Lookout Mobile Endpoint Security

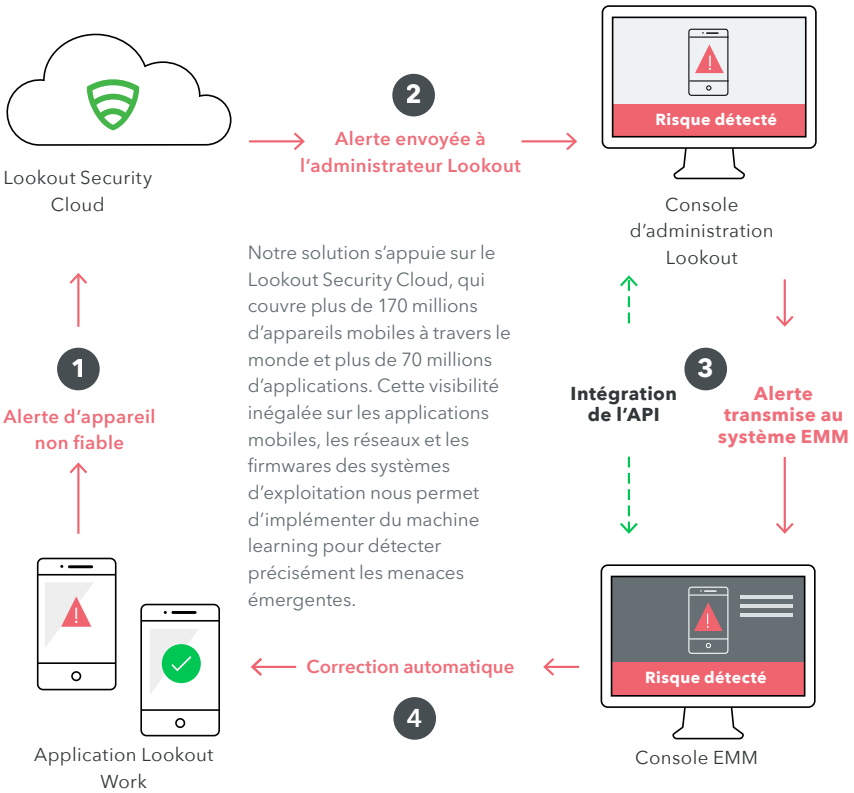
À mesure que vos données deviennent mobiles, Lookout renforce votre sécurité

Vue d'ensemble

De nombreuses entreprises décident aujourd'hui d'utiliser des smartphones et des tablettes pour accroître la productivité au travail. Avec toutefois de plus en plus de données sensibles disponibles sur mobile, les politiques de sécurité de votre entreprise doivent également englober vos points de terminaison mobiles. Lookout Mobile Endpoint Security vous offre une parfaite visibilité sur tout le spectre des risques mobiles et vous permet d'appliquer des politiques pour réduire ces risques de façon mesurable, tout en s'intégrant à vos solutions existantes de gestion de la sécurité et de la mobilité.

Fonctionnement

Lookout Mobile Endpoint Security repose sur l'utilisation d'une application endpoint discrète installée sur les appareils des employés. L'accès à la console d'administration cloud offre une visibilité en temps réel sur les risques mobiles et l'intégration aux principales solutions de gestion de la mobilité d'entreprise (EMM).



Avantages

Réduction mesurable des risques

Comblez vos principales lacunes en matière de sécurité et mesurez la réduction des risques grâce aux fonctionnalités d'analyse et de reporting de Lookout.

Interopérabilité parfaite

Lookout s'intègre à tous les systèmes SIEM via notre API Mobile Risk, y compris **Splunk, Windows Defender ATP, Micro Focus, ArcSight, IBM Security et QRadar**.

Visibilité sur les incidents mobiles

Bénéficiez d'une visibilité en temps réel sur les incidents détectés sur les appareils mobiles afin de pouvoir y répondre de manière rapide et efficace.

Mobilité sécurisée

Adoptez des programmes de mobilité plus flexibles, y compris le BYOD, afin d'améliorer la productivité des employés et rester compétitifs.

Protection des données dès la conception

Garantissez la souveraineté des données et le respect de la vie privée de vos collaborateurs grâce à nos fonctionnalités de contrôle de la confidentialité.

Facilité de maintenance et de déploiement

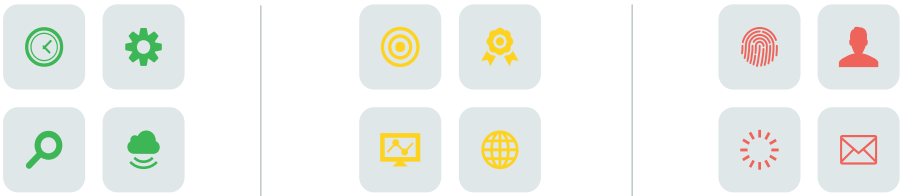
Nous l'intégrons avec n'importe quel système EMM (comme **VMware Workspace ONE® UEM, Microsoft Intune, BlackBerry® UEM, IBM MaaS360®**, et **MobileIron**) pour un déploiement et une gestion simplifiés.

Mobile Endpoint Security pour les menaces

Plus on accède aux données sensibles depuis des appareils mobiles, plus celles-ci deviennent la cible d'attaques informatiques. Lookout Mobile Endpoint Security identifie les menaces mobiles en ciblant ces principaux vecteurs d'attaque :

- Les menaces applicatives : logiciels malveillants, rootkits et logiciels espions
- Les menaces basées sur le réseau : attaques de type man-in-the-middle
- Les menaces inhérentes à l'appareil : appareils jailbreakés/rootés, systèmes d'exploitation obsolètes, configurations à risque

Mobile Endpoint Security pour les risques applicatifs



Aucun comportement à risque | **Certains comportements à risque** | **Comportements malveillants**

Certaines applications iOS et Android ne sont pas malveillantes en elles-mêmes, mais elles peuvent présenter des comportements à risque ou contenir des vulnérabilités qui contreviennent aux politiques de sécurité d'une entreprise, voire même enfreignent les exigences réglementaires concernant la perte de données. Lookout offre une visibilité complète sur ces risques applicatifs dans votre parc mobile, ce qui permet aux administrateurs de les surveiller et de définir des politiques actionnables pour les applications qui risquent d'enfreindre les exigences internes ou réglementaires.

Ce qui rend Lookout différent

- Grâce à notre présence mondiale et à l'importance que nous accordons au mobile, Lookout a réuni l'un des ensembles de données sur la sécurité mobile les plus importants au monde. Lookout a ainsi collecté les données de sécurité de plus de 170 millions d'appareils à travers le monde et de plus de 70 millions d'applications, avec jusqu'à 90 000 nouvelles applications ajoutées chaque jour.
- Ce réseau de capteurs mondial intègre la notion de prévisibilité à notre plate-forme en laissant l'intelligence artificielle identifier les modèles complexes synonymes de risque, modèles qui autrement échapperaient aux analystes humains.
- La mobilité a fait entrer l'informatique dans une nouvelle ère et nécessite une nouvelle solution de sécurité conçue exclusivement pour ses besoins. Lookout sécurise les appareils mobiles depuis 2007 et possède une solide expérience en la matière.

En fournissant aux équipes informatiques et de sécurité la visibilité dont elles ont besoin, Lookout offre à votre entreprise la possibilité d'intégrer la mobilité à son écosystème en toute sécurité sans sacrifier la productivité. Pour savoir dès aujourd'hui comment sécuriser votre parc mobile, contactez-nous à l'adresse lookout.com/fr.

Lookout Mobile Endpoint Security
Mobile Endpoint Security pour les menaces
Protection contre les menaces applicatives
Logiciel malveillant
Rootkits
Logiciel espion
Ransomware
Protection contre les menaces basées sur le réseau
Attaques de type man-in-the-middle
Attaques SSL
Protection contre les menaces inhérentes à l'appareil
Détection avancée des appareils jailbreakés/rootés
Vulnérabilités des systèmes d'exploitation
Configurations à risque des appareils
Protection contre les menaces Web et de contenu
Attaques de phishing depuis divers canaux
Des URL malveillantes aux sites Web à risque
Politiques personnalisées pour les menaces
Tableau de bord des menaces
Mobile Endpoint Security pour les risques applicatifs
Contrôle des fuites de données depuis les applications qui :
Accèdent aux données sensibles, telles que les calendriers
Envoient des données sensibles (ou personnelles) en dehors de l'entreprise
Communiquent avec des services cloud
Ne sécurisent pas suffisamment le stockage/transfert des données
Tableau de bord des applications à risque
Politiques personnalisées pour les applications à risque
Mise sur liste noire des applications
Analyse des applications de l'entreprise
Gestion et support
Intégration aux sytèmes EMM (VMware Workspace ONE® UEM, Microsoft Intune, Blackberry® UEM, IBM MaaS360®, et MobileIron)
Intégration aux systèmes SIEM via l'API Mobile Risk (Splunk, Windows Defender ATP, Micro Focus, ArcSight, IBM Security et QRadar)
Rapports de niveau exécutif montrant la réduction des risques
Contrôles d'accès basés sur des rôles
Contrôles de la confidentialité des données
Support accessible 24 h/24, 7 j/7

Lookout

lookout.com/fr