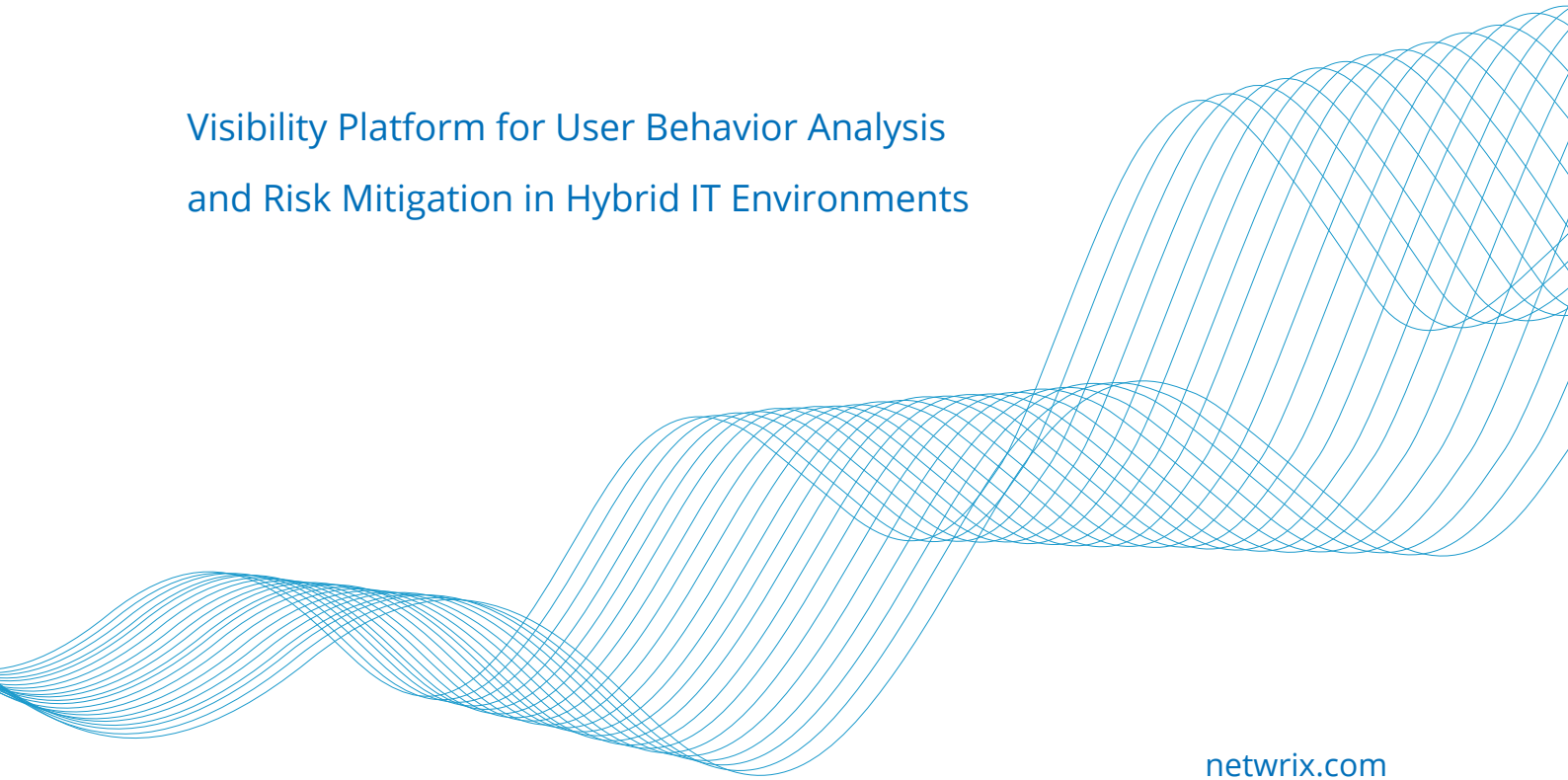
netwrix

Netwrix Auditor

Visibility Platform for User Behavior Analysis
and Risk Mitigation in Hybrid IT Environments

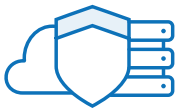


netwrix.com

01
Product Overview

Netwrix Auditor Platform

Netwrix Auditor is a **visibility platform for user behavior analysis and risk mitigation** that enables control over changes, configurations and access in hybrid IT environments **to protect data regardless of its location.** The platform provides security intelligence to **identify security holes, detect anomalies in user behavior** and **investigate threat patterns** in time to prevent real damage.



Detect data security threats, both on premises and in the cloud.

Pass compliance audits with less effort and expense.

Increase the productivity of IT security and operations teams.

02
Applications

Netwrix Auditor Applications

Netwrix Auditor includes applications for Active Directory, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware and Windows Server. Empowered with the **RESTful API** and **user activity video recording,** the platform delivers **visibility and control** across all of your on-premises or cloud-based IT systems in a unified way.

Netwrix Auditor for **Active Directory**	Netwrix Auditor for **Azure AD**	Netwrix Auditor for **Exchange**	Netwrix Auditor for **Office 365**
Netwrix Auditor for **Windows File Servers**	Netwrix Auditor for **EMC**	Netwrix Auditor for **NetApp**	Netwrix Auditor for **SharePoint**
Netwrix Auditor for **Oracle Database**	Netwrix Auditor for **SQL Server**	Netwrix Auditor for **Windows Server**	Netwrix Auditor for **VMware**

03
Benefits

Detect data security threats, both on premises and in the cloud

Netwrix Auditor bridges the visibility gap by delivering security intelligence about critical changes, data access and configurations in hybrid IT environments. Organizations can use this data to continuously assess and proactively mitigate security risks. The platform identifies users with the most anomalous activity over time, and alerts on behavior patterns that indicate a possible insider threat or account takeover. And it makes it easy to investigate any suspicious action or security policy violation so you can quickly determine the best response.

Pass compliance audits with less effort and expense

Netwrix Auditor provides the evidence required to prove that your organization's IT security program adheres to PCI DSS, HIPAA/HITECH, SOX, GLBA, FISMA/NIST800-53, FERPA, CJIS, NERC CIP, ISO/IEC 27001, GDPR and other standards. It also ensures easy access to your complete audit trail for more than 10 years.

Increase the productivity of IT security and operations teams

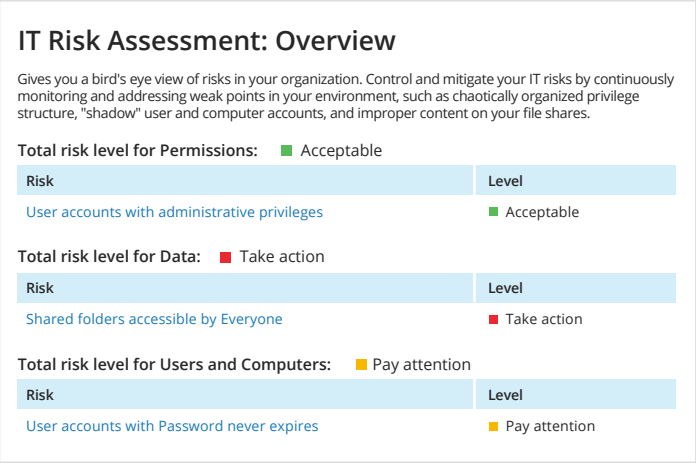
With Netwrix Auditor, there's no need to crawl through weeks of log data to answer questions about who changed what or when and where a change was made. Nor do you need to painstakingly write, maintain and run PowerShell scripts to identify inactive users, report on effective user permissions or perform software inventory tasks. The platform delivers actionable audit data to anyone in your organization who needs it.

04

In Action: Detect Data Security Threats

Continuously assess and mitigate data security risks

Identify high-risk configurations, such as excessive access permissions for the “Everyone” group or an abundance of directly assigned permissions, that need your immediate attention. Adjust your policy settings or permissions as necessary to minimize the ability of intruders and insiders to cause damage.



IT Risk Assessment: Overview

Gives you a bird's eye view of risks in your organization. Control and mitigate your IT risks by continuously monitoring and addressing weak points in your environment, such as chaotically organized privilege structure, "shadow" user and computer accounts, and improper content on your file shares.

Total risk level for Permissions: Acceptable

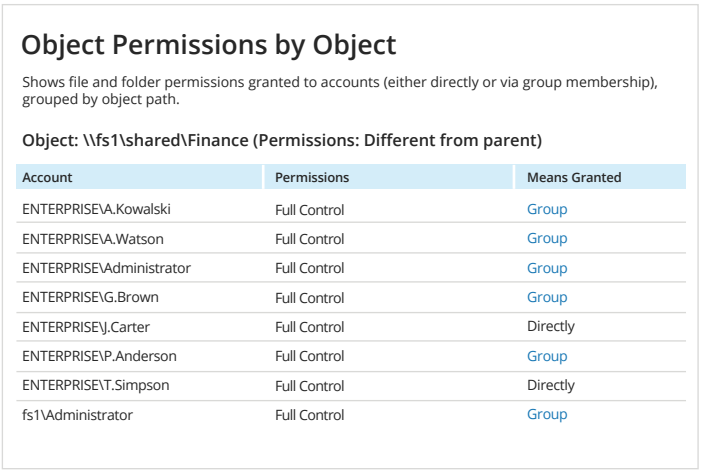
Risk	Level
User accounts with administrative privileges	Acceptable

Total risk level for Data: Take action

Risk	Level
Shared folders accessible by Everyone	Take action

Total risk level for Users and Computers: Pay attention

Risk	Level
User accounts with Password never expires	Pay attention



Object Permissions by Object

Shows file and folder permissions granted to accounts (either directly or via group membership), grouped by object path.

Object: \\fs1\shared\Finance (Permissions: Different from parent)

Account	Permissions	Means Granted
ENTERPRISE\A.Kowalski	Full Control	Group
ENTERPRISE\A.Watson	Full Control	Group
ENTERPRISE\Administrator	Full Control	Group
ENTERPRISE\G.Brown	Full Control	Group
ENTERPRISE\J.Carter	Full Control	Directly
ENTERPRISE\P.Anderson	Full Control	Group
ENTERPRISE\T.Simpson	Full Control	Directly
fs1\Administrator	Full Control	Group

Prevent privilege abuse and data breaches

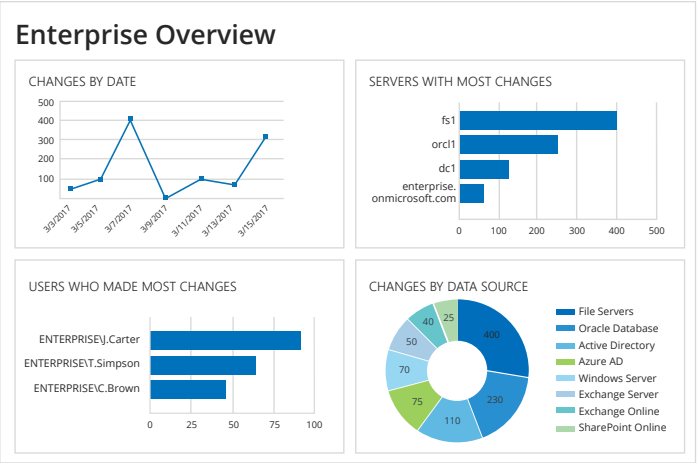
Get a complete picture of effective user permissions in Active Directory and file servers. Lock down overexposed data and make sure that only eligible employees have access to critical resources. Stay aware of any modifications that affect user privileges so you can respond immediately.

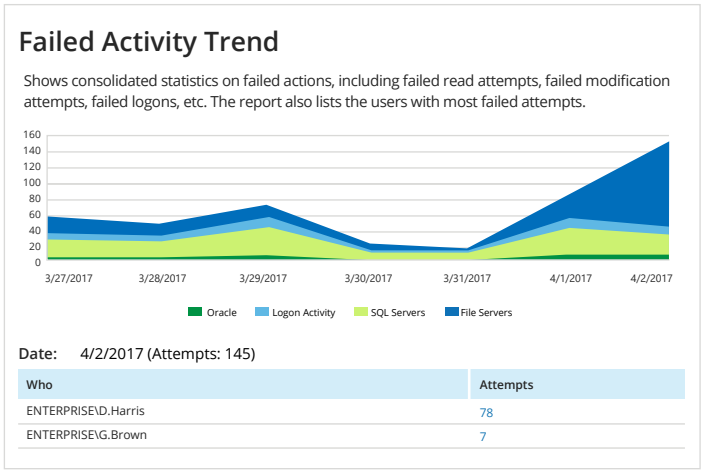
05

In Action: Detect Data Security Threats

Gain a bird's-eye view of activity across your IT environment

Get a high-level view of what's going on in your hybrid IT infrastructure with enterprise overview dashboards. Spot surges in anomalous activity, see which users are most active and determine which systems are most affected.





Spot abnormal user behavior that would otherwise go unnoticed

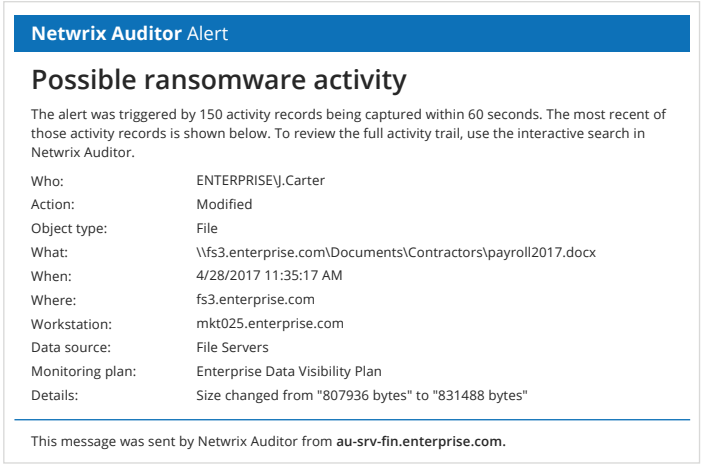
Quickly identify subtle signs of possible threats, such as unusual logons that might indicate user identity theft or a disgruntled privileged user trying to hide his or her activity behind temporary accounts. With the user behavior and blind spot analysis reports, no malicious activity can slip under your radar.

06

In Action: Detect Data Security Threats

Receive alerts on threat patterns

Be alerted about unauthorized activity as it happens so you can prevent security breaches. For example, you can choose to be notified whenever someone has been added to the Enterprise Admins group or a user has modified many files in a short period of time, which could indicate a ransomware attack.



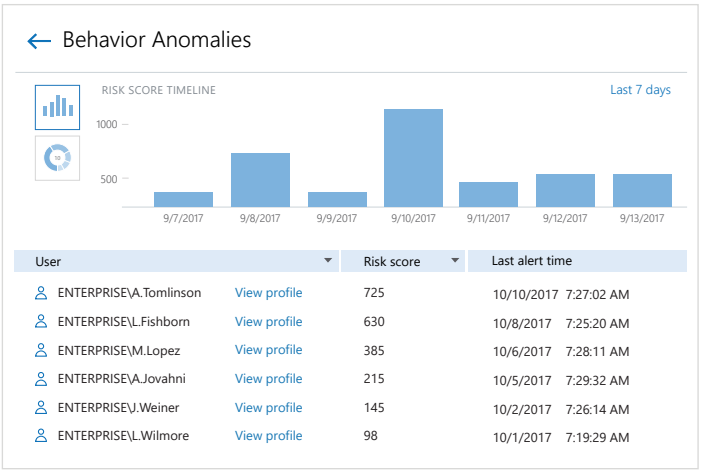
Netwrix Auditor Alert

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:	4/28/2017 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.**



Identify high-risk user accounts

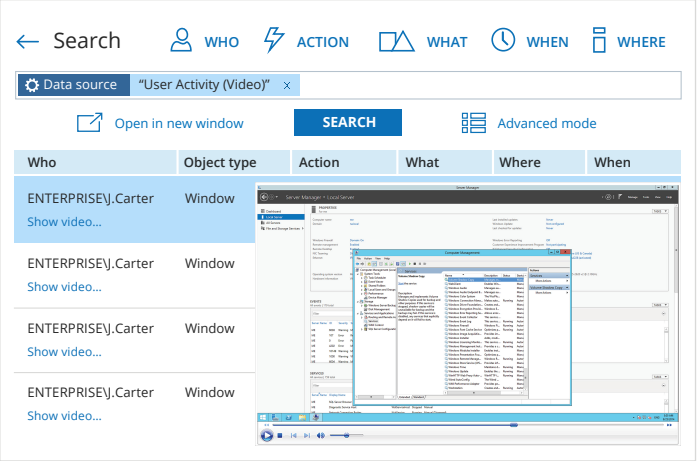
Improve the detection of rogue insiders and accounts compromised by external attackers with a single aggregated view of anomalous activity by each individual. Use the associated risk scores to prioritize incidents so you can investigate and determine the best response.

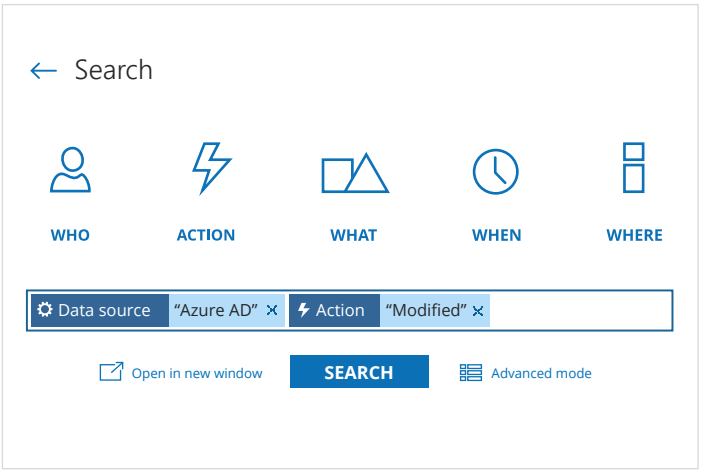
07

In Action: Detect Data Security Threats

Detect the undetectable

Gain visibility into any system or application, even if it doesn't produce any logs, by video recording a user's screen activity. You can search and replay the recordings to determine exactly what actions were performed.





Investigate anomalies in user behavior

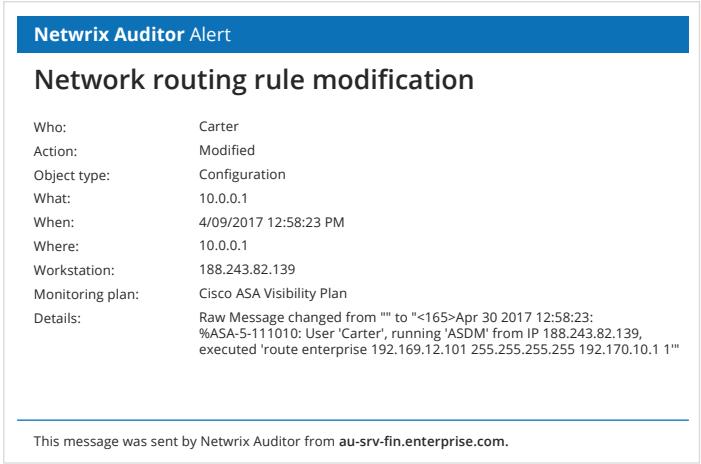
Whenever you detect user activity that violates your corporate security policy, use our interactive Google-like search to investigate how it happened so you can prevent similar incidents from occurring in the future.

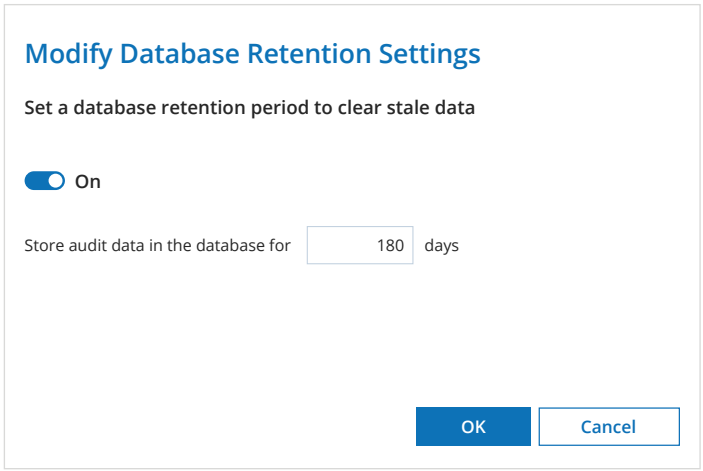
08

In Action: Detect Data Security Threats

Centralize IT security monitoring with API-enabled integrations

Centralize security monitoring and reporting by feeding Netwrix Auditor data from other on-premises or cloud applications. You can also use the actionable security intelligence from Netwrix Auditor to augment the output data of your SIEM solution.





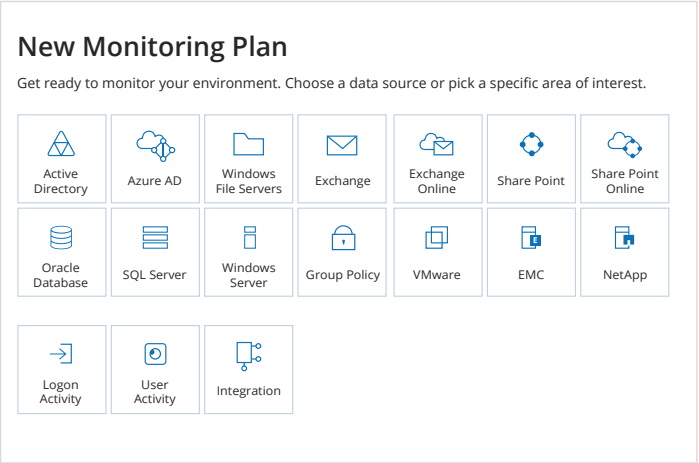
Archive security analytics data for years

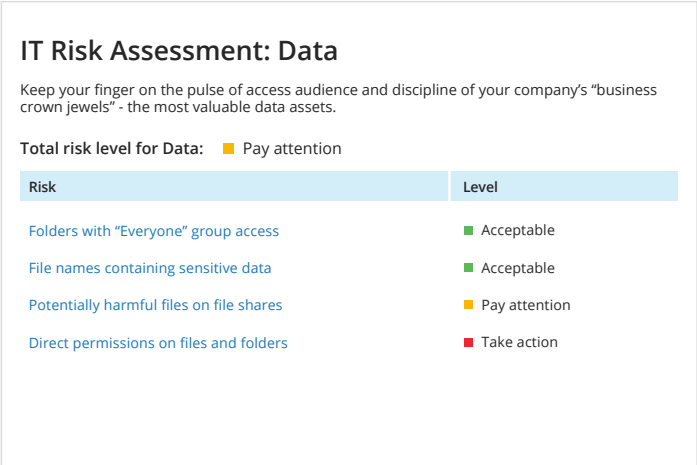
The two-tiered (file-based + SQL database) AuditArchive™ storage enables you to keep your big data archived for historic e-discovery or security investigations for more than 10 years.

09
In Action: Pass Compliance Audits

Enable control over security policies

By supporting the broadest variety of IT systems, Netwrix Auditor helps you implement compliance controls across your entire infrastructure. It serves as a single point of access to the audit trail and enables you to easily provide proof that your security policies are enforced.





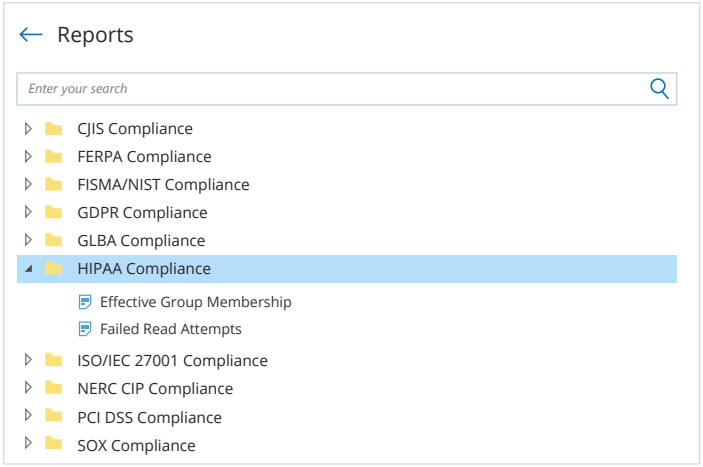
Demonstrate a proactive approach to risk mitigation

Visualize your security posture and impress auditors with interactive risk assessment dashboards. Use them to prove your ability to continuously evaluate and reduce risks to protected data.

10
In Action: Pass Compliance Audits

Take advantage of out-of-the-box compliance reports

Slash preparation time for audits and prove your compliance using out-of-the-box reports aligned with the compliance controls of FISMA, GDPR, HIPAA/HITECH, PCI DSS, SOX and many other common regulations.



Members of Local Administrators Group

Shows Windows servers, with members of the local Administrators group for each server. You can apply baseline filter to highlight servers with security issues, e.g., those where the Administrators group include users not in your baseline list. Use this report to prevent rights elevation and exercise security control over your organization.

Server	Members	Status
fs1.enterprise.com	Administrator, fs1local, ENTERPRISE\Domain Admins	Issues Detected
sql01.enterprise.com	Administrator, J.Carter, ENTERPRISE\Domain Admins	Issues Detected
srv01.enterprise.com	Administrator, T.Simpson, ENTERPRISE\Domain Admins	Issues Detected
srv02.enterprise.com	Administrator, ENTERPRISE\Domain Admins	OK
srv03.enterprise.com	Administrator, ENTERPRISE\Domain Admins	OK
srv04.enterprise.com	Administrator, ENTERPRISE\Domain Admins	OK

Prove that compliance controls are — and have always been — in place

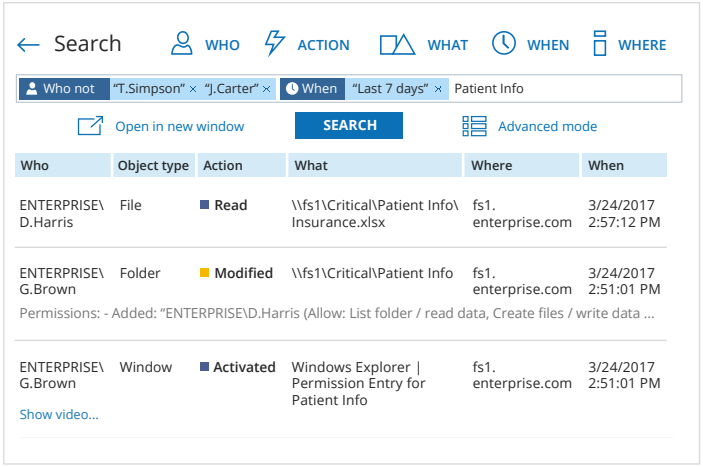
Demonstrate to auditors that group membership, effective user permissions and other configurations in your environment have always been in line with security policies. Easily compare current and past configurations to prove that no unauthorized changes took place.

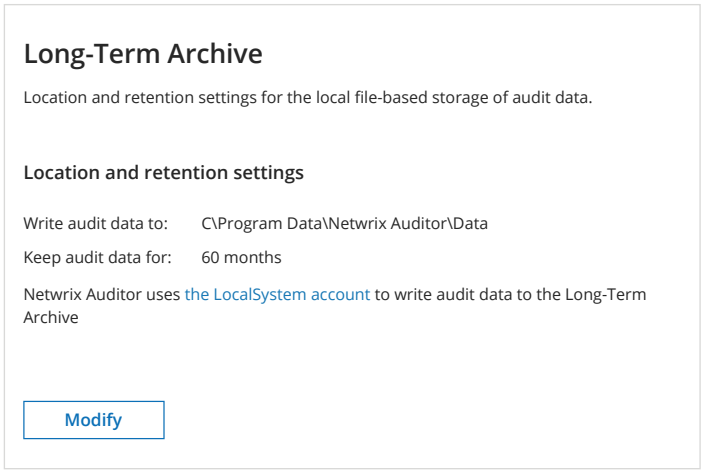
11

In Action: Pass Compliance Audits

Address auditor's questions faster

Quickly provide answers to unexpected questions from auditors, such as who accessed a particular sensitive file, or how access rights to a protected folder were modified during the past year and who made those changes. With Netwrix Auditor, what used to take weeks now takes minutes.





Store and access your audit trail for years

Many compliance regulations require organizations to retain their audit trails for extended periods. Netwrix Auditor enables you to keep your audit trail archived in a compressed format for more than 10 years, while ensuring that all audit data can easily be accessed by authorized users at any time.

12

In Action: Increase the Productivity of IT Teams

Keep tabs on what's happening in your environment

Monitor all changes across your on-premises and cloud-based IT systems. See when a specific change was made, who made it, and what was changed, with the before and after values. Use this information to verify the purpose of each change and revert unwanted modifications before they turn into a problem.

All Group Policy Changes

Shows all changes to Group Policy objects, settings, links, and permissions, with the name of the originating workstation.

Action	What	Who	When
Modified	Security Policy	ENTERPRISE\J.Smith	3/23/2017 7:55:11 AM
Where:	dc1.enterprise.com		
Workstation:	172.17.35.12		
Path:	Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/ Account Policies/Password Policy		
Modified	Policy: Enforce password history; Setting: 24 passwords remembered -> 3 passwords remembered;		
Modified	Modified Policy: Maximum password age; Setting: 20 days -> 200 days;		
Modified	Modified Policy: Minimum password length; Setting: 7 characters-> 4 characters;		

Account Permissions in Active Directory

Shows Active Directory objects that the security principal has explicit or inherited permissions on (either granted directly or through group membership). Use this report to see who has permissions to what in your Active Directory domain and prevent rights elevation. The permissions are reported only for users that belong to the monitored domain.

Account: \com\enterprise\Users\John Carter

Object Name	Object Type	Means Granted
\com\enterprise\Computers	container	Directly
\com\enterprise	domainDNS	Group
\com\enterprise\Builtin	builtinDomain	Group
\com\enterprise\Builtin\Account Operators	group	Group
\com\enterprise\Builtin\Administrators	group	Group
\com\enterprise\Builtin\Backup Operators	group	Group

Maintain good IT hygiene

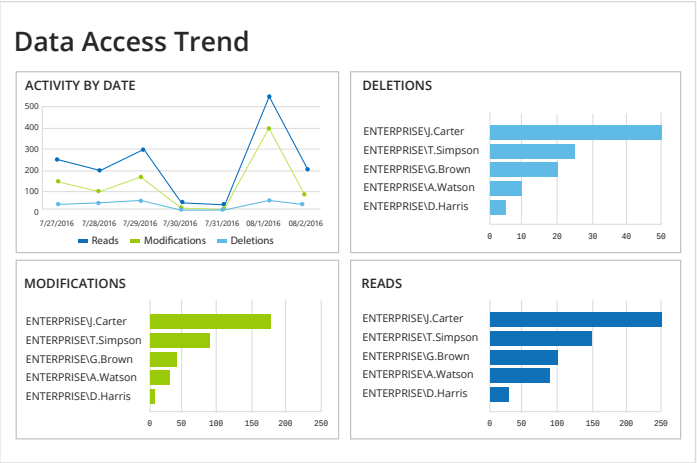
Create a cleaner and more manageable environment using Netwrix Auditor's state-in-time reports. Regularly review your identity and access configurations, and easily verify that they match a known good state.

13

In Action: Increase the Productivity of IT Teams

Simplify reporting routines

Netwrix Auditor supplies more than 200 predefined reports and dashboards that are easy to narrow down using built-in filtering, grouping and sorting. You can also easily address any specific security and compliance concerns by building custom reports using the Interactive Search feature.



Speed report delivery

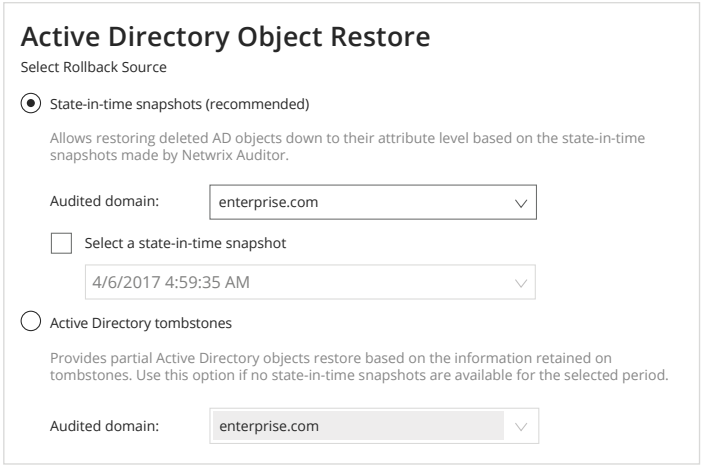
Netwrix Auditor can automatically generate reports on the schedule you specify and either email them to stakeholders or save them in a dedicated file share for easy reference. Alternatively, you can give stakeholders access to Netwrix Auditor so they can generate the reports they need on demand.

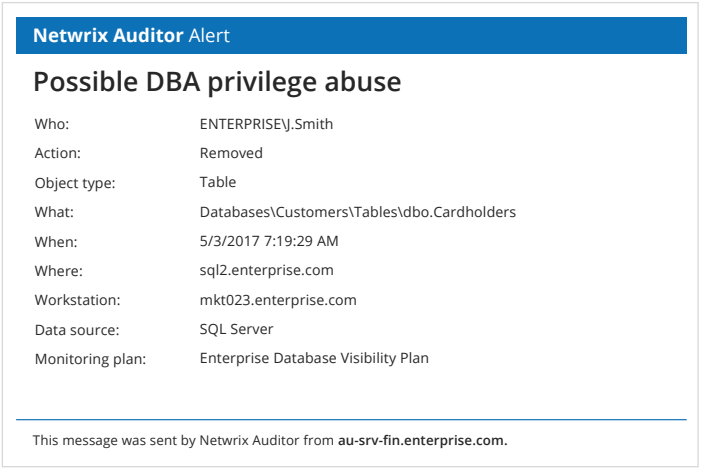
14

In Action: Increase the Productivity of IT Teams

Minimize system downtime

If an unauthorized or inappropriate change is made to your environment, you can quickly turn back the clock by reverting the settings to a previous state — without any downtime or having to restore from backup.





Focus on what's really important

Regularly run risk assessments to pinpoint the areas that need your immediate attention. Use alerts to stay aware of actions you consider critical, such as the deletion of business-critical files or changes to your SQL Server configuration.

Addressing the Security and Compliance Challenges of Your Department and Your Business

CIO/IT Director

Keep your IT environment clean, manageable and secure.

CISO

Prevent data breaches and minimize compliance costs.

IT Manager

Take back control over your IT infrastructure and eliminate the stress of your next compliance audit.

Security Analyst

Identify security gaps and investigate suspicious user activity in time to prevent real damage.

System Administrator

Generate and deliver security and compliance reports faster.

MSP

Increase revenue by enabling transparency of managed environments and offering compliance as a service.

Deployment Options

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

On-premises

Fully supported on **Microsoft's Windows Server** Platform

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

#completevisibility

RESTful API — endless integration capabilities for improved visibility and streamlined reporting

Centralize auditing and reporting

Netwrix Auditor collects activity trails from any existing on-premises or cloud applications and stores in a secure central repository, ready for search and reporting.

Get the most from your SIEM investment

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

Automate IT workflows

You can feed audit data from Netwrix Auditor into other critical IT processes, such as change management or service desk, thereby automating and improving their workflows.

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

HERITAGE BANK

Banking and Finance, 100 employees

Heritage Bank relies on Netwrix Auditor to govern essential security and compliance policies.

DONOHOE

Construction, 1,4K employees

The Donohoe Companies deployed Netwrix Auditor to solve its data security and accountability challenges.

american career college

Education, 5,5K employees

American Career College ensures campus data security with Netwrix Auditor for Active Directory.

Maine.gov

Government, 25K employees

State of Maine meets state and federal security guidelines with 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**

Test Drive: virtual POC, try in a Netwrix-hosted test lab **netwrix.com/testdrive**

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

netwrix.com/social