MobileIron pour Samsung KNOX Android

Avec un milliard d'appareils sous Android et 1,5 million d'appareils supplémentaires activés chaque jour, Android domine actuellement le marché du mobile grand public. En revanche, dans les entreprises, l'adoption de ces mobiles a progressé beaucoup plus lentement du fait d'une inquiétude persistante concernant la sécurité et la fragmentation d'Android. Mais cette situation est sur le point d'évoluer radicalement, car les organisations ne peuvent plus ignorer la place prépondérante des smartphones et des tablettes Android sur le marché, ni l'émergence d'une forte demande de la part des employés pour les utiliser au travail.

Pour autoriser en toute sécurité l'utilisation d'Android dans l'entreprise, les équipes informatiques doivent pouvoir appliquer les exigences de sécurité et de conformité à tous les appareils sans aucune incidence sur les applications et données personnelles. Pour répondre à ces exigences complexes, il est nécessaire de disposer d'une plateforme informatique conçue spécialement pour sécuriser les contenus, les applications et les appareils dans des environnements multi-OS. Ainsi, les équipes informatiques peuvent garantir la protection des données tout en offrant aux utilisateurs la liberté et le choix qu'ils demandent.

MobileIron et Samsung : accélérer l'adoption de Samsung Android dans l'entreprise

Pour permettre une utilisation sécurisée d'Android dans l'entreprise, MobileIron et Samsung collaborent afin de fournir les solutions de mobilité les plus sécurisées et les plus puissantes pour les déploiements d'appareils Samsung Android personnels ou fournis par l'entreprise.

MobileIron a longtemps été un champion de l'adoption d'Android dans l'entreprise, et il a été le premier fournisseur à proposer une boutique d'applications professionnelles, des contrôles de la confidentialité BYOD et la gestion des identités à l'aide de certificats pour Android. La plateforme globale de gestion de la mobilité en entreprise (Enterprise Mobility Management, EMM) est entièrement compatible avec la plateforme Samsung KNOX, pour un meilleur contrôle de la sécurité pour Android.

Les appareils Samsung KNOX fournissent les services matériels et systèmes d'exploitation sur lesquels MobileIron s'appuie pour répondre aux besoins des entreprises en matière de messagerie, d'accès Wi-Fi et VPN. Samsung KNOX fournit également une sécurité de classe militaire intégrée au matériel et la séparation entre les données personnelles et professionnelles sur les appareils Android. L'alliance de MobileIron et de Samsung fournit une solution complète de sécurisation des appareils et des applications Android répondant aux exigences uniques de tout service informatique.

Défi

- Renforcer la sécurité des données sensibles sous Android
- Aider les entreprises à développer des applications Android
- Aider les entreprises à mettre en œuvre des initiatives BYOD avec des appareils Android
- Effectuer la transition depuis BlackBerry

Solution

- MobileIron pour Samsung KNOX Android

Atouts

- Sécurisation du cycle de vie des applications mobiles
- Configuration de tous les services principaux
- Établissement de contrôles de sécurité et de protection de la vie privée
- Protection des données statiques grâce aux contrôles DLP (prévention de la perte de données) et au chiffrement
- Gestion du cycle de vie de l'application
- Déploiement à grande échelle

Récompenses récentes

- Gartner : en 2014, et pour la quatrième année consécutive, MobileIron figure parmi les premières entreprises du Magic Quadrant pour les suites de gestion de la mobilité en entreprise (EMM)

MobileIron - 415 East Middlefield Road - Mountain View, CA 94043, États-Unis Tél. +1 650 919 8100 - Fax +1 650 919 8006 - info@mobileiron.com

Sécurisation des appareils avec Samsung KNOX

Samsung KNOX est une structure de sécurité Android spécifiquement développée pour l'entreprise. KNOX comporte des fonctionnalités de sécurité matérielle et logicielle qui aident les équipes informatiques à déployer Android comme principale plateforme informatique. Voici les principaux composants de cette solution :

- Amélioration de la détection des manipulations des systèmes d'exploitation et du root via la fonction Trusted Boot (démarrage fiable) et des mécanismes de sécurité intégrés au matériel tels que TrustZone-based Integrity Measurement Architecture (TIMA) qui empêchent l'accès aux données de l'entreprise par des appareils piratés.
- Le magasin de clés TIMA intégré au matériel protège les clés de chiffrement : celles-ci sont accessibles uniquement par des appareils conformes et exécutant des logiciels fiables et approuvés par des technologies de validation spéciales.
- Séparation des données pour les services d'applications et de systèmes grâce aux améliorations apportées à SE pour Android et à une API SEAMS (SE for Android Management) utilisée pour sécuriser les conteneurs d'applications.

Sécurité des applications : deux solutions conteneurisées

Les fonctions de renforcement de la sécurité Android indiquées ci-dessus portent principalement sur la surveillance de l'intégrité des logiciels et la sécurisation de l'appareil. Samsung KNOX et MobileIron proposent deux options de protection des applications : Samsung KNOX Workspace et MobileIron AppConnect pour KNOX. Chacune de ces options fournit des niveaux divers de contrôle et de sécurité granulaires en fonction des besoins de l'organisation.

Option 1 : Samsung KNOX Workspace

Samsung KNOX Workspace est un conteneur sécurisé qui forme une barrière de protection autour des applications et des données qu'il contient en bloquant tout accès par des applications résidant à l'extérieur du conteneur. Par exemple, il n'est pas possible d'ouvrir les documents stockés dans l'espace de travail KNOX Workspace si les éditeurs à utiliser ne résident pas dans le conteneur.

Cet espace de travail comprend tout un éventail de règles pour l'authentification, la sécurité des données, les VPN par application, la messagerie, la distribution d'applications et le contrôle des informations échangées entre le conteneur et le reste de l'appareil. L'ensemble de ces processus est géré via la plateforme EMM de MobileIron.

KNOX Workspace est plus spécialement approprié aux entreprises présentant les caractéristiques suivantes :

- Déploiements mobiles prêts à l'emploi sur les appareils Samsung KNOX
- Déploiement d'applications conteneurisées tierces et personnalisées ne nécessitant pas de configurations propres à l'application
- Activité dans des secteurs hautement réglementés avec des exigences spécifiques de conformité et de contraintes réglementaires

KNOX Workspace est idéal pour gérer les types d'environnements suivants :

Déploiements haute sécurité : le flux d'informations doit être géré rigoureusement et la protection des données assurée par des contrôles de prévention de perte de données (DLP). La plateforme Samsung KNOX fournit des fonctions de chiffrement et d'authentification de classe militaire telles que le chiffrement avec validation FIPS et la prise en charge de l'authentification par carte CAC.

Appareils en mode kiosque : KNOX Workspace est idéal pour un grand nombre d'entreprises des secteurs du service sur site, de la logistique et de la distribution dans lesquels le processus métier principal est contenu dans une application unique. Par exemple, dans un environnement de prestation de service, KNOX Workspace permet de maintenir un appareil et une application de commande dans un état de disponibilité sécurisée permanente pour permettre à l'employé de traiter rapidement les commandes.

Option 2 : MobileIron AppConnect pour KNOX

MobileIron AppConnect pour Samsung KNOX isole les applications dans des conteneurs pour protéger les données statiques sans toucher aux données personnelles. Chaque application se transforme en un conteneur sécurisé dont les données sont cryptées, protégées contre tout accès non autorisé et amovibles. Étant donné que chaque utilisateur a recours à un grand nombre d'applications d'entreprise, tous les conteneurs sont également connectés à d'autres conteneurs d'applications sécurisés. De la sorte, les règles, comme la signature unique pour les applications, et les données, comme les documents, peuvent être partagées. Tous les conteneurs d'applications sont connectés à MobileIron à des fins de gestion des règles.

Grâce à AppConnect pour Samsung KNOX, les clients combinent la solution de conteneurisation AppConnect multiplateforme aux fonctionnalités avancées de sécurité des appareils Samsung KNOX.

AppConnect pour Samsung KNOX est plus spécialement approprié aux entreprises présentant les caractéristiques suivantes :

- Environnement multi-OS avec divers systèmes d'exploitation mobiles tels qu'iOS et différents modèles d'appareils Android
- Déploiement d'applications encapsulées avec prise en charge de la signature unique pour les applications, du contrôle des accès de niveau application et la possibilité d'appliquer des configurations propres à l'application
- Besoin d'applications fournissant un accès sécurisé et l'application des règles de prévention de la perte de données pour l'intranet de l'entreprise, avec partage des fichiers sans infrastructure VPN

AppConnect pour Samsung KNOX est idéal pour les environnements suivants :

Gestion de programme BYOD/COPE : le service informatique prend en charge à la fois des appareils BYOD et des appareils fournis par l'entreprise avec utilisation personnelle autorisée (COPE). Dans cet environnement, AppConnect pour Samsung KNOX permet au service informatique de créer une entité entreprise qui sépare les données et applications professionnelles des données personnelles sans modifier l'expérience utilisateur native.

Gestion granulaire des applications : la combinaison de la plateforme EMM globale de MobileIron avec les appareils Android d'entreprise de Samsung permet aux organisations d'autoriser en toute confiance et en toute sécurité l'utilisation

d'Android. Avec la solution MobileIron pour Samsung Android, les entreprises peuvent déployer des applications à grande échelle tout en automatisant les configurations et paramètres d'application. Cette solution est idéale pour les organisations qui ont besoin de déployer des applications encapsulées avec prise en charge de la signature unique pour les applications, du contrôle des accès de niveau application et des configurations propres à l'application. Elle garantit également un accès sécurisé par l'application des règles de prévention de la perte de données pour l'intranet de l'entreprise et le partage des fichiers sans infrastructure VPN.

Franchissez le pas

Pour en savoir plus sur la solution MobileIron pour Samsung Android, rendez-vous sur www.mobileiron.com.

MobileIron et Samsung offrent aux organisations la sécurité et la gestion des applications avancées dont elles ont besoin pour adopter massivement Android comme norme de leur informatique mobile.

Gartner, Inc., Leaders Quadrant for Enterprise Mobility Management, 2014. Gartner ne soutient ni ne promeut aucun fournisseur, produit, ni service mentionné dans ses publications de recherche et ne conseille pas aux utilisateurs de technologies de sélectionner uniquement les vendeurs présentant les meilleures évaluations. Les publications de recherche de Gartner sont constituées d'opinions du service de recherche de Gartner et ne doivent pas être considérées comme des déclarations factuelles. Gartner décline toute garantie, explicite ou implicite, relative aux présentes recherches, y compris toute garantie de valeur commerciale ou d'adaptation à un usage spécifique.

MobileIron - 415 East Middlefield Road - Mountain View, CA 94043, États-Unis Tél. +1 650 919 8100 - Fax +1 650 919 8006 - info@mobileiron.com