

# NetIQ Change Guardian™ for Windows

## Monitoree la Actividad de Usuarios y Cambios a Través de su Entorno Windows con Poco Impacto a los Servidores

### Resumen

NetIQ Change Guardian for Windows le ofrece invaluable información sobre las actividades y cambios implementados por usuarios privilegiados a través de sus sistemas Windows, proporcionando la visibilidad que usted necesita para proteger su entorno Windows de peligrosas exposiciones de seguridad.

### Soluciones de Hoy

La monitorización de cambios es a menudo considerada como una buena práctica IT, e incluso es obligatoria para requerimientos como Payment Card Industry Data Security Standard. Desafortunadamente, los enfoques actuales con frecuencia fallan en los sistemas de producción:

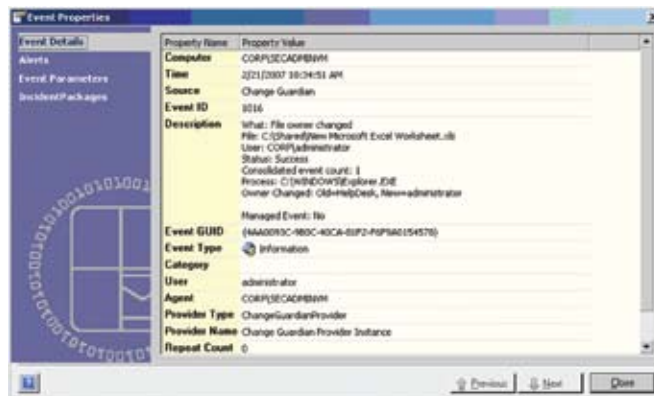
- La auditoría nativa a nivel de objeto a menudo degrada de manera desmedida el desempeño del servidor, y crea registros de auditoría confusos y abultados.
- Los comprobadores de la integridad de archivos frecuentemente causan picos inaceptables en la utilización del sistema. Son incapaces de identificar cuándo y quién ha hecho un cambio sin depender en los registros de auditoría a nivel de objeto.
- Las actualizaciones de código añadidas al kernel pueden introducir problemas en la confiabilidad del sistema, y son difíciles de distribuir a gran escala.

NetIQ Change Guardian for Windows resuelve estos retos a través de un enfoque único en la auditoría de cambios y actividades. Aprovechando un driver de filtrado soportado por el sistema de archivos de Microsoft, se capturan y procesan las actividades que se deseen, además de procesar los datos para proporcionar alertas y registros de auditoría valiosos, de forma simplificada pero poderosa. Siendo un módulo de NetIQ Security Manager™, funciona junto con la mejor tecnología de seguridad de la información y manejo de eventos, incluyendo el manejo de registros (logs).

### Principales Beneficios

**Proporciona una poderosa monitorización de cambios en tiempo real** – Monitorea cambios a través de archivos, directorios, recursos compartidos, entradas del registro y procesos del sistema, alertando de manera rápida sobre cambios potencialmente peligrosos a su entorno.

**Elimina la necesidad de la auditoría nativa a nivel de objeto, reduciendo de manera drástica la utilización del servidor** – Utiliza un mecanismo de monitorización aprobado por Microsoft para evitar la degradación del desempeño que



Los eventos sobre cambios producidos por NetIQ Change Guardian for Windows son útiles y fáciles de leer, reduciendo las habilidades requeridas para entender lo que está pasando. Se obtienen los valores de antes y después, y pocos registros individuales son requeridos para una actividad en particular (por ejemplo, cambios por tarea, archivo modificado, clave de registro añadida, etc.).

puede presentar la auditoría nativa, mientras proporciona alta fidelidad de la información sobre cambios.

### Valida y hace cumplir los procesos de control de cambios -

Identifica cambios "manejables" usando una interfaz de control autorizada o por medio de manera prescrita, contra los cambios no-manejables que pueden indicar que se han saltado controles de cambios.

### Registra y audita los cambios de manera centralizada -

Compila la información crítica de cambios de toda la organización para su subsecuente análisis, ayudando a eliminar las complejidades de agregar más eventos sobre cambios para el cumplimiento regulatorio y la investigación de incidentes.

### Ofrece detallados reportes sobre los cambios -

Captura los valores de antes y después de los objetos, permitiendo reportes detallados sobre cambios basados en uno o más usuarios o computadoras, ayudando a identificar anomalías rápidamente y permitiendo a los investigadores profundizar velozmente hacia información más detallada.

### Trabaja con la solución más amplia para el control de cambios en Windows -

Extiende la funcionalidad de NetIQ Security Manager y aumenta a NetIQ Change Administrator™ para proporcionar una completa solución para la asignación de privilegios, monitorización de usuarios privilegiados y seguridad del servidor.



# NetIQ Change Guardian™ for Windows

## Características Técnicas

**Monitorización y notificaciones en tiempo real de cambios en su entorno Windows** proporcionan información detallada sobre:

- **Archivos y Directorios** - Detalla quién creó, accedió, movió, editó o borró un archivo o un directorio, junto con la información previa y posterior a un cambio (incluyendo tamaño de archivo y autorizaciones de acceso).
- **Archivos Compartidos** - Identifica dónde fueron modificadas las autorizaciones de acceso para archivos o directorios.
- **Registro de Windows** - Incluye información acerca de quién hizo el cambio, así como los valores previos y posteriores al mismo.
- **Procesos del Sistema** - Monitorea la creación y terminación de procesos, identificando al usuario o aplicación que inició la acción y registra cualquier snap-ins del Microsoft Management Console (MMC) que haya sido ejecutada.

**Información mejorada de auditoría**, ofrece una fidelidad y claridad mayores de la que pueden proporcionar los eventos nativos, resolviendo los SIDs/GUIDs a descripciones del mundo real así como la información previa y posterior a los cambios para un mejor análisis de incidentes.

- **Máquina de reglas extensible**, permite una fácil creación y personalización de reglas por medio de asistentes intuitivos para incluir/excluir usuarios, computadoras, archivos, directorios, claves de registro y procesos a través de períodos definibles de tiempo.
- **Alertas Controlables**, permite la definición de qué cambios generarán una alerta, junto con el cuándo, a dónde y cómo estas alertas serán enviadas.
- **Reportes detallados sobre cambios**, ayudan a demostrar el cumplimiento con las directivas internas y los requerimientos regulatorios, también facilitando un mejor análisis de causas y diagnósticos.

## Contactos

### NetIQ, An Attachmate Business - Sede Central

1233 West Loop South  
Suite 1800  
Houston, TX 77027  
TEL +1 713.548.1700  
FAX +1 713.548.1771  
info@netiq.com - www.netiq.com

### Oficina Central Para EMEA

Países Bajos  
TEL +31 71 368 1100  
info-emea@netiq.com

### Oficina Central Para España

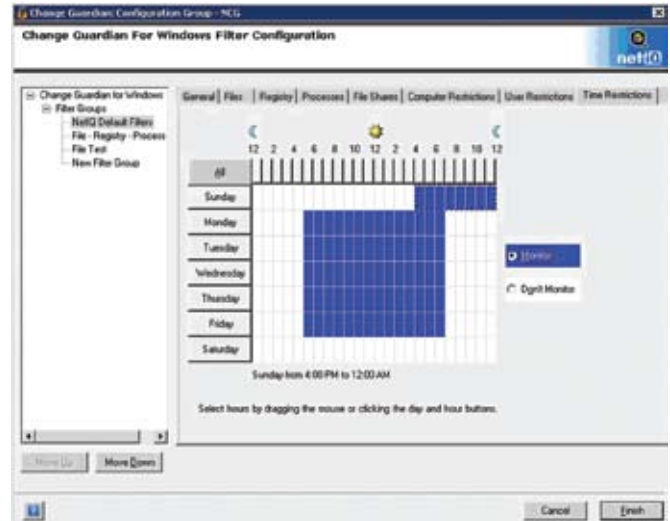
TEL +34 911517111  
info-es@netiq.com

Para información adicional sobre oficinas, socios y distribuidores, por favor visite nuestro sitio Web en [www.netiq.com/contacts](http://www.netiq.com/contacts)

NetIQ Change Guardian for Windows, NetIQ Change Guardian for Active Directory, NetIQ Security Manager, NetIQ y el logo NetIQ son nombres o marcas registradas de NetIQ Corporation o sus subsidiarias en EU y otra jurisdicciones. Todas las otras marcas o nombres de compañías pueden ser nombres o marcas registradas de sus respectivas compañías.

© 2008 NetIQ Corporation, todos los derechos reservados.

DS0507CGWIN EC 0507



NetIQ Change Guardian for Windows proporciona capacidades flexibles de monitorización, permitiéndole definir los parámetros de qué debe (o no) ser monitoreado, a través de qué sistemas y usuarios, y durante cuáles períodos de tiempo.

**Colección y auditoría centralizada de la información sobre cambios**, aprovechando la plataforma galardonada de NetIQ Security Manager, proporciona la certeza de una infraestructura de monitorización robusta que se escalará a las necesidades de su entorno.

## Requerimientos del Sistema

**Requerimientos del Sistema para la monitorización:**

- NetIQ Security Manager 5.6 SP1 o superior

**Plataformas Windows Monitoreadas:**

- Windows Server 2003 SP1

