Lookout Mobile Endpoint Security

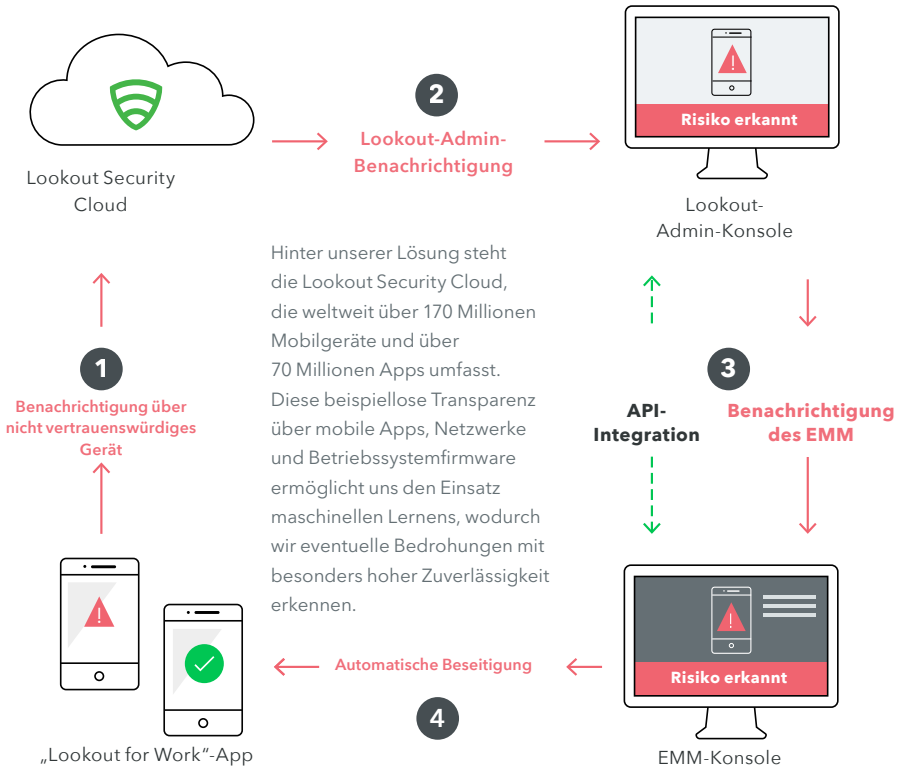
Mit Lookout sind Ihre mobilen Daten sicher

Überblick

Viele Unternehmen nutzen heute Smartphones und Tablets, um die Produktivität am Arbeitsplatz zu erhöhen. 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 Administratorkonsole, 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 kann über unsere „Mobile Risk"-API nahtlos mit allen SIEM-Systemen integriert werden, einschließlich **Splunk, Windows Defender ATP, Micro Focus, ArcSight, IBM Security und QRadar**.

Transparenz über mobile Sicherheitsvorfälle

Erhalten Sie Echtzeiteinblick in Sicherheitsvorfälle auf mobilen Geräten, damit Sie schnell und effektiv reagieren können

Sicheres mobiles Arbeiten

Fördern Sie flexiblere 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

Einfache Bereitstellung und Wartung

Die Integration in jedes EMM ist möglich (z. B. **VMware Workspace ONE® UEM, Microsoft Intune, BlackBerry® UEM, IBM MaaS360®** und **MobileIron**) – für eine einfache Bereitstellung und Verwaltung

Mobile Endpoint Security bei Bedrohungen

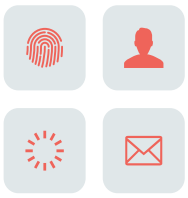
Mobile Geräte greifen heute auf immer mehr sensible Daten zu. Dadurch werden sie zunehmend zum Ziel für Angreifer. Lookout Mobile Endpoint Security identifiziert mobile Bedrohungen, die die folgenden Angriffsvektoren ausnutzen:

- Appbasierte Bedrohungen: Malware, Rootkits und Spyware
- Netzwerkbasierte Bedrohungen: Man-in-the-Middle-Angriffe
- Bedrohungen für Geräte: Jailbroken/gerootete Geräte, veraltete Betriebssysteme, riskante Gerätekonfigurationen

Mobile Endpoint Security bei App-Risiken

Kein ungewöhnliches Verhalten

Teilweise ungewöhnliches 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 bei allen Mobilgeräten Ihres Unternehmens. So können Administratoren jene Anwendungen, die den internen oder gesetzlichen Regelungen zuwiderlaufen könnten, sowohl überwachen als auch mithilfe durchsetzbarer Richtlinien kontrollieren.

Lookout – der feine Unterschied

- Dank unserer globalen Ausrichtung und unserer Konzentration auf Mobilgeräte verfügt Lookout über einen der weltweit größten Datensätze zur mobilen Sicherheit. Lookout hat Sicherheitsdaten von über 170 Millionen Geräten weltweit sowie über 70 Millionen Apps erfasst. Täglich kommen bis zu 90.000 neue Apps hinzu.
- Dank dieses globalen Sensorennetzwerks kann unsere Plattform Bedrohungen im Voraus erkennen. Wir setzen dafür 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 können Ihre Mitarbeiter sicher mobil unterwegs sein, und zwar ohne Einbußen bei der Produktivität, denn Lookout versorgt die IT- und Sicherheitsteams mit der erforderlichen Transparenz. Um zu erfahren, wie Sie Ihre Mobilflotte noch heute besser absichern können, kontaktieren Sie uns unter info@lookout.com.

Lookout Mobile Endpoint Security
Mobile Endpoint Security bei Bedrohungen
Schutz vor appbasierten Bedrohungen
Malware
Rootkits
Spyware
Ransomware
Schutz vor netzwerkbasierten Bedrohungen
Man-in-the-Middle-Angriffe
SSL-Attacken
Schutz vor Bedrohungen für Geräte
Erkennung von hoch entwickelten Jailbreak-/Root-Bedrohungen
Schwachstellen des Betriebssystems
Riskante Gerätekonfigurationen
Schutz vor web- und contentbasierten Bedrohungen
Phishing-Angriffe über jeden Kanal
URLs, die zu präparierten Websites führen
Benutzerdefinierte Bedrohungsrichtlinien
Dashboard für Bedrohungen
Mobile Endpoint Security bei 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
„Schwarze Listen" für gesperrte Apps
Überprüfung von Unternehmenssoftware
Management und Support
EMM-Integration (VMware Workspace ONE® UEM, Microsoft Intune, Blackberry® UEM, IBM MaaS360® und MobileIron)
SIEM-Integration über Mobile Risk API (Splunk, Windows Defender ATP, Micro Focus, ArcSight, IBM Security und QRadar)
Management-Berichte zeigen die Risikominderung
Rollenbasierte Zugriffskontrolle
Kontrolle über Datenschutzeinstellungen
Support rund um die Uhr

Lookout

lookout.com/de