Lookout Mobile Endpoint Detection und Response (EDR)

Suchen Sie nach den neuesten Bedrohungen auf Ihren Mobilgeräten

Erweitern Sie Ihre mobile Sicherheitsstrategie um eine proaktive Bedrohungsabwehr

Mit der zunehmenden Häufigkeit und den steigenden Kosten aufgrund von Cybersecurity-Verstößen haben Sicherheitsteams ihren Schwerpunkt vom Schutz des Endgeräts auf Datensicherheit verlagert. Neben der Blockierung von Malware benötigt Ihr Team auch Tools zur Untersuchung von dateilosen Cyberangriffen, die keine Malware verwenden, und von Insider-Bedrohungen. Zum Beispiel wenn ein Angreifer die durch einen Phishing-Betrug gestohlenen Anmeldeinformationen verwendet, um Daten zu exfiltrieren.

Cyberangriffe, die zu einer Datenschutzverletzung führen, sind selten ein einmaliges Ereignis. Cyberangreifer arbeiten langsam und unauffällig, um Schwachstellen zu entdecken, Anmeldeinformationen zu stehlen, bösartigen Code wie Ransomware einzufügen oder Daten zu exfiltrieren. Diese Schritte erfolgen über mehrere Endgeräte und über viele Wochen oder Monate hinweg.

Das mobile Arbeiten hat gänzlich neue Möglichkeiten für Cyberkriminelle eröffnet

Während viele Unternehmen über eine umfassende Aktivitätsüberwachung für Server, Desktop- und Laptop-Computer verfügen, fehlen ihnen diese Telemetriedaten für iOS-, Android- und Chrome-OS-Endgeräte. Da die Mitarbeiter vermehrt Mobilgeräte für ihre Arbeit nutzen, haben die Angriffe auf diese Geräte zugenommen.

Vorteile

- Schnelles Erkennen und Reagieren auf mobile Bedrohungen
- Erkennen von Angriffen ohne Malware
- Verhindern von Verstößen, die gestohlene Anmeldedaten verwenden
- Durchführen forensischer Analysen von Sicherheitsvorfällen
- Den Vorfall am Endgerät eindämmen
- Bereitstellen von Leitlinien zur Behebung
- Proaktives Abwehren von Bedrohungen

Um Datenverstöße wirksam zu verhindern, benötigen Sicherheitsteams für mobile Endgeräte die gleichen umfassenden Daten wie für Server, Desktops und Laptops. Da mobile Betriebssysteme niemals den Zugriff auf den Kernel zulassen und Anwendungen isoliert arbeiten müssen, wurde fälschlicherweise angenommen, dass die Erfassung umfassender Telemetriedaten nicht möglich sei.

Echtzeit-Telemetriedaten zur Verhinderung von Verstößen

Zur Bereitstellung der verhaltensbasierten Bedrohungsschutzfunktionen analysiert Lookout Tausende von Telemetriedaten, die von über 200 Millionen iOS-, Android- und Chrome-OS-Endgeräten mit unserer App gesammelt wurden. Wir sind die Experten für die Identifizierung von Gefahrenindikatoren, die für die Erkennung und Reaktion auf mobile Bedrohungen erforderlich sind.

Unsere Konsole für Mobile Endpoint Detection & Response 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.

Funktionen von Lookout Mobile EDR

Bedrohungen leicht erkennen und auf diese reagieren

Richten Sie regelbasierte Richtlinien ein, um eine schnelle Reaktion auf bösartige Aktivitäten zu automatisieren. Durch die Verwendung von voreingestellten Lookout-Richtlinien oder von Ihnen definierten Richtlinien können Sie mithilfe der Modern Endpoint Protection auf der Lookout Cloud Security Platform sofortige Maßnahmen ergreifen, die mit den Richtlinien Ihres Unternehmens zur Reaktion auf derlei Vorfälle übereinstimmen.

Vorfälle untersuchen

Mit unserer intuitiven und benutzerfreundlichen EDR-Konsole können Sie Bedrohungs- und forensische Analysen durchführen, um einen Angriff durch jede Phase der Kill Chain zu verfolgen. Vektorübergreifende Suchfunktionen zeigen schnell auf, wie sich Angreifer innerhalb Ihres Unternehmens bewegen. So erhalten Sie Antworten auf wichtige Fragen, z. B. wohin der Angreifer gegangen ist, was er getan hat und wie er vorgegangen ist. Dadurch können Sie notwendige Änderungen einführen, um zu verhindern, dass sich ein Angriff wiederholt.

Den Vorfall am Endgerät eindämmen

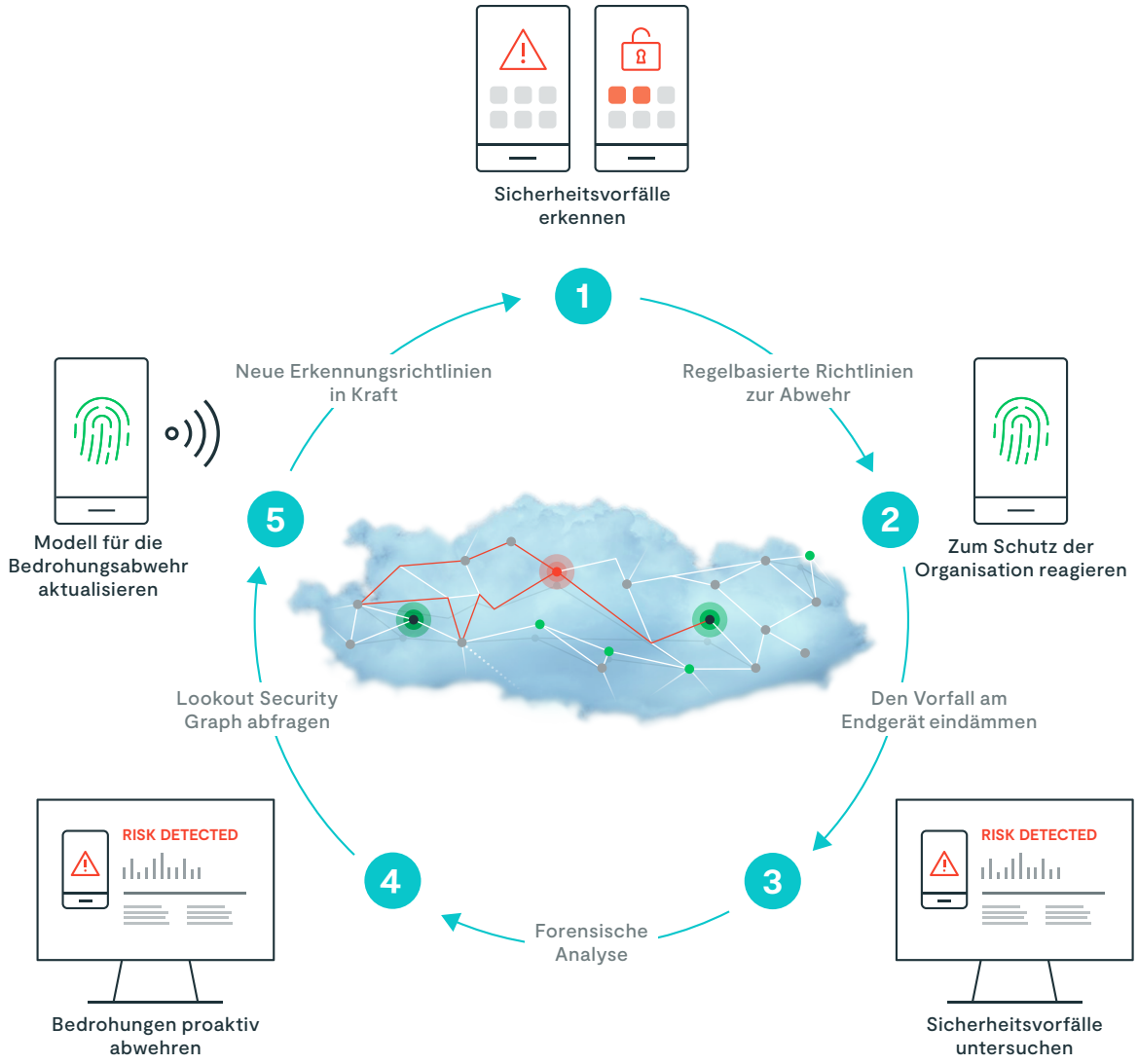
Sobald eine Bedrohung auf dem Gerät erkannt wird, kann die Lookout-Plattform das Endgerät sofort unter Quarantäne stellen, unabhängig davon, ob es verwaltet oder nicht verwaltet wird, und Verbindungen zum Internet oder zu bestimmten Unternehmensdomänen unterbinden.

Bedrohungen proaktiv abwehren

Mit dem weltweit größten Datensatz mobiler Bedrohungs-Telemetrie können Sie unsere globalen Daten abfragen oder in Ihre eigene Umgebung eintauchen und so die Reichweite Ihrer proaktiven Bedrohungsabwehr vergrößern. Führen Sie über unsere EDR-Konsole Abfragen und erweiterte Analysen durch, um tiefergehend Einsichten zu erhalten.

Leitlinien für Abhilfemaßnahmen bereitstellen

Lookout bietet Anwendern leicht verständliche Anleitungen zur Behebung von Risiken auf Mobilgeräten. 95 % der von Lookout entdeckten Bedrohungen werden von den Anwendern selbst behoben, ohne dass die IT- oder Sicherheitsabteilung eingeschaltet werden muss.


Sicherheitsvorfälle erkennen
1
Regelbasierte Richtlinien zur Abwehr
2
Zum Schutz der Organisation reagieren
Den Vorfall am Endgerät eindämmen
3
RISK DETECTED
Sicherheitsvorfälle untersuchen
Forensische Analyse
4
RISK DETECTED
Bedrohungen proaktiv abwehren
Lookout Security Graph abfragen
5
Modell für die Bedrohungsabwehr aktualisieren
Neue Erkennungsrichtlinien in Kraft

Über Lookout

Lookout ist der Anbieter für Cybersicherheit vom Endgerät bis in die Cloud, der Zero Trust Sicherheit bietet, um Risiken zu reduzieren und Unternehmensdaten zu schützen. Unsere zentrale, Cloud-native Plattform schützt digitale Informationen über Geräte, Anwendungen, Netzwerke und Clouds hinweg und passt sich modernen Arbeitsplatz-Anforderungen an. Unternehmen und Behörden jeder Größe vertrauen auf Lookout, um sensible Daten zu schützen, sowie frei und sicher arbeiten und sich vernetzen zu können. Um mehr über die Lookout Cloud Security Platform zu erfahren, besuchen Sie www.de.lookout.com und folgen Sie Lookout auf unserem Blog, LinkedIn und Twitter.

Weitere Informationen finden Sie unter
de.lookout.com

Fordern Sie eine Demo an unter
de.lookout.com/demo-anfragen

© 2023 Lookout, Inc. LOOKOUT®, das Lookout Shield Design® und LOOKOUT mit Shield Design® sind eingetragene Marken von Lookout, Inc. in den Vereinigten Staaten und anderen Ländern. DAY OF SHECURITY®, LOOKOUT MOBILE SECURITY® und POWERED BY LOOKOUT® sind eingetragene Marken von Lookout, Inc. in den Vereinigten Staaten. Lookout, Inc. unterhält gewohnheitsrechtliche Markenrechte an EVERYTHING IS OK, PROTECTED BY LOOKOUT, CIPHERCLOUD, dem 4-Balken-Schild-Design und dem mehrfarbigen/mehrschattigen Lookout Wingspan-Design.