Microsoft GOLD CERTIFIED Partner

GFI LANguard

Escáner de seguridad de red, escáner de puertos y administración de parches

- Tecnologíade vanguardia
- Preciocompetitivo
- Másde **20.000** clientes

La solución No. 1 en escáner de seguridad de red y gestión de vulnerabilidad

GFI LANguard™ es una galardonada solución de escáner de red y de seguridad utilizada por más de 20.000 clientes que le permite analizar su red y puertos para detectar, evaluar y rectificar vulnerabilidades de seguridad con el mínimo esfuerzo administrativo. Como administrador, usted tiene que tratar diferentemente problemas relacionados con problemas de seguridad, administración de parches y auditoría de red, a veces utilizando varios productos. Sin embargo, con GFI LANguard estos tres pilares de la gestión de vulnerabilidad son abordados en un paquete, permitiéndole tener una panorámica completa de su configuración de red y mantener seguro el estado de la red más rápida y eficientemente.

Gestión de vulnerabilidad

GFI LANguard realiza análisis de red utilizando bases de datos de vulnerabilidad basadas en OVAL y SANS Top 20, proporcionando más de 15.000 evaluaciones de vulnerabilidad cuando su red, incluyendo cualquier entorno virtual, es analizada. GFI LANguard le permite analizar el estado de seguridad de su red y tomar acciones antes de que sea comprometida. La última versión detecta equipos que son vulnerables a la infección por el gusano Conficker así como equipos que han sido infectados.

BENEFICIOS

- **Potente escáner de red, seguridad y puertos con capacidades de auditoría de red**
- **Más de 15.000 estimaciones de vulnerabilidad realizadas a través de su red, incluyendo el entorno virtual**
- **Reduce el coste total de propiedad centralizando el escáner de vulnerabilidad, la gestión de actualizaciones y la auditoría de red**
- **Las opciones automátizadas le ayudan a mantener el estado de seguridad de su red con el mínimo esfuerzo administrativo**
- **Las funciones de auditoría de toda al red proporcionan una imagen completa de la configuración de seguridad y puertos de la red**
- **• Escáner comercial de seguridad Windows No 1 (votado por los usuarios de NMAP dos años consecutivos) y premio Best of TechEd 2007 (seguridad).**

Solución integrada de administración de vulnerabilidades

GFI LANguard es una galardonada solución que aborda los tres pilares de la gestión de vulnerabilidad: análisis de seguridad, administración de parches y auditoría de red mediante una única e integrada consola. Mediante el análisis de toda la red, identifica todos los posibles problemas de seguridad y utilizando sus extensas funcionalidades de generación de informes le proporciona las herramientas que necesita para detectar, valorar, informar y rectificar cualquier amenaza.

- Análisis de vulnerabilidad
- Gestión y corrección de actualizaciones
- Auditoría de red y de software

Análisis de vulnerabilidad

Durante las auditorías de seguridad, se realizan más de 15.000 valoraciones de vulnerabilidad y las redes se escanean IP por IP. GFI LANguard le da la capacidad de realizar análisis multi plataforma ((Windows, Mac OS, Linux) a través de todos los entornos incluyendo Máquinas Virtuales y de analizar el estado y configuración de la seguridad de su red. Esto asegura que sea usted capaz de identificar y rectificar cualquier amenaza antes de que lo hagan los hackers.

Detección de Máquinas Virtuales

GFI LANguard ya puede detectar si un equipo analizado es real o virtual. Actualmente se soportan ambas aplicaciones VMware y Virtual PC.

configure a medida sus propias evaluaciones de vulnerabilidad

GFI LANguard le permite crear fácilmente y a medida evaluaciones de vulnerabilidad a través de unas sencillas pantallas de configuración asistidas. El asistente también es suficientemente potente para permitir la creación de complejas evaluaciones de vulnerabilidad. El motor de scripting también es compatible con Python y VBScript. GFI LANguard incluye un editor y depurador de scripts para ayudar en su desarrollo.

Base de datos de vulnerabilidades de gran alcance y potencia industrial

GFI LANguard se entrega con una completa base de datos de evaluación de vulnerabilidad, que incluye estándares como OVAL (más de 2.000+ comprobaciones) y SANS Top 20. Esta base de datos se actualiza regularmente con información de BugTraq, SANS Corporation, OVAL, CVE y otras. Mediante su sistema de auto-actualización, GFI LANguard se mantiene siempre actualizado con la información sobre las actualizaciones de seguridad de Microsoft recientemente liberadas así como de las nuevas comprobaciones de vulnerabilidad publicadas por GFI, y otros almacenes de información basados en comunidades tales como la base de datos OVAL.

Identifica vulnerabilidades de seguridad y toma medidas correctoras

GFI LANguard escanea equipos, identifica y clasifica vulnerabilidades de seguridad, recomienda un curso de acción y proporciona herramientas que le permiten resolver estos asuntos. GFI LANguard también hace uso de un indicador gráfico del nivel de amenaza que proporciona una importante e intuitiva valoración del estado de vulnerabilidad de un equipo o grupo de equipos analizados. Cuando es posible se proporciona un enlace web o más información sobre un asunto de seguridad concreto, como un BugTraq ID o un artículo de la Base de Conocimientos de Microsoft.

Asegura que las aplicaciones de seguridad de terceros como anti-virus y anti-spyware ofrecen la protección óptima

GFI LANguard también comprueba que las aplicaciones de seguridad soportadas como anti-virus y anti-spyware están actualizadas con los últimos archivos de definición y que están funcionando correctamente. Por ejemplo, puede asegurar que las aplicaciones de seguridad soportadas tienen habilitadas todas las características clave (como el análisis en tiempo real).

Lanzar un nuevo análisis

Análisis completo de GFI LANguard en curso

Requerimientos del sistema

- Windows 2000 (SP4), Windows XP SP2 (x86 & x64), Windows 2003 (x86 & x64), Windows Vista (x86 & x64) o Windows 2008 (x86 & x64).
- Soporte de MS SBS 2003 & 2008 (MS SBS no requerido)
- .NET Framework versión 2.0 o posterior.
- Si analiza equipos Linux entonces Secure Shell (SSH) debe estar habilitado – está incluido por defecto en cada paquete de distribución del SO Linux.
- También podrían requerirse algunos cambios en el cortafuegos - http://kbase.gfi.com/showarticle.asp?id=KBID002344

↓ Para más información y para descargar su versión de evaluación gratuita por favor visite http://www.gfihispana.com/es/lannetscan/

Microsoft GOLD CERTIFIED Partner

GFI