

Prevención de filtraciones de información en estaciones de trabajo

Las estadísticas del sector muestran sistemáticamente que la amenaza más importante para las organizaciones reside dentro de ellas. Debido a que más del 70% de los datos corporativos están situados en las estaciones de trabajo, las soluciones de seguridad en la puerta de enlace y las políticas de seguridad no pueden por sí solas mitigar los riesgos de las pérdidas de datos. Las cantidades cada vez mayores de dispositivos extraíbles, interfaces físicas e inalámbricas, y usuarios con acceso a datos importantes, ha convertido la pérdida de datos a través de estaciones de trabajo (tanto accidental como intencionada) en una verdadera amenaza contra la empresa. Es demasiado fácil conectar una unidad USB, cámara digital o iPod a una estación de trabajo de una organización y sacar material confidencial. Igual de fácil es utilizar Wi-Fi, Bluetooth o un módem 3G para entrar en las redes confidenciales internas y abrir redes externas.

Éste es exactamente el tipo de riesgo de seguridad para el cual SafeGuard PortProtector está diseñado. Controla cada estación de trabajo en cada dispositivo, en cualquier interfaz y garantiza la prevención fácil y flexible de la pérdida de datos. SafeGuard PortProtector controla el tráfico en tiempo real y aplica políticas de seguridad personalizadas y granulares para todos los tipos de interfaces y dispositivos de almacenamiento externo:

Interfaces físicas: USB, FireWire, PCMCIA, puertos paralelos, puertos de serie, etc.

Interfaces inalámbricas: Wi-Fi, Bluetooth, infrarrojos (IrDA)

Dispositivos de almacenamiento externo: medios extraíbles, CD/DVD, unidades de disco, etc.

SafeGuard PortProtector detecta y permite las restricciones según el tipo de dispositivo, el modelo o, incluso, el número de serie específico. SafeGuard PortProtector permite que los administradores bloqueen completamente el uso de todos los dispositivos de almacenamiento, que permitan el modo de sólo lectura o que cifren todos los datos en los dispositivos. Además, los administradores pueden controlar, bloquear y registrar los archivos que fueron escritos o leídos por estos dispositivos.

Junto con SafeGuard PortProtector, la solución integral SafeGuard PortAuditor ayuda a los administradores a controlar quién está conectado a las estaciones de trabajo corporativas. Con SafeGuard PortAuditor, los administradores pueden distinguir entre los dispositivos seguros, como los tokens de autenticación, y las amenazas potenciales contra la seguridad, como los reproductores de MP3 de almacenamiento masivo. Al utilizar esta información, los administradores de TI pueden desplegar las políticas de seguridad pormenorizadas que se adaptan exactamente a las necesidades de la empresa. La prevención integral de filtraciones de información, la administración sencilla y la facilidad de uso convierten a SafeGuard PortProtector en la mejor solución.

La prevención integral de filtraciones de información, la administración sencilla y la facilidad de uso convierten a SafeGuard PortProtector en la mejor solución.

Ventajas clave

Mayor seguridad

- » Previene la filtración y el robo de datos, intrusiones en la empresa y la introducción de programas maliciosos
- » Informes completos de las amenazas de seguridad con SafeGuard PortAuditor
- » Detecta y limita la transferencia de datos por tipo de dispositivo, modelo de dispositivo y número de serie específico
- » Inspecciona los archivos por tipo y controla la transferencia de tipos de archivos no autorizados hacia y desde dispositivos externos de almacenamiento
- » Permite el duplicado de archivos y almacena los archivos copiados de forma segura en un repositorio central
- » Protege los datos en movimiento de la empresa mediante el cifrado de los datos en dispositivos externos de almacenamiento y el seguimiento del uso fuera de línea
- » Bloquea los registradores de pulsaciones de tecla de hardware tanto USB como PS/2

Fácil de gestionar

- » Se pueden definir políticas separadas para cada dominio, grupo, ordenador o usuario
- » Administración más sencilla gracias a la integración con Microsoft Active Directory y Novell eDirectory
- » Administración delegada
- » Los registros y alertas cifrados pueden visualizarse en la consola de gestión para crear informes y auditorías de forma sencilla o bien pueden integrarse con software de terceros para un análisis integral

Fácil de usar

- » Funciona de forma transparente en segundo plano
- » No se producen cambios en los hábitos de trabajo de los usuarios y no es necesaria formación para el usuario final

Funciones principales

»

Seguridad

- Control granular: detecta y limita las transferencias de datos por tipo de dispositivo, modelo de dispositivo, número de serie específico, tipo de archivo y contenido
- Protección de datos: protege los datos de la empresa en movimiento mediante el cifrado de los datos en dispositivos externos de almacenamiento y el seguimiento del uso fuera de línea
- Duplicación de archivos: el administrador decide quién y qué archivos deben duplicarse y si ha de iniciarse alguna acción (registro, alertas)
- Agente seguro: el despliegue silencioso, redundante, de múltiples niveles y anti-manipulaciones previene la infracción de las políticas de seguridad
- Detección de datos: control de la transferencia de archivos hacia y desde dispositivos externos de almacenamiento basado en los tipos de archivo

Auditoría del estado de seguridad de la estación de trabajo

- Visibilidad integral de quién está conectando en las estaciones de trabajo corporativas
- Visibilidad en todos los puertos USB, PCMCIA, FireWire y Wi-Fi
- Registro granular de todas las conexiones actuales y pasadas a un dispositivo
- Funciones de generación de informes sencillas y potentes

Administración del sistema

- Flexibilidad de políticas: se pueden definir políticas separadas para cada dominio, grupo, ordenador o usuario, y las políticas se pueden asociar fácilmente con objetos organizativos de Microsoft Active Directory o Novell eDirectory
- Configuración de permisos de administración jerárquicos mediante una gestión basada en funciones
- Gestión intuitiva: se integra plenamente en Microsoft Active Directory, Novell eDirectory u otros software de gestión de red

- Facilidad de auditoría y visibilidad: los registros y las alertas cifrados pueden visualizarse en la consola de gestión o integrarse en software de terceros para un análisis integral o notificaciones inmediatas
- Aplicación de políticas avanzadas mediante el análisis independiente, a nivel de kernel y en tiempo real del tráfico de puertos de bajo nivel
- Equilibrado automático de la carga entre todos los servidores de SafeGuard, con servidores de gestión sincronizados que actúan como uno solo
- Políticas de cumplimiento integradas: cuenta con configuraciones detalladas para aplicar políticas de seguridad asociadas a estándares de cumplimiento normativo específico, como por ejemplo PCI, HIPAA, SOX y FISMA

Fácil de usar

- No hay necesidad de cambios en los hábitos de trabajo de los usuarios
- Alto nivel de aceptación por parte de los usuarios, ya que no se necesita formación adicional

Funciones de seguridad

- Control de puertos
- Control de dispositivos
- Control de almacenamiento
- Cifrado de medios extraíbles
- Control de tipos de archivos
- Inspección de contenido
- Registro de nombres de archivo
- Seguimiento del uso fuera de línea de dispositivos cifrados
- Control inalámbrico granular
- Listas blancas de medios CD/DVD
- Bloqueo de la transición híbrida de red
- Control de puertos internos
- Control inalámbrico granular
- Control de U3 y ejecución automática
- Bloqueo de los registradores de pulsaciones de tecla de hardware tanto USB como PS/2
- Integración con NAC de Cisco

Requisitos del sistema

Hardware

- » PC con procesador Intel Pentium o similar
- » 25 MB como mínimo de espacio libre en el disco duro

Sistemas operativos

- » Microsoft Windows 2000
- » Microsoft Windows XP Professional (todos los service packs)
- » Microsoft Windows XP Tablet PC Edition
- » Microsoft Windows 2003 (todos los service packs)
- » Microsoft Windows Vista Business/Enterprise/Ultimate (SP1-2) 32 bits
- » Microsoft Windows 7 Business/Enterprise/Ultimate 32 bits

Idiomas disponibles

- » Inglés, alemán* y japonés*
- » Los mensajes que se muestran a los usuarios finales pueden ser personalizados por el administrador en cualquier idioma

Resumen del control de puertos

Interfaces físicas

- » USB
- » FireWire
- » PCMCIA
- » Secure Digital (SD)
- » Puerto paralelo
- » Puerto serie
- » Módem
- » Puertos internos

Interfaces inalámbricas

- » Wi-Fi
- » Bluetooth
- » Infrarrojos (IrDA)

Resumen del control del almacenamiento

- » Dispositivos de almacenamiento extraíbles
- » Discos duros externos
- » Unidades de CD/DVD
- » Unidades de disquete
- » Unidades de cinta