

Lookout + Microsoft protègent les terminaux BYOD

Protégez vos applications Office 365 contre les menaces mobiles de vos terminaux non managés

Protection d'Office 365 sur mobile

Dans de nombreuses organisations, les applications Microsoft 365 sont très utilisées pour accéder à des données d'entreprise à partir d'appareils mobiles personnels. Jusqu'à présent, ces terminaux très connectés se sont montrés davantage vulnérables face au phishing mobile et aux menaces de cybersécurité inhérentes aux applications, aux réseaux et aux appareils. Fort heureusement, l'intégration de Lookout Mobile Endpoint Security aux politiques de protection des applications Microsoft Intune renforce la sécurité mobile à l'heure où les stratégies BYOD, et donc les appareils non gérés, prédominent.

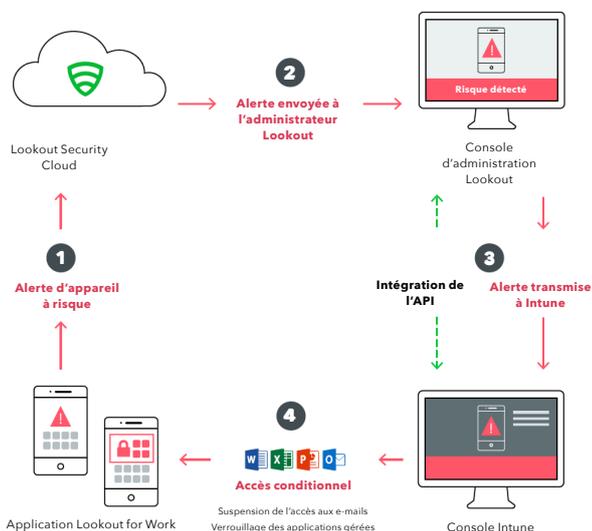
Politiques de protection des applications Microsoft Intune

Les politiques de protection des applications permettent aux entreprises de limiter certaines actions, comme le fait de pouvoir copier-coller des données d'entreprise dans des applications personnelles, ou d'imposer le chiffrement des données dans les applications protégées par Intune. Lookout s'intègre facilement aux politiques de protection des applications Microsoft Intune, sans qu'une solution MDM ne soit requise.

« D'ici 2020, 90 % des entreprises mondiales auront mis en œuvre des processus commerciaux dépendants des appareils mobiles. »

« How to Successfully Navigate the Hurdles of Global-Scale BYOD Implementations » (Comment bien surmonter les obstacles de la mise en œuvre d'un programme BYOD à l'échelle mondiale)

- Gartner, le 13 juin 2019



Comment cela fonctionne-t-il ?

En contrôlant l'état de santé des appareils en continu, Lookout est en mesure de leur attribuer un niveau de risque et de le communiquer à Intune. En exploitant les renseignements de Lookout sur les menaces mobiles, les politiques de protection des applications Intune assurent la protection des données issues d'applications protégées par Intune contre les menaces au niveau des appareils.

Lookout informe Intune dès lors que les niveaux de risque de l'appareil dépassent ceux définis par l'administrateur. L'application Intune bloque l'accès aux données d'entreprise jusqu'à ce que l'appareil soit remis en conformité.

Comment le déployer ?

Lookout s'ajoute aux systèmes Microsoft pour une installation simplifiée.

Ensemble, Microsoft et Lookout offrent une sécurité mobile complète aux utilisateurs BYOD d'Office 365.