Lookout + VMware Workspace ONE UEM

Avec Accès Conditionnel Continu (ACC) pour les applications de productivité VMware Workspace ONE

À mesure que les données d'entreprise deviennent mobiles, le fait d'intégrer une solution unifiée de gestion des terminaux et une solution de détection des menaces mobiles basée sur le Cloud permet de protéger et de contrôler les appareils et les applications en dehors du périmètre de sécurité classique :

VMware Workspace ONE UEM

- Applications et données d'entreprise placées dans un conteneur
- Séparation des données d'entreprise et des données à caractère personnel
- Accès aux e-mails d'entreprise
- Accès fluide aux applications d'entreprise avec SSO
- Gestion unifiée des règles
- Distribution sécurisée des contenus mobiles
- DLP avancé pour les e-mails, les contenus et les applications

Lookout Mobile Endpoint Security

- Évaluation continue des risques liés aux applications placées dans un conteneur
- Protection contre le phishing
- Détection de jailbreak ou de rootage avancés
- Détection d'attaques de type man-in-the-middle
- Contrôle des fuites de données d'application pour garantir la conformité
- Visibilité dans les applications sideloadées
- Politique personnalisée de correction selon les types de menaces

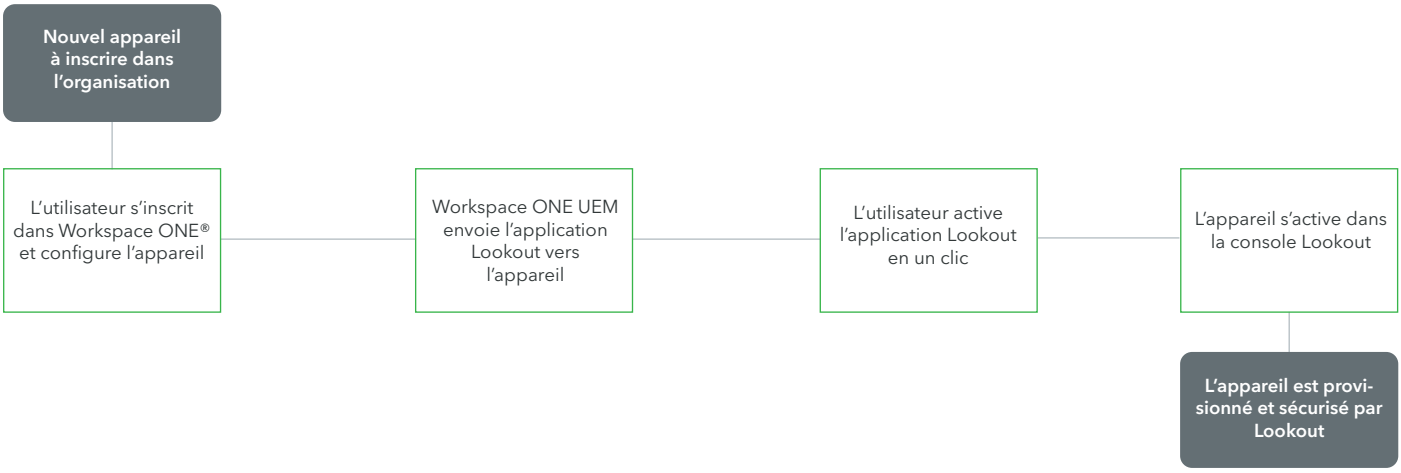
Intégration transparente pour la sécurité des mobiles

Risques	VMware Workspace ONE UEM	Workspace ONE UEM + Lookout
Distribution des applications	Sécurise la distribution des applications d'entreprise aux employés	Distribue facilement les applications de terminaux de Lookout sur les appareils des employés
Violation des règles	Si un appareil non conforme est détecté, des mesures sont prises automatiquement pour remettre l'appareil en conformité	Les décisions de conformité peuvent désormais prendre en compte l'existence de menaces ou d'applications risquées détectées par Lookout
Risques applicatifs	Place dans un conteneur les applications et données d'entreprise, telles que les e-mails ou les contenus	Offre une visibilité sur les applications qui présentent des fuites de données ainsi que sur les logiciels malveillants tels que les chevaux de Troie et les logiciels espions
Réseaux non protégés	La mise en tunnel du trafic permet de limiter l'accès au réseau par l'appareil aux applications d'entreprise gérées sur l'appareil	Protection contre les attaques de type man-in-the-middle qui ciblent des données d'entreprise chiffrées en transit
Accès Conditionnel Continu	L'accès aux ressources de l'entreprise peut être révoqué automatiquement en cas de violation des règles de conformité	L'accès aux applications de productivité VMware® Workspace ONE peut être révoqué si Lookout détecte des menaces inhérentes au réseau, à une application ou au système d'exploitation
Jailbreak et root	Détection de base des appareils jailbreakés et rootés	Analyse des centaines de signaux de système d'exploitation pour identifier les tentatives de contournement de la détection de base du jailbreak et du root
Attaques de phishing	Aucune	Empêche les connexions via des URL malveillantes contenues dans des e-mail, des SMS ou des applications de messageries, ou intégrées dans des applications
Appareils perdus/volés	Détecte les appareils perdus ou volés, ou efface à distance les données et les applications d'entreprise	Détecte les appareils perdus ou volés, ou efface à distance les données et les applications d'entreprise
Authentification non sécurisée	Connexion mobile unique one touch sur le Web, le Cloud et les applications mobiles	Connexion mobile unique one touch sur le Web, le Cloud et les applications mobiles

Fonctionnement de l'intégration

Provisionnement d'appareil

En intégration avec la solution Workspace ONE® Unified Endpoint Management (UEM) optimisée par AirWatch®, l'application de terminaux Lookout peut être facilement distribuée sur l'ensemble des appareils mobiles gérés, permettant un provisionnement d'appareil rapide et évolutif. Le processus de provisionnement d'appareil suit ces étapes de base :



Accès Conditionnel Continu (ACC) pour les applications de productivité VMware Workspace ONE

Au moyen de notre intégration Workspace ONE UEM, les appareils à risque peuvent être mis en quarantaine en temps réel grâce à des politiques de correction personnalisées. Il est notamment possible de bloquer l'accès aux applications placées dans un conteneur VMware Boxer sur des appareils non gérés, conformément au statut de risque indiqué par Lookout. 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 des menaces suit les étapes de base suivantes :