



Netwrix Auditor

Detect **Security** Threats, Prove **Compliance**
and Increase IT Team **Efficiency**

01

Product Overview

Ease the burden of IT auditing

Internal and external IT audits are becoming an integral part of the daily grind for more and more organizations. After all, IT audits are not only crucial for ensuring security and regulatory compliance; they also help organizations find and eliminate inefficiencies in their operational processes. Unfortunately, conducting these regular audits is usually far more cumbersome and time-consuming than it should be.

With Netwrix Auditor, you can ease your IT auditing burden and achieve your goals with far less effort. Its ready-to-use intelligence empowers you to automate many of the security, compliance and IT operations-related tasks that previously required hours to complete, so you can meet the demands of your organization without constantly being overburdened.



"We don't like vendors; we like partnerships. Netwrix has virtually become part of our staff. With Netwrix Auditor, our IT team gets back valuable time, which makes our organization more efficient in accomplishing our goals for the county."

John Adams, IT Director, Washington County, Arkansas



02

Product Overview



Detect threats faster to avoid being the next breach headline

Reduce the exposure of your critical assets by identifying your top security risks and tightening loose permissions. Ensure timely detection and response to threats by setting up alerts with automated actions and performing faster, more accurate investigations.



Save time and money during compliance audits

Achieve, prove and maintain compliance with less effort and expense by slashing the time required to prepare for audits by up to 85%. Stop wasting hours combing through the audit trail whenever you need to answer ad-hoc questions from auditors.



Increase IT team efficiency without compromising on work-life balance

Enable your IT team to do more with less and achieve high KPIs without constantly staying late. Resolve critical issues before users get frustrated or the business is affected, and produce the information required by stakeholders faster than you could using manual processes.

03

Detect threats faster to avoid being the next breach headline

Assess and mitigate IT risks

Find and close data and infrastructure security gaps across your IT environment, such as a large number of directly assigned permissions or too many inactive user accounts, to reduce your attack surface.

| 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 |

Gain deep insight into sensitive data

Locate and classify sensitive information, including bank card data, medical records and other PII, and spot any that surfaces in an unsecure location to minimize the risk of a breach.

04

Detect threats faster to avoid being the next breach headline

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.

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 |

Establish strict accountability over the use of privileged accounts

Monitor the activity of privileged users across your critical IT systems to ensure that they follow internal policies and don't misuse their privileges.

05

Detect threats faster to avoid being the next breach headline

Be the first to know about suspicious activity

Detect security threats, such as SQL Server activity during non-business hours or a large number of repeated file modifications that might indicate a ransomware attack in progress, so you can respond before significant damage is done.

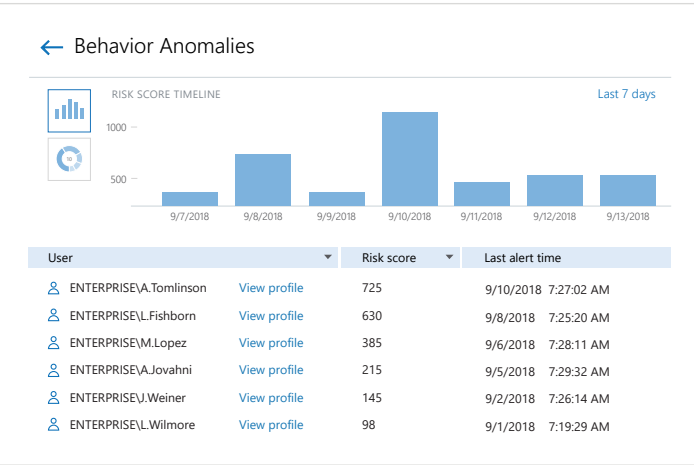
Netwrix Auditor Alert

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](#).



Detect compromised accounts and malicious insiders

Pinpoint subtle signs of possible security threats, such as unusual logons or unsanctioned remote access to your network. Identify and investigate the users who pose the most risk with an aggregated view of the anomalous activity by each individual.

06

Detect threats faster to avoid being the next breach headline

Reduce the mean time to respond

React to security threats faster by automating response to anticipated incidents. Provide initial incident support by integrating Netwrix Auditor into your SecOps process.

←

Mass Data Removal from SharePoint

Home > All Alerts > Mass Data Removal from SharePoint

General

Recipients

Filters

Thresholds

Risk Score

Response Action

Take action when alert occurs

On

Run: C:\Users\J.Carter\Scripts\KillSessions.txt

With parameters: Enter parameters

Save & Close

Save

Discard

← Search

WHO ACTION WHAT WHEN WHERE

Who

ENTERPRISE\Key

Open in new window

SEARCH

Advanced mode

| Who | Object type | Action | What | When |
|---------------------|-------------|--------|--|-----------------------|
| ENTERPRISE\Key File | Read | | \\fileserv1\shared\Finance\Q4_2018\Revenue Forecast.xlsx | 10/25/2018 9:01:13 AM |
| ENTERPRISE\Key File | Read | | \\fileserv1\shared\Finance\Q4_2018\Risk Assessment.pdf | 10/25/2018 9:00:10 AM |
| ENTERPRISE\Key File | Copied | | \\fileserv1\shared\Finance\Q4_2018\Audit Report.docx | 10/25/2018 9:00:02 AM |
| ENTERPRISE\Key File | Removed | | \\fileserv1\shared\Finance\Q4_2018\Revenue Forecast draft.xlsx | 10/25/2018 8:59:45 AM |
| ENTERPRISE\Key File | Modified | | \\fileserv1\shared\Finance\Workflows\Billing workflow.pdf | 10/25/2018 8:59:23 AM |

Streamline incident investigation

Get to the bottom of incidents involving sensitive data in minutes using the Google-like search: Understand exactly what happened, how it happened, who was behind it and which pieces of information were affected.

07

Save time and money during compliance audits

Ensure your security controls are effective

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, fix your faulty security controls before auditors discover them.

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 |

← Reports

Enter your search

Q

▸

Folder icon

 CJIS Compliance

▸

Folder icon

 FERPA Compliance

▸

Folder icon

 FISMA/NIST Compliance

▸

Folder icon

 GDPR Compliance

▸

Folder icon

 GLBA Compliance

▾

Folder icon

 HIPAA Compliance

Effective Group Membership

Failed Read Attempts

▸

Folder icon

 ISO/IEC 27001 Compliance

▸

Folder icon

 NERC CIP Compliance

▸

Folder icon

 PCI DSS Compliance

Slash time spent on compliance preparation

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

08

Save time and money during compliance audits

Answer ad-hoc questions from auditors

If there are unexpected questions during the audit, use the Google-like search to pull up the requested information right on the spot.

← Search

WHO

ACTION

WHAT

WHEN

WHERE

Action

Removed ×

Who

ENTERPRISE\J.Carter ×

Open in new window

SEARCH

Advanced mode

| Who | Object type | Action | What | Where | When |
|---------------------|-------------|---------|---|----------------|----------------------|
| ENTERPRISE\J.Carter | File | Removed | \\ntnx\Internal\Revenue\Revenue_2018.xlsx | afs1.nut.local | 10/2/2018 8:56:10 PM |
| ENTERPRISE\J.Carter | File | Removed | \\ntnx\Internal\Revenue\Revenue_2017.xlsx | afs1.nut.local | 10/2/2018 8:55:45 PM |
| ENTERPRISE\J.Carter | File | Removed | \\ntnx\Internal\Revenue\Revenue_2016.xlsx | afs1.nut.local | 10/2/2018 8:52:14 PM |

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:\Program Data\Netwrix Auditor\Data

Keep audit data for: 60 months

Netwrix Auditor uses [the LocalSystem account](#) to write audit data to the Long-Term Archive

Modify

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 be accessed by authorized users at any time.

09

Increase IT team efficiency without compromising on work-life balance

Resolve user issues before they become real problems

Whenever users want to know why their file is gone and how they can get them back or why they can't access a virtual machine running a business-critical application, get the answer in a few clicks and enable the users to get right back to work.

| ← Search | WHO | ACTION | WHAT | WHEN | WHERE |
|---|--------------|---------------|-----------------|----------------------------|----------------------|
| ○ Data source | "Azure AD" × | ○ When | "Last 7 days" × | | |
| Open in new window | SEARCH | Advanced mode | | | |
| Who | Object type | Action | What | Where | When |
| W.Smith@enterprise.onmicrosoft.com | Application | Removed | Baidu | Enterprise.onmicrosoft.com | 2/26/2019 9:21:01 AM |
| M.Hudson@enterprise.onmicrosoft.com | Application | Modified | CollectorApp | Enterprise.onmicrosoft.com | 2/26/2019 9:29:37 AM |
| M.Gold@enterprise.onmicrosoft.com | Group | Added | Administrators | Enterprise.onmicrosoft.com | 2/26/2019 9:42:59 AM |
| Member added: "W.Smith" Origin: "Azure AD" | | | | | |

Netwrix Auditor Alert

A SQL Server database has been deleted

Who: ENTERPRISE\J.Smith
Action: Removed
Object type: Database
What: Database\Main\Customers
When: 4:57:40 PM 4/24/2019 4:57:40 PM
Where: sql1
Workstation: mkt023.enterprise.com
Data source: SQL Server
Monitoring plan: SQL Server Monitoring

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

Swiftly react to events that might cause downtime

Get notified about events early, such as the deletion of an organizational unit or a database with customer information, and fix them fast before the business is affected.

10

Increase IT team efficiency without compromising on work-life balance

Get a clear picture of what was changed

Keep tabs on what's changing across your on-premises and cloud-based IT systems so you can spot and remediate issues before they stifle business activity and user productivity. As a result, you can deliver uninterrupted IT services and meet your SLAs and user expectations consistently.

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: ENTERPRISEM.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: ENTERPRISEJ.Hanson, Version: 3.5.3.44396 |

Quickly review system configurations and spot deviations from a known good baseline

Determine the current state of your critical assets faster than you could using manual processes so you can check whether your configurations match a known good baseline. If not, remediate the issues to prevent system downtime and user disruption.

11

Increase IT team efficiency without compromising on work-life balance

Answer questions in minutes, not hours

Whenever stakeholders ask for information, such as a list of who has access to a particular folder or proof that there are no inactive users in the IT environment, respond quickly with ready-to-use, human-readable reports.

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 |

| Subscriptions | | | | | |
|--|--------|-------------|--|---------------------------|----------|
| Home > Subscriptions | | | | | |
| <input type="text" value="Enter your search..."/> | | | | | |
| Name | Type | Status | Mode | Recipients | Schedule |
| Administrative Group and Role Changes | Search | ✓ Completed | <input type="checkbox"/> Off | sysadmins@enterprise.com | Daily |
| J.Carter's Activity | Search | ✓ Scheduled | <input checked="" type="checkbox"/> On | T.Simpson@enterprise.com | Weekly |
| Subscription to the 'Windows Server Configuration Details' report | Report | ✓ Scheduled | <input checked="" type="checkbox"/> On | sysadmins@enterprise.com | Weekly |
| Subscription to the 'Overexposed Files and Folders' report | Report | ✓ Scheduled | <input checked="" type="checkbox"/> On | J.Phillips@enterprise.com | Daily |
| Subscription to the 'Sensitive File and Folder Permissions Details' report | Report | ✓ Scheduled | <input checked="" type="checkbox"/> On | J.Phillips@enterprise.com | Daily |

Stop being a reporting bottleneck

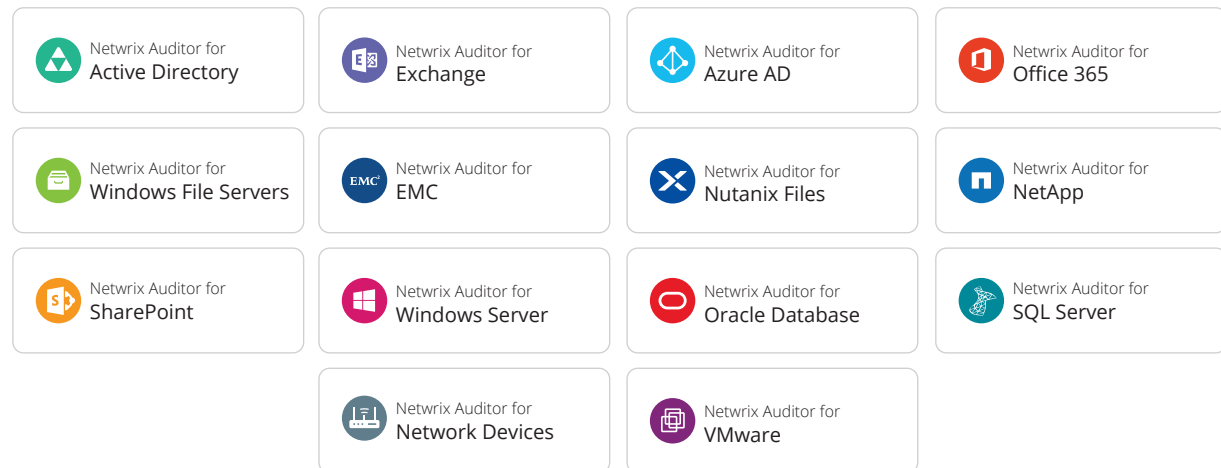
Automatically send stakeholders the information they demand on the schedule they prefer. Alternatively, give stakeholders granular access to Netwrix Auditor so they can get just the information they need whenever they like.

12

Netwrix Auditor Applications

Audit your most important IT systems from a single place

Stop juggling multiple tools in an attempt to collect audit information from all your on-premises and cloud-based systems and let Netwrix Auditor deliver the information you need in a unified and consistent way.



13

Netwrix Auditor Integration API

Take advantage of endless integration, auditing and reporting capabilities



Centralize auditing and reporting

Collect activity trails from any on-premises or cloud application and store them in a single place to keep threats to the IT environment at bay, simplify security investigations and streamline audit checks.



Get the most from your SIEM investment

Get far less cryptic output from your SIEM and speed investigations by feeding the human-readable and actionable data collected by Netwrix Auditor into it.



Automate IT workflows

Integrate Netwrix Auditor with your security, compliance and IT operations tools to streamline your IT workflows, such as change or incident management.



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

14

Why Netwrix Auditor

Review the top reasons why customers choose Netwrix Auditor



Quick win

Start getting value right out of the box and receive return on your investment in days, not months. Don't pay for expensive professional services or spend time on a lengthy deployment process.



Reasonable pricing

Get a solution that comes at a reasonable price and with transparent and predictable operating expenses. Hit multiple security, compliance and IT operations goals without spending a fortune on disparate tools.



Non-intrusive architecture

Avoid the nightmare of dealing with intrusive agents and undocumented data collection methods.



First-class technical support

Have your issues promptly resolved by first-class technical support with a 97% satisfaction rate.



"Netwrix Auditor gives the best bang for the buck, bar none."

IT operations manager in the financial industry



15

Customer Success

Read how our customers achieve their goals with Netwrix Auditor

Join more than 10,000 organizations from various industries around the globe that are already using Netwrix Auditor to secure their business-critical assets, pass compliance audits and efficiently manage their on-premises, cloud and hybrid IT environments.



Nonprofit

Netwrix Auditor empowers Horizon Leisure Centres to ensure the security of sensitive data and comply with the GDPR.



Insurance

First Insurance Company of Hawaii uses Netwrix Auditor to increase system stability and speed investigations.



Food & Beverage

Perfetti Van Melle Turkey complies with ISO/IEC 27001 and enforces internal security policies with Netwrix Auditor.



Energy

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



About Netwrix

Netwrix is a software company that enables information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides. Over 10,000 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com.

Next Steps

Start a free trial

netwrix.com/freetrial

Schedule a live demo

netwrix.com/livedemo

Launch in-browser demo

netwrix.com/browser_demo

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

Copyright © Netwrix Corporation. All rights reserved. Netwrix is trademark of Netwrix Corporation and/or one or more of its subsidiaries and may be registered in the U.S. Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are the property of their respective owners.