

netwrix

Netwrix Auditor

Complete Visibility into Hybrid Cloud IT Environments



netwrix.com | netwrix.com/social

Netwrix Auditor Platform

Netwrix Auditor is a **visibility and governance platform that enables control** over changes, configurations and access in hybrid cloud IT environments **to protect unstructured data regardless of its location**. The platform provides **security analytics** to detect anomalies in user behavior and investigate threat patterns **before a data breach occurs**.



Detect data security threats — on premises and in the cloud.

Pass compliance audits with less effort and expense.

Increase the productivity of security and operations teams.

Netwrix Auditor Applications

Netwrix Auditor includes applications for Active Directory, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp file appliances, SharePoint, 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
Office 365



Netwrix Auditor for
NetApp



Netwrix Auditor for
EMC



Netwrix Auditor for
Active Directory



Netwrix Auditor for
File Servers



Netwrix Auditor for
Windows Server



Netwrix Auditor for
VMware



Netwrix Auditor for
Exchange



Netwrix Auditor for
SQL Server



Netwrix Auditor for
SharePoint

03

Benefits

Detect Data Security Threats – On Premises and in the Cloud

Netwrix Auditor bridges the visibility gap by delivering security analytics about critical changes, state of configurations and data access in hybrid cloud IT environments and enables investigation of suspicious user behavior. The platform also provides alerts about patterns that violate corporate security policies and indicate a possible insider threat.

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, FISMA/NIST800-53, COBIT, ISO/IEC 27001 and other standards. It also ensures easy access to compliance reports for more than 10 years.

Increase the Productivity of Security and Operations Teams

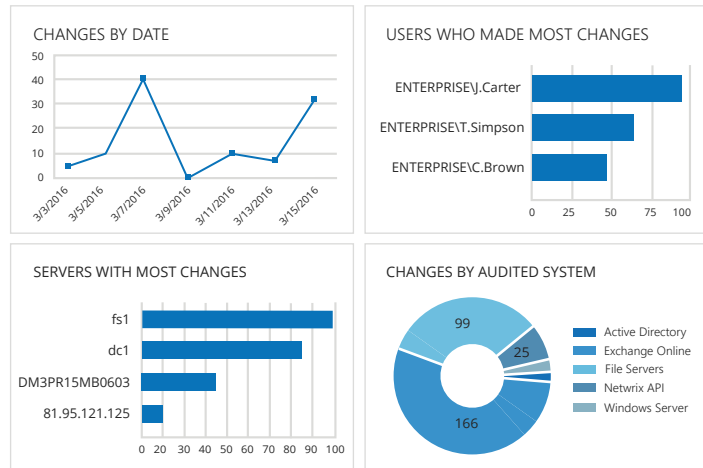
With Netwrix Auditor, there's no need to crawl through weeks of log data to answer questions about who changed what, when and where a change was made, or who has access to what. The platform delivers actionable audit data to anyone in your organization who needs it.

04

In Action: Detect Data Security Threats

Detect Suspicious Insider Activity at Early Stages

Get a high-level overview of employee activity across your IT infrastructure with Enterprise Overview dashboards. See how often changes are made, which users are performing suspicious actions, which systems are affected and more.



Search

WHO ACTION WHAT WHEN WHERE ADVANCED TOOLS

Who "John Smith" X Actions "Read" X Where "ESX01" X SEARCH

Investigate Anomalies in User Behavior

Whenever you detect a change or data access attempt that violates your corporate security policy, use our interactive Google-like search to investigate why and how it happened so you can prevent similar incidents from occurring in the future.

05

In Action: Detect Data Security Threats

Prevent Data Exfiltration

Make sure that only the eligible employees in your organization have access to critical resources by getting a complete picture of effective permissions and file activity on your file servers and NAS.

Object Permissions by Object

Shows accounts with their inherited or explicitly assigned basic permissions allowing them to access folders and subfolders, results are grouped by object path.

Folder path: \\fs1\Management\Finance

User Account	Permissions	User Permissions Inheritance
ENTERPRISE\Administrators	List folder/ read data Read attributes Read extended attributes Read permissions Change permissions	Explicit
ENTERPRISE\J.Smith	List folder/ read data Read attributes Read extended attributes Read permissions Change permissions	Inherited

Failed Read Attempts

Shows unauthorized file access attempts. This report can be used for compliance audit to show that all unauthorized data access activities are traceable and easily auditable.

Action	Object Type	What	Who	When
■ Read (Failed Attempt)	File	\\fs1\Finance\Cardholders\Overview.xlsx	ENTERPRISE\B.Green	9/26/2015 3:03:08 PM
Where:	ENTWKS0412			
■ Read (Failed Attempt)	File	\\fs1\Finance\Accounting\Statement0313.xlsx	ENTERPRISE\S.Hernandez	9/26/2015 3:05:38 PM
Where:	ENTWKS0524			
■ Read (Failed Attempt)	File	\\fs1\HR\NewHire\SalaryList.xlsx	ENTERPRISE\K.Davis	9/26/2015 3:07:23 PM
Where:	172.17.4.34			

Monitor Access to Unstructured Data

Whether your files contain cardholder data, medical records or financial statements, Netwrix Auditor will show who attempted (successfully or unsuccessfully) to access those files, and when and where the attempt occurred.

06

In Action: Detect Data Security Threats

Lock Down Overexposed Data

Spot unnecessary permissions to unstructured data so you can lock down overexposed data and mitigate the risk of privilege abuse.

Excessive Access Permissions


Shows accounts with permissions for infrequently accessed files and folders. Use this report for spotting unnecessary permissions and preventing data leaks.

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

Action	Permissions	Means Granted	Times Accessed
ENTERPRISE\Administrator	Full Control	Group	258
ENTERPRISE\B.Atkins	Read (Execute, List folder content)	Group	14280
ENTERPRISE\H.Malicious	Read (Execute, List folder content)	Group	1745
ENTERPRISE\K.Smith	Read (Execute, List folder content)	Group	10020

Object: \\fs1\shared\Finance (Permissions: Same as parent)

Action	Permissions	Means Granted	Times Accessed
ENTERPRISE\B.Atkins	Modify (Read, Write, Execute)	Group	8680
ENTERPRISE\H.Malicious	Full Control	Directly	966



Changes to Admin Group Memberships

☒ Enable

Description:

Alert on changes to the Domain Admins and Enterprise Domain Admins groups

^

v

Edit...

Alert Filters

Specify filters for the changes that must trigger alerts:

Addition to Enterprise Admins Group

Removal from Enterprise Admins Group

Addition to Domain Admins Group

Removal from Domain Admins Group

Add...

Remove

Edit...

Notifications

Recipient	Type	Format
Administrator@enterprise.com	Email	Html

Add...

Receive Alerts on Threat Patterns


Be alerted about unauthorized changes as they happen so you can prevent security breaches. For example, you can choose to be notified whenever someone is added to the Enterprise Admins group or a user has accessed too many files at a time.

07

In Action: Detect Data Security Threats

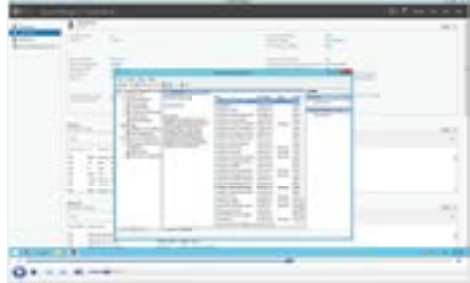
Detect the Undetectable


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.

**Activity Records**
Generate a summary of video records

Date 9/25/2014

Computer	User	Start Time	End Time	Duration
dc1.enterprise.com	ENTERPRISE\J.Smith	9/25/2015 4:12 PM	9/25/2015 4:17 PM	00:05:15
dc1.enterprise.com	ENTERPRISE\J.Smith	9/25/2015 5:12 PM	9/25/2015 5:13 PM	00:01:15



**Long Term Archive**
Location and retention settings for the local file-based storage of audit data.

Location and retention settings

Write audit data to:

C:\ProgramData\Netwrix Auditor\Data

Keep audit data for:

24 months

Modify...

Archive Security Analytics Data for Years

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

08

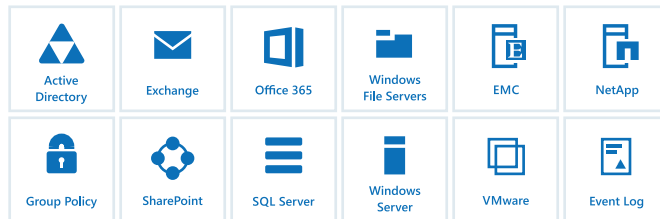
In Action: Pass Compliance Audits

Enable Control Over Security Policies

By supporting the broadest variety of on-premises and cloud-based IT systems, Netrix Auditor enables compliance controls across your entire IT infrastructure and serves as a single point of access to the audit trail.

Welcome to Netrix Auditor

Click the tile below to create a Managed Object to define the auditing scope.



Search	WHO	ACTION	WHAT	WHEN	WHERE
Audited system	"Active Directory"	Object type	"Group"	SEARCH	
Who	Object type	Action	What	Where	When
ENTERPRISE\J.Smith	Group	Modified	\\enterprise\Users\Domain Admins	dc1.enterprise.com	4/28/2015 1:05:34 PM
Security Global Group Member: -Added: "\\enterprise\Users\George Moore"					
ENTERPRISE\G.Davis	Group	Modified	\\enterprise\Users\Accountants	dc1.enterprise.com	4/29/2015 11:25:36 AM
Security Global Group Member: -Added: "\\enterprise\Users\Roy Taylor"					

Address Auditor's Questions Faster

Quickly provide answers to auditors' questions, such as what changes were made to the Enterprise Domain Admins group during the past year and who made those changes. With Netrix Auditor, what used to take weeks now takes minutes.

09

In Action: Pass Compliance Audits

Take Advantage of Out-of-the-box Compliance Reports

Auditors require proof that specific processes and controls are — and have always been — in place. Prove your compliance with out-of-the-box reports aligned with compliance controls.

The screenshot shows the 'Reports' section of the Netwrix Auditor interface. The 'COMPLIANCE' tab is selected, displaying a list of compliance reports on the left and a detailed view of a specific report on the right.

Reports List:

- FISMA Compliance
- HIPAA Compliance
- ISO/IEC 27001 Compliance
- PCI DSS v3.0
- SOX Compliance

Group name: \Enterprise\Users\Domain Users

Action	Who	What	When
Added	ENTERPRISE\J.Brown	Audit Object Access Policy	4/30/2015 2:29:11 AM

Where: dc1.enterprise.com
Workstation: 172.17.34.23

Report Details:

- User Accounts Group Membership
- User Accounts Last Logon Time
- All Group Policy Changes by Group
- Account Policy Changes
- Audit Policy Changes
- Interactive Logon Settings Changes
- Password Policy Changes
- Restricted Groups Policy Changes



AuditIntelligence

Default Audit Database settings required to take advantage of AuditIntelligence provided by the Netwrix Auditor client.

Database Retention

Modify...

Database retention enabled: Yes

Store audit data in the database for: 180 days

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 at any time.

10

In Action: Increase the Productivity of IT Teams

Keep Tabs on What's Changing in Your Environment

See when a specific change was made, who made it, and what was changed, including the values before and after the change. This detailed information is available for every change in your on-premises and cloud-based IT systems.

All Changes by User

Shows all changes across the entire IT infrastructure grouped by the users who made the changes.

Who Changed: ENTERPRISE\F.Wilson

Audited System: Active Directory

Action	Object Type	What	When
Modified	User	\enterprise\Users\Glen Williams	9/09/2015 4:31:49 PM

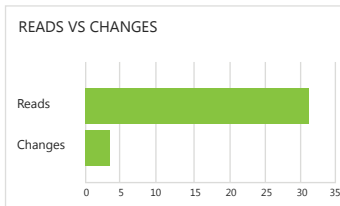
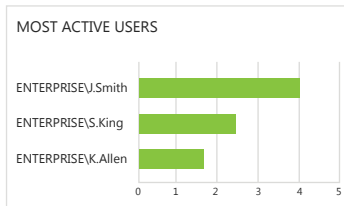
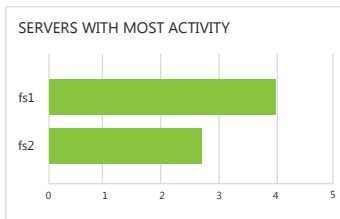
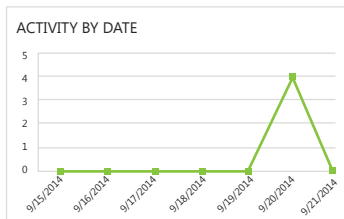
Where: ex1.enterprise.com
Principal Name set to "Glen.Williams@enterprise.com"

Audited System: VMware

Action	Object Type	What	When
Removed	VirtualMachine	\ha-folder-root\ha-datacenter\vm1	9/11/2015 3:11:41 PM

Where: https://vmhost1.enterprise.com:433

File Servers Overview



Simplify Reporting

Netwrix Auditor supplies more than 200 predefined reports and dashboards that are easy to customize using built-in filtering, grouping and sorting. You can export the data to PDF, XLS and other formats, set up email subscriptions, and much more.

11

In Action: Increase the Productivity of IT Teams

Speed Report Delivery

Jettison slow, manual reporting processes that require users to request the reports they need from IT and wait their turn in the queue. With Netwrix Auditor, stakeholders can subscribe to scheduled reports or use Netwrix Auditor client to create reports on demand.



Active Directory Object Restore

Select Rollback Source

☒ Restore from state-in-time snapshots

This option allows restoring deleted AD objects down to their attribute level based on the state-in-time snapshots made by Netwrix Auditor.

Monitored domain:

☐ Select a state-in-time snapshot

☐ Restore from AD tombstones

This option provides partial AD objects restore based on the information retained on deleted AD objects tombstones. Use this option if no state-in-time snapshots are available for the selected period.

Audited domain:

Minimize System Downtime

In the event that an unauthorized change affecting system availability does occur, you can quickly turn back the clock by reverting the settings to a previous state — without any downtime or having to restore from backup.

12

In Action: Increase the Productivity of IT Teams

Focus on What's Really Important

Use alerts to ensure you are notified about critical system configuration changes as they happen. You can choose the specific types of changes you want to be alerted about, such as changes to the membership of the Domain Admins group.

Real-time Alert

Changes to Admin Group Membership

Severity	Critical
Domain	ENTERPRISE.COM
Change Type	Modified
Object Type	Group
When Changed	7/6/2015 4:58:53 AM
Who Changed	ENTERPRISE\J.Smith
Where Changed	dc1.enterprise.com
Object Name	\enterprise\Users\Domain Admins
Details	Security Global Group Member: <ul style="list-style-type: none">• Added: "\enterprise\Users\Nick White"

All Group Policy Changes

Shows all changes to Group Policy objects, settings, GPO links and permissions with the name of the originating workstation from which a user made the change.

Action	What	Who	When
Modified	Security Policy	ENTERPRISE\J.Smith	7/23/2015 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;		

Troubleshoot Faster

When a problem arises, Netwrix Auditor delivers not mountains of raw data to pore through, but meaningful and actionable intelligence that enables you to quickly investigate the sequence of events involved and determine the underlying root cause of the issue.



13

Addressing the IT Auditing Challenges of Your Department and Your Business



Generate and deliver audit and compliance reports faster.

Investigate suspicious user activity before it becomes a breach.



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

Prevent data breaches and minimize compliance costs.



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

Analyst Coverage



Gartner

"...configuration auditing tools help you analyze your configurations according to best practices, enforce configuration standards and adhere to regulatory requirements..."



Redmond
MAGAZINE

"...auditing is generally a rather difficult task, especially if done manually. All of the many details you need to consider and remember are taken care of by Netwrix Auditor..."



Windows IT Pro

"...best Active Directory/Group Policy product and Best Auditing/Compliance product 4 years in a row..."



Petri
IT Knowledgebase

"...full five out of five stars and recommended to anyone with an AD environment give the product a whirl..."

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

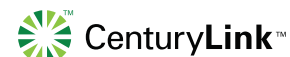
Available in appliances for
**VMware and Microsoft
Hyper-V**

Cloud

Fully supported and tested
in **Microsoft Azure**

Fully supported in
AWS Marketplace

Fully supported in
**CenturyLink Cloud
Marketplace**



RESTful API — endless integration, auditing and reporting capabilities



Centralize auditing and reporting

Netwrix Auditor collects audit data 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.

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



**Aerospace & Defense,
45K employees**

L-3 Communications
uses Netwrix to track
Active Directory and
Group Policy changes
to fulfill SOX compliance
requirements.

american
career
college

**Education,
5,5K employees**

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



**Technology,
1,3K employees**

Even with IT expansion,
Belkin controls changes
in Active Directory
and Exchange Server
with Netwrix.



**Banking and Finance,
100 employees**

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



Next Steps

Free Trial: setup in your own test environment netwrix.com/freetrial

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 1100, Irvine, CA 92618

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



netwrix.com/social