

Cifrado transparente para redes de archivos protegidos

Protección única de archivos confidenciales contra el acceso de personas no autorizadas tanto internas como externas a la organización.

La mayoría de las medidas de protección de datos están diseñadas para resguardar a la organización contra las amenazas externas, mientras que, con frecuencia, se descuidan o pasan por alto buena parte de los riesgos internos. El peligro potencial resultante del uso inapropiado de los datos confidenciales de la empresa, sin embargo, es exactamente el mismo independientemente de dónde provenga la amenaza. Prácticamente en todas las organizaciones, la información valiosa, como informes comerciales, documentación de RR. HH., datos sobre clientes y resultados de investigaciones, se guarda de manera electrónica y sin protección. Almacenar los datos de modo centralizado en servidores, participar en redes de trabajo de varios sitios y usar medios de datos móviles son algunas de las prácticas actuales que aumentan considerablemente los riesgos para la seguridad. Además, a medida que más organizaciones subcontratan las actividades del departamento de TI con el objeto de reducir costes, aumentan las preocupaciones en torno a la confidencialidad de los datos.

Las organizaciones necesitan una solución de seguridad que únicamente permita el acceso a datos confidenciales a los grupos de usuarios autorizados. Con políticas de seguridad en funcionamiento, es posible restringir el acceso a los datos confidenciales para evitar que tanto el personal de una empresa externa como, incluso, los administradores de sistema internos lleguen a ellos.

SafeGuard LAN Crypt usa un cifrado de archivos totalmente automatizado para brindar protección eficaz a los archivos confidenciales. Además, SafeGuard LAN Crypt no obliga a los usuarios a cambiar su metodología de trabajo, ya que el proceso de cifrado es transparente y se ejecuta en segundo plano, sin afectar sus tareas. Esto significa que a cada usuario se le asigna un "grupo clave" único según su perfil. El usuario se vale de ese grupo clave para leer los archivos publicados en texto simple. Si alguna persona no autorizada tuviera acceso a ellos, lo único que vería es una secuencia de caracteres cifrados e ilegibles.

En SafeGuard LAN Crypt, las funciones del administrador del servidor y del responsable de seguridad están definidas con estricta precisión, lo que confiere a la solución una ventaja única en el manejo de la seguridad de la información. El administrador del servidor se encarga del sistema como siempre, pero no cuenta con los medios para descifrar ningún archivo. Para garantizar la división de tareas, el responsable de seguridad administra las claves y es también quien define los derechos de acceso individuales para los grupos de trabajo o los usuarios individuales de acuerdo con las pautas de seguridad de la empresa.

SafeGuard LAN Crypt brinda una amplia protección para toda la información de la empresa. Es escalable, de modo que puede usarse en equipos pequeños y temporales, en departamentos y en grupos de proyectos, o bien en toda la organización.

SafeGuard LAN Crypt: cifrado de archivos inteligente.

Ventajas clave

Seguridad mejorada

- » Seguridad de datos transparente para grupos de usuarios y usuarios individuales.
- » Cifrado en todos los medios estándar y en entornos heterogéneos.
- » Separación de tareas entre la administración de seguridad y la administración de servidores.
- » Implementación sencilla de una política de seguridad a nivel empresarial.
- » Definición flexible de reglas de cifrado para grupos de usuarios.
- » Sencilla integración de PKI y compatibilidad con certificados, tarjetas inteligentes y tokens USB.

Fácil de implementar

- » Perfecta integración con infraestructuras de TI heterogéneas.
- » Administración central sencilla mediante directorios o dominios existentes.
- » Sin necesidad de actualizaciones adicionales a la infraestructura de TI existente.
- » Escalable desde grupos de usuarios individuales hasta implementaciones a nivel empresarial.

Fácil de usar

- » Facilidad de uso con integración en entornos de trabajo conocidos.
- » Transparencia para los usuarios y funcionalidades que se explican por sí mismas alcanzan mayores niveles de aceptación por parte de los usuarios.

Características principales y funciones

Seguridad

- Solución completa de seguridad para evitar el acceso no autorizado a los datos.
- Protege información valiosa de la empresa e información personal confidencial.
- Distingue con precisión las responsabilidades inherentes a la administración del servidor y a la administración de seguridad.
- La protección de datos ideal en caso de que una empresa externa realice las tareas de TI ya que, si bien el personal de esa empresa puede administrar archivos, no puede leerlos en texto simple.
- Utiliza algoritmos de seguridad probados y evaluados.
- Autenticación de usuarios mediante certificados X.509.
- Compatible con tarjetas inteligentes y tokens USB.

Administración del sistema

- Instalación, configuración y administración sencillas y centrales, gracias a la integración con los entornos de TI existentes y al uso de dominios o servicios de directorio existentes.
- Perfecta integración con los sistemas PKI existentes.
- Solución rentable y de rápida implementación que no necesita ninguna infraestructura adicional.
- Incluye una estrategia de recuperación para que, en caso de urgencia, también sea posible acceder a los datos cifrados.

Fácil de usar

- Los usuarios autorizados guardan con seguridad la información, sin riesgo de que alguna persona externa no autorizada tenga acceso.
- Cifrado constante
- No es necesario realizar cambios en el entorno de trabajo conocido para los usuarios ni en sus hábitos de trabajo.
- Alto nivel de aceptación por parte de los usuarios: no es necesaria ninguna capacitación adicional.
- No afecta el rendimiento del servidor de archivos: un agente cliente de estaciones de trabajo realiza las tareas de cifrado y descifrado.

Interoperatividad

- Compatible con SafeGuard Data Exchange 5.40 y posterior.
- Proporciona acceso seguro a archivos cifrados a los servicios autorizados, como Sophos, contra programas maliciosos.
- Compatible con bases de datos de Oracle y Microsoft SQL Server.
- Compatible con Microsoft Active Directory y Novell eDirectory.
- Integración con sistemas de aprovisionamiento mediante API de administración.
- Compatible con proveedores de servicio criptográfico (CSP) para que cualquier componente compatible con RSA de terceros (como tarjetas inteligentes o tokens USB) pueda implementarse para la autenticación de usuarios.
- Con certificación de Aladdin eToken.

Más información

Para obtener más información acerca de Sophos y de nuestra completa línea de soluciones SafeGuard, visite www.sophos.com.

ds/070607

Requisitos del sistema

Hardware

- » Ordenador con procesador Intel Pentium o compatible

Sistema operativo

- » Microsoft Windows Vista Business, Professional y Ultimate
- » Microsoft Windows XP Professional

Compatibilidad con sistemas operativos de servidor de archivos

- » Microsoft Windows (versiones NT, 2000, 2003 y 2008)
- » Novell NetWare

Compatibilidad con servidores de terminales

- » Microsoft Windows Server 2003 Terminal Services
- » Citrix MetaFrame

Medios compatibles

- » Unidades de redes; discos duros locales; CD, DVD, unidades USB y unidades de memoria flash

Estándares y protocolos

- » Autenticación: autenticación de usuarios mediante certificados X.509v3
- » PKCS#12
- » Protocolo LDAP para acceder a Microsoft Active Directory y Novell eDirectory
- » Cifrado: 3DES (168 bits), IDEA (128 bits), AES (128 bits) y AES (256 bits)
- » Hash: MD5, SHA (256)
- » Tokens: tarjetas inteligentes y tokens USB mediante CryptoAPI

Idiomas disponibles

- » Inglés, alemán y francés