

Reflection for Secure IT

Reflection for Secure IT le permite proteger su red de espías, eliminando riesgos en las transferencias de archivos y las aplicaciones corporativas.

Reflection for Secure IT está basado en el estándar SSH y funciona en ambientes UNIX y Windows; y es el mejor replazo en en las empresas de FTP y TELNET.

¿Qué puede hacer con Reflection for Secure IT?

Construir túneles encriptados para aplicaciones no-seguras

Un túnel encriptado hace posible el envío de datos de forma segura del punto A al punto B sin ser interceptados. Nuestras opciones de seguridad, le permiten a las organizaciones IT construir túneles encriptados cuando y donde ellos los necesiten, también pueden proteger sus aplicaciones basadas en TCP/IP no-seguras, sin tocar a las aplicaciones mismas.

Proteger la transferencia de archivos importantes

Usando los poderosos métodos de validación y cifrado ofrecido por nuestros productos, los expertos en IT pueden, de manera efectiva, salvaguardar la información privada que se envía sobre redes TCP/IP poco confiables. Ellos también pueden usar nuestras capacidades de verificación de mensajes para asegurar que los datos no hallan sido manipulados.

Mantener la compatibilidad del sistema con los estándares de seguridad

Proporciona un completo soporte en los estándares de seguridad que están siendo usados en las plataformas de IBM, UNIX, Linux, OpenVMS, y Windows. Estos estándares incluyen a SSL/TLS, SSH, y Kerberos. Permite tener accesos seguros a cualquier aplicación basada en TCP/IP, a través de un túnel seguro de transmisión.

Mejorar los métodos de autenticación y autorización ya existentes

Reflection trabaja con un amplio rango de métodos de autenticación y autorización, por lo que usted puede fácilmente usarlos junto con su actual esquema de seguridad. Verificar la identidad de usuarios o sistemas –y bloquear el acceso a datos privados o a sistemas por medio de prácticas ilegales—soporta Kerberos, PKI, LDAP, tarjetas inteligentes, Active Directory y portales.

Salvaguardar el acceso remoto a aplicaciones empresariales

Secure Token Authorization (STA) (patente pendiente), asegura que los usuarios remotos puedan acceder solo a las aplicaciones host aprobadas. STA

funciona con nuestro administrador de servidor para establecer derechos de usuario, y es entonces cuando firma digitalmente sobre demanda los. No se requiere ninguna configuración por parte del usuario.

Administrar remotamente servidores críticos

Permite la administración remota, aun sobre Internet, a través de passwords encriptados, y creando túneles de acceso seguro entre las estaciones de trabajo y los servidores de misión crítica utilizando los protocolos de Secure Shell , que incluye a SSH, SFTP, y SCP y aprovechando métodos de autenticación y autorización para proteger a los datos de espías, hackers y otras amenazas a la seguridad.

Simplificar la administración de contraseñas y reducir las llamadas al escritorio de ayuda

Nuestras opciones para un solo inicio de sesión, da a los usuarios una conveniente alternativa para manejar múltiples hosts IDs y contraseñas. Evita tener que memorizar contraseñas o usar recordatorios en papel, ya que los usuarios pueden acceder con una sola contraseña, a todos los hosts y servidores que tengan autorizados. Esto ahorra tiempo al usuario y facilita la carga del personal del escritorio de ayuda.

Agregue fácilmente una capa esencial de protección a su infraestructura existente de seguridad.