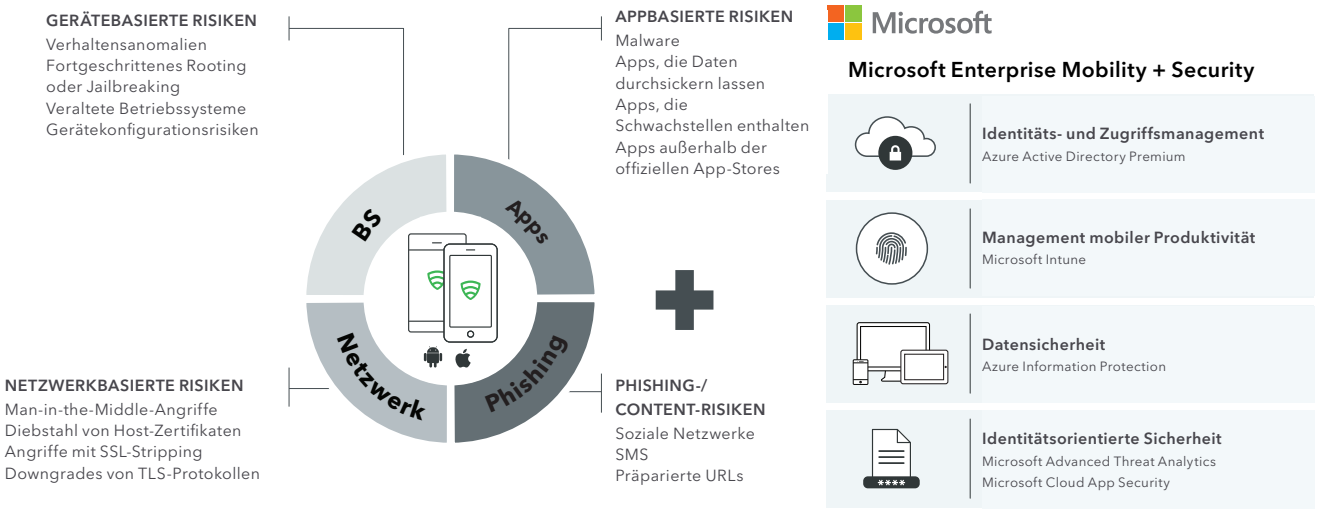
Lookout + Microsoft

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 über 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 auf Mobilgeräte und die Cloud ausgerichteten 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 EMS für die Vergabe entsprechender Zugangsberechtigungen. Lookout berücksichtigt dabei vier Angriffsvektoren:

1. Appbasierte Bedrohungen: Trojaner, Spyware, Rootkits und nicht konforme Apps, die zu einem ungewollten Verlust sensibler Daten führen
2. Netzwerkbasierte Bedrohungen: Phishing-, 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
4. Phishing und Content-Bedrohungen: Phishing in privaten und geschäftlichen E-Mails, Textnachrichten, SMS und Apps

Risikobasierte Zugriffsberechtigungen

Anhand von Richtlinien in Intune können Sie E-Mails, Dateien und weitere Ressourcen in Unternehmen vor unbefugtem Zugriff schützen. Dabei werden anpassbare Faktoren wie Standort, Gerät, Anwenderstatus, Anwendungssensitivität und Risiko zugrunde gelegt, um die Sicherheit und Compliance zu gewährleisten. Die Integration ermöglicht den Einbezug von Lookout-Bedrohungsdaten in die Richtlinien für den bedingten Zugang, die Sie in Intunes definiert haben, um den Zugang zu Apps wie mobilen Office-Anwendungen zu verwalten und zu sichern sowie Daten selektiv von Geräten zu löschen.

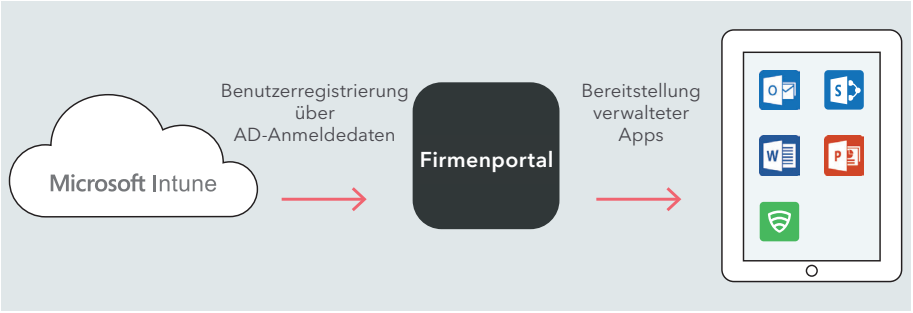
Anwenderfreundlich

Die Integration ermöglicht ein nahtloses Deployment. Zudem kann die Lookout-App komfortabel mit zwei Tools gemanagt werden: Microsoft Intune mit integriertem Richtlinienmanagement für Benutzer und Gruppen sowie mit dem integrierten Identitätsmanagement von Azure Active Directory, das Single Sign-on (SSO) für Endanwender und Administratoren erlaubt.

So funktioniert die Integration

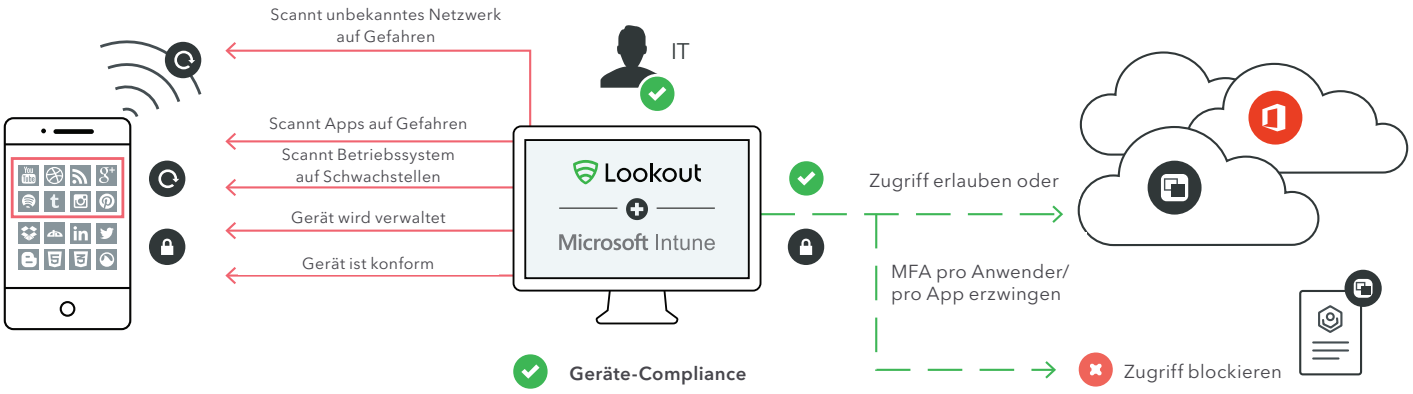
Gerätebereitstellung

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



Risikobasierte Zugriffsberechtigungen

Lookout bietet Transparenz über Bedrohungen und Apps, die zu einem ungewollten Abfluss sensibler Unternehmensdaten führen können, und informiert Intune über den Compliance-Status des Gerätes. Wenn ein Mitarbeiter in der Finanzabteilung z. B. unbeabsichtigt eine präparierte App herunterlädt, identifiziert Lookout diese Bedrohung und veranlasst Intune, den Zugriff auf Unternehmensdaten so lange einzuschränken, bis die Bedrohung beseitigt wurde.



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