Fact sheet

Lookout Mobile Endpoint Security

Available through the Verizon Business Marketplace.



Why Verizon Business Marketplace?

A smarter way to buy software: Help streamline your tech stack with a platform designed for modern business needs.

- **The all-in-one advantage:** A true one-stop destination for software designed to help your essential daily operations.
- **Seamless compatibility:** Curated applications to help ensure smooth integration across your network.
- **Administrative ease:** Help reduce overhead with unified software vendor management and a single bill.
- **Effortless procurement:** Help simplify how you find, buy and deploy the software tools your team needs to get work done.

What it is

Phones are computers. Lookout secures them like it.

Lookout Mobile Endpoint Security protects every smartphone and tablet in your business from the threats that hit mobile hardest: phishing and smishing links, malicious apps, risky Wi-Fi and compromised devices. It stops AI-powered scams too, including texts that impersonate your executives.

It's a lightweight app for iOS and Android, managed from the cloud. It works on company-owned and personal phones, with or without an MDM, and never reads personal messages, photos or content.

What problem does it solve?

Your business runs on mobile. So do today's attacks.

Email, banking, payroll approvals, customer records and AI tools all live on the phone, and the same phone texts family and scrolls social media. Attackers know it. They send texts that look like your bank, a delivery service or your CEO, hide spyware inside apps and wait on public Wi-Fi. Device management and laptop security weren't built to stop those attacks:

#1 target for attacks outside a secure corporate network: mobile devices.[1]

62% of confirmed breaches involve a human element.[2]

39% clicked a malicious link in smishing tests.[3]

verizon business

What Lookout stops:

The problem	How Lookout solves it
Phishing and smishing	Blocks malicious links in texts, messaging apps, email and browsers before anyone clicks.
Malicious apps	Detects spyware, trojans and apps with risky behavior.
Risky networks	Flags man-in-the-middle attacks and unsafe public Wi-Fi.
Device compromise	Detects jailbreaks, rooting, outdated software and risky settings.
Executive impersonation	Flags fraudulent texts posing as company leaders, including AI-generated ones.
No security team	Detection and blocking are automatic, and employees get clear steps to fix issues themselves.

Competitive positioning

Your MDM manages devices. Lookout secures what it can't see.

Most businesses assume their MDM or their laptop security already covers phones. It doesn't. Those tools manage settings and protect desktops. Lookout was built to stop the attacks that happen on a phone.

Why Lookout:

Mobile-first: More than 15 years focused on mobile security. Built for iOS and Android threats, not a desktop tool adapted for the phone.

Unmatched intelligence: Powered by more than 230 million protected devices and 400 million apps analyzed. Lookout researchers helped uncover Pegasus spyware on iOS.

Stops the attacks that happen on phones: Message-level protection against phishing, smishing and executive impersonation that many desktop-first security tools don't provide.

No security team required: Detects and blocks automatically, so lean IT teams are protected from day one without an analyst watching alerts.

Works with what you have: Integrates with leading MDM/UEM platforms such as Microsoft Intune and Workspace ONE, plus SIEM tools or runs on its own.

Privacy on personal phones: Protects BYOD devices without reading personal messages, photos or content.

Carrier-trusted: Used and sold by the largest telco carriers across five continents.

Price plans

Simple per-device pricing, billed monthly on your Verizon account. One license covers one smartphone or tablet.

Plan	Verizon SKU	Price	Best for
Essentials	MES-E-PD	$2.50/ device/mo	Businesses with an MDM or SIEM that want central visibility and policies by group.
Advanced	MES-A-PD	$3.50/ device/mo	Businesses that need control over risky apps and compliance reporting.
Premium	MES-P-PD	$14.40/ device/mo	Organizations with a security team extending threat hunting and forensics to mobile organizations with a security team extending threat hunting and forensics to mobile.

- **Social engineering protection:** included in Premium; optional add-on for Advanced.
- **Volume discounts:** Available for 1,000+ licenses on select plans.

Comparison of plans

Every plan includes everything in the plan before it, then adds more. Customers can start small and step up as their needs grow, with no rip-and-replace.

- **Essentials:** A unified incident view, security policies by user group, fleet-wide vulnerability analysis and MDM and SIEM integrations. Core mobile threat defense: phishing and smishing protection, malicious app and device threat detection, network protection and web content filtering. No MDM required.
- A**dvanced:** Adds deep app analysis, automated policy escalation, custom employee alerts and threat feed integration. Social Engineering Protection available as an add-on.
- **Premium:** Adds Social Engineering Protection, proactive threat hunting, forensic investigation tools and comprehensive threat intelligence reporting.

verizon business

Features

Capability	Essentials	Advanced	Premium
Core threat defense			
Web Protection & Anti-Phishing: SMS, WhatsApp and email across all channels.	✓	✓	✓
Blocking Malicious Connections: C2 servers, malicious QR codes, harmful plugins.	✓	✓	✓
DNS Privacy & Protection: Encrypted, secure domain name resolution.	✓	✓	✓
Proactive Smishing Alerts: Warns on malicious SMS/RCS links before they're clicked.	✓	✓	✓
Device Integrity Monitoring: Detects root and jailbreak attempts.	✓	✓	✓
Content Filtering: Customizable web filtering policies for corporate devices.	✓	✓	✓
Device Vulnerability Management: Flags outdated OS and risky configs to reduce attack surface.	✓	✓	✓
Network Security: Detects MITM attacks and suspicious public Wi-Fi.	✓	✓	✓
Mobile App Malware Visibility: Spyware, trojans and botnet protection.	✓	✓	✓
Fleet management and visibility			
Unified Incident Visibility (EDR): Centralized “Issues” view of device, network and app threats.	✓	✓	✓
Dynamic Security Policies: Segment users into groups with tailored policies.	✓	✓	✓
Fleet Vulnerability Analysis: CVE summary mapped across the entire mobile fleet.	✓	✓	✓
Enterprise Integrations: MDM (Intune, Workspace ONE) + SIEM / SOAR / XDR export.	✓	✓	✓
Advanced response and control			
Deep Application Analysis: Flags risky app behavior: clipboard, contacts, cloud access.	●	✓	✓
A**utomated Policy Escalation:** Timeout-triggered responses for unremediated devices.	●	✓	✓
Personalized Corporate Alerts: Org-specific instructions and support links in user alerts.	●	✓	✓
Threat Feed Integration: Ingest custom prohibited-domain block lists via API.	●	✓	✓
Social Engineering Protection: Executive impersonation and AI-based smishing defense.	●	Add-on	✓
SOC and threat intelligence			
SOC-Ready Research Capabilities: Proactive threat hunting and forensic incident response.	●	●	✓
Comprehensive Threat Intelligence: World's largest mobile dataset, exec summaries and reports.	●	●	✓
Forensic Investigation Tools: Link incidents and IOCs to global campaigns and kill chains.	●	●	✓
Proactive Breach Protection: Global threat hunting with instant policy push.	●	●	✓
Advanced Artifact Mapping: Access to technical mobile IOCs.	●	●	✓

✓ **Included** ● **Not included** **Add-on:** Optional purchase

verizon business

What's included?

Every plan includes:

- The Lookout app for iOS and Android smartphones and tablets.
- Phishing and smishing protection across texts, messaging apps, email and the web.
- Detection of malicious apps, risky networks and compromised devices.
- Web content filtering and encrypted DNS protection.
- Alerts for outdated operating systems and risky device settings.
- Protection for company-owned and personal devices, with employee privacy built in.
- One charge on your Verizon bill.
- Fleet visibility, group policies and MDM/SIEM integrations.

Higher plans add

Advanced: deep app analysis, automated response and custom threat feeds.

Premium: Social Engineering Protection, threat hunting, forensics and threat intelligence reporting.

What customers need

An active Verizon Business account and an email address for the welcome email. No MDM required.

Billing

One account-level charge on the Verizon bill, not tied to a phone number. The license count doesn't have to match the number of lines. Licenses can protect devices on any carrier.

Deployment options

Set-up	What happens
With an MDM (fastest)	The app installs silently through the MDM. Employees register with one tap.
No MDM	No device enrollment needed. Employees download Lookout from the App Store or Google Play and register with one tap.



How to get it?

1. Visit the Verizon Business Marketplace at verizon.com/business/shop/marketplace/lookout or contact your Verizon Business representative.
2. Choose a plan and the number of licenses (one per smartphone or tablet).
3. Check out with your Verizon Business (My Business) account.
4. Your admin receives a welcome email with activation steps within 24 to 48 hours.
5. Employees install the Lookout app and activate it with one tap. With an MDM, the app can be pushed to devices silently.

1. Source: Lookout Threat Intelligence
2. Source: Verizon Data Breach Investigations Report
3. Source: Verizon Mobile Security Index

© 2026 Verizon. VZFS4551026

verizon business