



# VARONIS

DATALEERT

# VARONIS DATALEERT

El 70% de las compañías se entera de brechas de seguridad a través de sus clientes o terceras partes.

## **MUCHAS ORGANIZACIONES NO TIENEN FORMA DE DETECTAR CUANDO:**

- Se tiene acceso a archivos sensibles o cuando éstos son eliminados.
- Grupos de seguridad, GPOs y otros objetos de Active Directory son modificados o removidos.
- Ocurren escaladas de privilegios injustificadas
- Se modifican los permisos sobre directorios sensibles.

Para responder estas preguntas se requiere de un trabajo de auditoria continuo y discreto de cada uno de los eventos de acceso a su red.

Mejore su habilidad de detectar posibles brechas de seguridad, desconfiguraciones y otros problemas con Varonis. Este programa provee alertas a tiempo real basadas en la actividad de archivos, cambios realizados en Active Directory, cambios de permisos, y otros eventos.

Los parámetros y salidas de alerta son de fácil configuración para que los sistemas y personas correctas sean notificados acerca de los eventos adecuados, en el momento adecuado y de la manera adecuada.

## **CASOS DE USO COMÚN**

- Monitorea la configuración de archivos sensibles en servidores Windows y UNIX/Linux
- Detecta cambios generados fuera de las ventanas de control de cambio
- Alerta de accesos a datos altamente sensibles
- Alerta de escaladas de privilegios

## **RECIBA NOTIFICACIONES INMEDIATAS ACERCA DE:**

- Archivos accedidos, modificados y/o eliminados
- Membresías grupales, políticas grupales y otros cambios en Active Directory
- Cambios de permisos.

## **RECIBA ALERTAS DE LA MANERA QUE USTED PREFIERA**

- Syslog, Registro de eventos, SNMP, Correo electrónico
- Gatilla la ejecución de línea de comando
- De fácil integración con el sistema SIEM y soluciones de administración de redes.

# ¿CUÁLES SON LOS EVENTOS QUE DATALEERT PUEDE INFORMARLE A TIEMPO REAL?

A continuación presentamos un resumen de los eventos para los cuales DatAlert puede gatillar alarmas a tiempo real. Para obtener una lista más completa así como también compatibilidad con diferentes plataformas y versiones visite: <http://www.varonis.com/products/dataleert>

Muchos de los eventos mostrados a continuación pueden ser usados en conjunto con nuestros resultados de clasificación de datos, para que usted pueda ser alertado, por ejemplo, de acceso o eliminación de contenido sensible.

## EVENTOS CIFS Y NFS

<ul style="list-style-type: none"><li>• Crear archivo</li><li>• Borrar archivo</li><li>• Abrir archivo</li><li>• Renombrar archivo</li><li>• Modificar archivo</li><li>• Permiso de Instalación de archivo</li><li>• Crear directorio</li><li>• Borrar directorio</li><li>• Renombrar Directorio</li></ul>	<ul style="list-style-type: none"><li>• Permisos de instalación de Directorio</li><li>• Acceso Denegado – Abrir Archivo</li><li>• Acceso Denegado – Borrar Archivo</li><li>• Acceso Denegado - Permisos de Instalación de archivo</li><li>• Acceso Denegado – Borrar Directorio</li><li>• Acceso Denegado - Permisos de Instalación de Directorios</li></ul>	Las plataformas CIFS y NFS respaldadas incluyen Windows, NetApp, EMC VNX/Celerra, HP IBRIX, Hitachi NAS, UNIX, Linux, Solaris, AIX.
--	--	---

## EVENTOS SHAREPOINT

<ul style="list-style-type: none"><li>• Crear archivo</li><li>• Borrar archivo</li><li>• Abrir archivo</li><li>• Renombrar archivo</li><li>• Modificar archivo</li><li>• Seguridad de instalación de archivos</li></ul>	<ul style="list-style-type: none"><li>• Crear Directorio</li><li>• Borrar Directorio</li><li>• Renombrar Directorio</li><li>• Seguridad de Instalación de Directorio</li><li>• Instalación de Rol</li><li>• Crear Sitio</li></ul>	<ul style="list-style-type: none"><li>• Crear lista de Ítem</li><li>• Borrar Lista de Ítem</li><li>• Abrir Lista de Ítem</li><li>• Renombrar Lista de Ítem</li><li>• Modificar Lista de Ítem</li></ul>
---	---	--

## EVENTOS DE EXCHANGE

<ul style="list-style-type: none"><li>• Abrir Carpeta</li><li>• Crear Carpeta</li><li>• Borrar Carpeta</li><li>• Renombrar Carpeta</li><li>• Agregar permisos de Carpeta</li><li>• Remover Permisos de Carpeta</li><li>• Cambiar Permisos de Carpeta</li><li>• Mover Carpeta</li><li>• Vaciar Carpeta</li><li>• Copiar Carpeta</li><li>• Marcar todo como leído</li><li>• Enviar Mensaje</li></ul>	<ul style="list-style-type: none"><li>• Enviar Mensaje (A nombre de X)</li><li>• Enviar Mensaje (Como X)</li><li>• Mensaje Recibido</li><li>• Editar Mensaje</li><li>• Borrar Mensaje</li><li>• Copiar Mensaje</li><li>• Mover Mensaje</li><li>• Crear Mensaje</li><li>• Mensaje Marcado como no Leído</li><li>• Mensaje Marcado como Leído</li><li>• Inicio de Sesión</li></ul>
--	--

## EVENTOS DE ACTIVE DIRECTORY

<ul style="list-style-type: none"><li>• Proceso de creación y borrado de todos los objetos</li><li>• Cambios en membresías grupales</li><li>• Cambios en el servicio de directorio de propiedades de objeto para cualquier propiedad</li><li>• Reinicio de Password</li><li>• Bloqueo y Desbloqueo de Cuentas</li><li>• Activar o Desactivar Cuentas</li><li>• Cambios en Membresías Grupales</li></ul>
---

### AMÉRICA LATINA, PUERTO RICO Y REPÚBLICA DOMINICANA

Cesar Mahecha **T** +1 646 341 8581 **E** [cmahecha@varonis.com](mailto:cmahecha@varonis.com) **W** [www.varonis.com](http://www.varonis.com)

### ESPAÑA, ANDORRA - CEUTA Y MELILLA

Tamer Dessouki **T** +33 6 58 96 03 48 **E** [tdessouki@varonis.com](mailto:tdessouki@varonis.com) **W** [www.varonis.com](http://www.varonis.com)