Lookout + EMM

La mobilité sécurisée pour votre organisation

De plus en plus, les organisations adoptent des programmes de mobilité formels pour renforcer la productivité mobile. Alors que les données deviennent jour après jour plus mobiles, associer une solution de gestion de la mobilité d'entreprise à une solution de sécurité mobile basée sur un service cloud fournit les couches défensives nécessaires pour protéger vos données d'entreprise :

EMM

- Gestion des appareils et effacement des données
- Séparation des données d'entreprise et des données à caractère personnel
- Accès aux applications d'entreprise
- Authentification et identification unique
- Accès mobile au contenu

Lookout Mobile Endpoint Security

- Protection contre les risques applicatifs
- Détection des risques réseau
- Détection des risques liés aux appareils
- Politique personnalisée de correction selon les types de menace
- Facilité de maintenance et de déploiement avec votre EMM

Intégration transparente pour fournir la mobilité sécurisée

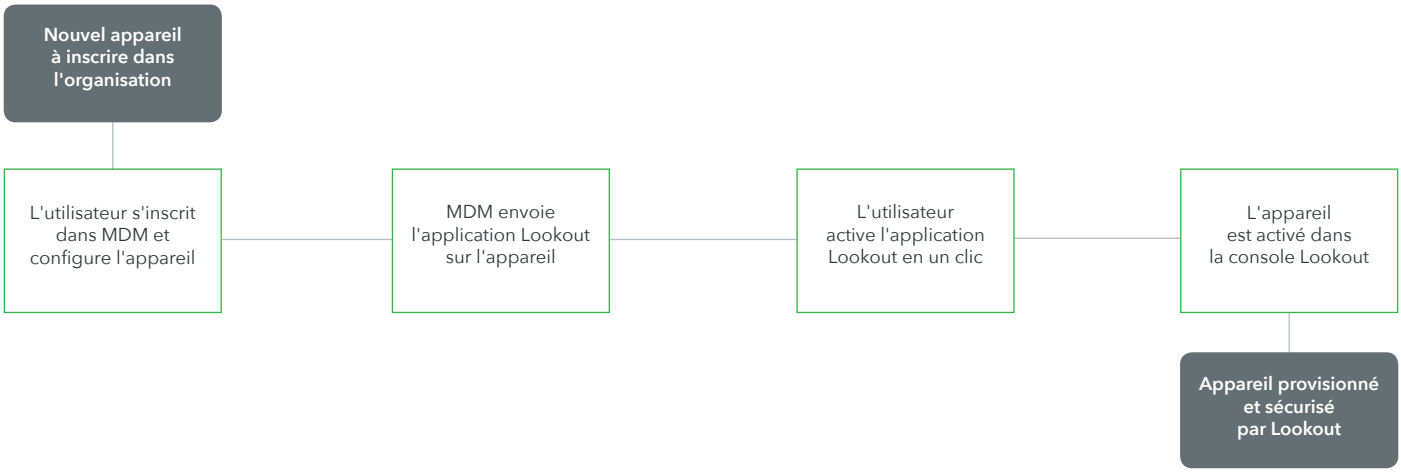
Risques	MDM uniquement	Lookout + MDM
Perte de l'appareil	✔ Localise l'appareil et efface son contenu à distance	✔ Localise l'appareil et efface son contenu à distance
Distribution des applications	✔ Distribution sécurisée des applications d'entreprise	✔ Distribution de l'application Lookout via MDM
Violation des règles	⚠ Établissement d'une liste noire des applications identifiées comme contraires à la politique de la société	✔ Détection et correction automatiques des applications violant les règles de sécurité
Fuite de données	⚠ Protection contre la fuite de données des employés à l'aide de conteneur	✔ Visibilité totale sur les fuites de données, y compris les comportements risqués des applications tels que l'envoi de données d'agenda vers l'extérieur
Jailbreak et root	⚠ Pas toujours efficace du fait de la nature des attaques ciblant le noyau du système d'exploitation	✔ Détection avancée du jailbreak/root par l'analyse de centaines de signaux de systèmes d'exploitation
Systèmes d'exploitation obsolètes	⚠ Possibilité d'indiquer manuellement une version de système d'exploitation minimale requise	✔ Visibilité totale sur les appareils avec systèmes d'exploitation et niveaux de correctif de sécurité Android obsolètes
Configurations à risque des appareils	⚠ Peut appliquer un mot de passe sur un appareil	✔ Visibilité sur plusieurs configurations à risque, comme le débogage USB activé
Vulnérabilités applicatives	X Aucune	✔ Détection des applications utilisant des méthodes de transfert/stockage de données non sécurisées
Applications malveillantes	X Aucune	✔ Détection intégrale des applications mobiles malveillantes passant inaperçues grâce aux technologies de réputation des applications
Exploits de conteneur	X Aucune	✔ Détecte les modifications des droits d'accès caractéristiques d'un exploit
Attaques de type man-in-the-middle	X Aucune	✔ Protection contre les attaques réseau malveillantes sur les données d'entreprise chiffrées en transit

X Aucune protection ⚠ Protection limitée ✔ Protégé

Fonctionnement de l'intégration

Provisionnement d'appareil

À l'aide de votre solution MDM, l'application de point de terminaison Lookout peut être facilement distribuée à l'ensemble de vos appareils mobiles, permettant un provisionnement d'appareil rapide et évolutif. Le processus de provisionnement d'appareil suit ces étapes de base :



Correction de risque

Grâce à notre intégration MDM, les appareils à risque peuvent être mis en quarantaine en temps réel grâce à des politiques de correction personnalisées. Lorsque Lookout détecte une menace, il classe l'appareil dans la catégorie « à haut risque », « à risque modéré » ou « à faible risque » selon les paramètres de votre politique de sécurité. Le processus de correction de risque suit ces étapes de base :