

Change Auditor

Auditorías de cambios en tiempo real para el entorno de plataformas de Microsoft

El registro de eventos y los informes de cambios para las aplicaciones y servicios empresariales son engorrosos, llevan tiempo y, en algunos casos, son imposibles mediante el uso de herramientas de auditoría nativas. Como no hay una consola central, se debe repetir el proceso para cada servidor, por lo que usted termina con un enorme volumen de datos sin contexto y una infinidad de informes.

Esto significa que demostrar el cumplimiento o reaccionar rápidamente a los eventos es un desafío constante. La seguridad de los datos también se encuentra en riesgo porque los detalles de eventos nativos son escasos y difíciles de interpretar. Por consiguiente, puede que descubra los problemas cuando ya sea demasiado tarde. Además, como las herramientas nativas no pueden evitar que el usuario con privilegios elimine un registro de eventos, podría perder los datos del

registro, y, en consecuencia, eliminar el propósito de auditorías en primer lugar.

Afortunadamente, existe Quest® Change Auditor. Esta familia de productos le permite auditar, alertar e informar sobre todos los cambios realizados en Active Directory (AD), Azure AD, Exchange, Office 365, SharePoint, Skype for Business, VMware, EMC, NetApp, SQL Server y servidores de archivos de Windows, así como consultas sobre LDAP en AD, todo en tiempo real y sin habilitar las auditorías nativas.

Puede instalar, implementar y administrar su entorno con facilidad, desde una sola consola central. El seguimiento de lo que se crea, de lo que se elimina y de las modificaciones e intentos de acceso no podría ser más fácil, y entender qué sucedió es muy sencillo porque cada evento y todos los eventos relacionados se muestran en términos simples, por lo que puede saber estos datos esenciales:



Con Change Auditor, obtendrá información sobre quién, qué, cuándo, dónde y desde qué workstation se producen todos los cambios, en orden cronológico, incluidas las identidades correlacionadas locales y en la nube.

"Change Auditor fue, por lejos, la mejor solución en lo que respecta a funcionalidad y costo. Nos sedujo la simplicidad y la facilidad de uso de la herramienta, lo que nos permitió crear consultas sin ninguna experiencia técnica en particular".

Stephane Malagnoux
Jefe del Departamento de Informática BPCI Insurance

BENEFICIOS:

- Elimina las inquietudes de seguridad desconocidas y de ese modo garantiza el acceso continuo a las aplicaciones, los sistemas y los usuarios con un seguimiento de todos los eventos y los cambios relacionados con incidentes específicos.
- Reduce el estrés y la complejidad al interpretar automáticamente los datos crípticos y su gravedad, lo que permite tomar decisiones de manera más rápida y adecuada.
- Disminuye los riesgos de seguridad en segundos con alertas en tiempo real a cualquier dispositivo para una respuesta inmediata, dentro de la oficina o fuera de ella.
- Reduce el arrastre de rendimiento en los servidores mediante la recopilación de eventos sin el uso de auditorías nativas.
- Optimiza los informes de cumplimiento aislados para políticas internas y normas externas, incluidas SOX, PCI DSS, HIPAA, FISMA y SAS 70, entre otras.
- Proporciona a los gerentes y auditores prueba de controles informáticos apropiados para darles tranquilidad.

“Change Auditor ha sido una herramienta muy intuitiva, pero muy eficaz, que me permitió comprender los cambios realizados por el personal. Me permitió aplicar políticas, restringir el acceso y recibir alertas sobre infracciones”.

Arquitecto sénior de TI, empresa de servicios profesionales para medianas empresas

Fuente: TechValidate. TVID: B4A-A84-619

PRODUCTOS

Detección de amenazas de Change Auditor

Change Auditor for Active Directory

Consultas sobre Change Auditor for Active Directory

Change Auditor for EMC

Change Auditor for Exchange

Change Auditor for FluidFS

Change Auditor for Logon Activity

Change Auditor for NetApp

Change Auditor for SQL Server

Change Auditor for SharePoint

Change Auditor para Skype for Business

Change Auditor for VMware vCenter

Change Auditor for Windows File Servers

quién, qué, cuándo, dónde y desde qué workstation, además de la configuración actual y anterior.

Gracias a esta amplitud del análisis de datos, puede tomar medidas inmediatas cuando surgen problemas y acceder a la información acerca de qué otros cambios provinieron de workstations y usuarios específicos, lo que elimina las suposiciones y las inquietudes de seguridad desconocidas adicionales. Tanto para satisfacer las demandas de cumplimiento cada vez mayores como para cumplir con las políticas de seguridad internas, Change Auditor es la solución en la que puede confiar.

CARACTERÍSTICAS

Auditorías de entornos híbridos con una vista correlacionada: audite entornos híbridos, incluidos AD/Azure AD, Exchange/Exchange Online, SharePoint/SharePoint Online/OneDrive para la Empresa, así como inicios de sesión en AD y en Azure AD. A diferencia de las auditorías nativas, Change Auditor ofrece una visualización simple y correlacionada de la actividad en todos los entornos híbridos, lo que asegura la visibilidad de todos los cambios que se están realizando, ya sea de manera local o en la nube.

Prevención de cambios: protéjase contra cambios a los datos críticos dentro de AD, Exchange y los servidores de archivos de Windows, incluidos grupos con privilegios, objetos de política grupal y buzones de correo importantes.

Informes listos para el auditor: genere informes integrales para las mejores prácticas y el cumplimiento de las normativas para SOX, PCI DSS, HIPAA, FISMA, GLBA y GDPR, entre otras.

Panel alojado con On Demand Audit: vea la actividad híbrida de AD y Office 365 juntos desde un panel de SaaS alojado con búsqueda receptiva, visualización interactiva de datos y almacenamiento de eventos a largo plazo.

Detección de amenazas proactiva con Change Auditor Threat Detection: simplifique la detección de amenazas de usuarios mediante el análisis de

actividades inusuales para clasificar los usuarios que más riesgos presentan a su empresa, identificar amenazas potenciales y disminuir el ruido producto de alarmas falsas positivas.

Motor de auditorías de alto rendimiento: elimine las limitaciones de las auditorías y capture la información de los cambios sin la necesidad de registros de auditoría nativa, para obtener resultados más rápidos y ahorros significativos de los recursos de almacenamiento.*

Bloqueo de cuentas: capture la dirección IP y el nombre de la workstation de origen en caso de eventos de bloqueos de cuenta, y vea los intentos de acceso y de inicio de sesión relacionados en una línea de tiempo interactiva. Esto ayuda a simplificar la detección y la investigación de amenazas de seguridad internas y externas.

Alertas en tiempo real: envíe alertas de patrones y cambios críticos al correo electrónico y a los dispositivos móviles para indicar una medida inmediata, lo que le permite responder más rápido ante las amenazas, incluso cuando no se encuentre en el lugar.

Reenvío de eventos integrado: integre fácilmente con soluciones de SIEM para reenviar eventos de Change Auditor a Splunk, Arcsight o QRadar. Además, Change Auditor se integra con Quest® InTrust® para el almacenamiento de eventos comprimidos 20:1 y la recolección, el análisis y el estudio de registros nativos o de terceros con alertas y acciones de respuesta automática ante eventos sospechosos.

ACERCA DE QUEST

Quest provee soluciones de software para el mundo cambiante de las empresas de TI. Ayudamos a simplificar los desafíos causados por la explosión de datos, la expansión en la nube, los centros de datos híbridos, las amenazas de seguridad y los requisitos regulatorios. Nuestro portafolio incluye soluciones para la administración de bases de datos, la protección de datos, la administración de endpoints unificada, la administración de entidades y accesos, y la administración de plataformas de Microsoft.

* No se aplica a FluidFS, SharePoint, EMC, NetApp y VMware.