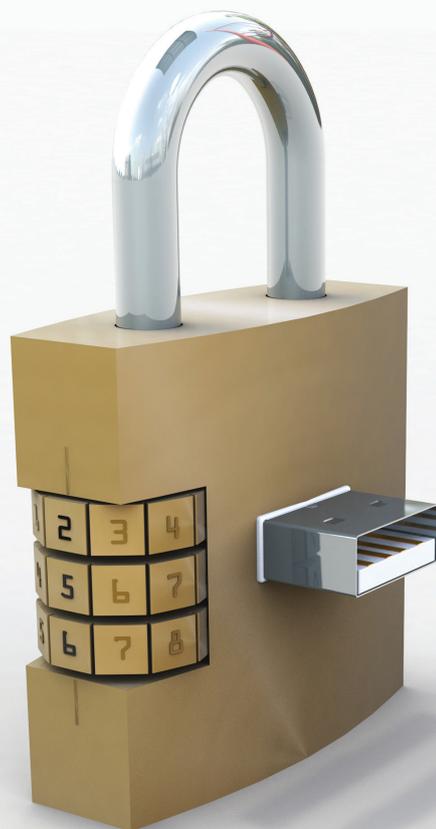


Control integral del uso de almacenamiento USB y otros dispositivos portátiles



- 🌐 Conciencia de la información
- 👁️ Valoración del riesgo de fugas de información
- 🔑 Control de acceso



Descubra más y comience su evaluación GRATUITA:

gfihispana.com/endpointsecurity

Microsoft Partner
Gold Application Development
Silver Midmarket Solution Provider

GFI EndPointSecurity™
Control de unidades USB, iPods y otros dispositivos de punto final

Control integral del uso de almacenamiento USB y otros dispositivos portátiles

La proliferación de dispositivos de consumo como smartphones, reproductores multimedia, dispositivos portátiles de almacenamiento, dispositivos conectados a red y unidades USB fácilmente ocultables ha aumentado el riesgo de fugas de información, infecciones por virus, introducción de aplicaciones y juegos sin licencia y otras actividades maliciosas en las redes.

Aunque la mayoría de empresas tienen antivirus, cortafuegos y seguridad de contenido de correo y web para protegerse contra amenazas externas, pocos se dan cuenta de lo sencillo que es para un empleado copiar enormes cantidades de información confidencial y comercialmente sensible en un dispositivo portátil de almacenamiento sin el conocimiento de nadie.

Bloquear físicamente todos los puertos USB no es sostenible ni viable. La clave para administrar el uso de los dispositivos portátiles es instalar una solución de seguridad de punto final que proporcione a los administradores el control sobre qué dispositivos están en uso, si han sido utilizados y por quien, así como un conocimiento en profundidad de la información ha sido copiada.

Cómo funciona

Para controlar el acceso, GFI EndPointSecurity instala automáticamente en su red un agente oculto y a prueba de manipulación. Este agente puede desplegarse a todos los equipos de la red con unos pocos clics. Este agente proporciona una protección sin paralelo contra manipulaciones incluso frente a usuarios con derechos administrativos, permitiendo a los administradores de TI mantener el control sí o sí.

Administre el acceso de los usuarios y proteja su red de las amenazas de los dispositivos portátiles

Utilizando GFI EndPointSecurity puede deshabilitar centralizadamente a los usuarios el acceso a medios portátiles de almacenamiento, evitando el robo de información o la entrada de información que podría ser peligrosa para su red. Aunque puede deshabilitar algunos puertos físicos de conexión desde la BIOS, en realidad esta solución no es práctica y los usuarios avanzados pueden hackear la BIOS con facilidad. GFI EndPointSecurity le permite tomar el control sobre una amplia variedad de dispositivos.

Registre la actividad de acceso a dispositivos portátiles en su red

Además de bloquear el acceso a medios portátiles de almacenamiento, GFI EndPointSecurity registra la actividad de los usuarios relacionada con los dispositivos en el registro de sucesos y en un Servidor SQL central. Se registra una lista de los archivos a los que se ha accedido desde un dispositivo autorizado cada vez que se conecta.

Encripte los dispositivos portátiles

Se puede conceder permiso a los usuarios para almacenar información en dispositivos USB siempre que sean encriptados. El acceso a esta información fuera de la red de la empresa puede controlarse estrictamente mediante una aplicación específica, que está incluida con GFI EndPointSecurity.

Otras características:

- Asistente de creación de directivas para un avanzado control de acceso granular.
- Resumen diario/semanal
- Monitorización de estado y alertas en tiempo real
- Completos informes sobre el uso de dispositivos con el complemento GFI ReportPack
- Soporta Windows 7 Bitlocker To Go
- Envía mensajes emergentes personalizados a los usuarios cuando se les ha bloqueado el uso de un dispositivo
- Permite el examen de los registros de actividad de usuarios y dispositivos mediante una base de datos de respaldo
- Puede agrupar los equipos por departamento, dominio, etc.
- Soporta sistemas operativos en cualquier lenguaje que cumpla Unicode
- ¡Y más!

Beneficios a simple vista

Evita la fuga/robo de información mediante el control del acceso a dispositivos portátiles de almacenamiento con el mínimo esfuerzo administrativo

Evita la pérdida accidental de información cuando se pierden o roban los dispositivos extraíbles de almacenamiento mediante el uso de encriptación.

Evalúa el riesgo de fuga de información de los dispositivos extraíbles a nivel de punto de conexión y proporciona información sobre cómo mitigarlo

Protege la información en movimiento con la encriptación de volúmenes extraíbles

Permite a los administradores bloquear dispositivos por clase, extensión de archivo, puerto físico o identificador de dispositivo

Permite a los administradores conceder acceso temporal al dispositivo o puerto durante un periodo de tiempo estipulado

Para una lista completa de beneficios visite: www.gfihispana.com/endpointsecurity

Requerimientos del sistema

Windows 2000 (SP4), XP, Vista, 7 y 8, Windows Servers 8 y 2012 (versiones x86 y x64)

Internet Explorer 5.5 o posterior

.NET Framework versión 4.0

Puerto: puerto TCP 1116 (predeterminado)

Base de datos: SQL Server 2000/2005/2008; si no está disponible,

GFI EndPointSecurity puede descargar, instalar y configurar automáticamente una versión de SQL Server Express.



www.gfihispana.com

Para una lista completa de oficinas GFI/datos de contacto en todo el mundo, por favor visite: www.gfihispana.com/contact-us

© 2015 GFI Software – Windows XP (SP 2)/Vista/7/8 son marcas registradas de Microsoft Corporation.

GFI EndPointSecurity es una marca registrada, y GFI y el logotipo de GFI son marcas registradas de GFI Software en Alemania, Estados Unidos de América, Reino Unido y otros países.

Todos los nombres de productos y empresas incluidos pueden ser marcas registradas de sus respectivos propietarios.

Comience su evaluación gratuita en gfihispana.com/endpointsecurity