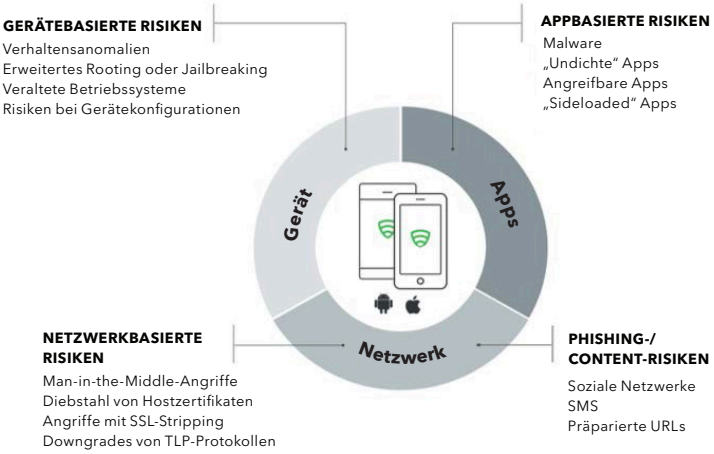
Lookout + Microsoft Windows Defender ATP

Gemeinsam für sichere Mobilität im Unternehmen

Schutz der Unternehmensdaten vor mobilen Bedrohungen

Unternehmen setzen zunehmend auf Mobilitätsmanagementstrategien, um die Produktivität ihrer mobilen Mitarbeiter zu fördern. In der heutigen komplexen Bedrohungslandschaft ist es jedoch schwieriger denn je, den Schutz von Unternehmensdaten und -ressourcen zu gewährleisten. Lookout schützt iOS- und Android-Mobilgeräte im Verbund mit den Mobilitäts- und Sicherheitslösungen von Microsoft. So können Unternehmen die Mitarbeiterproduktivität steigern und gleichzeitig sensible Daten während des Zugriffs über ihre Mobilgeräte schützen.



Umfassende mobile Sicherheit

Dank cloudbasierter Bedrohungsanalyse erkennt Lookout die gesamte Bandbreite mobiler Risiken und bietet geeignete Schutzmaßnahmen:

- Phishing per E-Mail, SMS, Textnachrichten und Apps
- Präparierte und per Sideloading installierte Anwendungen
- Risiken durch Betriebssysteme, Konfigurationen, Rooting/Jailbreaking
- Netzwerk- und Man-in-the-Middle-Angriffe

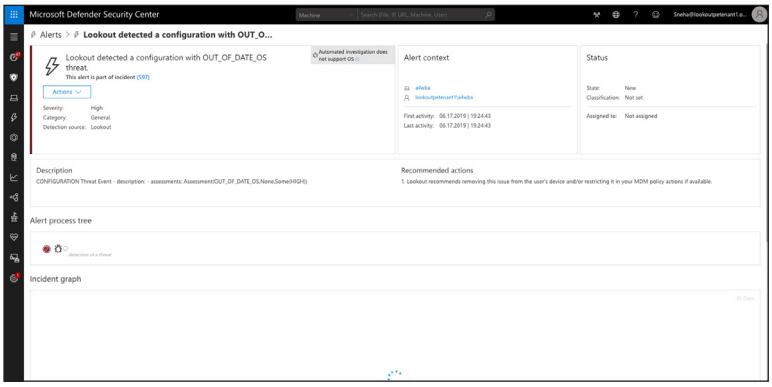
Lookout und Microsoft Windows Defender ATP

Die Lookout-Lösung zum Schutz mobiler Endgeräte (Mobile Endpoint Security) ist mit dem Microsoft-Produkt Windows Defender Advanced Threat Protection (ATP) integriert. Dadurch können Microsoft-Kunden aktuelle Cyberangriffe sowie Datenlecks auf iOS- und Android-Geräten erkennen, beobachten und untersuchen. Diese Aktionen und das Einleiten von Schutzmaßnahmen erfolgen über das Portal von Windows Defender ATP. Das integrierte Portal zeigt Bedrohungs- und Systemzustandsinformationen zu Lookout-Geräten an. Somit verfügen Sie über eine voll ausgestattete Infozentrale.

Sie informiert über die Art der Bedrohung und liefert eine Beschreibung sowie eine Einstufung der Risikolage. Maßnahmen werden ebenfalls empfohlen. Sobald präparierte Anwendungen, Phishing auf Mobilgeräten, Netzwerkangriffe und Schwachstellen des Betriebssystems erkannt werden, werden sowohl der Anwender als auch das Windows Defender ATP-Portal unverzüglich benachrichtigt. Die Kombination aus den Bedrohungsdaten zum Mobilgerät des Anwenders und denen der Windows-Geräte des Anwenders sorgt für tiefere Einblicke in die Unternehmensumgebung und die Sicherheitsrisiken für Anwender.

So funktioniert die Integration

Bei der Integration zwischen Lookout und Windows Defender ATP werden Informationen zu Mobilgeräten und deren Bedrohungen von der Lookout-API für Mobilgeräterisiken über den Lookout-ATP-Konnektor an die Windows Defender ATP-API weitergegeben. Intune oder andere MDM-Lösungen sind nicht erforderlich, da die Dienste von Lookout und Windows Defender direkt miteinander kommunizieren. Die von Lookout bereitgestellten Informationen werden über das Windows Defender ATP-Portal integriert. Ein Haupt-Dashboard für Bediener, ein Analyse-Dashboard sowie Warnungen und maschinenspezifische Masken vervollständigen die Integration.



Funktionsübersicht

- Integrierte Konsole für mobile Bedrohungen
- Dashboard mit Bedrohungszusammenfassung
- Verknüpfungen zwischen Anwendergeräten
- Warnungen inkl. Bedrohungsbeschreibung und -einstufung sowie empfohlener Maßnahmen
- Ereignisverlauf für Mobilgeräte

„Die Integration zwischen Lookout Mobile Threat Defense und Microsoft Windows Defender ATP wird ein ganz neues Maß an Einblick und Reaktionsfähigkeit auf all den unterschiedlichen Gerätetypen ermöglichen, die Unternehmenskunden absichern müssen."

Moti Gindi

General Manager Windows Cyber Defense, Microsoft

Argumente für Lookout

Microsoft und Lookout arbeiten zusammen, um eine sichere Nutzung von Smartphones und Tablets in Unternehmen zu ermöglichen. Dabei verfolgen beide Unternehmen denselben Ansatz: Methoden des maschinellen Lernens auf eine große Menge an Sicherheitsdaten anzuwenden, um neue Bedrohungen schnell erkennen und eindämmen zu können. Lookout hat hierzu sicherheitsrelevante Informationen von weltweit über 170 Millionen Geräten gewonnen und so mehr als 70 Millionen iOS- sowie Android-Apps mit seinen Machine-Learning Algorithmen analysiert, um Risiken kenntlich zu machen. Als Microsoft-Partner überzeugt Lookout mit den verschiedensten Microsoft-Integrationen, darunter **Microsoft Intune und Enterprise Mobility + Security, Microsoft Intelligent Security Graph** und **Microsoft Intune MAM**.