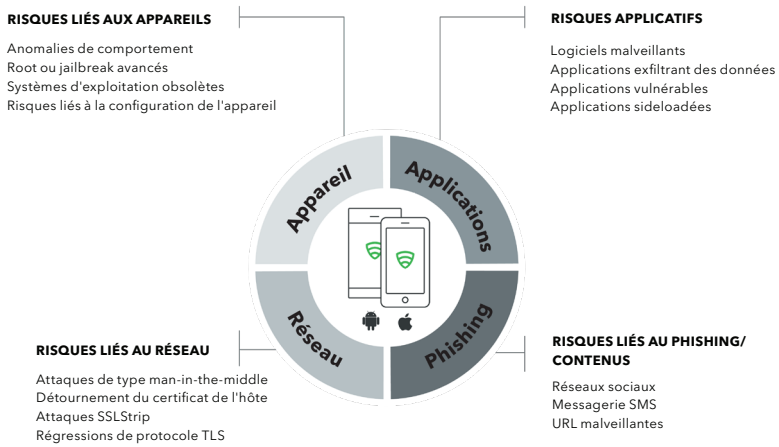
Partenariat Lookout + Microsoft

Lookout + Microsoft unissent leurs forces pour sécuriser la mobilité des entreprises

Vue d'ensemble

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. En combinant la protection mobile pour terminaux iOS et Android de Lookout et les solutions mobiles et de sécurité de Microsoft, les entreprises peuvent adopter une approche donnant la priorité au mobile et au cloud pour accroître la productivité de leurs employés tout en protégeant les données sensibles auxquelles ils accèdent via leurs terminaux mobiles.



Sécurité mobile complète

Lookout protège votre entreprise face au spectre des risques mobiles en utilisant sa Threat Intelligence basée sur le cloud pour détecter et prévenir :

- Le phishing par e-mail, SMS, messagerie et applications
- Les applications malveillantes et sideloadées
- Les risques de système d'exploitation, de configuration et de root/jailbreak
- Les attaques de type man-in-the-middle et de réseau

Lookout + Microsoft Azure Active Directory (AAD) et Intune

Accès conditionnel basé sur le risque

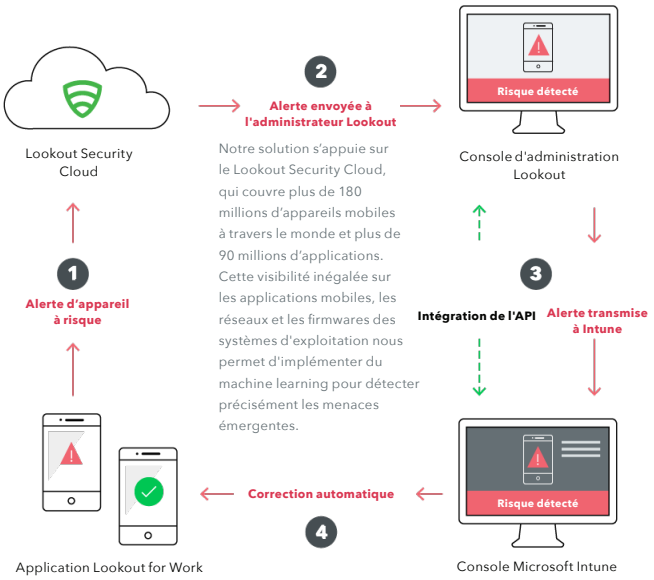
Avec l'intégration de Microsoft EMS et Lookout, Lookout peut informer Intune des risques liés aux appareils, comme les applications malveillantes, les vulnérabilités du système d'exploitation, les attaques du réseau, les tentatives de phishing et même les violations des politiques du RGPD par les applications. Ces alertes sont intégrées à la console d'administration Intune et peuvent servir à alimenter les politiques d'accès conditionnel, afin d'empêcher les terminaux à risques d'accéder aux ressources de l'entreprise tant que le défaut de conformité n'a pas été corrigé.

Facilité d'utilisation

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

Sécurité et conformité

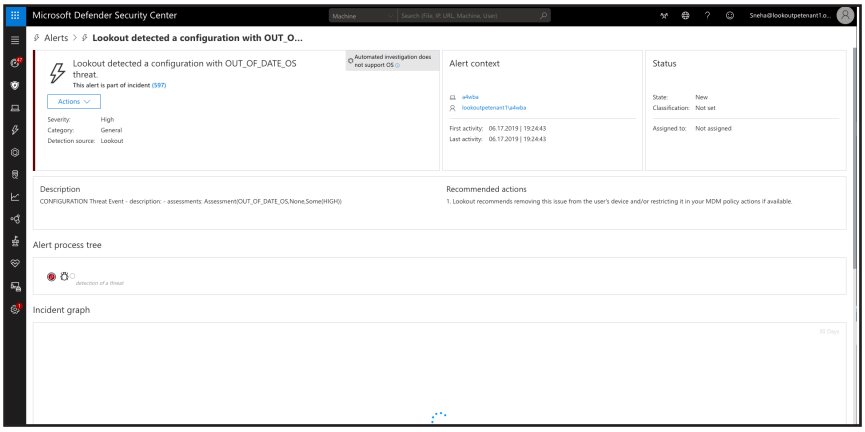
Grâce à la fonctionnalité de contrôle de la conformité des applications de Lookout, les entreprises peuvent identifier les applications mobiles qui enfreignent leurs politiques de gouvernance, de confidentialité ou de sécurité. Par exemple, il est possible de blacklister les applications révélant la liste de contacts ou la localisation de l'utilisateur et d'envoyer des informations à Intune pour la mise en place de politiques d'accès conditionnel.



Lookout + Microsoft Defender ATP

Intégration des alertes de sécurité mobile dans Defender ATP

La solution Lookout Mobile Endpoint Security est intégrée à la solution Defender Advanced Threat Protection (ATP) de Microsoft. Grâce cette intégration, les clients Microsoft peuvent détecter, afficher et examiner les cyberattaques avancées et les violations de données sur les appareils iOS et Android, et réagir depuis la console d'administration Microsoft Defender ATP. La console intégrée affiche les informations de Lookout sur la santé et les menaces des appareils sur le tableau de bord principal et dans les sous-sections, pour une expérience administrateur la plus complète.



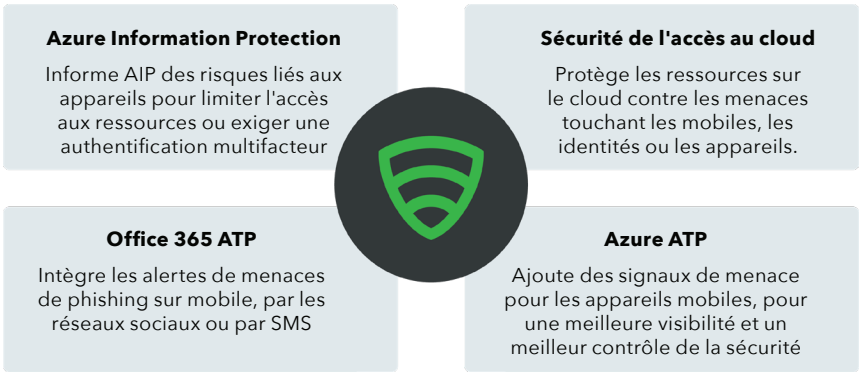
Meilleure visibilité sur les menaces mobiles

- Console intégrée pour les alertes mobiles
- Tableau de bord avec synthèse des menaces
- Corrélation entre les appareils de l'utilisateur
- Informations sur les alertes et recommandations de correction
- Historique des incidents de l'appareil mobile

Lookout + Microsoft Graph Security API

Données sur les menaces touchant les appareils mobiles en complement des outils de sécurité existants de Microsoft

Avec l'intégration de Lookout dans Microsoft Graph Security API, les clients peuvent consulter, recevoir, corréler et signaler la télémétrie des menaces mobiles depuis un écosystème d'applications connectées à Microsoft Graph. La télémétrie de Lookout peut être combinée en plus des signaux de sécurité issus de produits, de services et de solutions de sécurité Microsoft, ainsi qu'à d'autres fournisseurs Graph API.



Télémétrie des menaces à la puissance inégalée

- Pour que seuls les appareils sûrs aient accès aux ressources de l'entreprise
- Exploitation des signaux de menace pour alimenter l'accès conditionnel
- Les signaux d'alerte de phishing amplifient d'autres alertes d'ATP
- Intégration des signaux mobiles d'autres solutions Microsoft

Pourquoi choisir Lookout ?

Microsoft et Lookout se sont associés pour permettre aux entreprises d'utiliser des smartphones et des tablettes en toute sécurité sur le lieu de travail. Lookout et Microsoft partagent une même vision : appliquer les techniques de machine learning à un grand ensemble de données de sécurité pour détecter les nouvelles menaces et y réagir rapidement. Lookout a collecté les données de sécurité de plus de 180 millions d'appareils dans le monde et analysé plus de 90 millions d'applications iOS et Android à l'aide de techniques avancées de machine learning pour identifier les risques de ces plateformes. Partenaire privilégié de Microsoft, Lookout a été aux avant-postes de plusieurs intégrations précieuses dans Microsoft :

- **Microsoft Intune et Enterprise Mobility + Security.** Grâce à l'activation en toute transparence avec Azure Active Directory, Lookout applique le système d'accès conditionnel en continu de Lookout en fonction des risques en temps réel pour le réseau et l'appareil.
- **Microsoft Windows Defender ATP.** Grâce cette intégration, les clients Microsoft peuvent détecter, afficher et examiner les cyberattaques et les violations de données sur les appareils iOS et Android et y réagir depuis la console d'administration MD-ATP.
- **Microsoft Intelligent Security Graph.** Intégration en toute transparence pour partager les menaces mobiles basées sur la télémétrie de Lookout.
- **Microsoft Intune MAM :** Lookout évalue la santé des appareils mobiles et applique la politique d'accès conditionnel en continu aux applications compatibles avec MAM.

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