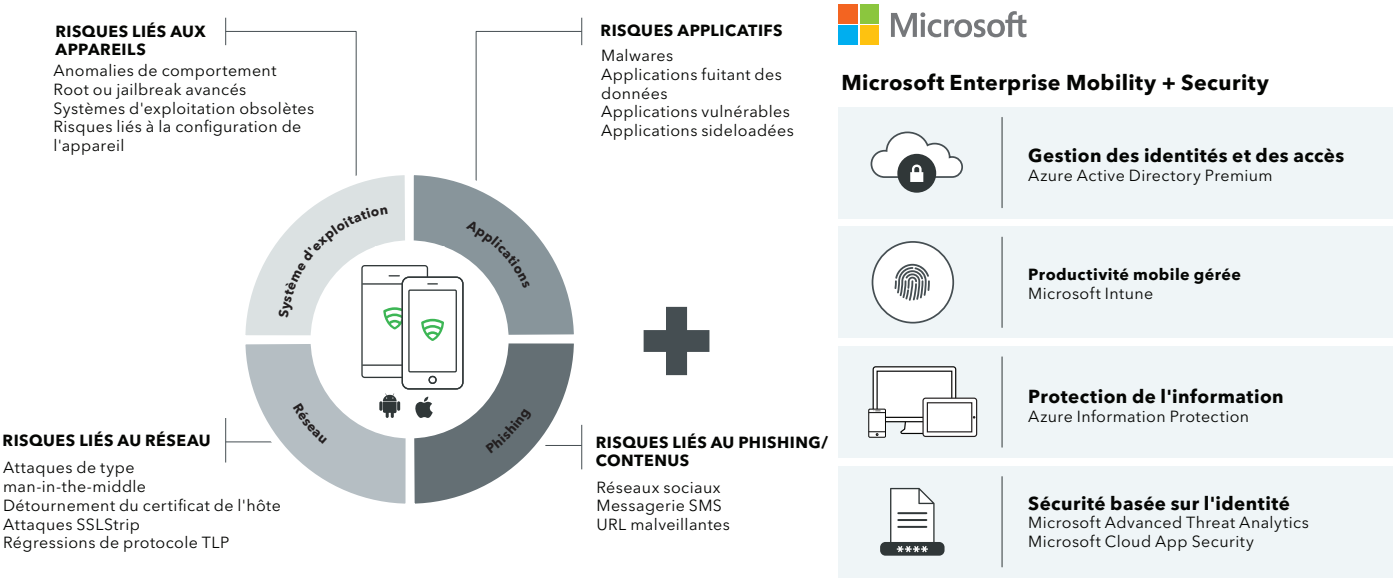
Lookout + Microsoft

Collaborer pour sécuriser la mobilité d'entreprise

Les entreprises sont de plus en plus nombreuses à adopter des stratégies de gestion mobile pour accroître leur productivité mobile, mais avec l'arrivée de menaces toujours plus sophistiquées, il est plus difficile que jamais de garantir la protection des données et des actifs. Avec Lookout et Microsoft Enterprise Mobility + Security (EMS), les entreprises sont en mesure d'adopter une approche qui privilégie le mobile et le cloud pour fournir à leurs employés les outils dont ils ont besoin, tout en protégeant les données sensibles auxquelles ils accèdent via leurs appareils mobiles.



Avantages clés de l'alliance Lookout + Microsoft EMS

Une sécurité mobile totale pour libérer la productivité

Microsoft EMS fournit une solution de sécurité basée sur l'identité qui offre une approche holistique des défis de sécurité à l'heure où le mobile et le cloud sont rois. Lookout complète la sécurité d'EMS basée sur l'identité grâce à sa riche Threat Intelligence, en surveillant en continu l'appareil à la recherche de menaces mobiles, en transmettant ces informations directement à EMS afin d'informer les politiques d'accès conditionnel. Lookout protège des menaces utilisant quatre vecteurs d'attaque :

1. Les menaces applicatives : chevaux de Troie, logiciels espions, rootkits et applications non conformes diffusant des données sensibles
2. Les menaces basées sur le réseau : le phishing, les attaques man-in-the-middle et SSL capables de voler des données chiffrées en transit
3. Les menaces inhérentes au système d'exploitation : jailbreak avancé d'appareils iOS et root d'appareils Android
4. Le phishing et les menaces portant sur les contenus : les attaques de phishing touchant la messagerie électronique personnelle et professionnelle, la messagerie instantanée, les SMS et les applications

Accès conditionnel basé sur le risque

Les politiques d'accès conditionnel au sein d'Intune vous permettent de protéger la messagerie, les fichiers et autres ressources d'entreprise contre l'accès non autorisé, sur la base de facteurs personnalisables assurant la sécurité et la conformité, tels que l'emplacement, le statut de l'appareil ou de l'utilisateur, le degré de sensibilité et de risque des applications installées sur le terminal. Grâce à l'intégration Microsoft EMS et Lookout, vous pouvez intégrer la Threat Intelligence de Lookout aux politiques d'accès conditionnel définies dans Intune pour gérer et sécuriser l'accès à vos applications, comme les applications Office mobiles, et prendre des mesures pour effacer de manière ciblée des données sur les appareils.

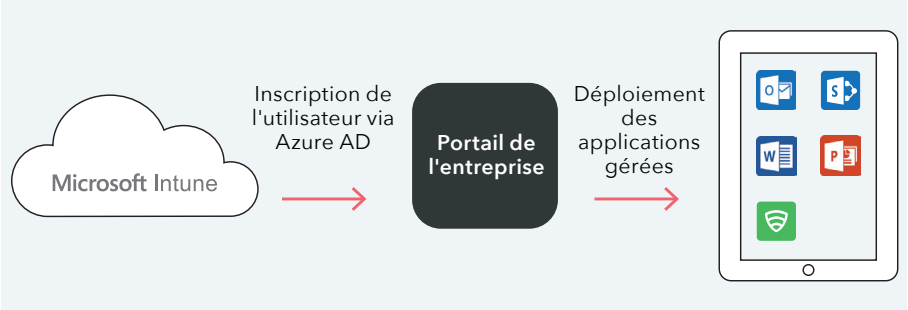
Facilité d'utilisation

L'intégration de Lookout et EMS permet un déploiement et une gestion en toute transparence de l'application client Lookout via Microsoft Intune, une gestion de politique intégrée pour les utilisateurs et les groupes, ainsi que de l'intégration à Azure Active Directory pour l'authentification unique des utilisateurs finaux et des administrateurs.

Fonctionnement de l'intégration

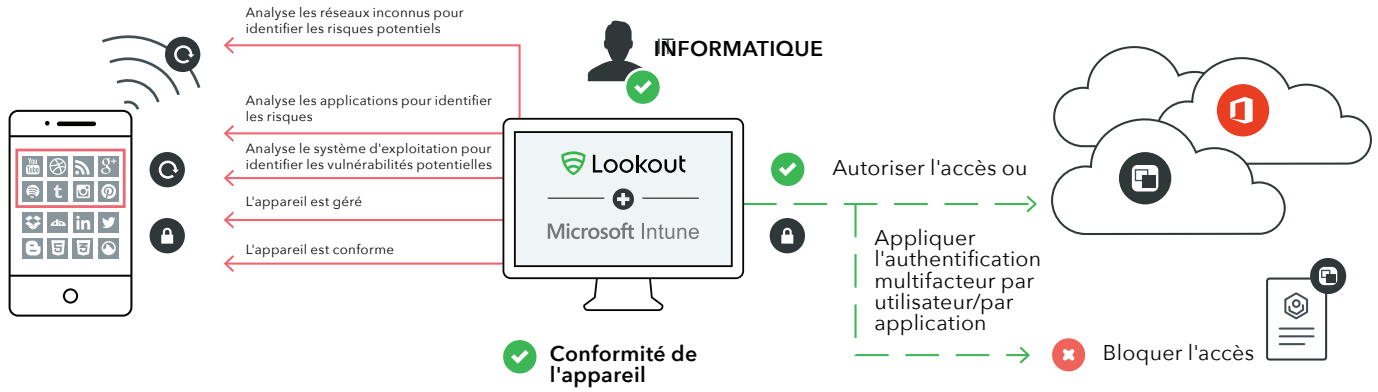
Provisionnement d'appareil

À l'aide de Microsoft Intune, l'application Lookout for Work peut être facilement distribuée sur l'ensemble de vos appareils mobiles, permettant un déploiement rapide, même sur plusieurs milliers de terminaux.



Accès conditionnel basé sur le risque

Lookout offre une visibilité sur les applications malveillantes ou la présence d'applications diffusant des données sensibles, ce qui permet à Intune d'évaluer l'état de conformité de l'application. Par exemple, si un employé du service des finances télécharge involontairement une application mobile malveillante, Lookout identifiera cette menace et déclenchera les politiques d'accès conditionnel d'Intune pour restreindre l'accès à vos données d'entreprise tant que la menace n'aura pas été écartée.



Pour en savoir plus sur la façon dont Microsoft EMS + Lookout peut vous aider à protéger votre organisation, rendez-vous sur lookout.com/microsoft.