Mobile Endpoint Detection and Response (EDR) with Lookout MES

Hunt for the latest threats on your mobile devices

Add proactive threat hunting to your mobile security strategy

With the increase in frequency and cost of cybersecurity breaches, security teams have shifted their focus from protect-the-endpoint to protect-the-data. In addition to blocking malware, your team needs tools to investigate file-less cyberattacks that do not use malware, and insider threats. An example is when an attacker uses credentials stolen through a phishing scam to exfiltrate data.

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. These steps take place across multiple endpoints, and over many weeks or months.

Mobile has opened new opportunities for cybercriminals

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.

Benefits

- Rapidly detect and respond to mobile threats
- Detect attacks that don't use malware
- Stop breaches that use stolen credentials
- Perform security incident forensics
- Contain the incident at the endpoint
- Provide guidance for remediation
- Proactively hunt for threats

To be effective at stopping data breaches, security teams need the same comprehensive data for mobile endpoints that they have for servers, desktops and laptops. Because mobile operating systems never permitted kernel access and required apps to operate in isolation, it had been incorrectly assumed that collecting comprehensive telemetry was not possible.

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 over 215 million iOS, Android, and Chrome OS endpoints running our lightweight app. We are the experts at identifying indicators of compromise necessary to detect and responding to mobile threats.

Our mobile endpoint detection and response console presents this device and app telemetry data for your mobile fleet in a way that you can easily query. This console also enables you to search the continuously updated results of our analyses of malicious and phishing websites.

Searching within this comprehensive mobile endpoint security graph enables security teams to understand if an active attack involves mobile devices, where the attacker is and what they are doing. Answering these questions empowers them to contain the attack, prevent a data breach and model the necessary changes to prevent the attack from happening again.

Capabilities of Mobile EDR

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, you can leverage Modern Endpoint Protection on the Lookout Cloud Security Platform to take immediate action that is in line with your organization's incident response policies.

Investigate incidents

Our intuitive and easy-to-use EDR console enables you to 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

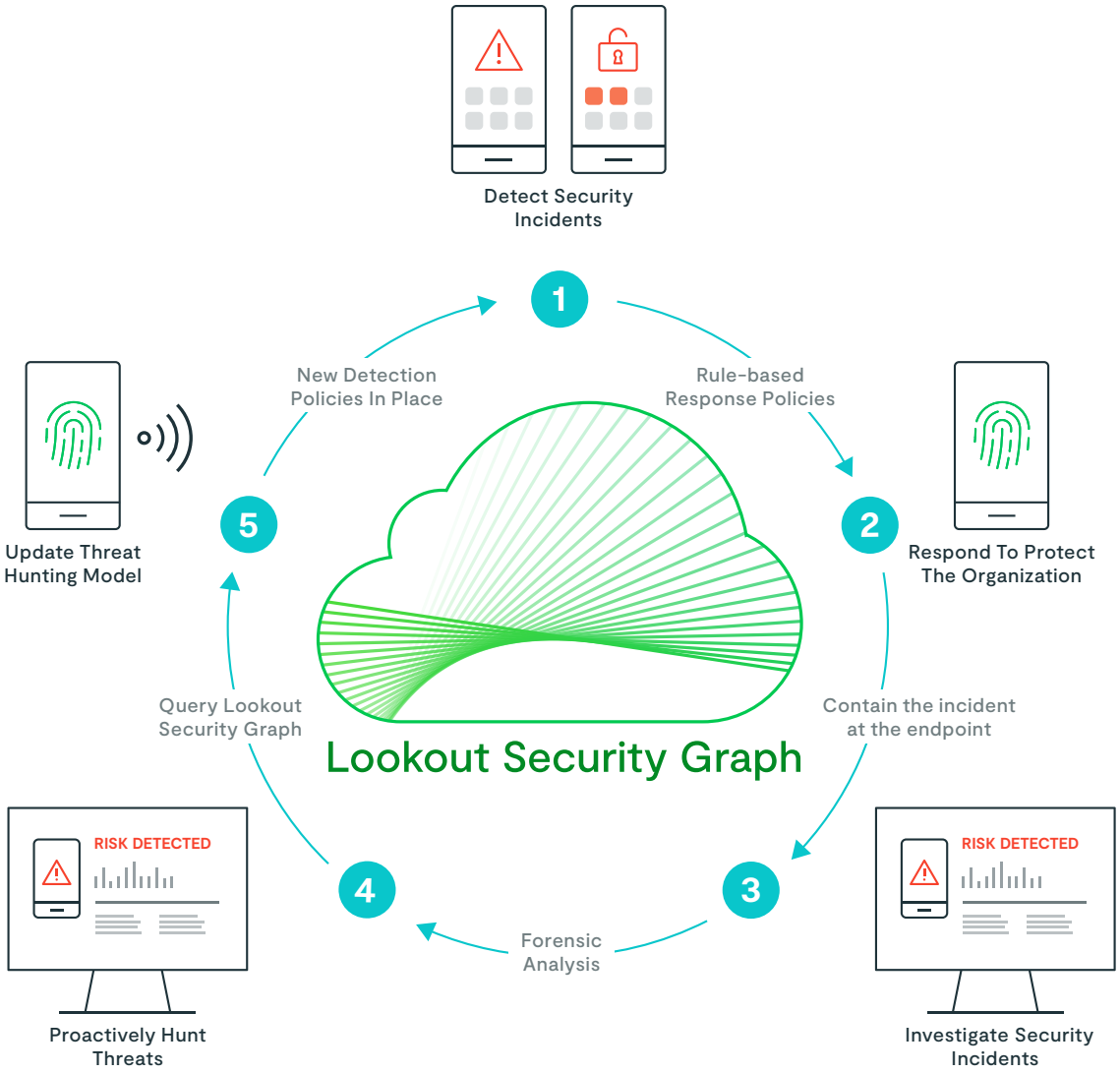
Once a threat is detected on the device, the Lookout platform can immediately quarantine the endpoint, whether managed or unmanaged, stopping connections to the internet or specific company domains.

Hunt for threats proactively

With the world's largest dataset of mobile threat telemetry at your fingertips, you can query our global dataset, or dive into your own environment, 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.


Detect Security Incidents
1
Rule-based Response Policies
2
Respond To Protect The Organization
Contain the incident at the endpoint
3
RISK DETECTED
Investigate Security Incidents
Forensic Analysis
4
RISK DETECTED
Proactively Hunt Threats
Query Lookout Security Graph
5
Update Threat Hunting Model
New Detection Policies In Place
Lookout Security Graph

About Lookout

Lookout, Inc. is the endpoint to cloud security company purpose-built for the intersection of enterprise and personal data. We safeguard data across devices, apps, networks and clouds through our unified, cloud-native security platform — a solution that's as fluid and flexible as the modern digital world. By giving organizations and individuals greater control over their data, we enable them to unleash its value and thrive. Lookout is trusted by enterprises of all sizes, government agencies and millions of consumers to protect sensitive data, enabling them to live, work and connect — freely and safely. To learn more about the Lookout Cloud Security Platform, visit www.lookout.com and follow Lookout on our blog, LinkedIn, and Twitter.

For more information visit
lookout.com

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