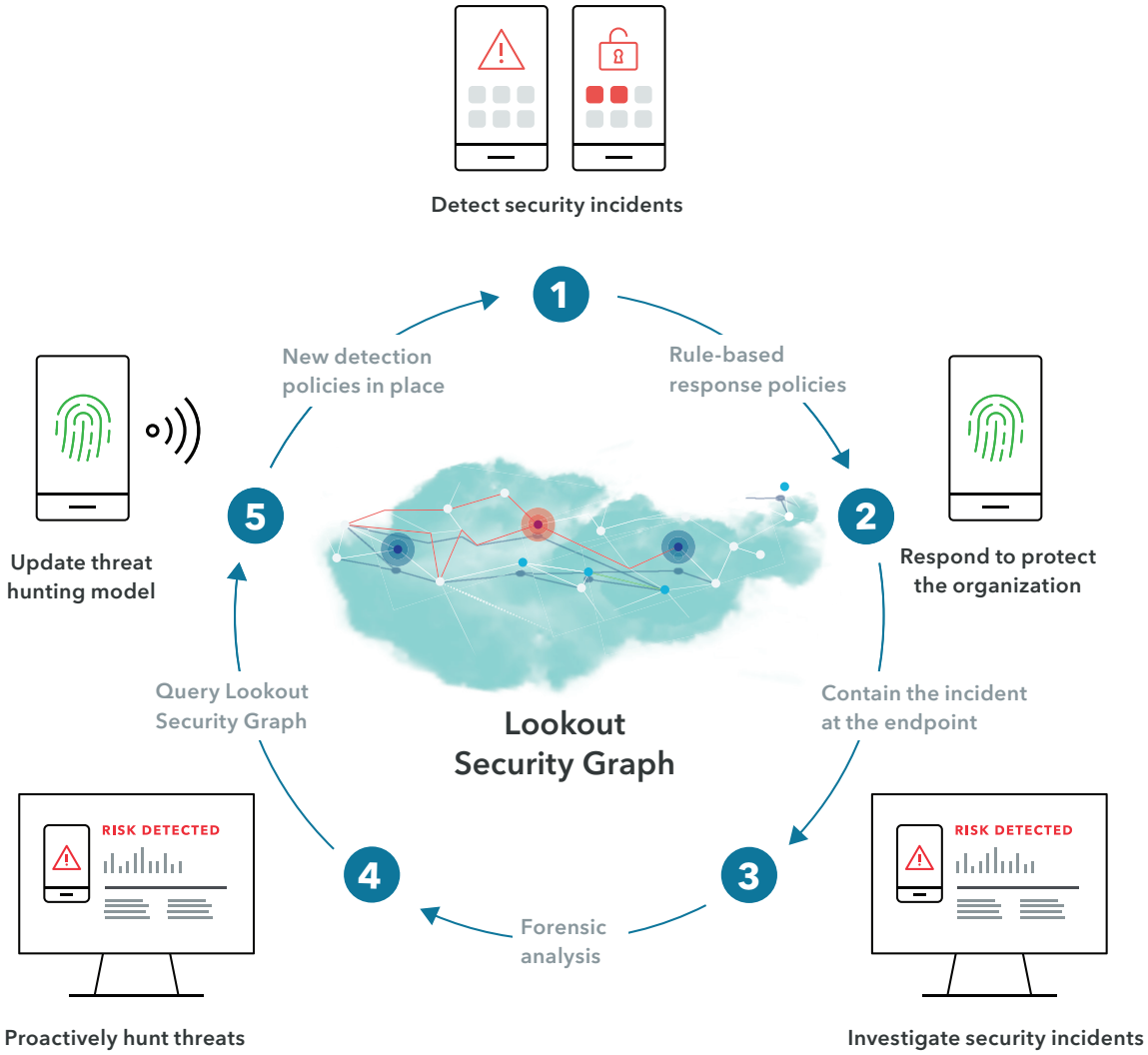
Set up rule-based policies to automate rapid responses when anomalous activity is detected. By using Lookout's preset policies in addition to custom policies that you develop, you can augment your mobile security policies based on data discovered in your threat hunting and investigation processes.

Investigate incidents and hunt for threats

Mobile EDR with Lookout Mobile Endpoint Security grants access to the world's largest mobile security analysis dataset. This enables you to query the Lookout global dataset in the context of your mobile fleet to build proactive protection policies, improve your threat hunting workflow, and quickly identify how attackers leverage sophisticated campaigns to target your organization. This enables you to model the necessary changes to prevent an incident from recurring.

Contain the incident at the endpoint

Once an incident is detected on the device, the Lookout platform can immediately quarantine the endpoint, regardless of if it's managed or unmanaged. Policies can also stop connections to the Internet or specific company domains and trigger additional remediations through a collection of available integrations such as Intune, Workspace One, Google, and MobileIron.


Detect security incidents
1
Rule-based response policies
2
Respond to protect the organization
Contain the incident at the endpoint
3
Investigate security incidents
RISK DETECTED
Forensic analysis
4
Proactively hunt threats
RISK DETECTED
Query Lookout Security Graph
5
Update threat hunting model
New detection policies in place
Lookout Security Graph

About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud 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. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, VMware, Vodafone, Microsoft, Google, and Apple.

For more information visit
lookout.com

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

Lookout®