Mobile EDR for MSSPs

Close your customer's mobile security gap with the industry's leading mobile endpoint detection and response (EDR) solution, built with native multitenancy to simplify and streamline service delivery.

Empowering MSSPs to Stop Mobile Threats and Meet Compliance for Customers

As part of the Lookout Cloud Security Platform, Lookout Mobile Endpoint Security empowers MSSPs to protect their customers from mobile threats including phishing attacks, apps threats, device exploits, and risky networks. Lookout also enables the proactive enforcement of compliance policies based on the NIST Cybersecurity Framework to address GDPR, CCPA, HIPAA, and other regulations.

Designed for MSSPs with Native Multitenancy to Simplify and Scale Management

We know that managing security to address evolving security threats across different customers can be time consuming and that protecting customer privacy is important. This is why we have designed our solution with multi-tenancy, built-in workflows, and privacy-mode, so that service delivery is simple, seamless, and private. From a single console, you can manage security policies across all your customers, saving you time while ensuring consistency.

Snapshot: Mobile Threats

- Phishing: SMS, email, messaging apps, and malicious websites
- Apps: Malware, including surveillanceware, ransomware, and spyware, and risky sideloaded apps, including apps that leak data to foreign countries
- Devices: Device jailbreaks/roots, privilege escalation, and OS vulnerabilities
- Network: Man-in-the-middle attacks, hostile networks, including unsecure Wi-Fi

Mobile is increasingly becoming the primary attack vector for cybercriminals because it provides a silent, highly distributed entry point into organizations. Whether it is a phishing attack, spyware, operating system vulnerability, or zero-day threat, Lookout empowers you to detect and respond to these threats, improve your customer's mobile security posture, and ensure you meet their compliance requirements.

Key Benefits

- Reduces risk of a data breach from mobile threats, including phishing, ransomware, and exploitation of device and app vulnerabilities.
- Eases delivery of mobile security as part of your existing managed services stack through zero-touch deployment and seamless integrations with MDM, SIEM, and IDP solutions.
- Reduces security policy administration time by 80% by enabling administrators to centrally define policies and propagate them to all customer tenants with just a few clicks.
- Alleviates 95% of mobile security support issues by enabling users to self-remediate threats, uses only 1-3% of their device's battery, and increases security awareness with threat detection information.
- Provides two competitive solution bundles supported by three flexible commercial models to match your specific business need.

Delivering the Industry's Most Advanced Mobile EDR

Lookout provides detection and response across the four primary categories of mobile threats — phishing and content, apps, device exploits, and network attacks. These attacks know no limits and seek to exploit corporate resources to gain access to sensitive data.

Our solution is powered by the world's largest mobile telemetry from over 200 million devices, 180 million apps, and millions of URLs ingested everyday.

Protection alone isn't enough.

Having protection for endpoints is a great start, but not every attack starts with something malicious. You need to be able to hunt down the file-less attacks, regardless of which endpoint it comes from.

Every employee has a mobile device.

If you only have EDR for your traditional endpoints, you will miss all the attacks that originate from mobile devices, leaving your organization with a critical security gap.

Traditional EDR doesn't work on mobile.

Mobile operating systems never permitted access to their kernel and require apps to operate in isolation. The traditional approach based on perimeter networks and content inspection no longer works.

Key Solution Capabilities

Comprehensive Mobile EDR

Lookout Mobile Endpoint Security provides comprehensive real-time protection against all mobile threats across all iOS, Android, and Chrome OS devices. We stop known and unknown phishing attacks, protect against malicious apps, device exploits, and risky networks. We do all this while enabling end users to self-remediate security issues, greatly alleviating the need for you to support end users.

Proactive Analysis and Compliance Policy Enforcement

Lookout enables you to proactively assess the risk of your customer's mobile devices and apps and reduce risk to their organizations. Our powerful app vetting capability enables you to set policies to block apps that violate corporate policy and industry regulations. You also get full visibility into outdated device OS versions and security patch levels to eliminate vulnerabilities.

These advanced capabilities along with our core mobile protections, help organizations address compliance set forth in frameworks and regulations including NIST, CIS Controls, Mitre Att&ck, ISO 27001, HITRUST, CMMC, HIPAA, GDPR, Cyber Essentials, and others. For more information on how we address privacy compliance, visit our privacy and compliance page.

Risk-Based Continuous Conditional Access

Lookout Mobile Endpoint Security continuously monitors the risk level of mobile devices and passes this information to your customer's mobile device management (MDM) solution for policy enforcement. In this way, you can reduce the risk of a compromised device gaining access to your customer's sensitive data.

We can integrate with any MDM but have preset integrations with Microsoft Endpoint Manager, Google Workspace, VMware Workspace ONE, Ivanti, IBM MaaS360, Jamf Pro, SOT MobiControl, Citrix, and BlackBerry.

Solution Bundles

Lookout provides two options to fit the way you want to work:

- The **Essentials** bundle enables you to protect your customers from the four primary mobile threat vectors - phishing, device, app, and network threats.
- The **Advanced** bundle not only provides all the protections in Essentials but also enables you to perform more proactive analysis of your customer's mobile fleet. With this level of analysis, you can enforce compliance policies to meet industry requirements and further reduce risk for your customers. The Advanced bundle provides the most insight and is best for supporting customers in regulated industries.

Capabilities	Essentials	Advanced
Detect and block malware like rootkits, spyware, and ransomware	■	■
Detect unauthorized camera and microphone access from surveillanceware	■	■
Detect and prevent credential theft and data exfiltration through network attacks	■	■
Detect device compromise (root / jailbreak)	■	■
Detect and block phishing attempts	■	■
Web content filtering	■	■
Multitenancy view for MSSPs	■	■
EMM Integration/conditional access (Intune, WS1, Ivanti, MaaS360, Jamf, XenMobile, BES12)	■	■
SIEM Integrations (Splunk, ArcSight, Qradar, Azure Sentinel)	■	■
Mobile risk API for workflow automation	■	■
Mobile app reputation services		■
Manage allow or deny lists of apps based on behavior and capabilities (e.g. TikTok)		■
Public and private app upload and analysis		■
Risky apps dashboard		■
Detect and manage app and OS vulnerabilities		■
Advanced PCP / DNS privacy and protection (Secure DNS)		■

Flexible Commercial Models

We understand your need for flexible commercial models, so we provide the following three options:

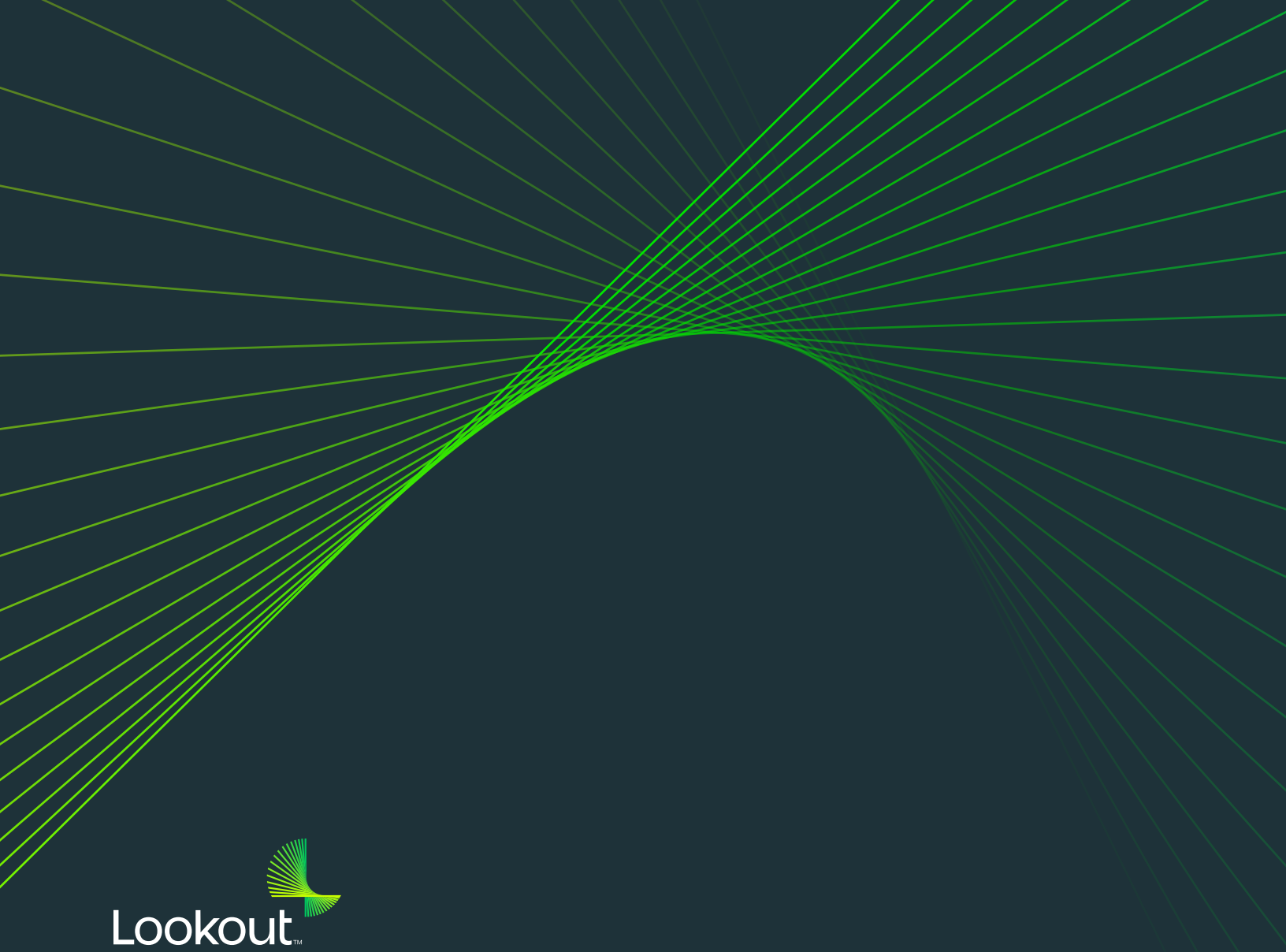
- 12 Month commit, paid upfront
- 12 Month commit, paid monthly
- 1 Month commit, paid monthly

Enablement

We understand that you need to be self-sufficient when it comes to marketing, sales, deployment, and support. So we provide you the tools and content to create your own sales and marketing campaigns, to implement mobile EDR, and provide ongoing SOC and support services. The Lookout Partner Hub is your central portal where you will find all these resources including campaigns-in-a-box, collateral, video tutorials, and more.

Getting Started with Us

To become a partner, visit lookout.com/partners/mssp, or email us at partners@lookout.com.



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