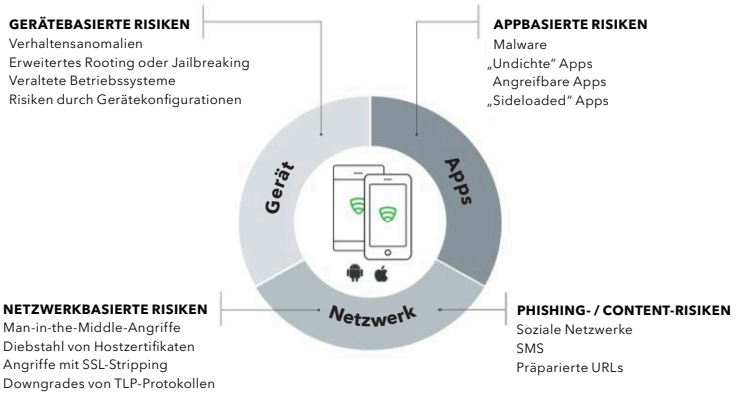
Lookout + Microsoft = Partnerschaft

Gemeinsam schützen Lookout und Microsoft Ihre Mobilität besser

Überblick

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. Gemeinsam mit den Mobilitäts- und Sicherheitslösungen von Microsoft schützt Lookout iOS- und Android-Mobilgeräte. So können Unternehmen mobiles Arbeiten und die Cloudnutzung priorisieren, um die Mitarbeiterproduktivität zu steigern, und gleichzeitig sensible Daten während des Zugriffs durch 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 + Microsoft Azure Active Directory (AAD) und Intune

Risikobasierte und bedingte Zugriffe

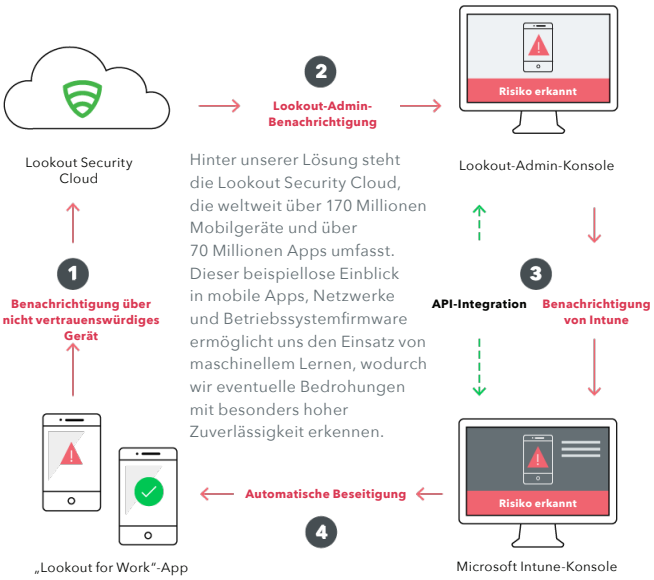
Durch die Integration mit Microsoft EMS ist Lookout in der Lage, Intune über Geräterisiken wie präparierte Anwendungen, Betriebssystem-Schwachstellen, Netzwerkangriffe, Phishing-Versuche und sogar von der DSGVO abweichende Anwendungen zu informieren. Diese Warnungen werden in der Intune-Verwaltungskonsole angezeigt und können für bedingte Zugangsberechtigungen verwendet werden, mit denen risikobehaftete Geräte so lange vom Zugriff auf Unternehmensressourcen ausgeschlossen werden, bis die Ursache der Nichtkonformität beseitigt ist.

Anwenderfreundlich

Die Integration zwischen Lookout und Azure Active Directory ermöglicht eine nahtlose Bereitstellung. Zudem kann die Lookout-App auf diese Weise komfortabel mit Intune verwaltet werden. Dies umfasst ein integriertes Richtlinienmanagement für Benutzer und Gruppen sowie das integrierte Identitätsmanagement mit Azure Active Directory, das die Einmalanmeldung für Anwender und Administratoren erlaubt.

Sicherheit und Compliance

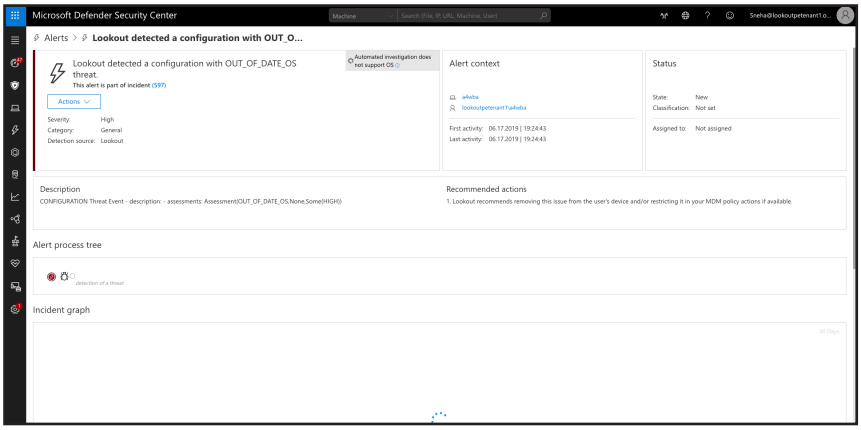
Die Lookout-Funktion für Anwendungsrichtlinien erkennt mobile Apps, die gegen Sicherheits-, Datenschutz- oder Governance-Vorgaben des jeweiligen Unternehmens verstoßen. Beispielsweise, wenn Kontaktlisten oder Standorte von Anwendern öffentlich zugänglich gemacht werden. Solche Anwendungen werden auf eine schwarze Liste gesetzt und ihre Nutzungsdaten zur Berichterstellung und für bedingte Zugangsberechtigungen an Intune gesendet.



Lookout + Microsoft Windows Defender ATP

Warnungen zu mobiler Sicherheit auf Windows-Geräten

Die Lookout-Lösung ist in das Microsoft-Produkt Windows Defender Advanced Threat Protection (ATP) integriert, um mobile Endgeräte zu schützen (Mobile Endpoint Security). Dadurch können Microsoft-Kunden aktuelle Cyberangriffe sowie Datenlecks auf iOS- und Android-Geräten erkennen, beobachten und untersuchen. Diese Aktionen und das Einleiten von Gegenmaßnahmen erfolgen über die Verwaltungskonsole von Windows Defender ATP. Die integrierte Konsole zeigt Bedrohungs- und Systemzustandsinformationen zu Geräten im Haupt-Dashboard und in den Unterabschnitten an. Somit verfügen Sie über eine voll ausgestattete Infozentrale.



Mehr Einblick in mobile Bedrohungen

- Integrierte Konsole für mobile Bedrohungen
- Dashboard mit Bedrohungszusammenfassung
- Verknüpfung von Anwendergeräten
- Details und Aktionshinweise bei Bedrohungen
- Ereignisverlauf für Mobilgeräte

Lookout + Sicherheits-API von Microsoft Graph

Daten zu Mobilgerätebedrohungen für erweiterte Sicherheits-Workloads von Microsoft

Durch die Integration von Lookout in die Microsoft Graph-Sicherheits-API können Kunden über verbundene Anwendungen Lookout-Telemetriedaten abrufen, empfangen und vergleichen sowie entsprechende Berichte erstellen. Lookout-Telemetriedaten können durch weitere Gefahren- und Sicherheitshinweise aus Microsoft-Produkten, -Diensten und -Sicherheitslösungen sowie durch Warnungen von Microsoft Graph-Drittanbietern ergänzt werden. Dies ermöglicht die Erkennung und Abwehr von Cyberbedrohungen.

Azure Information Protection

Geräterisiko für AIP zur Einschränkung von Ressourcenzugriffen oder für die Mehrfaktor authentifizierungsanforderung

Zugriffsschutz für die Cloud

Zum Schutz cloudbasierter Ressourcen vor Identitätsdiebstahl und Gerätebedrohungen

Office 365 ATP

Integrierte Warnungen zu mobilen Phishing-Bedrohungen über soziale Netzwerke und SMS

Azure ATP

Bessere Einblicke und Kontrolle dank Hinweisen zu mobilen Bedrohungen

Äußerst leistungsstarke Risikotelemetrie

- Nur einwandfreie Geräte haben Zugriff auf Unternehmensressourcen.
- Bedrohungshinweise werden für den bedingten Zugang verwendet.
- ATP-Warnungen werden um Phishing-Warnungen erweitert.
- Mobilitätshinweise sind auch in anderen Microsoft-Produkten nutzbar.

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: Maschinelles Lernen 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:

- **Microsoft Intune und Enterprise Mobility + Security:** Über die nahtlose Aktivierung per Azure Active Directory erzwingt Lookout den Continuous Conditional Access auf Basis von Echtzeitdaten zu netzwerk- und gerätebasierten Risiken.
- **Microsoft Windows Defender ATP:** Durch diese Integration können Microsoft-Kunden Cyberangriffe sowie Datenlecks auf iOS- und Android-Geräten erkennen, beobachten und untersuchen. Die Aktionen erfolgen über die WDATP-Verwaltungskonsole.
- **Microsoft Intelligent Security Graph:** Nahtlose Integration für den Austausch von Lookout-Telemetriedaten zu mobilen Bedrohungen.
- **Microsoft Intune MAM:** Lookout bewertet den Gerätezustand und erzwingt für MAM-fähige Apps den Continuous Conditional Access.

Informationen darüber, wie Microsoft EMS + Lookout einen Beitrag zum Schutz Ihres Unternehmens leisten können, finden Sie unter lookout.com/microsoft