MobileIron

MobileIron AppConnect et AppTunnel :

Sécurité avancée pour les données et les applications mobiles

La multiplication des technologies mobiles et cloud a permis aux entreprises du monde entier d'augmenter leur productivité comme jamais auparavant. Toutefois, la sécurisation des appareils, des applications et des services cloud qui accèdent aux données d'entreprise critiques représente un défi permanent pour votre équipe de sécurité mobile. Vous devez par exemple :

- autoriser en toute sécurité les appareils personnels pour une utilisation professionnelle ;
- vous assurer que les applications personnelles ne peuvent pas accéder aux données et aux services cloud de l'entreprise ;
- protéger les données statiques sur les appareils et les données transférées vers le cloud ou vers un backend de l'entreprise ;
- empêcher l'accès aux données ou leur partage via des applications non autorisées, comme une version personnelle d'Office 365.

MobileIron AppConnect et AppTunnel fonctionnent ensemble pour vous permettre de respecter toutes ces exigences en matière de sécurité cloud et mobile.

MobileIron AppConnect

MobileIron AppConnect isole les applications dans des conteneurs pour protéger les données d'entreprise statiques sans toucher aux données personnelles. Chaque application se transforme en un conteneur sécurisé dont les données sont chiffrées, protégées contre tout accès non autorisé et supprimables. Chaque conteneur d'application est connecté à d'autres conteneurs d'application sécurisés par le biais de la plateforme de gestion MobileIron, de sorte que les règles, telles que l'authentification unique, puissent être facilement partagées et mises à jour sur les appareils.

MobileIron AppTunnel

MobileIron AppTunnel protège les données réseau à l'aide d'un VPN innovant, compatible avec plusieurs systèmes d'exploitation et qui prend en charge les appareils iOS, Android et Windows 10. AppTunnel offre une sécurité précise qui agit application par application afin de connecter chaque conteneur d'application au réseau de l'entreprise. Ainsi, les organisations peuvent sécuriser le trafic des applications d'entreprise sans interférer avec celui des applications personnelles, comme lorsqu'un utilisateur publie une photo de famille sur Facebook.

Principaux avantages

- Sécurisation des données d'application stockées sur l'appareil et des données transférées vers le cloud ou vers un backend de l'entreprise.
- Séparation des applications et données professionnelles et personnelles sur l'appareil.
- Accès sécurisé aux applications sans VPN.
- Configuration, déploiement et mise à jour des applications et des règles, sans intervention des utilisateurs.
- Prise en charge du SDK et des méthodes d'encapsulage pour la conteneurisation des applications.
- Déploiement sur les appareils iOS, Android et Windows 10.
- Administration des applications internes et publiques.

MobileIron

À propos de MobileIron

MobileIron propose un socle de sécurité pour le travail moderne aux entreprises du monde entier, quelle que soit leur taille. Pour obtenir plus d'informations, consultez le site **www.mobileiron.com** ou contactez votre représentant commercial MobileIron.

Fonctionnalités

AppConnect

MobileIron AppConnect crée un conteneur d'applications sécurisé, via un SDK et un encapsuleur pour iOS ou un encapsuleur pour Android. Ce conteneur est connecté à d'autres conteneurs d'applications sécurisés par le biais de la console MobileIron, et offre les fonctionnalités de gestion suivantes :

- **Authentication :** confirme l'identité à l'aide du nom d'utilisateur et du mot de passe de domaine ou des certificats afin que seuls les utilisateurs approuvés puissent accéder aux applications d'entreprise.
- **Authentification unique :** simplifie l'authentification des utilisateurs sur les conteneurs d'applications.
- **Autorisation :** autorise ou bloque l'utilisation ou le stockage des applications selon le statut des appareils.
- **Configuration :** configure et déploie en arrière-plan les paramètres personnalisés tels que le nom d'utilisateur, le nom du serveur ainsi que les attributs personnalisés, sans intervention des utilisateurs.
- **Chiffrement :** garantit que toutes les données d'application stockées sur l'appareil sont chiffrées.
- **Contrôles DLP :** définit des règles de prévention contre la perte de données (DLP), telles que les autorisations de copier/coller, d'impression et d'ouverture, afin que les données sensibles ne quittent pas le conteneur.
- **Règles dynamiques :** met à jour les règles des applications sur tous les appareils gérés ou sur un sous-ensemble d'appareils selon le groupe, le rôle d'utilisateur et d'autres facteurs.
- **Rapports :** génère des statistiques détaillées sur l'utilisation des applications, des journaux d'audit ainsi que d'autres rapports afin d'améliorer la gestion et de simplifier la mise en conformité.
- **Effacement sélectif :** supprime à distance les applications et les données d'entreprise sans toucher aux données personnelles.

AppTunnel

AppTunnel offre plusieurs couches de sécurité pour les données des applications mobiles sans VPN. Ses fonctionnalités comprennent les éléments suivants :

- **Connexion unique :** permet uniquement aux applications, utilisateurs et appareils autorisés de se connecter aux ressources de l'entreprise.
- **Authentification basée sur les certificats :** configure en toute simplicité les appareils à l'aide de certificats d'identité et de configurations VPN, permettant ainsi aux employés d'accéder aux ressources de l'entreprise en toute sécurité et en toute transparence.
- **Règles de contrôle d'accès :** bloque l'accès au réseau si la sécurité est menacée dans l'application.
- **MobileIron Sentry :** AppTunnel s'appuie sur la technologie Sentry, offrant une passerelle intégrée qui gère, chiffre et sécurise le trafic entre l'appareil mobile et les systèmes backend de l'entreprise.
- **MobileIron Access :** AppTunnel prend également en charge MobileIron Access, qui s'assure que seuls les terminaux, les utilisateurs, les applications et les services cloud autorisés peuvent accéder aux données de l'entreprise, et renforce la sécurité grâce à l'authentification multifacteur.