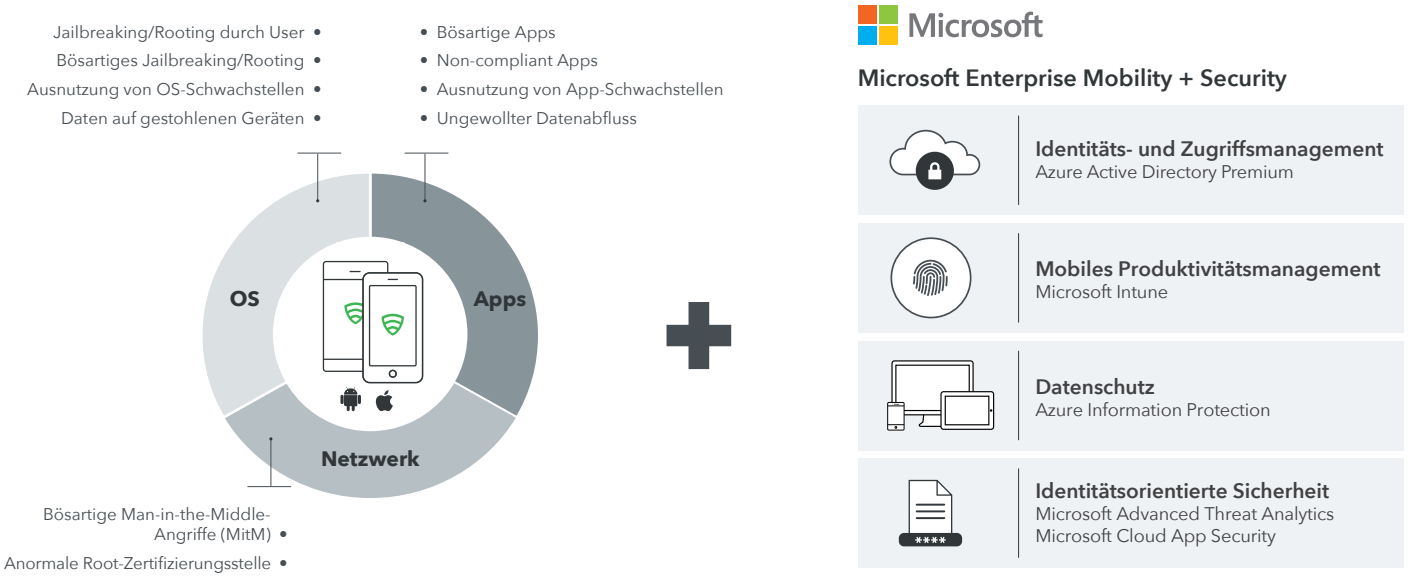
Lookout + Microsoft

Gemeinsam für sichere Mobilität im Unternehmen

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. Mit Lookout und Microsoft Enterprise Mobility + Security (EMS) sind Unternehmen in der Lage, einen für Mobilgeräte und die Cloud optimierten Sicherheitsansatz zu verfolgen. Er verschafft Mitarbeitern mehr Flexibilität und schützt gleichzeitig sensible Daten während des Zugriffs durch ihre Mobilgeräte.



Wesentliche Vorteile von Lookout + Microsoft EMS

Umfassende mobile Sicherheit zur Steigerung der Produktivität

Microsoft EMS ist eine identitätsorientierte Sicherheitslösung, die einen ganzheitlichen Ansatz für die Sicherheitsanforderungen in unserem „mobile-first", „cloud-first" Zeitalter bietet. Lookout ergänzt die identitätsbasierten Sicherheitsfunktionen von Microsoft EMS durch umfassende Informationen zu mobilen Bedrohungen: Es überwacht Geräte kontinuierlich im Hinblick auf Bedrohungen und übermittelt diese Informationen direkt an Microsoft EMS für die Vergabe entsprechender Zugangsberechtigungen. Lookout schützt vor Bedrohungen, die die folgenden drei Angriffsvektoren ausnutzen:

1. App-basierte Bedrohungen: Trojaner, Spyware, Rootkits und non-compliant Apps, die zu einem ungewollten Verlust sensibler Daten führen
2. Netzwerkbasierte Bedrohungen: Man-in-the-Middle- und SSL-Angriffe, bei denen während der Übertragung verschlüsselte Daten gestohlen werden können
3. Betriebssystembasierte Bedrohungen: Hoch entwickeltes Jailbreaking von iOS-Geräten und Rooting von Android-Geräten

Risikobasierte Zugangsberechtigungen

Anhand von Richtlinien für Zugangsberechtigungen in Intune können Sie E-Mails, Dateien und weitere Ressourcen in Unternehmen vor unbefugtem Zugriff schützen. Dabei werden anpassbare Faktoren wie Standort, Gerät, Anwenderstatus, Anwendungsempfindlichkeit und Risiko zugrunde gelegt, um die Sicherheit und Compliance zu gewährleisten. Die Integration zwischen Microsoft EMS und Lookout ermöglicht es Ihnen, Lookout Threat Intelligence in Ihre in Intune definierten Zugangsberechtigungsrichtlinien einzubeziehen. Auf diese Weise können Sie den Zugang zu Apps wie mobilen Office-Anwendungen verwalten und sichern sowie Daten selektiv von Geräten löschen.

Anwenderfreundlich

Die Integration zwischen Lookout und EMS ermöglicht ein nahtloses Deployment. Zudem kann die Lookout Client-App auf diese Weise komfortabel mit zwei Tools gemanagt werden: Microsoft Intune, einem integrierten Richtlinienmanagement für Benutzer und Gruppen, sowie Azure Active Directory, einem integrierten Identitätsmanagement, das Single Sign On für User und Administratoren gestattet.

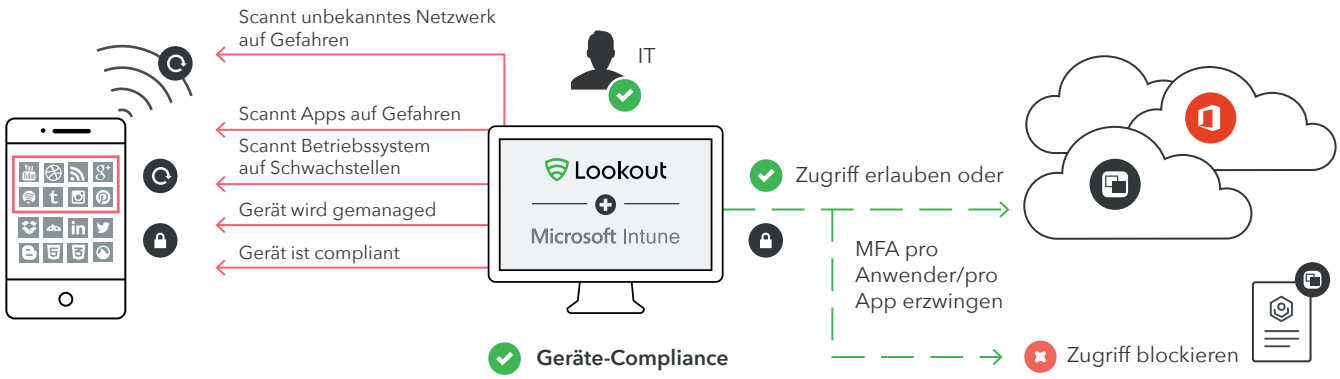
So funktioniert die Integration

Gerätebereitstellung

Mithilfe von Microsoft Intune kann die Lookout-Endpoint-App mühelos auf Ihre Mobilgeräte ausgespielt werden. Dadurch wird eine schnelle und skalierbare Bereitstellung ermöglicht.

Risikobasierte Zugangsberechtigungen

Lookout bietet Transparenz über bösartige Bedrohungen und Apps, die zu einem ungewollten Abfluss sensibler Unternehmensdaten führen, und informiert die Sicherheitsanalyse von Intune über den Compliance-Status des Geräts. Wenn ein Mitarbeiter in der Finanzabteilung z. B. unbeabsichtigt eine bösartige mobile Anwendung herunterlädt, identifiziert Lookout diese Bedrohung und veranlasst Intune mittels der Anpassung von Zugangsberechtigungen, den Zugriff auf Unternehmensdaten so lange einzuschränken, bis die Bedrohung beseitigt wurde.



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