Lookout + BlackBerry UEM

La mobilité sécurisée pour votre organisation

De plus en plus, les organisations adoptent des programmes de mobilité formels pour renforcer la productivité mobile. À mesure que les données d'entreprise deviennent mobiles, le fait d'associer une solution unifiée de gestion des terminaux à une solution de sécurité mobile basée sur le Cloud vous permet de bénéficier des couches défensives nécessaires à la protection de 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
- Protection contre le phishing
- Détection des risques réseau
- Détection des risques liés aux appareils
- Politique personnalisée de correction selon les types de menaces
- Facilité de maintenance et de déploiement avec votre EMM

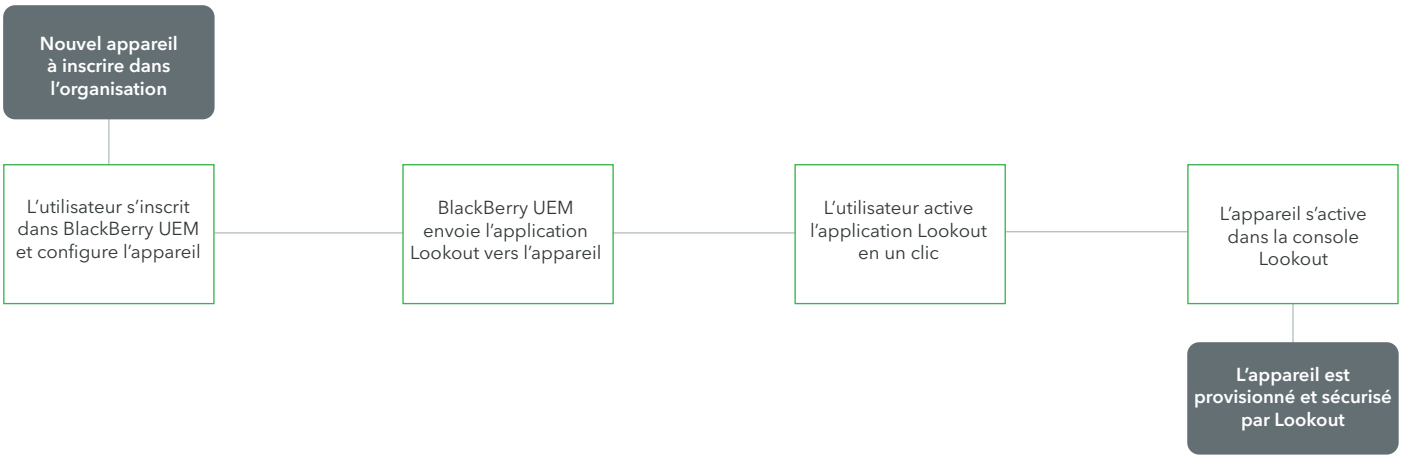
Intégration transparente pour sécuriser les mobiles

Risques	BlackBerry UEM seul	Lookout + BlackBerry UEM
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	Sécurise la distribution des applications d'entreprise	Distribution de l'application Lookout via BlackBerry UEM
Violation des règles	Possibilité de créer manuellement une liste noire des applications identifiées comme contraires à la politique de l'entreprise	Détection et correction automatique des applications qui violent des politiques de sécurité
Fuite de données	Protection contre la fuite de données des employés à l'aide de conteneurs	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 forcer la demande de mot de passe sur un appareil	Visibilité sur plusieurs configurations à risque, telles que l'activation du débogage USB
Vulnérabilités applicatives		Détection des applications qui utilisent des méthodes de stockage/transfert de données non sécurisées
Applications malveillantes		Détection intégrale des applications mobiles malveillantes qui passent inaperçues grâce aux technologies de réputation des applications
Attaques de phishing		Empêche les connexions via des URL malveillantes contenues dans des e-mails, des SMS ou des applications de messageries, ou intégrées dans des applications
Attaques de conteneur		Détecte les modifications des droits d'accès caractéristiques d'une attaque
Attaques de type man-in-the-middle		Protection contre les attaques réseau malveillantes qui ciblent des données d'entreprise chiffrées en transit

Fonctionnement de l'intégration

Provisionnement d'appareil

À l'aide de votre solution BlackBerry UEM, l'application de terminaux Lookout peut être facilement distribuée sur l'ensemble de vos appareils mobiles, pour 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 BlackBerry UEM, les appareils à risque peuvent être mis en quarantaine en temps réel grâce à des politiques de correction personnalisées. Lorsque Lookout détecte un risque, 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 :