MobileIron

MobileIron AppConnect y AppTunnel:

seguridad avanzada para aplicaciones y datos móviles

La proliferación de tecnologías móviles y en la nube ha hecho posible que las empresas internacionales hayan podido impulsar su productividad como nunca antes. Sin embargo, segurizar los dispositivos, las aplicaciones y los servicios en la nube que acceden a datos corporativos críticos supone un desafío constante para los equipos de seguridad móvil. Entre otras cosas, hay que hacer lo siguiente:

- Habilitar de forma segura los dispositivos personales para el trabajo.
- Garantizar que las aplicaciones personales no puedan acceder a datos corporativos ni a los servicios en la nube.
- Proteger los datos en reposo tanto en el dispositivo como en tránsito hacia la nube o en el *back-end* de la empresa.
- Prevenir que los datos se compartan o se acceda a ellos a través de aplicaciones no autorizadas, como la versión personal de Office 365.

MobileIron AppConnect y AppTunnel funcionan conjuntamente para ayudarle a cumplir todos estos requisitos de seguridad móvil y en la nube.

MobileIron AppConnect

MobileIron AppConnect guarda las aplicaciones dentro de contenedores para proteger los datos de aplicaciones en reposo sin tocar los datos personales. Cada aplicación se convierte en un contenedor extraíble y seguro cuyos datos están cifrados y protegidos frente a accesos no autorizados. El contenedor de cada aplicación está a su vez conectado a otros contenedores seguros de aplicaciones a través de la plataforma de administración de MobileIron, de forma que políticas como el inicio de sesión único (SSO) en aplicaciones se puedan compartir fácilmente y actualizarse en diferentes dispositivos.

MobileIron AppTunnel

MobileIron AppTunnel protege los datos en red con una innovadora VPN por aplicación para múltiples sistemas operativos que es compatible con dispositivos iOS, Android y Windows 10. AppTunnel ofrece una seguridad pormenorizada en sesiones por aplicación para conectar el contenedor de cada aplicación a la red corporativa. Gracias a esto, las organizaciones pueden segurizar el tráfico proveniente de aplicaciones corporativas sin que esto interfiera con el tráfico personal como, por ejemplo, cuando un usuario publica una foto familiar en Facebook.

Principales ventajas

- Segurice los datos de las aplicaciones tanto en el dispositivo como en tránsito hacia la nube, así como en el *back-end* de la empresa.
- Separe las aplicaciones y los datos corporativos de los personales en el dispositivo.
- Habilite un acceso seguro a las aplicaciones sin VPN.
- Configure, implemente y actualice las aplicaciones y las políticas, sin necesidad de que el usuario intervenga.
- Disponga de compatibilidad tanto con SDK como con métodos de ajuste para la colocación de las aplicaciones en contenedores.
- Implemente AppConnect en dispositivos iOS, Android y Windows 10.
- Administre las aplicaciones tanto internas como públicas.

MobileIron

Acerca de MobileIron

MobileIron ofrece una base segura para el trabajo moderno a empresas de todos los tamaños en todo el mundo. Para más información, visite **www.mobileiron.com** o póngase en contacto con un representante de ventas de MobileIron.

Prestaciones

AppConnect

AppConnect crea un contenedor de aplicaciones seguro mediante un SDK y un contenedor para iOS o mediante un contenedor para Android. Este contenedor está conectado a otros contenedores de aplicaciones seguros a través de la consola de MobileIron y ofrece las siguientes funciones de administración:

- **Autenticación:** confirme la identidad mediante el nombre de usuario y la contraseña del dominio o con los correspondientes certificados para que solamente los usuarios aprobados pueden acceder a las aplicaciones corporativas.
- **SSO (inicio de sesión único):** simplifique la autenticación del usuario en todos los contenedores de aplicaciones.
- **Autorización:** permita o bloquee el uso o el almacenaje de las aplicaciones en función de la posición del dispositivo.
- **Configuración:** configure e inserte de forma silenciosa ajustes personalizados, como el nombre de usuario, el nombre de servidor y los atributos personalizados, sin la necesidad de que el usuario intervenga para activarlos.
- **Cifrado:** asegúrese de que todos los datos de aplicaciones almacenados en el dispositivo estén cifrados.
- **Controles de DLP:** defina políticas de prevención de pérdida de datos (DLP), como copiar/pegar, imprimir y los permisos de «abrir en» para que los datos confidenciales no tengan que salir del contenedor.
- **Política dinámica:** actualice las políticas de aplicaciones en todos los dispositivos administrados o en un subgrupo de dispositivos en función del grupo, la función del usuario u otros factores.
- **Generación de informes:** genere estadísticas de uso detalladas sobre las aplicaciones, registros de auditorías y otros informes para mejorar la administración y simplificar el cumplimiento.
- **Borrado selectivo:** borre de forma remota las aplicaciones y los datos corporativos sin tocar los datos personales.

AppTunnel

AppTunnel ofrece varias capas de seguridad para los datos y las aplicaciones móviles sin necesidad de VPN. Estas son algunas de sus prestaciones:

- **Conexión exclusiva:** permita que solo las aplicaciones, los usuarios y los dispositivos autorizados se conecten a los recursos corporativos.
- **Autenticación de sesiones basada en certificados:** configure sin esfuerzo los dispositivos con certificados de identidad y configuraciones de VPN para permitir un acceso fluido y seguro por parte del empleado.
- **Reglas de control de acceso:** bloquee el acceso de red si se ve comprometida la seguridad en la aplicación.
- **MobileIron Sentry:** AppTunnel amplía la tecnología de Sentry, que ofrece una *gateway* integrada que administra, cifra y seguriza el tráfico entre el dispositivo móvil y los sistemas *back-end* de la empresa.
- **MobileIron Access:** AppTunnel también es compatible con MobileIron Access. De este modo, se garantiza que solo los puntos de conexión, los usuarios, las aplicaciones y los servicios en la nube autorizados puedan acceder a los datos corporativos y proporcionar seguridad adicional mediante la autenticación multifactorial.