



MobileIron AppConnect e AppTunnel:

sicurezza avanzata per dati e app mobili

Il costante aumento di tecnologie mobili e cloud ha consentito alle imprese globali di intensificare la produttività come mai prima d'ora. Tuttavia, la sicurezza dei dispositivi, delle app e dei servizi cloud che hanno accesso a dati aziendali critici rappresenta una sfida inesorabile per il team che si occupa della sicurezza mobile. È infatti necessario:

- Garantire un utilizzo sicuro dei dispositivi personali per le attività lavorative.
- Verificare che le app personali non possano accedere ai dati aziendali e ai servizi cloud.
- Proteggere i data-at-rest sul dispositivo e in transito verso il cloud o il backend aziendale.
- Evitare la condivisione dei dati o l'accesso ai dati tramite app non autorizzate, come la versione personale di Office 365.

MobileIron AppConnect ed AppTunnel lavorano in sinergia per soddisfare tutti questi requisiti di sicurezza mobile e sicurezza nel cloud.

MobileIron AppConnect

MobileIron AppConnect containerizza le app per proteggere i data-at-rest delle app senza interferire con i dati personali. Ogni app diventa un contenitore sicuro i cui dati sono crittografati, protetti da accessi non autorizzati e rimovibili. Ciascun contenitore di app è inoltre connesso ad altri contenitori di app sicure tramite la piattaforma di gestione MobileIron, in modo che le policy, come il Single Sign-On (SSO) per app, possano essere condivise e aggiornate facilmente tra i vari dispositivi.

MobileIron AppTunnel

MobileIron AppTunnel protegge i dati di rete con un'innovativa VPN per-app multi-OS che supporta dispositivi iOS, Android, e Windows 10. AppTunnel fornisce una sicurezza di sessione per-app granulare per connettere ciascun contenitore di app alla rete aziendale. Ciò consente alle aziende di proteggere il traffico proveniente dalle app aziendali senza interferire con il traffico personale, ad esempio nel caso in cui un utente pubblici una foto di famiglia su Facebook.

Principali vantaggi

- Protezione dei dati delle app sul dispositivo e in transito verso il cloud o il backend aziendale.
- Separazione di app e dati aziendali da app e dati personali sul dispositivo.
- Disponibilità di un accesso sicuro alle app anche senza VPN.
- Configurare, eseguire il deployment e aggiornare app e policy senza alcun intervento da parte degli utenti.
- Supportare metodi SDK e wrapping per la containerizzazione delle app.
- Eseguire il deployment su dispositivi iOS, Android e Windows 10.
- Amministrare app private e pubbliche.

Informazioni su MobileIron

MobileIron offre una base sicura per gli ambienti di lavoro moderni delle aziende globali di ogni dimensione. Per ulteriori informazioni, visitare www.mobileiron.com o contattare il rappresentante delle vendite di MobileIron.

AppConnect

AppConnect crea un contenitore di app sicuro tramite un SDK e un wrapper per iOS o tramite un wrapper per Android. Questo contenitore è connesso ad altri contenitori di app sicuri tramite la console MobileIron e offre le seguenti funzionalità di gestione:

- **Autenticazione:** conferma dell'identità tramite il nome utente e la password del dominio o tramite certificati, in modo che solo gli utenti autorizzati possano accedere alle app aziendali.
- **SSO:** autenticazione dell'utente semplificata per tutti i contenitori di app.
- **Autorizzazione:** possibilità di consentire o bloccare l'utilizzo o l'archiviazione di app in base alla postura del dispositivo.
- **Configurazione:** configurazione e invio automatico delle impostazioni personalizzate, come il nome utente, il nome del server e gli attributi personalizzati, senza alcun intervento degli utenti per l'attivazione.
- **Cifatura:** garanzia che tutti i dati delle app archiviati sul dispositivo siano cifrati.
- **Controlli DLP:** impostazione di policy di prevenzione della perdita dei dati (DLP), come autorizzazioni per le funzioni di Apri in, Copia/Incolla e Stampa, in modo che i dati sensibili non escano dal contenitore.
- **Policy dinamica:** aggiornamento delle policy delle app su tutti i dispositivi gestiti o su un sottoinsieme di dispositivi in base al gruppo, al ruolo dell'utente e ad altri fattori.
- **Reportistica:** generazione di statistiche dettagliate sull'utilizzo delle app, log di audit e altri report per migliorare la gestione e semplificare la conformità.
- **Cancellazione selettiva:** cancellazione di app e dati aziendali da remoto senza interferire con i dati personali.

AppTunnel

AppTunnel fornisce diversi livelli di sicurezza per i dati delle app mobili senza che sia necessaria alcuna VPN. Le funzionalità includono:

- **Connessione univoca:** solo le app, gli utenti e i dispositivi autorizzati possono connettersi alle risorse aziendali.
- **Autenticazione di sessione basata su certificato:** configurazione intuitiva dei dispositivi con certificati di identità e configurazioni VPN, che consentono un accesso aziendale semplice e sicuro per i dipendenti.
- **Regole di controllo degli accessi:** blocco dell'accesso alla rete se la sicurezza lato app risulta compromessa.
- **MobileIron Sentry:** AppTunnel si basa sulla tecnologia Sentry, che fornisce un gateway in-line che consente di gestire, crittografare e proteggere il traffico tra il dispositivo e i sistemi aziendali backend.
- **MobileIron Access:** AppTunnel supporta inoltre MobileIron Access, che consente solo a endpoint, utenti, app e servizi cloud autorizzati di accedere ai dati aziendali, e offre ulteriore sicurezza tramite l'autenticazione multifattore.