Lookout + Microsoft = sicheres BYOD

Schützt Office 365-Apps auf nicht verwalteten Geräten vor mobilen Bedrohungen

Schutz von Office 365 auf Mobilgeräten

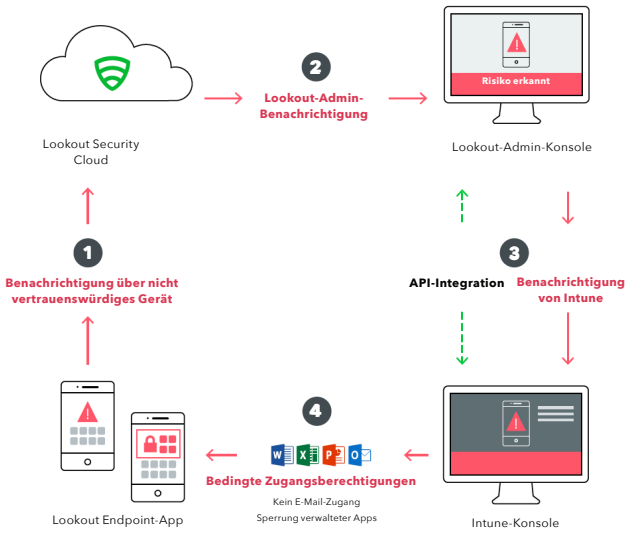
Über Microsoft Office 365-Apps auf privaten Mobilgeräten wird häufig auf arbeitsrelevante Unternehmensdaten zugegriffen. Gerade diese Geräte - und der Benutzer selbst - werden durch Phishing zum Angriffsziel und somit vermehrt geräte-, app- und netzwerkbasierten Cyberangriffen ausgesetzt. Lookout Mobile Endpoint Security in Verbindung mit Microsoft MAM ohne MDM bietet mehr Sicherheit für Mobilgeräte – ein Alleinstellungsmerkmal von Lookout zur Einhaltung von BYOD-Richtlinien und Datenschutzvorgaben.

„Bis 2020 werden rund 90% aller global agierenden Unternehmen Geschäftsprozesse eingeführt haben, welche von Mobilgeräten abhängig sein werden"

„How to Successfully Navigate the Hurdles of Global-Scale BYOD Implementations"

Gartner, 13. Juni 2019

Integration von Lookout + Intune MAM ohne MDM



Worum handelt es sich?

Zum Schutz von Unternehmensdaten in Intune-Apps lässt sich Lookout Continuous Conditional Access nahtlos in Microsoft Intune MAM integrieren. Eine Geräteverwaltung erfolgt dabei nicht.

Wie funktioniert es?

Durch die ununterbrochene Kontrolle des Gerätezustands stuft Lookout das vom Gerät ausgehende Risiko ein und gibt diese Information an Intune weiter. Intune-MAM-Richtlinien – angereichert mit Informationen von Lookouts „Mobile Threat Intelligence" – schützen die Daten der von Intune abgesi cherten Apps.

Wie läuft die Bereitstellung?

Für die nahtlose Installation integriert sich Lookout mit Microsoft-Systemen.

Sicheres BYOD für Mitarbeiter und Organisationen

BYOD ist in Unternehmen ein gängiges Modell, um Mitarbeitern die Nutzung privater Geräte für Arbeitszwecke zu erlauben, ohne dass der Arbeitgeber die Kontrolle über das Gerät erhält. Unternehmen können nun die nötige Sicherheit für Office 365 neben der Anwenderfreiheit ihrer Anwender schaffen.