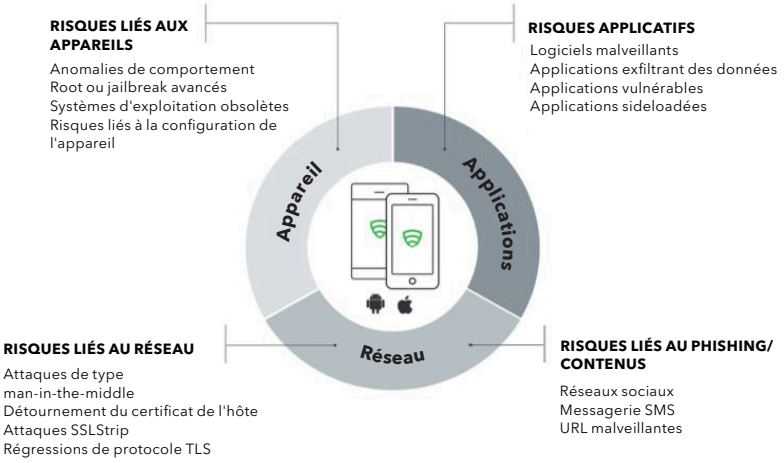
Lookout + Microsoft Windows Defender ATP

Un partenariat pour sécuriser la mobilité d'entreprise

Protection des données d'entreprise contre les menaces mobiles

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 appareils IOS et Android de Lookout et les solutions mobiles et de sécurité de Microsoft, les entreprises peuvent accroître la productivité de leurs employés tout en protégeant les données sensibles auxquelles ils accèdent via leurs appareils 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

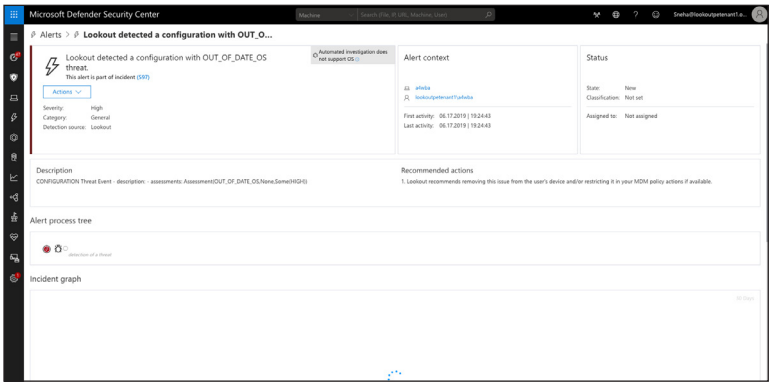
Lookout et Microsoft Windows Defender ATP

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

Parmi les informations, le type de menace, la description de la menace, le niveau de sévérité de la menace (faible, moyen, élevé) et des étapes de correction réalisées. Sont notamment identifiées les applications malveillantes, les attaques de phishing mobile, les attaques réseau et les vulnérabilités du système d'exploitation. Les notifications de menaces sont immédiatement envoyées à l'utilisateur et au portail Windows Defender ATP. L'intégration des informations sur les menaces des appareils mobiles, couplée avec celles des appareils Windows d'un même utilisateur donne une meilleure vue d'ensemble de la sécurité de l'environnement et des menaces auxquelles font face les utilisateurs.

Fonctionnement de l'intégration

L'intégration de Lookout et Windows Defender ATP se fait au moyen d'un connecteur Lookout ATP qui transmet les informations sur les menaces et les appareils mobiles de l'API Lookout Mobile Risk à l'API Windows Defender ATP. Cette intégration se fait sans Intune ou autre MDM, car le service de cloud de Lookout communique directement avec celui de Windows Defender. Les informations sur les menaces et les appareils mobiles mises en avant par Lookout sont propres à l'environnement du client et peuvent être intégrées au portail Windows Defender ATP, y compris le tableau de bord principal de l'administrateur, le tableau de bord analytique et les écrans sur les alertes et les appareils, pour une expérience administrateur simplifiée.



Fonctionnalités

- Console intégrée pour les alertes mobiles
- Tableau de bord de synthèse des menaces
- Corrélation avec les autres appareils de l'utilisateur
- Informations sur les alertes comprenant une description de la menace, la sévérité et des recommandations de correction
- Historique des incidents de l'appareil mobile

« L'intégration du service de protection contre les menaces mobiles de Lookout et du service Windows Defender ATP de Microsoft offre un niveau de visibilité et une capacité de réponse sans précédent sur tous les types d'appareils que nos clients doivent protéger. »

Moti Gindi

Directeur général de Windows Cyber Defense, 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. En tant que partenaire de Microsoft, Lookout est également aux avant-postes d'autres intégrations précieuses dans Microsoft, notamment **Microsoft Intune et Enterprise Mobility + Security Enterprise Mobility + Security, Microsoft Intelligent Security Graph** et **Microsoft Intune MAM**.