exaprobe

netwrix

Netwrix Auditor

Know Your Data. Protect What Matters.

www.netwrix.com

01
Product Overview

Netwrix Auditor Platform

Netwrix Auditor is an **agentless data security platform** that empowers organizations to accurately identify sensitive, regulated and mission-critical information and apply access controls consistently, regardless of where the information is stored. It enables them to **minimize the risk of data breaches** and **ensure regulatory compliance** by proactively reducing the exposure of sensitive data and promptly detecting policy violations and suspicious user behavior.

Identify
Understand which data needs protection and how exposed it is.

Protect
Minimize the risk of a data breach.

Detect
Promptly detect data security threats.

Respond
Make faster and more informed incident response decisions.

Recover
Facilitate the recovery of key data and learn from past incidents.

Comply
Achieve and prove regulatory compliance.

02
Benefits

Understand which data needs protection and how exposed it is

Identify and classify sensitive data, both structured and unstructured, and data and infrastructure risks that might endanger its security.

Minimize the risk of a data breach

See who has access to what and proactively remediate the overexposure of sensitive, regulated and mission-critical data.

Promptly detect data security threats

Spot abnormal user behavior and policy violations that threaten data security.

Make faster and more informed incident response decisions

Reduce mean time to respond to data security threats and contain incidents.

Facilitate the recovery of key data and learn from past incidents

Review comprehensive details about how a security incident happened and what data was affected.

Achieve and prove regulatory compliance

Proactively assess the effectiveness of your data security controls and prove your compliance to auditors with hard evidence.

03

Understand which data needs protection and how exposed it is

Prioritize the security of sensitive data across multiple data silos

Classify and tag both unstructured and structured data regardless of its location so you can prioritize the security of sensitive information. Apply security policies consistently across multiple data repositories.

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

Overexposed Files and Folders

Shows sensitive files and folders accessible by the specified users or groups, based on the combination of folder and share permissions. Clicking the "Object path" link opens the "Sensitive File and Folder Permission Details" report. Use this report to identify data at high risk and plan for corrective actions accordingly.

Group Name: Everyone

Object path	Categories
\\fs1\Accounting\Contractors	GDPR
	PCI DSS
	PII
\\fs1\Accounting\Payroll	GDPR
	PCI DSS
\\fs1\Accounting\Invoices	GDPR
	PCI DSS

Identify overexposed sensitive data

See which pieces of sensitive data are most at risk so you can prioritize remediation of those risks. Discover sensitive information that is exposed to a large number of users without a business need or that is stored in an unsecure location.

04

Understand which data needs protection and how exposed it is

Assess data and infrastructure security risks

Identify both data and infrastructure security gaps, such as a large number of directly assigned permissions or too many inactive user accounts. Continuously evaluate these security metrics and focus on what's most important.

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)
Disabled computer accounts	0% (0 of 20)	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%)
Administrative groups	12% (6 of 50)	High (3% - 100%)
Empty security groups	6% (3 of 50)	High (2% - 100%)
Data		
Shared folders accessible by Everyone	14% (2145 of 15321)	High (5% - 100%)
File names containing sensitive data	2	High (2 - unlimited)

05

Minimize the risk of a data breach

Automatically quarantine sensitive data to reduce the risk of a breach or loss

If a sensitive document pops up in an unexpected location, automatically move it to a quarantine area until you can determine where it should be stored and who should have access to it.

Immediately lock down sensitive data that is overexposed

If access controls around sensitive data are not risk-appropriate, automatically remove all rights to read or modify this information from global access groups like Everyone.

06

Minimize the risk of a data breach

Streamline regular privilege attestations

See who has access to what sensitive data and how they got that access, and enable data owners to regularly verify that these rights are in line with business needs. If they aren't, remove excessive permissions to enforce the least-privilege principle and keep risk at an acceptable level.

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, vie either group membershir or direct assignment. Reveal sensitive content that has permissions different from the parent folder.

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

Categories: GDPR, PCI DSS

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\Europe (Permissions: Different from parent)

Categories: GDPR

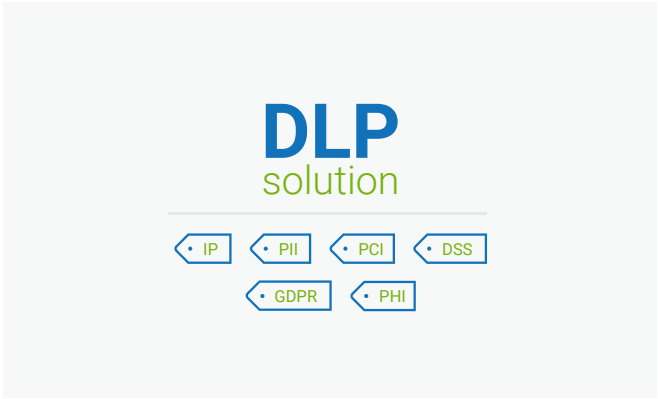
Account	Permissions	Means Granted
ENTERPRISE\M.Smith	Full Control	Group
ENTERPRISE\A.Gold	Full Control	Group

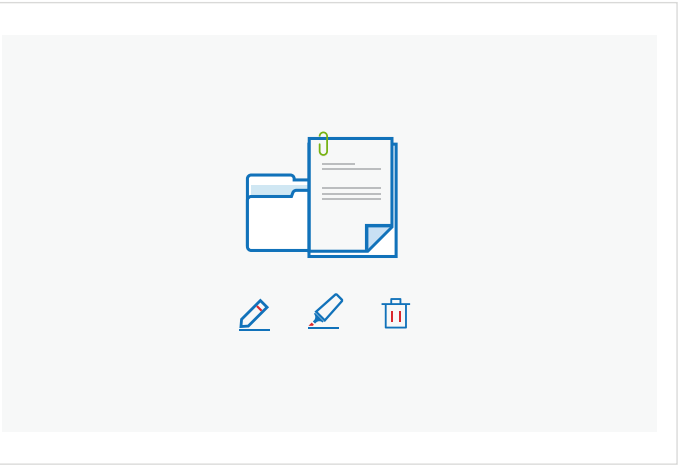
07

Minimize the risk of a data breach

Increase the precision of your DLP solution

Non-sensitive items tagged by mistake do not require protection. Optimize your data security efforts by increasing the accuracy of your data loss prevention (DLP) tool using the high-precision classification tags written by Netwrix Auditor.





Redact sensitive information based on corporate policy

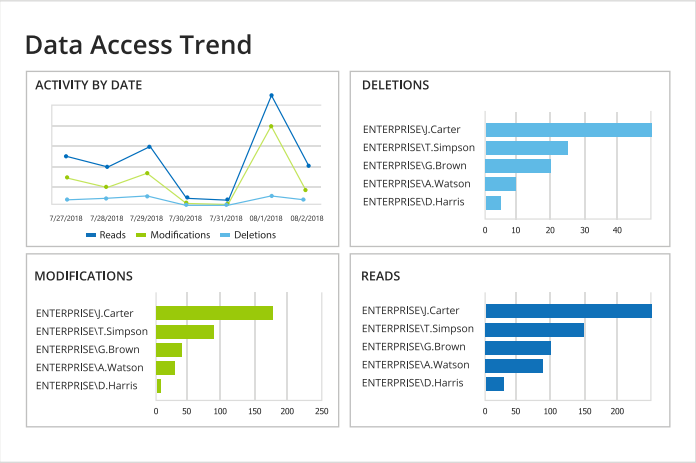
Reduce the risk of exposure of confidential information by automatically redacting sensitive content from documents if there's no business requirement for it to be there. Maintain productivity by keeping the rest of the document intact.

08

Promptly detect data security threats

Establish strict accountability over the use of privileged accounts

Continuously monitor the activity of privileged users across all systems to ensure that they follow internal policies and don't abuse their privileges to access, modify or delete sensitive data without being caught.



Administrative Group Membership Changes

Shows changes to membership of the Domain Admins, Enterprise Admins, Schema Admins, Account Operators, and other administrative groups.

Group name: \ENTERPRISE\Users\Domain Admins

Action	Member	Who	When
Added Where:	\ENTERPRISE\Users\Jack Falcon dc1.enterprise.com	ENTERPRISE\ R.Ferrano	9/17/2018 6:57:32 PM

Group name: \ENTERPRISE\Users\Domain Admins

Action	Member	Who	When
Added Where:	\ENTERPRISE\Users\Liza Lee dc1.enterprise.com	ENTERPRISE\ P.Jackson	9/16/2018 7:07:18 PM

Stay on top of privilege escalation

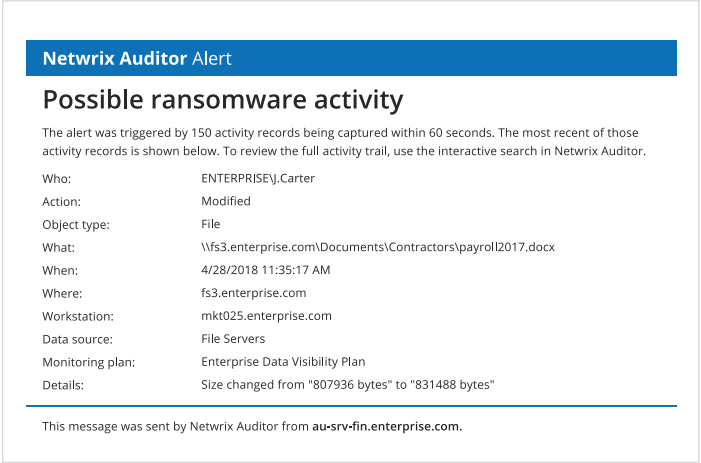
Detect any changes to access rights or group membership so you can assess whether any permissions to sensitive data have been modified without a legitimate reason. Quickly revert any improper changes to reduce risk.

09

Promptly detect data security threats

Detect ransomware attacks in progress

Get alerted about signs of possible ransomware activity, such as a large number of file modifications in a very short period of time. Quickly isolate the user account responsible to stop the ransomware from encrypting all the files that account has access to across your network.



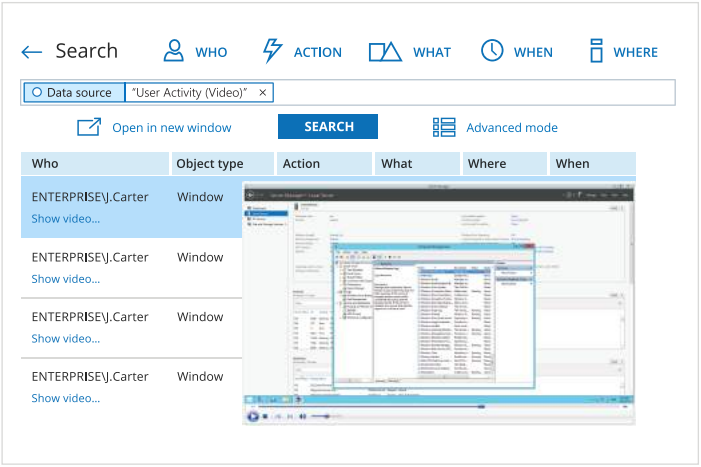
Netwrix Auditor Alert

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. To review the full activity trail, use the interactive search in Netwrix Auditor.

Who:	ENTERPRISE\J.Carter
Action:	Modified
Object type:	File
What:	\\fs3.enterprise.com\Documents\Contractors\payroll2017.docx
When:	4/28/2018 11:35:17 AM
Where:	fs3.enterprise.com
Workstation:	mkt025.enterprise.com
Data source:	File Servers
Monitoring plan:	Enterprise Data Visibility Plan
Details:	Size changed from "807936 bytes" to "831488 bytes"

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



Keep third-party activity under close scrutiny

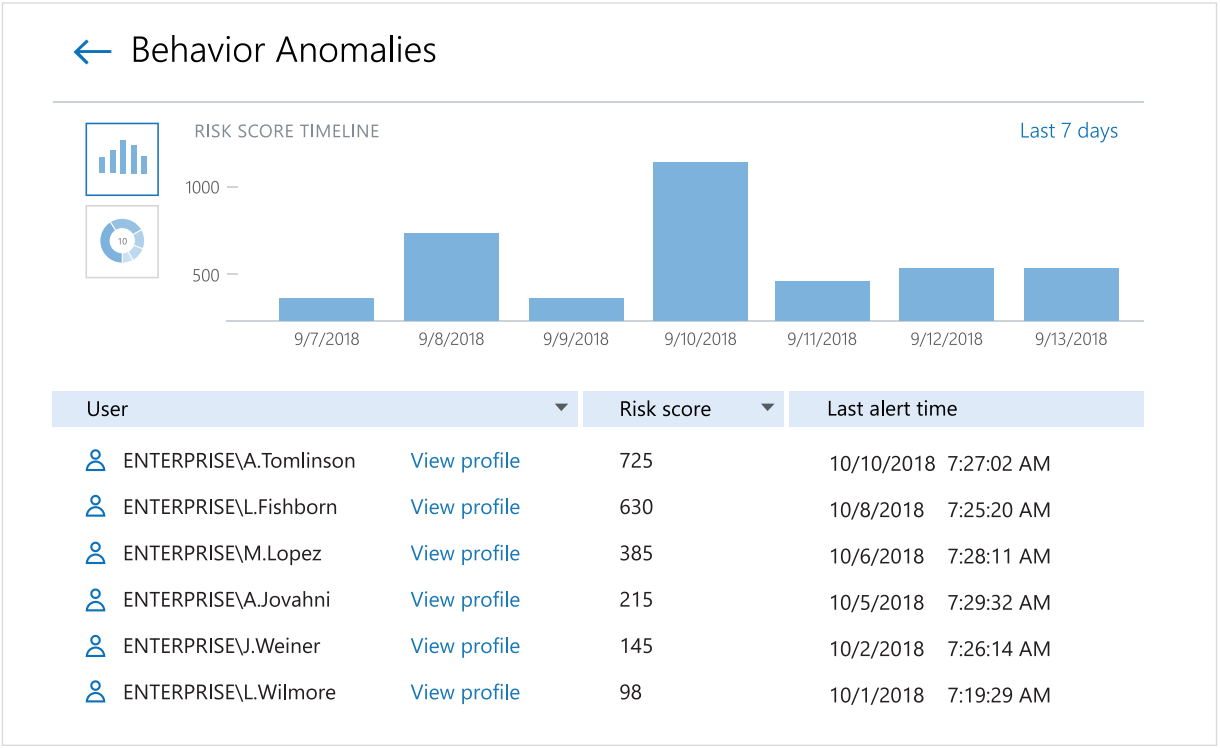
Carefully monitor the activity of third-party user accounts in any system or application, even if it doesn't produce any logs, to ensure full accountability. Get notified any time a vendor does something outside of their scope of activity, since their unauthorized actions could put your data at risk.

10

Promptly detect data security threats

Detect compromised accounts and malicious insiders

Promptly detect even subtle signs of possible data security threats in progress, such as unusual logons or users accessing sensitive data they haven't accessed before. Easily identify and investigate the users who pose the most risk with an aggregated view of the anomalous activity by each individual.

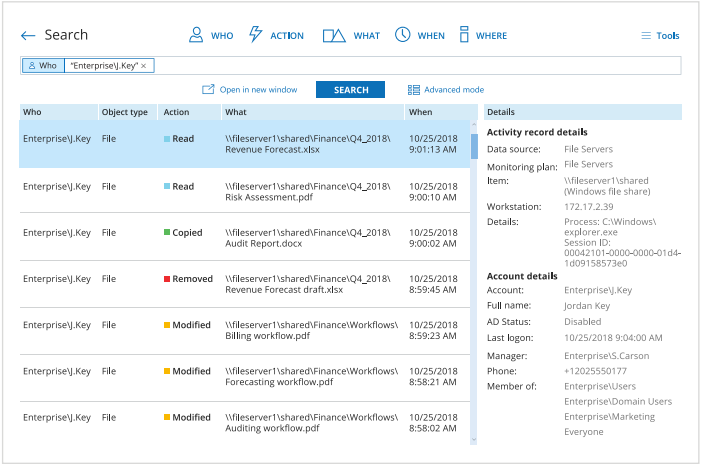


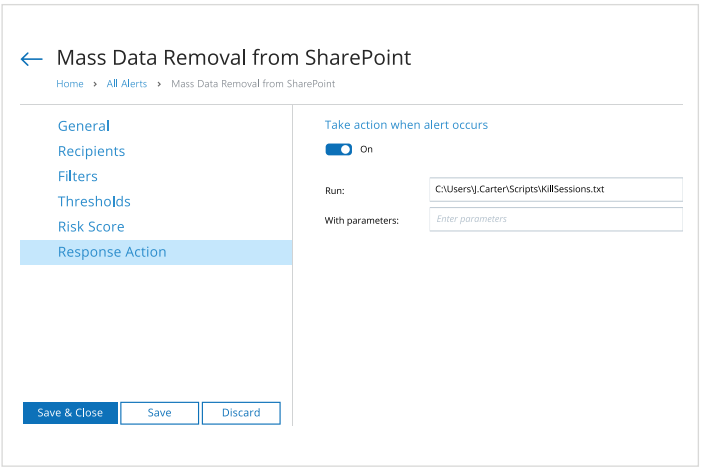
11

Make faster and more informed incident response decisions

Streamline incident investigation

Quickly get to the bottom of incidents involving sensitive data: Understand exactly what happened, how it happened, who was behind it and which pieces of information were affected. Use this context to formulate the best possible response to the incident.





Reduce the mean time to respond

React to data security threats faster by automating response to anticipated incidents. Provide initial incident support and enable faster, more accurate investigations by integrating Netwrix Auditor into your SecOps process.

12

Make faster and more informed incident response decisions

Determine and report the severity of a data breach

Analyze how much data a malicious insider or a compromised account had access to and exactly which pieces of data were actually viewed, modified or deleted. Use this information to determine whether you need to report the incident and, if necessary, to notify all affected parties and take other appropriate steps.

Activity Related to Sensitive Files and Folders

Shows all access attempts (failed and successful changes, and successful and failed read attempts) to files and folders that contain certain categories of sensitive data.

Action	Object type	What	Who	When
Read (Failed Attempt) Where: Workstation: Categories:	Folder fs1 192.168.77.25 PCI DSS	\\fs1\Accounting\Payroll	ENTERPRISE\M.Smith	3/12/2018 9:25:49 AM
Read Where: Workstation: Categories:	Folder fs1 192.168.77.25 PCI DSS	\\fs1\Accounting\Payroll	ENTERPRISE\M.Smith	3/12/2018 9:25:55 AM

13

Facilitate the recovery of key data and learn from past incidents

Understand the value and sensitivity of data to plan information recovery processes

Inventory your data and see where the most sensitive or valuable data is located. Create information recovery plans that prioritize the restoration of that data.

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

Activity Related to Sensitive Files and Folders

Shows all access attempts (failed and successful changes, and successful and failed read attempts) to files and folders that contain certain categories of sensitive data.

Action	Object type	What	Who	When
Removed	File	\\fs1\Finance\Revenue2018.xlsx	ENTERPRISE\ T.Simpson	12/22/2018 4:30:33 PM
Where: fs1 Workstation: 192.169.55.34 Categories: PCI DSS Date created: "1/24/2018 10:11:42 AM"				
Removed	File	\\fs1\Finance\Revenue2017.xlsx	ENTERPRISE\ T.Simpson	12/22/2018 4:35:47 PM
Where: fs1 Workstation: 192.169.55.34 Categories: PCI DSS Date created: "1/23/2017 11:34:54 AM"				

Get back up and running faster by prioritizing the recovery of key data

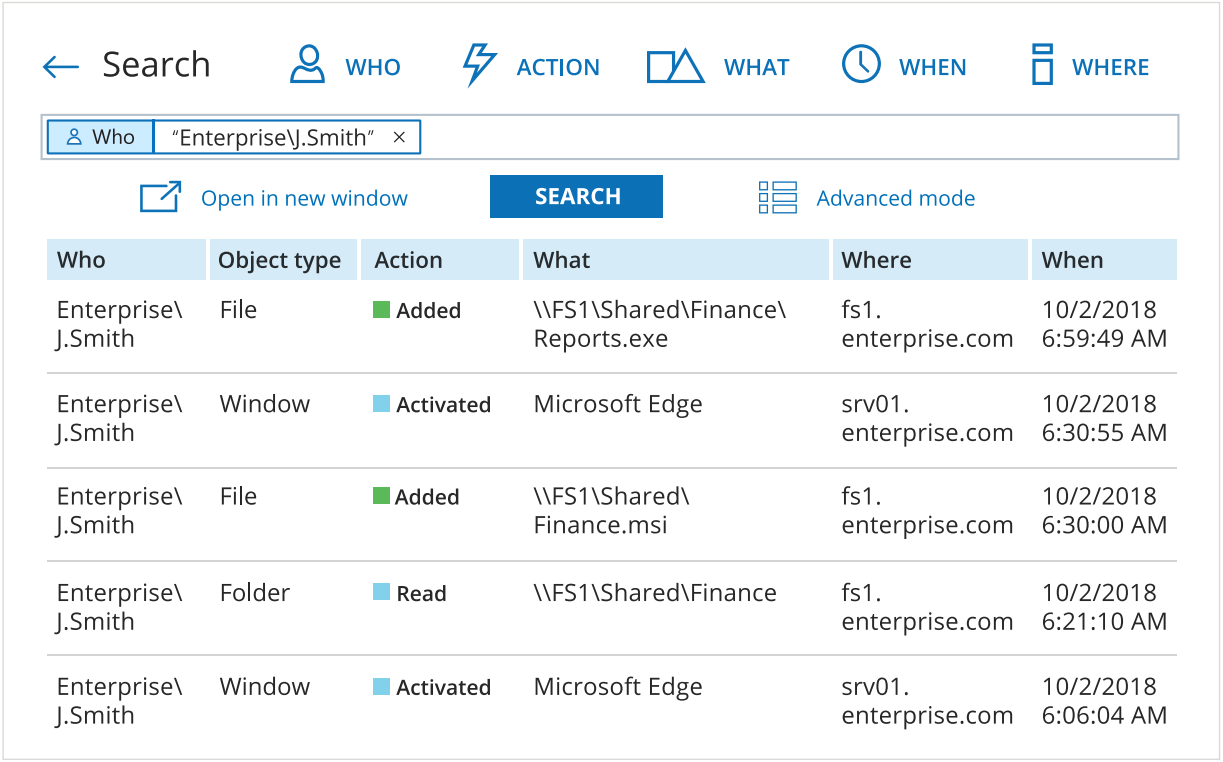
Determine which sensitive, confidential or mission-critical data was corrupted during an attack and prioritize its recovery. See who had what access to those documents to get your business users back up and running as soon as possible.

14

Facilitate the recovery of key data and learn from past incidents

Incorporate lessons learned into your data security strategy

Analyze exactly how a security incident occurred and use this information to improve your data security strategy and prevent similar incidents in the future.



Who	Object type	Action	What	Where	When
Enterprise\ J.Smith	File	Added	\\FS1\Shared\Finance\ Reports.exe	fs1. enterprise.com	10/2/2018 6:59:49 AM
Enterprise\ J.Smith	Window	Activated	Microsoft Edge	srv01. enterprise.com	10/2/2018 6:30:55 AM
Enterprise\ J.Smith	File	Added	\\FS1\Shared\ Finance.msi	fs1. enterprise.com	10/2/2018 6:30:00 AM
Enterprise\ J.Smith	Folder	Read	\\FS1\Shared\Finance	fs1. enterprise.com	10/2/2018 6:21:10 AM
Enterprise\ J.Smith	Window	Activated	Microsoft Edge	srv01. enterprise.com	10/2/2018 6:06:04 AM

15

Achieve and prove regulatory compliance

Assess the effectiveness of data security controls

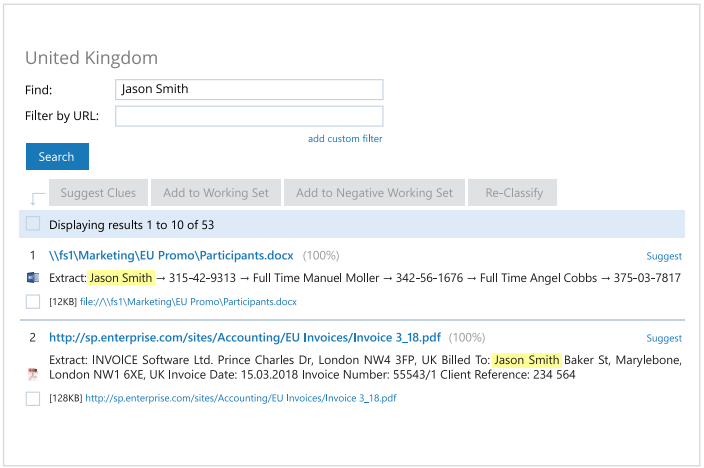
Implement compliance controls across your entire infrastructure and regularly assess whether they work as intended. If written security policies differ from what's actually in place, you can fix your faulty data security controls before auditors discover them.

Account Permissions

Shows accounts with permissions granted on files and folders (either directly or via group membership). Use this report to see who has access to files and folders and ensure these settings comply with your policies.

Group name: Everyone

Object Path	Permissions	Means Granted
\\pdc\shared\Accounting	Read (Execute, List folder content)	Directly
\\pdc\shared\Customer Data	Full Control	Directly
\\pdc\shared\Orders	Read (Execute, List folder content)	Directly
\\pdc\shared\Finance	Read (Execute, List folder content)	Directly
\\pdc\shared\Internal	Full Control	Directly
\\pdc\shared\Sales	Full Control	Directly



Comply with access requests

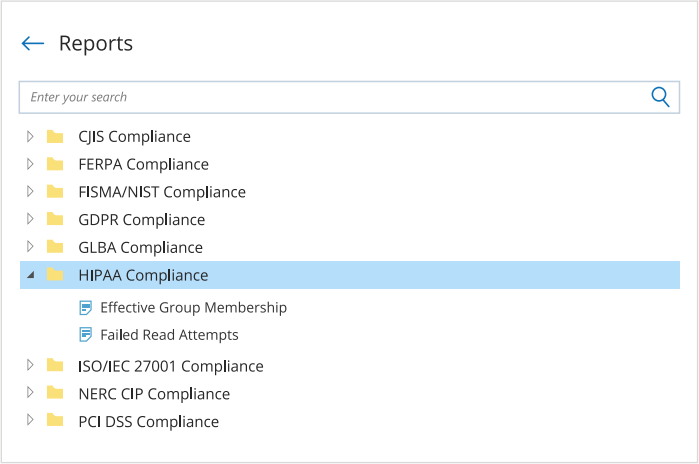
Easily find all data you store about a particular data subject when they exercise their privacy rights under GDPR, CCPA and other modern regulations. Provide them with a list of this information or erase it completely if they withdraw their consent.

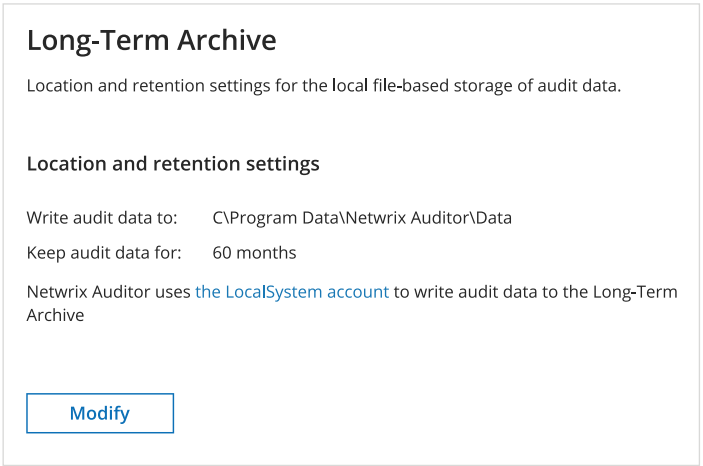
16

Achieve and prove regulatory compliance

Slash time spent on compliance preparation and audits

Prepare for the bulk of auditors' requests by taking advantage of out-of-the-box reports aligned to the compliance controls of HIPAA/HITECH, PCI DSS, GDPR and other common regulations.





Store and access your audit trail for years

Keep your audit trail archived in a compressed format for more than 10 years, as required by many regulations, while ensuring that all audit data can easily be accessed by authorized users at any time.

17
Applications

Netwrix Auditor Applications

Netwrix Auditor platform includes a broad range of applications that provide a single-pane-of-glass-view of what's going on across **both data storages** and **backbone IT systems**. This insight enables organizations to understand where sensitive data is located, what the risks around it are and what activity is threatening its security.

Infrastructure

- Netwrix Auditor for Active Directory
- Netwrix Auditor for Network Devices
- Netwrix Auditor for Windows Server
- Netwrix Auditor for VMware

Unstructured Data

- Netwrix Auditor for Windows File Servers
- Netwrix Auditor for SharePoint
- Netwrix Auditor for EMC
- Netwrix Auditor for NetApp
- Netwrix Auditor for Exchange

Structured Data

- Netwrix Auditor for SQL Server
- Netwrix Auditor for Oracle Database

Cloud

- Netwrix Auditor for Office 365
- Netwrix Auditor for Azure AD

Deployment Options

On-premises, virtual or cloud — deploy Netwrix Auditor wherever you need it

On-premises

Fully supported on **Microsoft Windows Server**

Virtual

Available in appliances for **VMware and Microsoft Hyper-V**

Cloud

Fully supported and tested in **Microsoft Azure**

Fully supported in **AWS Marketplace**

Windows Server

Microsoft Hyper-V

Microsoft Azure

vmware READY

awsmarketplace

RESTful API — endless integration capabilities for improved data security and streamlined reporting

Centralize auditing and reporting

Netwrix Auditor collects activity trails from any on-premises or cloud applications and stores them in a secure central repository, ready for historic reviews and compliance inquiries.

Get the most from your SIEM investment

By feeding granular audit data into your HP Arcsight, Splunk, IBM QRadar or other SIEM solutions, Netwrix Auditor increase the signal-to-noise ratio and maximizes SIEM value.

Automate IT workflows

Netwrix Auditor integrates with other IT security, compliance and data management tools, thereby automating and improving IT workflows and SecOps processes.

Visit the Netwrix Auditor Add-on Store at **www.netwrix.com/go/add-ons** to find free add-ons built to integrate Netwrix Auditor with your IT ecosystem.

Built for IT environments of all sizes, Netwrix Auditor architecture supports the growth of your organization

Horizon
Making Life Better!

Nonprofit, 150 employees

Horizon Leisure Centres accelerates data classification to ensure the security of sensitive data and comply with GDPR.

WILLIAM WOODS UNIVERSITY

Education, 1K employees

William Woods University uses Netwrix Auditor to reduce risk of data exposure and improve security posture.

JOHNSON COUNTY KANSAS

Government, 3,8K employees

Johnson County in Kansas streamlines detection and investigation of suspicious events with Netwrix Auditor.

PIKE CONSTRUCTION

Energy, 5,8K employees

Pike Electric troubleshoots security issues faster and ensures business continuity using Netwrix Auditor.

netwrix

Next Steps

Free Trial: setup in your own test environment

- On-premises: **netwrix.com/freetrial**
- Virtual: **netwrix.com/go/appliance**
- Cloud: **netwrix.com/go/cloud**

In-Browser Demo: interactive product demo in your browser **netwrix.com/browser_demo**

Live Demo: product tour with Netwrix expert **netwrix.com/livedemo**

Contact Sales to obtain more information **netwrix.com/contactsales**

Awards

Corporate Headquarters:

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

Phone: 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023 **marketing@exaprobe.com**