

Los datos sensibles y valiosos necesitan protección. Esto es especialmente importante en entornos móviles en los que existe riesgo de que personal no autorizado acceda a información confidencial. Hoy en día, muchas empresas y organizaciones proporcionan a su personal dispositivos móviles para aumentar la eficiencia. La información confidencial interna, como resultados de investigación, análisis de gestión o incluso datos del cliente, se almacena en estos portátiles y PDA. Si esta valiosa información estuviese en papel, los documentos se conservarían en armarios de archivo cerrados o cajas fuertes para evitar que fuesen robados o leídos por personas no autorizadas. SafeGuard PrivateDisk proporciona exactamente la misma protección a los documentos electrónicos. SafeGuard PrivateDisk genera una unidad de disco "virtual" cifrada en el dispositivo. Este disco es como una caja fuerte electrónica bien protegida en la que se pueden cifrar y almacenar de forma segura todos los datos críticos, delicados y de valor.

Existen dos versiones de SafeGuard PrivateDisk: Personal Edition está pensada para su uso en pequeñas y medianas empresas, mientras que Enterprise Edition, con su configuración ampliada y opciones de distribución, está pensada para cubrir las necesidades de organizaciones más grandes.

Muchos directivos y personal externo de servicios disfrutan ahora de las ventajas de SafeGuard PrivateDisk Portable: pueden leer datos encriptados en sus medios móviles de almacenamiento, estén donde estén, sin dejar de cumplir el estándar de seguridad de su empresa. Además, SafeGuard PrivateDisk Enterprise Edition proporciona herramientas administrativas e interfaces que aseguran una integración fácil y rentable en entornos de TI ya existentes.

SafeGuard PrivateDisk puede utilizarse como una solución de seguridad única o integrarse en una PKI (public key infrastructure) existente. En los despliegues a nivel de empresa, SafeGuard PrivateDisk también soporta el uso de tarjetas inteligentes para un sólido acceso de autenticación al volumen de ficheros.

Ventajas clave

Mayor seguridad

- » La caja fuerte electrónica protege datos valiosos y sensibles de la empresa
- » Protección flexible de datos en redes, discos duros locales, servidores terminales y medios portátiles
- » Implementa algoritmos de seguridad comprobados
- » Enterprise Edition también proporciona certificados de recuperación que garantizan que los datos encriptados puedan consultarse en caso de emergencia

Fácil de desplegar

- » Instalación central y sin complicaciones y distribución a través de Windows Installer u otros sistemas de gestión de software
- » No hay necesidad de actualizaciones adicionales a la infraestructura existente de TI
- » Escalabilidad: desde los dispositivos individuales a un despliegue a nivel de empresa

Fácil de usar

- » Funcionalidad de fácil comprensión, lo que se traduce en altos niveles de aceptación por parte del usuario
- » No son necesarias largas sesiones de formación para los usuarios o administradores
- » PrivateDisk Portable le proporciona una gran flexibilidad: con él, puede acceder a datos encriptados en otros dispositivos finales, pero no necesita instalarlo en ellos
- » La gestión integrada de claves opcional con la solución de datos de seguridad SafeGuard Enterprise proporciona una mayor transparencia al compartir datos de forma segura

Características principales/Funcionalidad

Seguridad

- Genera una unidad de disco virtual cifrada automáticamente
- Encriptación rápida y transparente al simular una unidad de disco adicional
- Protege datos en discos duros, unidades de red y medios portátiles como disquetes, CD-ROM, DVD, unidades USB y tarjetas de memoria flash
- Autenticación de usuario mediante contraseña y/o certificados X.509
- La gestión compartida opcional de depósito de claves con SafeGuard Enterprise permite un intercambio fácil y transparente de datos encriptados dentro de grupos de usuarios de la empresa sin necesidad de contraseñas separadas
- Compatible con tarjetas inteligentes y tokens USB
- En caso necesario, el fichero de intercambio de Windows puede borrarse cuando el ordenador esté apagado
- Implementa el algoritmo de encriptación AES más actualizado y moderno

Administración del sistema

- Solución rentable e implementación rápida sin necesidad de infraestructura o formación adicionales
- Instalación basada en Windows Installer (MSI) o instalación usando otros sistemas de gestión de software
- Administración central de configuraciones de seguridad a través de Objetos de Política de Grupo
- Integración opcional de Certificados de Recuperación para poder consultar datos encriptados también en situaciones de emergencia

Fácil de usar

- Alto nivel de aceptación por parte del usuario: no se requiere formación adicional
- Cada usuario puede utilizar varios PrivateDisks al mismo tiempo
- Varios usuarios autorizados pueden compartir un PrivateDisk para almacenar información compartida de forma segura
- Los usuarios pueden proteger y almacenar cualquier tipo de archivo confidencial en su PDA, portátil y PC
- Integración fluida en Windows Explorer
- PrivateDisk Portable permite un acceso seguro de datos (lectura) a dispositivos sin necesidad de instalar software especial

Certificación

- » FIPS 140-2 (biblioteca criptográfica en evaluación)
- » Certificado por Aladdin eToken
- » Gemalto Secure Digital Companion

Interoperabilidad

- » Integración API Microsoft Crypto: el uso de proveedores de servicio criptográficos (CSP) hace que cualquier componente habilitado para RSA de terceros (como tarjetas inteligentes o tokens USB) pueda ser implementado para la autenticación del usuario

Requisitos del sistema

Hardware

- » PC con Intel Pentium o procesador compatible

Sistema operativo

- » Microsoft Windows 7 de 64 bits
- » Microsoft Windows 7
- » Microsoft Windows Vista de 64 bits
- » Microsoft Windows Vista
- » Microsoft Windows XP

Interfaces

- » Crypto API/Microsoft Cryptographic Service Provider (CSP)
- » API de administración para la integración en procesos de administración automáticos
- » LDAP (solo para Enterprise Edition)

Estándares/Protocolos

- » Autenticación: autenticación del usuario a través de certificados X.509
- » Encriptación: AES (Rijndael)—128 y 256 bits
- » Hash: SHA-1

Idiomas

- » Inglés, alemán, francés, neerlandés, español, portugués (Portugal y Brasil), italiano, danés, sueco, finés, noruego, japonés, chino, coreano