Lookout Mobile Endpoint Security

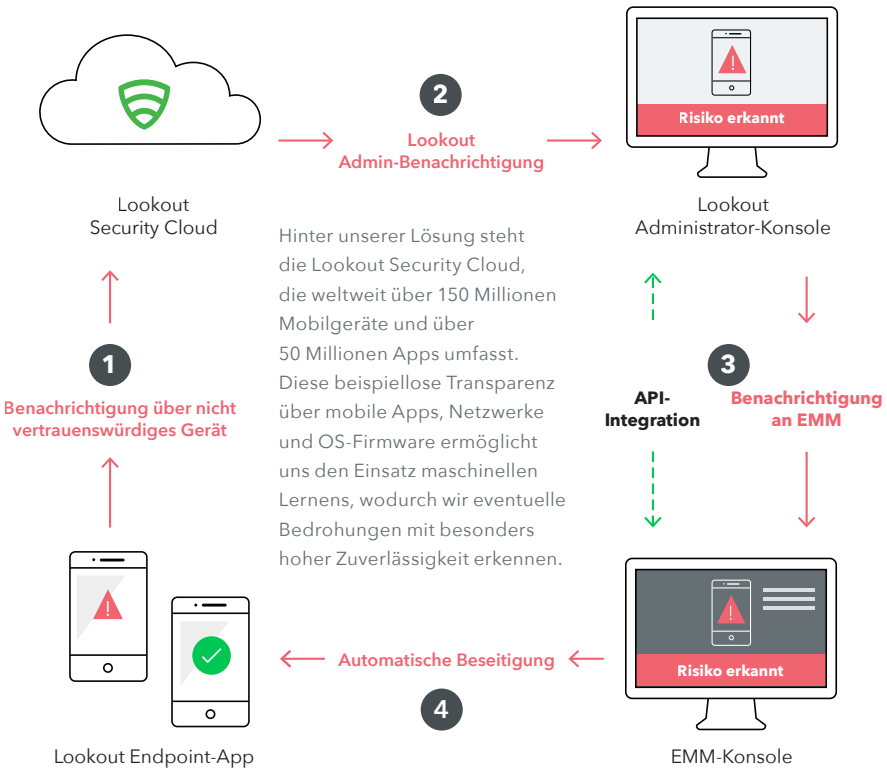
Lookout sorgt für die Sicherheit Ihrer mobilen Daten

Überblick

Viele Unternehmen nutzen heute Smartphones und Tablets, um die Produktivität am Arbeitsplatz zu steigern. Da der Zugriff auf sensible Daten verstärkt über Mobilgeräte erfolgt, müssen die Sicherheitsrichtlinien Ihres Unternehmens auch mobile Endgeräte abdecken. Lookout Mobile Endpoint Security erleichtert es Ihnen, vollständige Transparenz über die gesamte Bandbreite mobiler Risiken zu erhalten. Darüber hinaus vereinfacht es die Anwendung von Sicherheitsrichtlinien und lässt sich mühelos in vorhandene Lösungen für Security Management und Mobile Management integrieren.

So funktioniert es

Lookout Mobile Endpoint Security zeichnet sich vor allem durch folgende Punkte aus: eine schlanke Endpoint-App für Mitarbeitergeräte, eine cloudbasierte Admininistratorkonsole, die mobile Risiken in Echtzeit sichtbar macht, und durch die Integration mit führenden EMM-Lösungen (Enterprise Mobility Management).



Vorteile

Messbare Risikominderung

Schließen Sie eine große Sicherheitslücke und messen Sie die Risikominderung mithilfe der Analyse- und Reportingfunktionen von Lookout

Nahtlose Integration

Lookout fügt sich über unsere Mobile Risk API nahtlos in alle SIEM-Systeme ein, einschließlich **Splunk, ArcSight** und **QRadar**

Transparenz über mobile Sicherheitsvorfälle

Erhalten Sie Echtzeit-Transparenz über Sicherheitsvorfälle auf mobilen Geräten, damit Sie schnell und effektiv reagieren können

Sicheres Mobiles Arbeiten

Fördern Sie flexiblerer Mobilitätskonzepte, einschließlich BYOD („Bring-Your-Own-Device"), um die Mitarbeiterproduktivität zu erhöhen und wettbewerbsfähig zu bleiben

Eingebauter Datenschutz

Gewährleisten Sie die Einhaltung der Datenhoheit und den Schutz von Mitarbeiterdaten mithilfe unserer Kontrollfunktionen für Datenschutzeinstellungen

Einfaches Deployment und Management

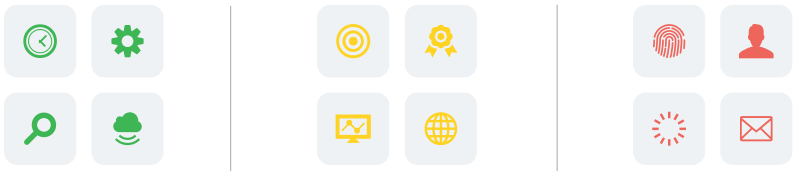
Nahtlose Integration mit sämtlichen MDMs (z. B. **Intune, AirWatch, MobileIron, MaaS360** und **BES12**) für ein einfaches Deployment und Management

Mobile Endpoint Security für Bedrohungen

Mobile Geräte greifen heute auf immer mehr sensible Daten zu. Dadurch werden sie zunehmend zum Ziel für Angreifer. Lookout Mobile Endpoint Security identifiziert mobile Bedrohungen, die die folgenden Angriffsvektoren ausnutzen:

- App-basierte Bedrohungen: Malware, Rootkits und Spyware
- Netzwerkbedrohungen: Man-in-the-Middle-Angriffe
- Gerätebedrohungen: Gejailbreakte/gerootete Geräte, veraltete Betriebssysteme, riskante Gerätekonfigurationen

Mobile Endpoint Security für App-Risiken



kein auffälliges Verhalten | **teilweise auffälliges Verhalten** | Bösartiges Verhalten

Manche iOS- und Android-Apps sind zwar nicht bösartig, sie können aber durch ihr ungewöhnliches Verhalten auffallen oder Schwachstellen haben. Sie verletzen so die Sicherheitsrichtlinie eines Unternehmens oder missachten sogar die gesetzlichen Vorschriften im Hinblick auf mögliche Datenverluste. Lookout sorgt bei diesen App-Risiken für umfassende Transparenz übe die gesamte Mobilgeräteflotte. So können Administratoren jene Anwendungen, die den internen oder gesetzlichen Regelungen zuwiderlaufen könnten, sowohl überwachen als auch mithilfe handlungsorientierter Richtlinien kontrollieren.

Das Lookout-Prinzip

- Dank unseres globalen Maßstabs und unserer Konzentration auf mobile Geräte verfügt Lookout über einen der weltweit größten Datensätze zur mobilen Sicherheit. Lookout hat Sicherheitsdaten von über 150 Millionen Geräten weltweit sowie über 50 Millionen Apps erfasst. Täglich kommen bis zu 90.000 neue Apps hinzu.
- Dank dieses globalen Sensorennetzwerks kann unsere Plattform Bedrohungen im Voraus erkennen. Dabei setzen wir maschinelle Intelligenz ein, um komplexe Muster zu identifizieren, die auf Risiken hindeuten. Diese Muster wären für menschliche Analysten nicht erkennbar.
- Die Mobilität hat eine neue Ära der Datenverarbeitung eingeläutet. Benötigt wird eine neue Generation von Sicherheitslösungen, die speziell für diese Plattform entwickelt wurden. Lookout spezialisiert sich bereits seit 2007 auf mobile Sicherheit und verfügt über das gebotene Expertenwissen in diesem Bereich.

Mithilfe von Lookout kann Ihr Unternehmen sicher mobil unterwegs sein, und zwar ohne Einbußen bei der Produktivität. Denn Lookout verschafft IT- und Sicherheitsteams die erforderliche Transparenz. Um zu erfahren, wie Sie Ihre mobile Flotte noch heute sichern können, kontaktieren Sie uns unter info@lookout.com

Lookout Mobile Endpoint Security
Mobile Endpoint Security für Bedrohungen
Schutz vor App-basierten Bedrohungen
Malware
Rootkits
Spyware
Ransomware
Schutz vor Netzwerkbedrohungen
Man-in-the-Middle-Angriffe
SSL-Attacken
Schutz vor Gerätebedrohungen
Erkennung von hoch entwickelten Jailbreak-/Root-Bedrohungen
Schwachstellen des Betriebssystems
Riskante Gerätekonfigurationen
Benutzerdefinierte Bedrohungsrichtlinien
Dashboard für Bedrohungen
Mobile Endpoint Security für App-Risiken
Kontrolle über Datenverluste durch Apps, die:
auf sensible Daten zugreifen, etwa Kalender
sensible Daten (PII) extern versenden
mit Clouddiensten kommunizieren
unsichere Datenspeicher-/ Datenübertragungsmethoden nutzen
Dashboard für riskante Apps
Benutzerdefinierte Richtlinien für riskante Apps
„Blacklists" für gesperrte Apps
Überprüfung von Unternehmenssoftware
Management und Support
EMM-Integration (Intune, AirWatch, MobileIron, MaaS360, BES12)
SIEM-Integration über Mobile Risk API (Splunk, ArcSight, QRadar)
Berichte auf Executive-Ebene zeigen die Risikominderung
Rollenbasierte Zugriffskontrolle
Kontrolle über Datenschutzeinstellungen
Support rund um die Uhr