Lookout Mobile Endpoint Security

Von Grund auf für Mobilgeräte entwickelt

Mobilgeräte sind immer dabei, vom Aufwachen bis zum Schlafengehen. Sie bilden die Schnittstelle zwischen Ihrer Arbeit und Ihrem persönlichen Leben.
Lookout wurde speziell für Mobilgeräte entwickelt und bietet Sicherheit, die Sie immer und überallhin begleitet.

Unbegrenzte Möglichkeiten für Schutz, Erkennung und Reaktion

Wir haben Mobile Endpoint Security speziell entwickelt, um Ihre sich ständig weiterentwickelnden Anforderungen an die Sicherheit von Mobilgeräten zu erfüllen. Lookout verfügt über eine graphenbasierte Architektur und lässt sich auf Hunderttausende von Geräten mit Cloud-Modulen skalieren, die auf Ihre Anforderungen ausgerichtet sind.

Egal, ob Ihre Mitarbeiter Apps mit Malware herunterladen, sie mit Ransomware in Berührung kommen oder von Phishing betroffen sind: Ihr Personal ist geschützt, ohne dass Sie einen Finger rühren müssen. Liegt eine Bedrohung oder ein Angriff vor, stellen wir Schritt-für-Schritt-Anleitungen zur Verfügung, um den Vorfall zu untersuchen und zu beheben.

Lookout bietet drei Bundles an, die auf das Anforderungsprofil Ihrer Mobilnutzung abgestimmt sind.

Vorteile der Lookout Security Platform

- Mobile Sicherheit aus der Cloud
- Schützt iOS, Android und Chrome
- Für die Prozessor-Performance und Akkulaufzeit optimierte, schlanke App
- Schützt firmeneigene und Mitarbeitergeräte
- Erfüllt Compliance-Anforderungen und schützt die Privatsphäre
- Nahtlose Bereitstellung auf allen Mitarbeitergeräten

Plattform-Bundles	Was die Bundles enthalten
Small Business	Mobile Sicherheit beruhend auf der gleichen Plattform, wie sie auch Weltkonzerne nutzen, angeboten als intuitiver, sofort einsatzbereiter Dienst für Kleinunternehmen zum Schutz ihrer Mitarbeiter.
Essentials	Essentials umfasst zwei Module, Modern Endpoint Protection und Phishing & Content Protection für die Geräte, die Ihre Mitarbeiter am häufigsten nutzen.
Advanced	Advanced erweitert den Funktionsumfang von Essentials um tiefgründige Erkenntnisse und Kontrollmöglichkeiten für App-Risiken und Sicherheitslücken auf Mobilgeräten, insbesondere für das Compliance-Reporting. Dieses Bundle umfasst außerdem die Module Mobile Risk & Compliance sowie Mobile Vulnerability & Patch Management.
Premium	Unser Premium-Bundle umfasst alle Funktionen von Advanced und bietet Ihren Sicherheitsteams zusätzlich die Möglichkeit, mit Mobile Endpoint Detection and Response (EDR) proaktiv Bedrohungen aufzuspüren. Mit Premium werden Ihre Richtlinien für mobile Sicherheit ständig weiterentwickelt und auf der Grundlage der Bedrohungen, denen Ihr Unternehmen ausgesetzt ist, angepasst.

Modern Endpoint Protection

Da verstärkt über Mobilgeräte auf sensible Daten zugegriffen wird, werden diese zunehmend zu einem Hauptziel für Akteure mit betrügerischen Absichten. Das Modul Lookout Modern Endpoint Protection ist in allen drei Bundles enthalten und identifiziert mobile Bedrohungen, die auf drei Angriffsvektoren abzielen: App-, Geräte- und Netzwerkbedrohungen. Lookout ermöglicht mit Continuous Conditional Access Zero-Trust-Sicherheit für mobile Endgeräte.

	Small Business	Essentials	Advanced	Premium
Schutz vor App-Bedrohungen				
Malware: Trojaner, Spyware, Ransomware, Surveillanceware, Klickbetrug und andere Bedrohungen	■	■	■	■
Erkennung von Rootkit-Exploits in Apps, die einen Jailbreak durchführen oder das Gerät rooten	■	■	■	■
Riskware: Adware, Spam, Chargeware	■	■	■	■
Erkennung von Apps, die per Sideload auf das Gerät gelangen	■	■	■	■
Schutz vor Gerätebedrohungen				
Durchsetzung des Passcodes	■	■	■	■
Durchsetzung der Geräteverschlüsselung	■	■	■	■
Jailbreak-/Root-Erkennung	■	■	■	■
Erweiterte Erkennung von Remote-Jailbreaks/Roots	■	■	■	■
Schutz vor Netzwerkbedrohungen				
Man-in-the-Middle-Angriffe auf Mobilfunk- und WLAN-Netzwerke	■	■	■	■
Angriffe auf Secure Sockets Layer (SSL)	■	■	■	■
Unerlaubte WLAN-Zugriffspunkte	■	■	■	■
Erkennung von Address Resolution Protocol (ARP)-Verschleierung	■	■	■	■
Integrationen				
Android Enterprise Dual Persona Protection		■	■	■
UEM-Integration für MDM und/oder MAM-Support		■	■	■
Identity Access Management (IAM)-Integration		■	■	■
Security Incident Event Management (SIEM)-Integration		■	■	■
Lookout Mobile Risk API		■	■	■

Continuous Conditional Access

On-Device-Kontrollen für den Datenzugriff	■	■	■	■
MDM-Zugriffskontrollen		■	■	■
MAM-Zugriffskontrollen		■	■	■
IAM-Zugriffskontrollen		■	■	■

Phishing & Content Protection

Lookout Phishing & Content Protection stoppt bekannte und unbekannte Phishing-Bedrohungen auf iOS-, Android- und Chrome-Geräten. Wir gleichen unsere KI-gestützte Phishing-Erkennung mit Listen bekannter Phishing-Sites ab. Unser Erkennungssystem überwacht ständig die Einrichtung neuer Websites speziell für Phishing-Zwecke. Mithilfe der Phishing-KI kann Lookout nahezu in Echtzeit vor Zero-Hour-Phishing-Angriffen schützen.

	Small Business	Essentials	Advanced	Premium
Phishing & Content Protection				
Blockiert in allen Apps den Zugriff auf Phishing-Links	■*	■	■	■
Blockiert bösartige Server, Command-and-Control-Systeme und Watering-Hole-Angriffe	■*	■	■	■
KI-gestützte Erkennung der neuesten Phishing-Bedrohungen	■*	■	■	■
Konfigurierbare Datenschutzkontrollen für Admins	■*	■	■	■
DNS-Datenschutz und -sicherheit (sicheres DNS)			■	■
Filtern von Inhalten aus dem Internet				
Identifiziert oder blockiert den Zugriff auf nicht jugendfreie, gewalttätige oder kriminelle Inhalte	■*	■	■	■
Genehmigung von Sites, die Mitarbeiter nutzen dürfen	■*	■	■	■
Blockierung von Sites, die sich negativ auf die Produktivität, Performance und Mobildatenkosten auswirken	■*	■	■	■

*Dieses Add-On wird üblicherweise mit Lookout for Small Business erworben

Mobile Risk & Compliance

Das Modul Lookout Mobile Risk & Compliance ist nur im Rahmen von Advanced und Premium verfügbar. Es bietet einen vollständigen Überblick über die Apps Ihrer Belegschaft und ermöglicht Ihnen die Umsetzung unternehmensweiter Governance-, Risiko- und Compliance-Richtlinien. Lookout bietet die besondere Fähigkeit, Apps in Hinblick auf ihr Risiko zu bewerten. Dies liefert notwendige Erkenntnisse in die Kontrolle der App-Berechtigungen und des Datenzugriffs.

	Small Business	Essentials	Advanced	Premium
App-Reputationsdienste				
Blockierung von nicht vertrauenswürdigen Apps			■	■
Identifizierung von Apps, die auf sensible Daten wie Termine oder Kontakte zugreifen			■	■
Identifizierung von Apps, die mit ausländischen Servern kommunizieren			■	■
Identifizierung von Apps, die mit Cloud-Diensten kommunizieren			■	■
Identifizierung von risikoreichen oder bösartigen SDKs			■	■
Identifizierung von Apps mit unsicherem Datenspeicher bzw. ungesicherter Übertragung			■	■
Risikoeinstufung für Out-of-the-Box-Apps			■	■
Risikoeinstufung für anpassbare Apps			■	■
Geräteschutzkontrollen				
Datenschutzkontrollen	■	■	■	■
Richtlinien für anpassbare Apps			■	■
Benutzerdefinierte Richtlinien für risikoreiche Apps			■	■
App-Positiv- und Negativlisten			■	■
Upload und Analyse öffentlicher und privater Apps			■	■

Mobile Vulnerability & Patch Management

Lookout Mobile Vulnerability & Patch Management ist in den Bundles Advanced und Premium enthalten. Mit diesem Modul können Sie sich über jede Betriebssystems- und App-Version in Ihrem Unternehmen informieren.
Wir bieten Einblicke in das Geräterisiko, und zwar unabhängig davon, ob es sich um firmeneigene Geräte oder Mitarbeitergeräte handelt und ob sie verwaltet werden oder nicht. Um zu verhindern, dass Sicherheitslücken in Apps, Betriebssystemen und Geräten Ihre Daten gefährden, schränkt Lookout den Zugriff auf die Unternehmensinfrastruktur ein, bis ein Gerät gepatcht ist.

	Small Business	Essentials	Advanced	Premium
Mobile Device Vulnerability Management				
Einblick in die Betriebssystemversionen	■	■	■	■
Geräte müssen mit einer Mindestversion betrieben werden	■	■	■	■
Identifizierung des Ausmaßen von Schwachstellen in der Belegschaft			■	■
Risikoreiche Gerätekonfigurationen			■	■
Schwachstellen von Betriebssystemen			■	■
Mobile App Vulnerability Management				
Identifizierung und Durchsetzung von aktualisierten App-Versionen			■	■
Aufforderung der Benutzer zur Aktualisierung anfälliger Anwendungen	■	■	■	■
Nutzung bestimmter anfälliger App-Versionen blockieren			■	■
Patch Management				
Identifizierung der aktuellsten Patches und Upgrades	■	■	■	■
Überblick über die firmenweite Patch-Integration	■	■	■	■
Durchsetzung von Patch-Installationen	■	■	■	■

Mobile Endpoint Detection & Response

Wir sind die Experten für die Identifizierung von Gefahrenindikatoren, die für die Erkennung und Reaktion auf mobile Bedrohungen erforderlich sind. Unsere Konsole für die Erkennung und Abwehr mobiler Bedrohungen stellt diese Geräte- und App-Telemetriedaten für die Mobilgeräte Ihrer Belegschaft in einer leicht abrufbaren Form bereit. Über diese Konsole können Sie auch die ständig aktualisierten Ergebnisse unserer Analyse von bösartigen und Phishing-Websites durchsuchen.

Durch die Suche in diesem umfassenden Security Graph können Sicherheitsteams erkennen, ob mobile Endgeräte von einem aktiven Angriff betroffen sind, wo sich der Angreifer befindet und was dieser gerade tut. Anhand dieser Informationen kann das Sicherheitsteam den Angriff eingrenzen, eine Datenverletzung verhindern und entsprechende Maßnahmen einführen, um einen Angriff dieser Art in Zukunft auszuschließen.

	Small Business	Essentials	Advanced	Premium
Forensische Untersuchung				
Bedrohungsabwehr in Web-Inhalten und Apps Ihrer Benutzer				■
Untersuchung und Analyse für die Reaktion auf Vorfälle				■
Verknüpfung von Vorfällen mit größeren Kampagnen oder Kill Chains				■
Schutz vor Sicherheitsverletzungen				
Proaktive Bedrohungsabwehr in globalen App-, Bedrohungs- und Web-Daten				■
Ausführung neuer Richtlinien auf Grundlage von entdeckten Bedrohungen				■
Lookout Security Graph API				
APIs zur Integration von Lookout Mobile EDR-Daten in bestehende Sicherheitstools				■
Abgleich von Bedrohungs-IOCs mit vorhandenen Bedrohungsdaten auf der Plattform				■

Über Lookout

Lookout, Inc. ist das Unternehmen für Sicherheit von Endgeräten bis in die Cloud speziell entwickelt für die Schnittstelle zwischen Unternehmens- und persönlichen Daten. Durch unsere einheitliche, Cloud-native Sicherheitsplattform schützen wir Daten über Geräte, Anwendungen, Netzwerke und Clouds hinweg — eine Lösung, die so fließend und flexibel ist wie die heutige digitale Welt. Indem wir Unternehmen und Privatpersonen mehr Kontrolle über ihre Daten geben, ermöglichen wir ihnen, ihr Potenzial voll auszuschöpfen und erfolgreich zu sein. Unternehmen jeder Größe, Behörden und Millionen von Privatpersonen vertrauen auf Lookout, um sensible Daten zu schützen, damit sie frei und sicher leben, arbeiten und sich vernetzen können. Um mehr über die Lookout Cloud Security Platform zu erfahren, besuchen Sie www.lookout.com und folgen Sie Lookout auf unserem Blog, LinkedIn und Twitter.

Weitere Informationen finden Sie unter **lookout.com**

Holen Sie sich Ihre Demo-Version unter **lookout.com/kontakt/demo**