netwrix

Netwrix Auditor

Detecte las amenazas de **seguridad**, demuestre el **cumplimiento normativo** e incremente la **eficacia del equipo de TI**

www.netwrix.es

01
Descripción general del producto

Alivie la carga de la auditoría de TI

Las auditorías internas y externas de TI se están convirtiendo en una parte integral de la rutina diaria para cada vez más organizaciones. Después de todo, las auditorías de TI no son únicamente cruciales para velar por la seguridad y el cumplimiento normativo; también ayudan a las organizaciones a identificar y eliminar las ineficiencias de sus procesos operativos. Desafortunadamente, realizar estas auditorías regulares suele ser bastante más laborioso y lento de lo que debería ser.

Con Netwrix Auditor, puede reducir su carga de auditoría de TI y lograr sus objetivos con bastante menos esfuerzo. Su inteligencia de proceso le permite automatizar muchas de las tareas relacionadas con la seguridad, cumplimiento normativo y operaciones de TI que antes requerían de mucho tiempo para ser completadas, de esta forma puede satisfacer las peticiones de su organización sin estar constantemente sobrecargado.

> *"No queremos proveedores; queremos socios. Netwrix prácticamente se ha convertido en parte de nuestro equipo. Con Netwrix Auditor, nuestro equipo de TI recupera tiempo muy valioso, lo que hace a nuestra organización más eficiente a la hora de cumplir con nuestros objetivos para el condado."*
>
> **John Adams**, Director de TI, Washington County, Arkansas

02
Descripción general del producto

Detecte las amenazas rápidamente para evitar ser noticia por una brecha de seguridad

Reduzca la exposición de sus activos críticos identificando sus mayores riesgos en el ámbito de la seguridad y reforzando los permisos que se han relajado. Asegure la detección a tiempo y la respuesta a las amenazas configurando alertas con acciones automatizadas y realizando investigaciones más rápidas y precisas.

Ahorre tiempo y dinero durante las auditorías de conformidad

Logre, pruebe y mantenga el cumplimiento normativo con menos esfuerzo y coste reduciendo el tiempo necesario para preparar las auditorías hasta en un 85%. Deje de perder horas rastreando a través de los registros de auditoría cuando necesite responder a preguntas muy específicas de los auditores.

Incremente la eficacia del equipo de TI sin comprometer el equilibrio entre trabajo y vida personal

Habilite a su equipo de TI para hacer más con menos y logre altos KPIs sin quedarse hasta tarde constantemente. Resuelva los problemas críticos antes de que los usuarios se sientan frustrados o el negocio quede afectado, y genere la información requerida por los interesados más rápidamente que si lo hiciera a través de procesos manuales.

03

Detecte las amenazas rápidamente para evitar ser noticia por una brecha de seguridad

Evalúe y mitigue los riesgos de TI

Encuentre y cierre las brechas de seguridad de datos e infraestructura en todo su entorno de TI, como un gran número de permisos asignados directamente o demasiadas cuentas de usuario inactivas, para reducir su superficie de ataque.

Risk Assessment – Overview

Risk name	Current value	Risk level
Users and Computers		
User accounts with Password never expires	2	Medium (1-4)
User accounts with Password not required	0	Low (0)
Inactive user accounts	10% (3 of 30)	High (1% - 100%)
Inactive computer accounts	20% (4 of 20)	High (3% - 100%)
Permissions		
User accounts with administrative permissions	20% (6 of 30)	High (3% - 100%)
Empty security groups	6% (0 of 50)	Low (0)
Data		
Shared folders accessible by Everyone	11% (1685 of 15321)	Medium (5% - 15%)
File names containing sensitive data	2	High (2 - unlimited)
Potentially harmful files on file shares	0	Low (0)
Direct permissions on files and folders	21% (10759 of 51237)	High (5% - 100%)

Sensitive Files Count by Source

Shows the number of files that contain specific categories of sensitive data. Clicking the "Categories" or "Source" link narrows your results down to a certain file in this report. Use this report to estimate amount of your sensitive data in each category, plan for data protection measures and control their implementation.

Content source	Categories	Files count
\\fs1\Accounting	GDPR	1300
	PCI DSS	585
\\fs1\Finance	GDPR	715
	HIPAA	1085
	PCI DSS	952
\\fs1\HR	GDPR	1500
	HIPAA	250
\\fs1\Public	PCI DSS	15

Obtenga una profunda visión sobre sus datos sensibles

Localice y clasifique la información sensible, incluyendo los datos de la tarjeta bancaria, registros médicos y otros PII, y detecte cualquier información sensible que aparezca en una ubicación no segura para minimizar el riesgo de una brecha.

04

Detecte las amenazas rápidamente para evitar ser noticia por una brecha de seguridad

Agilice las certificaciones regulares de privilegios

Vea quién tiene acceso a qué datos confidenciales y cómo han obtenido el acceso, y permita a los propietarios de los datos verificar regularmente que esos derechos están alineados con las necesidades de negocio.

Sensitive Data Object Permissions

For each SharePoint object (site, list or document) listed, this report shows the user accounts that have access to this object, their effective permissions and how those permissions were granted. Use this report to control access to SharePoint objects that contain sensitive data.

Object path: http://sp.enterprise.com/sites/HR/Shared/Candidates Info 2019.xlsx

Categories: PII

Total accounts count: 5

User account	Permissions	Means granted
ENTERPRISE\J.Carter	Full Control	Zone: Default (policy), Web application pool account
ENTERPRISE\T.Simpson	Full Control	Zone: Default (policy), Web application pool account
ENTERPRISE\A.Brown	Full Control	Farm Account
ENTERPRISE\B.Richter	Read	Permission level, Site collection administrator
ENTERPRISE\J.London	Contribute	Farm Account

User Sessions

Use this report to identify suspicious user sessions on Windows servers. Find out which users were active on critical or terminal servers and the total time during a day when their activity on the servers was monitored by Netwrix Auditor.

When: 4/23/2019

Who: ENTERPRISE\J.Carter

Where	Active time
audit.enterprise.com	3:05
dc1.enterprise.com	0:14

Who: ENTERPRISE\T.Simpson

Where	Active time
audit.enterprise.com	0:09
dc1.enterprise.com	0:32

Establezca una estricta responsabilidad en el uso de cuentas privilegiadas

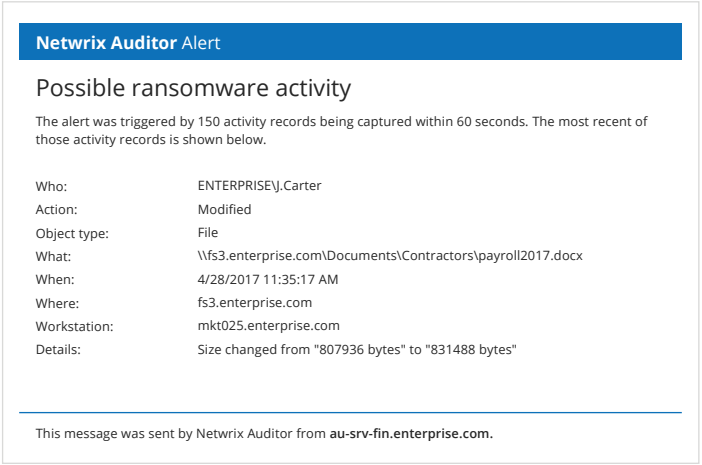
Monitorice constantemente en todos los sistemas la actividad de los usuarios con privilegios para asegurar que siguen las políticas internas y no abusan de sus privilegios para acceder.

05

Detecte las amenazas rápidamente para evitar ser noticia por una brecha de seguridad

Sea el primero en estar informado sobre actividades sospechosas

Detecte amenazas de seguridad, como la actividad del SQL Server fuera del horario de negocio o un gran número de modificaciones de ficheros repetidas que podrían indicar un ataque ransomware en progreso, de forma que pueda actuar antes de que se realice un daño significativo.



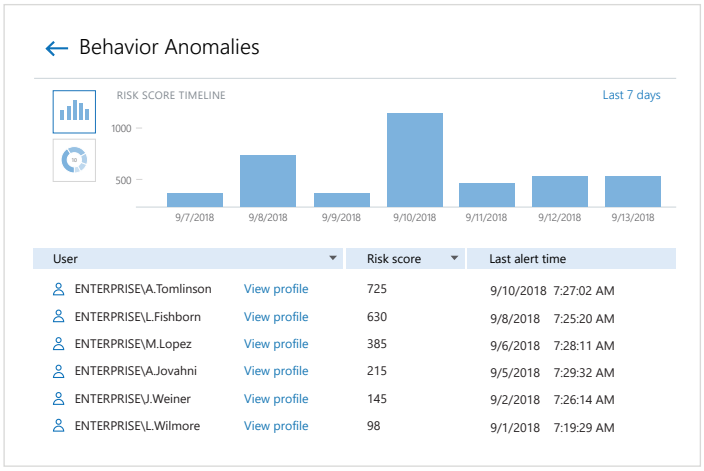
Netwrix Auditor Alert

Possible ransomware activity

The alert was triggered by 150 activity records being captured within 60 seconds. The most recent of those activity records is shown below.

Who:	ENTERPRISE\J.Carter
Action:	Modified
Object type:	File
What:	\\fs3.enterprise.com\Documents\Contractors\payroll2017.docx
When:	4/28/2017 11:35:17 AM
Where:	fs3.enterprise.com
Workstation:	mkt025.enterprise.com
Details:	Size changed from "807936 bytes" to "831488 bytes"

This message was sent by Netwrix Auditor from **au-srv-fin.enterprise.com.**



← Behavior Anomalies

RISK SCORE TIMELINE — Last 7 days

1000
500

9/7/2018 9/8/2018 9/9/2018 9/10/2018 9/11/2018 9/12/2018 9/13/2018

User		Risk score	Last alert time
ENTERPRISE\A.Tomlinson	View profile	725	9/10/2018 7:27:02 AM
ENTERPRISE\L.Fishborn	View profile	630	9/8/2018 7:25:20 AM
ENTERPRISE\M.Lopez	View profile	385	9/6/2018 7:28:11 AM
ENTERPRISE\A.Jovahni	View profile	215	9/5/2018 7:29:32 AM
ENTERPRISE\J.Weiner	View profile	145	9/2/2018 7:26:14 AM
ENTERPRISE\L.Wilmore	View profile	98	9/1/2018 7:19:29 AM

Detecte cuentas comprometidas y usuarios maliciosos

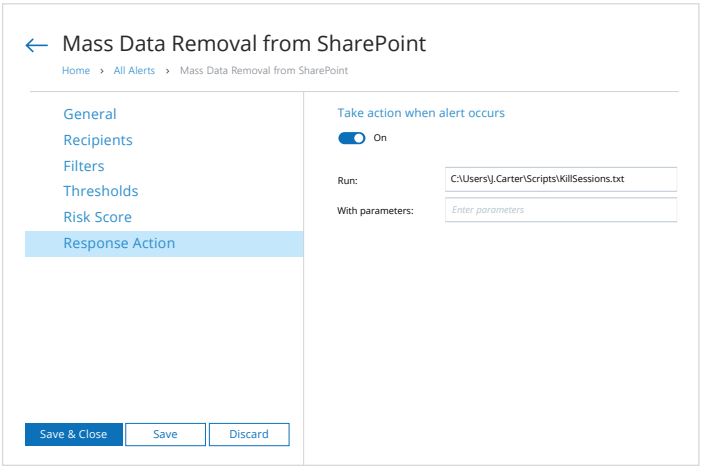
Identifique indicios sutiles de posibles amenazas de seguridad, como inicios de sesión inusuales o accesos remotos a su red no autorizados. Identifique fácilmente e investigue a los usuarios que suponen un mayor riesgo a través de una vista agregada de las actividades anómalas de cada individuo.

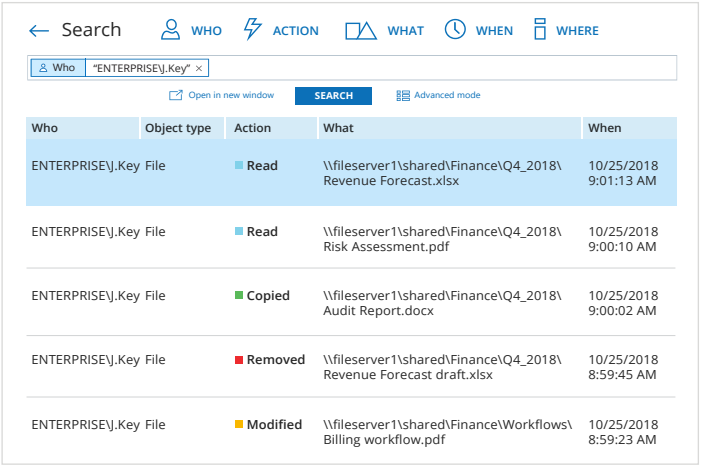
06

Detecte las amenazas rápidamente para evitar ser noticia por una brecha de seguridad

Reduzca el tiempo medio de respuesta

Reaccione a las amenazas de seguridad sobre los datos más rápidamente automatizando la respuesta anticipada a los incidentes. Proporcione el soporte inicial a las incidencias integrando Netwrix Auditor ensu proceso SecOps.





Agilice la investigación de los incidentes

Llegue al fondo de los incidentes que han involucrados datos sensibles en minutos usando una búsqueda similar a la de Google: Comprenda exactamente qué pasó, cómo pasó, quién estaba detrás y qué partes de la información estuvieron afectadas.

07

Ahorre tiempo y dinero durante las auditorías de conformidad

Compruebe que sus controles de seguridad son efectivos

Implemente controles de cumplimiento en toda su infraestructura y evalúe regularmente si funcionan según lo previsto. Si sus políticas de seguridad escritas difieren de las que están actualmente en marcha, corrija sus controles de seguridad defectuosos antes de que los auditores los descubran.

Sensitive File and Folder Permissions Details

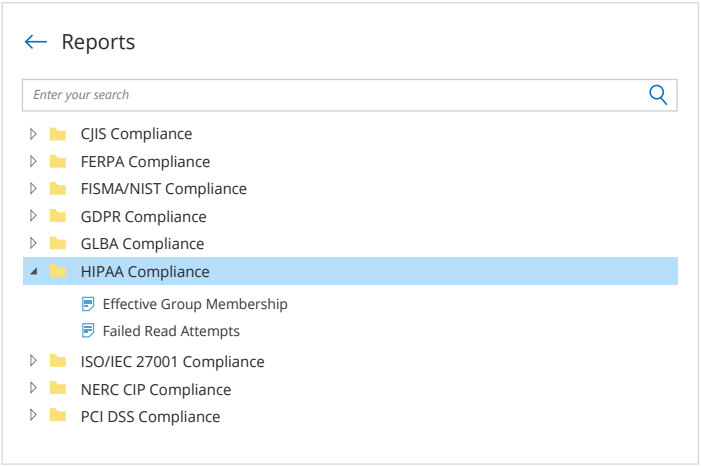
Shows permissions granted on files and folders that contain certain categories of sensitive data. Use this report to see who has access to a particular file or folder, via either group membership or direct assignment. Reveal sensitive content that has permissions different from the parent folder.

Object: \\fs1\Accounting (Permissions: Different from parent)
Categories: GDPR

Account	Permissions	Means granted
ENTERPRISE\J.Carter	Full Control	Group
ENTERPRISE\T.Simpson	Full Control	Directly
ENTERPRISE\A.Brown	Full Control	Group

Object: \\fs1\Accounting\Contractors (Permissions: Different from parent)
Categories: GDPR

Account	Permissions	Means granted
ENTERPRISE\M.Smith	Full Control	Group
ENTERPRISE\A.Gold	Full Control	Group



Reduzca el tiempo dedicado a la preparación de la conformidad

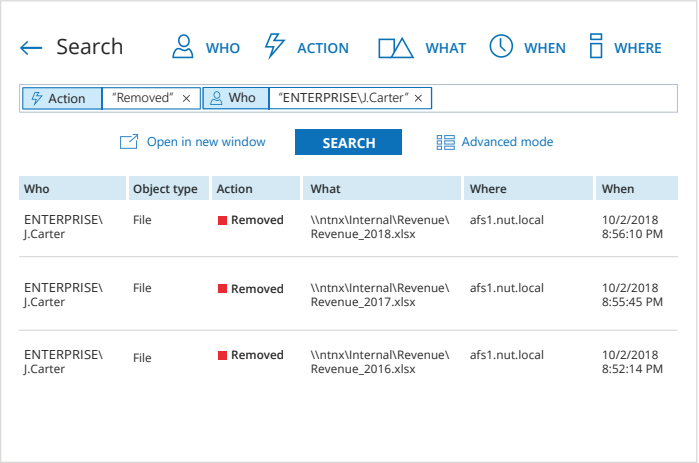
Prepare el grueso de las peticiones de los auditores aprovechando los informes predefinidos ajustados a los controles de conformidad de HIPAA/HITECH, PCI DSS, GDPR y otras normativas comunes.

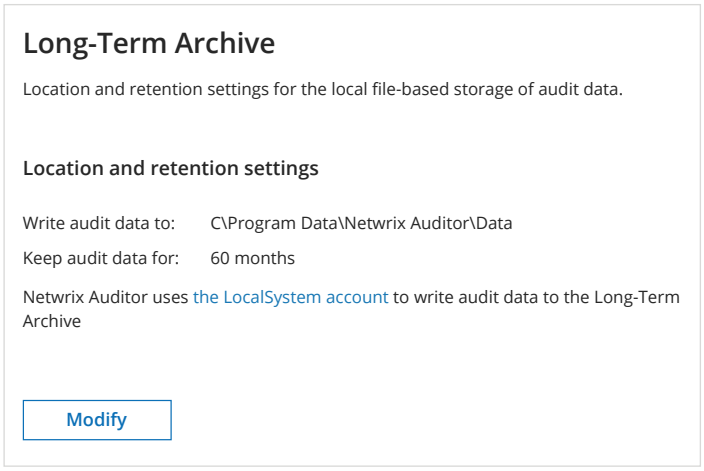
08

Ahorre tiempo y dinero durante las auditorías de conformidad

Responda a las preguntas específicas de los auditores

Si hay preguntas inesperadas durante la auditoría, utilice la búsqueda similar a la de Google para obtener la información requerida en el acto.





Almacene y acceda a sus registros de auditoría durante años

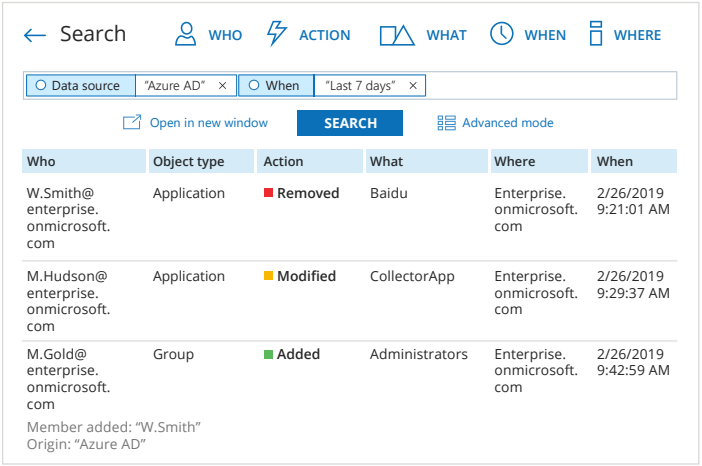
Guarde sus registros de auditoría archivados en un formato comprimido durante más de 10 años, tal y como es exigido por muchas normativas, mientras asegura que todos los datos de auditoría son, en cualquier momento, fácilmente accesibles a los usuarios autorizados.

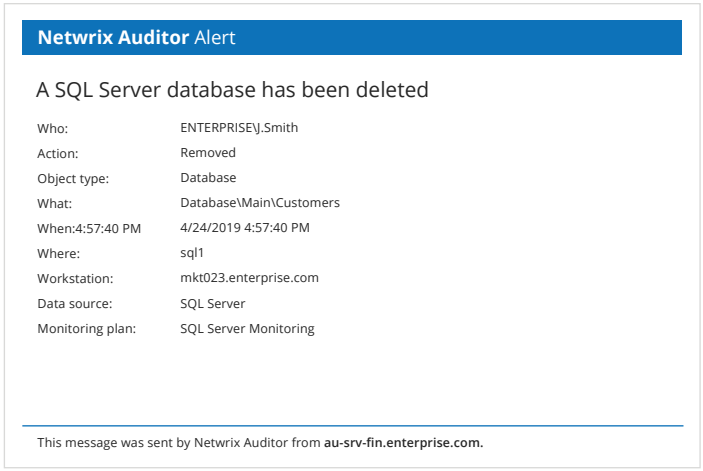
09

Incremente la eficacia del equipo de TI sin comprometer el equilibrio entre trabajo y vida personal

Resuelva las cuestiones de los usuarios antes de que se conviertan en problemas reales

Siempre que los usuarios quieran saber por qué su fichero ha desaparecido y cómo lo pueden recuperar o por qué no pueden acceder a una máquina virtual donde se ejecuta una aplicación de negocio crítica, obtenga las repuestas en unos pocos clics y permita a los usuarios volver de nuevo al trabajo.





Reaccione rápidamente a los eventos que puedan ocasionar tiempos de inactividad

Reciba de forma inmediata las notificaciones sobre eventos, como el borrado de una unidad organizativa o de una base de datos con información del cliente, y resuélvalos rápidamente antes de que el negocio se vea afectado.

10

Incremente la eficacia del equipo de TI sin comprometer el equilibrio entre trabajo y vida personal.

Obtenga una clara imagen de lo que fue cambiado

Mantenga el control de lo que está cambiando en todos sus sistemas de TI tanto en sus instalaciones como en la nube de forma que pueda detectar y resolver los problemas antes de que afecten a la actividad de negocio y a la productividad del usuario. Como resultado, podrá suministrar los servicios de TI de forma ininterrumpida y cumplir con sus SLAs y las expectativas de los usuarios de forma sistemática.

Sharing and Security Changes

Shows changes to security group membership, policies, and sharing settings, such as promoting a user to site collection administrator or sharing data with external users.

Action	Object Type	What	Who	When
Modified	Group	GroupName1	T.Simpson @enterprise. onmicrosoft.com	9/1/2018 8:56:10 AM
Where:	https://enterprise-my.sharepoint.com/sites/Test_Do_Not_Delete			
Workstation:	81.09.21.122			
Modified	List	https://enterprise -my.sharepoint.com/ Lists/Customers	T.Simpson @enterprise. onmicrosoft.com	9/1/2018 8:35:44 AM
Where:	https://enterprise-my.sharepoint.com			
Workstation:	81.09.21.122			
Permissions: • **Added:** "User Account Administrator (Edit)"				

Windows Server Configuration Details

Provides review of Windows server configuration. For a server, the following details are reported: its OS, antivirus, local users and groups, files shares, installed programs, and services. You can apply baseline filters to highlight security issues, such as outdated operating system or improper antivirus. Use this report to examine server configuration details and proactively mitigate risks in your environment.

Category: General

Server	OS Name	OS Version	Antivirus Status
audit.enterprise.com	Microsoft Windows Server 2012 R2 Standard	6.3.9600	Issues Detected

Category: Software

Object Type	Object Name	Properties
Software	Microsoft OneDrive	Available: ENTERPRISE\M.Peterson, Version: 17.3.4604.0120
Software	Trojan	Available: All users, Version: 6.9.5.2956
Software	Google Chrome	Available: All users, Version: 66.0.3359.139
Software	uTorrent	Available: ENTERPRISE\J.Hanson, Version: 3.5.3.44396

Descubra las desviaciones producidas respecto a una línea base correcta y conocida

Determine el estado actual de sus activos críticos más rápidamente de lo que lo haría con procesos manuales de forma que pueda verificar si su configuración coincide con una línea base correcta y conocida. Si no es así, resuelva los problemas para prevenir tiempos de inactividad de los sistemas y la interrupción de los usuarios.

11

Incremente la eficacia del equipo de TI sin comprometer el equilibrio entre trabajo y vida personal.

Responda a las preguntas en minutos, no horas

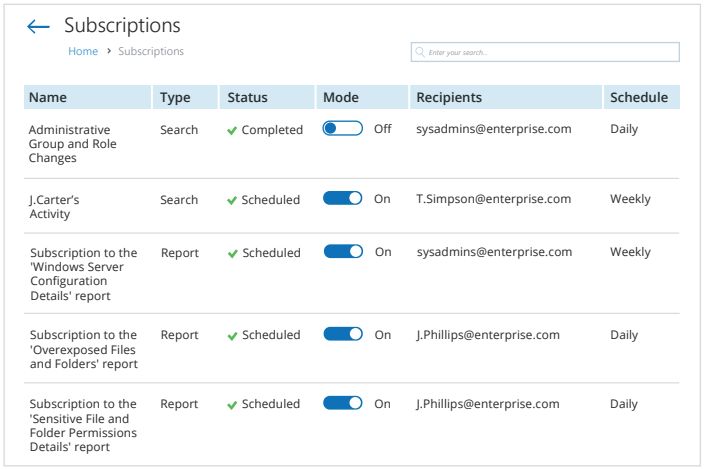
Cuando los interesados soliciten una información, como por ejemplo la lista de quién ha accedido a una carpeta concreta o la prueba de que no hay usuarios inactivos en el entorno de TI, responda rápidamente con informes legibles para el usuario y listos para su uso inmediato.

Folder and File Permission Details

Shows permissions granted on a shared folder, its subfolders and files (either directly or via group membership). Use this report to see who has access to a particular folder and its contents, and reveal objects that have permissions different from their parent. Clicking the group link opens the "Group Membership by User" report.

Object: \\fs1\Accounting\Contractors (Permissions: Different from parent)

Account	Permissions	Means Granted
ENTERPRISE\J.Carter	Full Control	Group
ENTERPRISE\T.Simpson	Read (Execute, List folder content)	Group
ENTERPRISE\J.Smith	Full Control	Directly
ENTERPRISE\A.Tompson	Full Control	Group
ENTERPRISE\M.Brown	Full Control	Directly



Deje de ser el cuello de botella en la generación de informes

Envíe de forma automática a los interesados la información que pidan con la periodicidad que prefieran. O bien, proporcione a los interesados un acceso granulado a Netwrix Auditor para que puedan obtener ellos mismos la información que necesitan cuando quieran.

12
Netwrix Auditor Applications

Audite sus sistemas informáticos más importantes desde un único punto

Deje de hacer malabarismos con múltiples herramientas en un intento de recoger la información de auditoría de todos sus sistemas tanto los de sus instalaciones como los basados en la nube y deje que Netwrix Auditor le proporcione toda la información que necesita de una manera unificada y consistente.

- Netwrix Auditor for Active Directory
- Netwrix Auditor for Exchange
- Netwrix Auditor for Azure AD
- Netwrix Auditor for Office 365
- Netwrix Auditor for Windows File Servers
- Netwrix Auditor for EMC
- Netwrix Auditor for Nutanix Files
- Netwrix Auditor for NetApp
- Netwrix Auditor for SharePoint
- Netwrix Auditor for Windows Server
- Netwrix Auditor for Oracle Database
- Netwrix Auditor for SQL Server
- Netwrix Auditor for Network Devices
- Netwrix Auditor for VMware

13

API de integración con Netwrix Auditor

Saque provecho de unas capacidades de integración sin límites, auditoría y generación de informes

Centralice la auditoríia y la presentación de informes

Netwrix Auditor recoge registros de actividad desde cualquier aplicación on-premises o cloud y los almacena en un repositorio central seguro, preparados para revisiones de históricos y peticiones de conformidad.

Get the most from your SIEM investment

Obtenga el máximo su inversión en SIEM
Obtenga resultados mucho menos crípticos de su SIEM y acelere las investigaciones introduciendo en este los datos legibles y tratables recogidos por Netwrix Auditor.

Automatice los procesos TI

Netwrix Auditor se integra otras herramientas de seguridad, conformidad y gestión de datos, automatizando y mejorando los procesos de TI y de SecOps.

Visite el Netwrix Auditor Add-on Store en **netwrix.com/go/add-ons** para conseguir aplicaciones complementarias gratuitas e integrar su Netwrix Auditor a su ecosistema de TI.

14
Por qué Netwrix Auditor

Revise las principales razones por las que los clientes escogen Netwrix Auditor

Ganancias rápidas

Empiece a obtener valor desde el primer momento y obtenga un retorno de la inversión en días, y no en meses. No pague por servicios profesionales caros o pierda el tiempo en largos procesos de instalación.

Precios razonables

Obtenga una solución a un precio razonable con gastos operativos transparentes y predecibles. Alcance múltiples objetivos en materia de seguridad, cumplimiento normativo y operaciones de TI sin gastar una fortuna en herramientas heterogéneas.

Arquitectura no intrusiva

Evite la pesadilla de tratar con agentes intrusivos y métodos de recolección de datos indocumentados.

Soporte técnico de primera clase

Resuelva sus problemas de manera rápida a través de un soporte técnico de primer nivel con una tasa de satisfacción del 97%.

"Netwrix Auditor permite sacar el máximo rendimiento al dinero, sin competencia."

"Gestor de operaciones de TI del sector financiero" Gartner peerinsights

15
Éxito del cliente

Descubra como nuestros clientes logran sus objetivos gracias a Netwrix Auditor

Únase a más de 10.000 organizaciones de diversas industrias de todo el mundo que ya están utilizando Netwrix Auditor para asegurar sus activos críticos de negocio, superar las auditorías de conformidad y administrar de manera eficaz y eficiente sus entornos de TI en sus instalaciones, en la nube e híbridos.

Sin ánimo de lucro

Horizon Leisure Centres acelera la clasificación de datos para asegurar la seguridad de datos confidenciales y cumplir con la GDPR.

Alimentos y bebidas

Perfetti Van Melle Turkey cumple con la norma ISO/IEC27001 y hace cumplir sus políticas de seguridad internas con Netwrix Auditor.

Seguros

First Insurance Company of Hawaii utiliza Netwrix Auditor para mejorar la estabilidad de los sistemas y acelerar las investigaciones.

Energía

Pike Electric resuelve los problemas de seguridad más rápido y asegura la continuidad de negocio usando Netwrix Auditor.

Acerca de nosotros

Netwrix permite a los profesionales de la seguridad de la información y del gobierno recuperar el control de los datos sensibles, regulados y críticos para el negocio, independientemente de donde estén. Más de 10.000 organizaciones en todo el mundo confían en las soluciones de Netwrix para proteger datos sensibles, ser consciente del valor de negocio de su contenido empresarial, superar las auditorias de cumplimiento con menos esfuerzo y coste e incrementar la productividad de los equipos de TI y de los empleados.

Fundada en 2006, Netwrix ha ganado más de 150 premios de la industria y ha sido incluida en la Inc. 5000 y en la Deloitte Technology Fast 500 listas de las empresas con el crecimiento más rápido en los EE.UU.

Para más información, visite www.netwrix.es.

Próximos pasos

Inicie una prueba gratuita

netwrix.es/freetrial

Agende una demo en vivo

netwrix.es/livedemo

Inicie la demo desde el navegador

netwrix.com/browser_demo

Sede corporativa:

300 Spectrum Center Drive, Suite 200, Irvine, CA 92618

Teléfono: +34 911 982608 **Toll-free:** 888-638-9749

netwrix.com/social