Best Practices Guide

Reach Your Objectives Using the Netwrix Auditor Platform

www.netwrix.com

About this Guide

Netwrix Auditor is an industry-leading visibility platform for user behavior analysis and risk mitigation in hybrid IT environments. Because of its powerful functionality, scalability and ease of use, organizations of different sizes and from multiple industry verticals rely on it every day to protect their sensitive data.

Regardless of your company's profile, this guide will help you unlock the full power of Netwrix Auditor in addressing your unique needs. The first section includes four modules; each one covers a specific objective, so you can quickly navigate to exactly the pieces of guidance you need the most and skip the less relevant parts.

In addition to learning how Netwrix Auditor can help your achieve your specific business objectives, be sure to read the six general guiding principles in the second part of this guide; they reveal some universal recommendations for using Netwrix Auditor to improve security, compliance and operational effectiveness.

Netwrix welcomes your feedback. If you have any suggestions on how we can improve this document, please send them to us through **this form**.

Contents

Netwrix Auditor by Objective

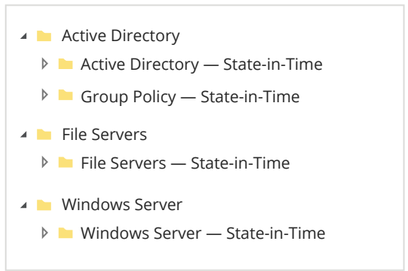
To maximize the value you get from using Netwrix Auditor, you should start by determining which main problems you want to address with the software, be it hardening overall security, detecting breaches, streamlining compliance or optimizing IT operations. Depending on your priorities, different functionality of Netwrix Auditor will be of most interest to you. Just select the objectives that are most important to you in the **Contents** section of this guide and proceed to the corresponding pages for the most suitable guidance.

1. Hardening Information Security

1.1 Become more resilient to cyber threats

The first step in hardening information security is making your organization more resilient to both external cyber attacks and insider misconduct. You need to identify and remediate security gaps that attackers could use to establish footholds inside your environment or that make it harder for you to recognize that something bad is going on. Although you cannot eliminate all risks, you can reduce both the likelihood and the impact of security issues by simply improving your system hygiene.

Netwrix Auditor's **state-in-time reports** are daily snapshots of your environment that provide valuable information about what needs to be locked down in your Active Directory, Group Policy, file servers and Windows Server.



You can use these reports to perform privilege attestation, software inventory, Group Policy validation, and user/device identification and lifecycle management.

First, you need to be able to control both the permissions assigned to critical folders and the membership of Active Directory groups, because this will largely define the level of access available to users. The Active Directory state-in-time reports show what groups exist in your directory and who is in those groups. These reports enable you to adhere to the best practices of least privilege and segregation of duties (SoD), thus reducing risk.

For example, use the **Effective Group Membership** report to see if you have any nesting inside important groups and reveal any unexpected or improper permissions.

Effective Group Membership

Group: Domain Admins

Name	Member Through	Type	Status
Administrator	Explicit	user	Enabled
Administrator	Nebraska HR → HR	user	Enabled
Administrator	Nebraska Sales → Nebraska HR → HR	user	Enabled
Ali Lombardi	HR	user	Enabled

Next, since compromising a user's identity is one of the most common ways for an attacker to get into your network, you need to find all accounts that are particularly vulnerable. Using the state-in-time reports, you can quickly review all user and computer accounts and their last logon times, as well as reveal expired accounts, locked accounts, and accounts with passwords that never expire or that are not required. You can also improve individual accountability by finding all shared non-user-specific accounts, which could hamper efforts to attribute actions to a particular person.

You can also quickly check whether a particular user has access to anything not required for her role. The **User Accounts – Group Membership** report enables you to drill directly into the user you need to review, instead of having to page through a long report on all users.

Other state-in-time reports will help you review your Group Policy object (GPO) configurations, installed software, members of local administrative groups, account permissions and shared folder permissions. With this information at hand, you can make necessary changes to minimize the risk of security compromise.

You can run any state-in-time reports on demand or subscribe to receive them via email on schedule. By using that information to make your environment accurate, transparent and well organized, you can harden your organization's overall security.

1.2 Reduce the risk of misuse, exfiltration or corruption of sensitive data

Excessive or otherwise inappropriate permissions are a security hole that enables both inadvertent and intentional data misuse. For example, if too many users have permissions to access sensitive data, an attacker who compromises one of those accounts will be able to steal all that data. To establish and maintain a least-privilege access model, you need to define the level of access each individual should have to critical information resources — and review that access regularly, because both internal conditions and the threat landscape will change over time.

Use Netwrix Auditor's Active Directory and file server **state-in-time reports** to analyze the current state of access. For instance, the **Excessive Access Permissions** report lists all users who have permissions to specific folders but use the data rarely or not at all.

Excessive Access Permissions

Object: \\fs1\Patient History (Permissions: Different from parent)

Account	Permissions	Means Granted	Times Accessed
ENTERPRISE\N.Key	Full Control	Directly	0
ENTERPRISE\T.Simpson	Full Control	Group	0
ENTERPRISE\P.Anderson	Full Control	Group	0
ENTERPRISE\K.Miller	Write and list folder content	Directly	0
ENTERPRISE\T.Allen	Read (Execute, List folder content)	Group	0

To facilitate the best practice of granting access rights only through group membership, other file server reports show all permissions that were granted directly, and therefore need to be revised.

To protect your most valuable data, use the **Sensitive File and Folder Permissions Details** report from the **Data Discovery and Classification** report pack to review who can access specific folders containing PII, PHI, PCI or other types of sensitive data, exactly what permissions those users have, and how they got those permissions. If the access rights come from group membership, you will be able to see the exact groups, so you easily modify group membership as appropriate.

Of course, providing access through group membership means you have to be vigilant about what groups you have and how group membership changes over time. State-in-time reports like **Effective Group Membership** and **Administrative Group Members** make routine review and validation of groups and group membership much easier.

Administrative Group Members

Group Path: \com\enterprise\Builtin\Administrators

Member Path	Type	Status
\com\enterprise\Inactive Users\Phil Jackson	user	Enabled
\com\enterprise\Users\Administrator	user	Enabled
\com\enterprise\Users\Elena Anderson	user	Enabled
\com\enterprise\Users\John Brown	user	Enabled

More broadly, regular review of state-in-time reports will help you create a cleaner and more manageable environment, which will further limit the ability of both insiders and external attackers to view, steal or damage your data.

You also need to keep a close eye on users' attempts to access your critical information assets. You can get this visibility by regularly reviewing the File Server Activity reports and setting up **email alerts**.

For example, simply subscribe to the **Activity Related to Sensitive Files and Folders** report to easily see who has tried (successfully or not) to read, modify or delete specific sensitive folders or files since your previous review. Or create an alert that will be triggered any time someone attempts to read or modify too many files in a short period of time or tries to add a new member to the Enterprise Admins group.

In addition to state-in-time reports, Data Discovery and Classification reports, **change reports**, **activity reports** and alerts on threat patterns, Netwrix Auditor offers other ways to identify exposed data or improper user activity. In particular, **security analytics reports** (such as **Data Access Trend, Data Access Surges, Access to Archive Data** and **Non-Owner Mailbox Access**) and the **Behavior Anomaly Discovery** dashboard will help you spot the first signs of inappropriate data access or unusual data usage patterns.

Using these Netwrix Auditor capabilities, you can establish a convenient, iterative audit and review process that will significantly reduce risks to the confidentiality, integrity and availability of your sensitive data.

1.3 Ensure user accountability

The insider threat is one of the most urgent and devastating threats organizations face today. You need effective ways to control user activity inside your environment, deter privilege abuse and ensure personal accountability.

Netwrix Auditor can help you strike the right balance between trust and tight security by enabling you to hold individuals accountable for any deviations from policy with evidence of their actions across the entire IT environment.

Use **change reports**, **activity reports**, and **security analytics reports** to get granular details about what a particular user did. Use the report filters to specify exactly what you want to look at. You can have any report delivered to your inbox regularly, thanks to the report subscription feature.

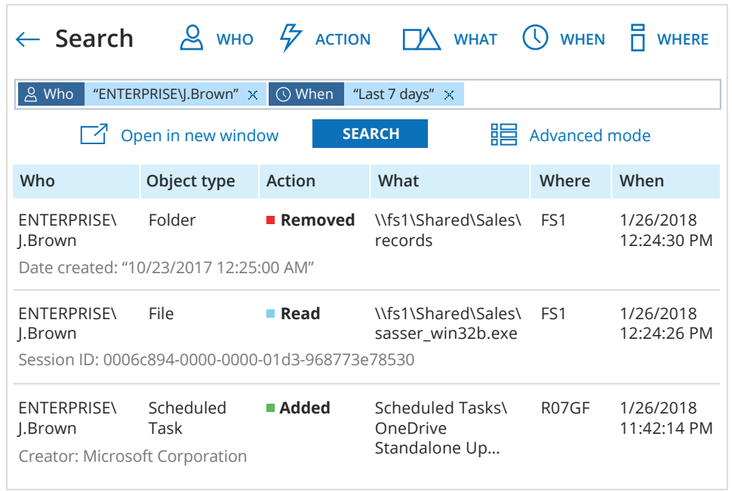
All Changes by User

Who: ENTERPRISE\T.Simpson
Data Source: Active Directory

Action	Object Type	What	When
Added	**user**	\com\enterprise\Users\Spiceworks Portal	2/6/2018 3:04:45 AM
Where: exchange.enterprise.com			
Modified	**group**	\com\enterprise\Managers\Managers	2/6/2018 4:06:29 AM
Where: pdc.enterprise.com **Security Global Group Member:** • **Added:** "enterprise.com/Users/Administrator"			

Often, you need to review a user's actions not just in one system, but across multiple systems. Netwrix Auditor displays this information on a single screen — unlike competitors' products that require you to jump between different tabs or even several applications.

The easiest method is to use Netwrix Auditor's **Interactive Search** functionality. You can start off broad and then get more granular. For example, you can search for all activity by a particular user during the past month, and then narrow down your search to a specific day, type of action, object type or system. You'll get the exact information you need in a human-readable format with full details — saving you hours of manual scripting, data consolidation and analysis work.



You can easily export the results to share with your business associates. You can also save any search as a custom report for later use, or use it to create an **alert**. For example, if a spot check on the activity of a particular user comes up empty, you can immediately create a new alert based on your search criteria, so if the user performs those actions in the future, you'll get an email notification right away.

Netwrix Auditor also includes a number of activity summary reports, such as **Data Access Surges, Access to Archive Data, Activity Outside Business Hours** and **User Activity Summary**. These reports give you the evidence required to hold individuals accountable for unwarranted actions, such as deleting archived records or accessing information systems late at night when they think no one is watching. Just be sure to provide meaningful values for the report filters.

To further bolster your body of evidence about a user's actions, take advantage of Netwrix Auditor's **user activity video recording**. You can capture the screen activity of any user on your mission-critical servers or even while they're using applications that do not generate logs. When you need to investigate an incident, the video recordings will provide both the evidence and the context you need to determine whether the incident was a malicious attack or an accidental violation of policies. Moreover, this functionality in itself is an effective deterrent to would-be insider attackers, since people who know that their activity might be monitored are less likely to act maliciously or carelessly, or otherwise violate company security policies.

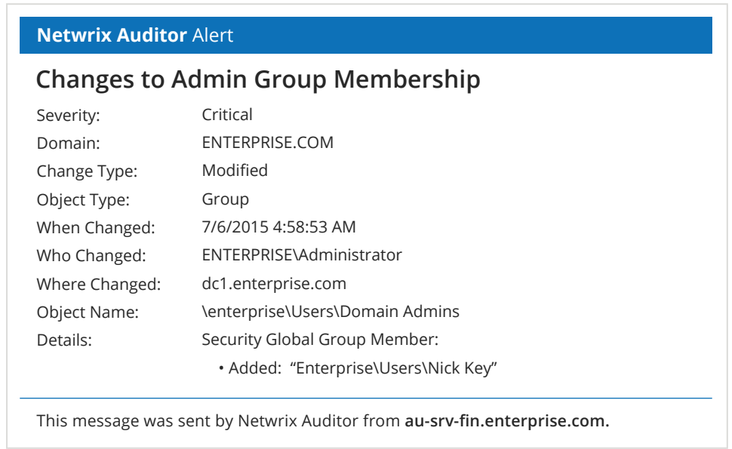
2. Identifying Breaches and Reducing Intruder Dwell Time

2.1 Detect suspicious events early

The earlier you recognize signs indicating an attack in progress or inappropriate insider activity, the better your chances of avoiding massive damage from data loss or disclosure, or disruption of critical operations. Attackers can lurk in your network for months, stealthily scoping out your data and escalating their permissions to get at it, so you need to constantly review and analyze activity in your environment.

Netwrix Auditor's alerting engine, security analytics reports, enterprise overview dashboards, Behavior Anomaly Discovery feature and Interactive Search enable you to proactively detect actions directed at critical system configurations, user access rights and sensitive data assets.

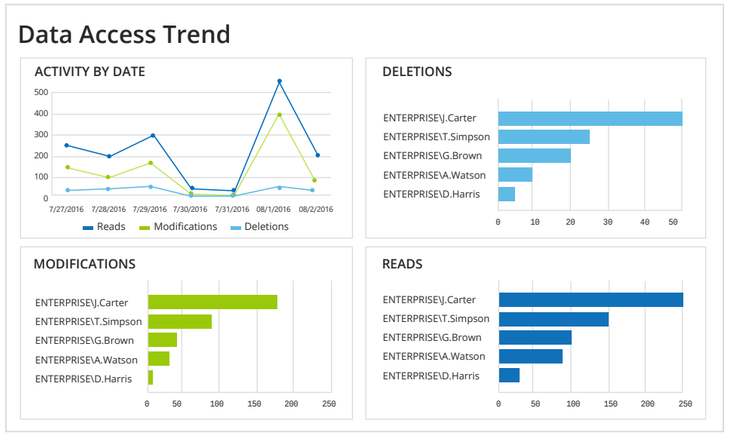
Start by setting up **alerting** to get notified about possible ransomware activity, privilege escalation, placement of potentially harmful files on your shares, installation of potentially harmful programs, strange logons to systems, failed actions on protected resources, log clearing and many other important types of activity. You can get alerts about individual events, as well as threshold-based alerts on a set of events that are not individually alarming but together comprise a suspicious pattern (such as a large number of file modifications in a short period of time, which can indicate ransomware in progress).



Review **activity reports** to spot suspicious behavior across your environment. For example, you can review logon activity, or successful and failed attempts to read, modify or delete data. With full details about user actions, you can proactively investigate the users and data involved for additional signs of trouble. You can have these reports sent to your security professionals automatically on the schedule you choose using the report subscription feature.

Also take advantage of the **change reports**. Regular review of what is changing in your environment improves your chances of detecting insider misdeeds or the activity of external attackers. Be sure to check out the flexible filters available in each report because they will help you specify the area you want to spotlight.

Use the **overview dashboards** to get a high-level view of what's going on across your systems. For instance, at a glance you can see the top servers by volume of activity and the most active users on each IT system. If an action seems strange, simply click on it to drill down to a detailed report.



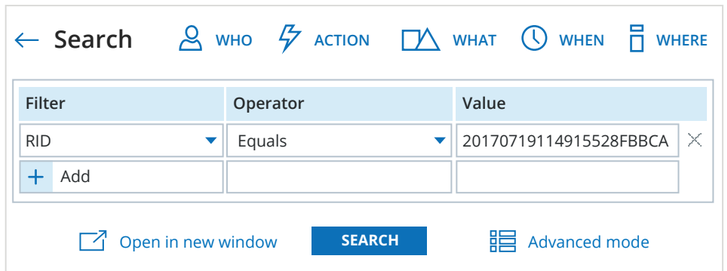
Use the **Behavior Anomaly Discovery** dashboard to see the riskiest users in your environment and dig into their activity, and view a timeline that illustrates when surges of risky activity occurred.

When you spot something potentially malicious, use the **Interactive Search** to investigate. By discovering how far the attackers managed to go, you can find all affected areas, respond effectively to the current threat, and take steps to prevent similar attacks from succeeding in the future.

2.2 Determine the true scope and duration of an attack quickly

As you review and analyze the audit intelligence that Netwrix Auditor supplies through alerts, reports and graphical dashboards, you might identify user actions or other events that could compromise information security or business operations. Use Netwrix Auditor's **Interactive Search** to immediately initiate a security investigation to determine whether the threat is real and, if it is, how long it has been present and the severity of your exposure.

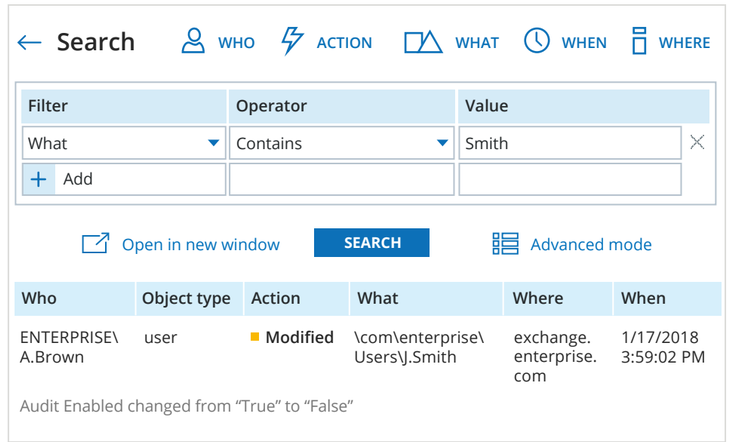
If you received an email **alert** from Netwrix Auditor, start by reviewing the event in it. Simply copy the record identifier (RID) from the alert message and paste it in the Value field of the Interactive Search, type "RID" for the filter name, and choose the operator "Contains".



If you didn't get an alert, start your investigation with a focused review of a short period of time immediately before and after the incident you discovered. Make your search criteria as specific as possible — use the filter "Who" and the operator "Equals" to specify the user or users involved in the incident, and other filters to specify the actions taken, the objects the actions were directed at, and the system where it occurred.

In the case of a real attack or malicious activity by rogue insiders, the incident you came across might be just the tip of the iceberg — the full compromise might affect a lot more than you first think. To find out, start broadening your search criteria. You can extend the time period, remove limitations such as a specific data location or IT system, and search for all activity by the user instead of just one particular type of activity.

One specific search technique has proven to be especially effective in practice: Broaden your search from specific actions by a particular individual to all activity related to that user. Just specify the user's name (or a part of it) as before, but use the filter "What" instead of "Who", and the operator "Contains" instead of "Equals". That way, you will see actions that were performed by someone else in relation to the user account in question. For example, suppose you've been alerted to inappropriate data usage by J.Smith. But that might be just a dummy account an attacker is using to try to cover their tracks. By applying the method just described, you will find out who created the J.Smith account.



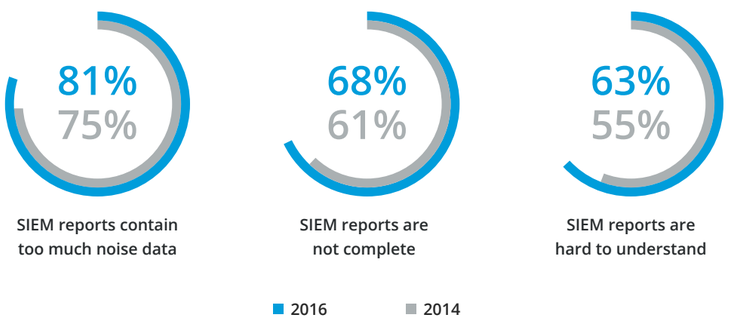
Going broad with more general search criteria to see the bigger picture will usually result in a lot of irrelevant information. Fortunately, the Interactive Search makes it extremely easy to cut through that noise. Just double-click on any activity record and you'll see the two buttons: "Exclude from search" and "Include to search". If you click on either of them, a drop-down menu will appear and you can simply select what you want to include or exclude. For example, when you're looking at activity inside Active Directory, you'll see a lot of logon activity. If you have reason to believe that's not where the true problem is, just click to exclude logons, and they will be immediately filtered out.

This model of investigation — from narrow to broad, with the continuous alignment of search criteria that the Interactive Search makes easy — will eventually lead you to the root of a problem, so you can plan an effective response.

2.3 Increase the efficiency of your SIEM

Security information and event management (SIEM) systems are often used to help identify cyber attacks, especially during their lateral expansion and privilege escalation stages. However, once a SIEM issues a warning about a possible attack, the information security (InfoSec) teams need to quickly and efficiently analyze the log data — and SIEMs lack the capabilities to facilitate these investigations.

Specifically, most SIEM solutions have a log-based architecture, so instead of actionable intelligence, they provide a huge set of events with data as it appears in the logs. To piece together enough context to investigate an incident, you have to analyze individual records and manually consolidate related events into a user activity trail, which often means you can't respond promptly to an attack. Moreover, the vast number of events that SIEMs report can easily obscure a truly important action, and you might not get some critical details if they aren't recorded in the native event logs and Syslog.



Netwrix 2016 SIEM efficiency report

You can address all these issues by integrating Netwrix Auditor with your SIEM solution. Free add-ons built using our RESTful API make the integration process easy.

After integration, Netwrix Auditor will transform a disparate array of related events into a single record enriched with actionable who, what, when and where details, along with the before and after values. As a result, you get more valuable context about user behavior and threat patterns in your critical IT systems.

For example, this is how the Splunk SIEM would report a change to folder permissions when working alone:

Permissions Change:

Original Security Descriptor: D:PAI(A;OICI;FA;;;S-1-5-21-210521867-2639090965-1213260628-1106)(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-210521867-2639090965-1213260628-1143)(A;OICI;FA;;;SY)(A;OICI;FA;;;S-1-5-21-210521867-2639090965-1213260628-1138)

New Security Descriptor:

D:PARAI(A;OICI;FA;;;S-1-5-21-210521867-2639090965-1213260628-1106)(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-210521867-2639090965-1213260628-1143)(A;OICI;FA;;;SY)(A;OICI;FA;;;S-1-5-21-210521867-2639090965-1213260628-1138)(A;OICI;FA;;;S-1-5-21-210521867-2639090965-1213260628-1174)

And this is what the event is transformed into after integrating Splunk and Netwrix Auditor:

Message=The following audit event was detected:
Who: **ENTERPRISE\J.Carter**
What: **\\fs1\shared\Managers**
When: **12/25/2015 4:05:49 PM**
Where: **fs1**
Change type: **Modified**
Object type: **Folder**
Managed object: **FS1**
Change details:
Permissions: Added: 'ENTERPRISE\C.Hoffman
(Allow: List folder / read data, Create files / write data, Create folders / append data, Read extended attributes, Write extended attributes, Traverse folder / execute file, Delete subfolders and files, Read attributes, Write attributes, Delete, Read permissions, Change permissions, Take ownership, Synchronize)
Apply onto: This folder, subfolders and files'
Detected by: ny.enterprise.com at 12/25/2015 4:08:16 PM

The contextual awareness achieved through integration will help your InfoSec teams determine the true scope of an attack, including its probable duration, faster and with far less effort. You will be able to see what steps the attackers took, how they changed system configurations, when they did it and how far they got, so you can respond effectively.

In addition, many SIEMs are licensed by the amount of data indexed each day. Integration with Netwrix Auditor can reduce the amount of data by cutting out the noise — and therefore the ongoing cost of your SIEM.

Netwrix has created a number of free add-ons that streamline integration with leading SIEM solutions, including Splunk, HP ArcSight, IBM QRadar and LogRhythm. These add-ons and all related documentation are available for download in the **Netwrix Auditor Add-on Store**.

3. Validating Internal Controls and Proving Regulatory Compliance

3.1 Provide assurance around security policies and implemented controls for internal and external stakeholders

Regulatory standards obligate organizations to comply with extensive information security requirements in accordance with their business needs, threat environment and risk appetite. Even if your organization is not subject to any industry or government regulations, you still have to demonstrate to customers and vendors that you have a strong commitment to protecting their data, and fulfill similar requirements from stakeholders, such as investors.

With Netwrix Auditor, you have the means to provide assurance around security policies to satisfy both internal and external stakeholders.

Use snapshot-based **state-in-time reports** to demonstrate that group membership, effective user permissions, password policies and other configurations have always been in line with security policy requirements. You can show stakeholders how things are configured today, or how they were configured on any day in the past.

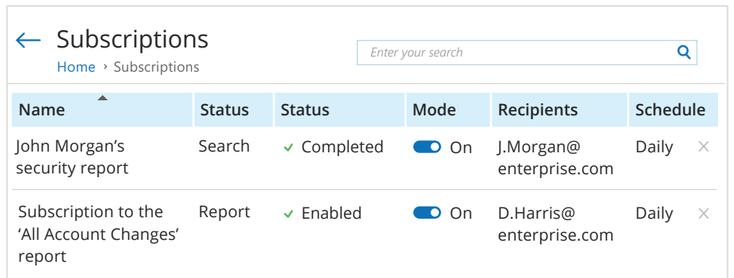
Use **Data Discovery and Classification reports** to prove that regulated data is restricted to members of appropriate groups, and not to groups like Everyone or Authenticated users. You can also demonstrate that the right individuals have the right permissions.

Sensitive File and Folder Permissions Details

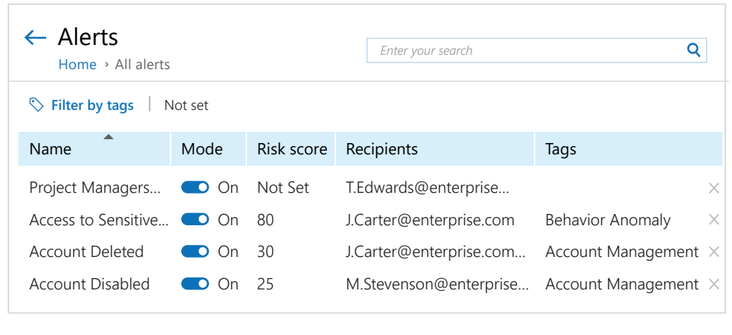
Object: \\fs1\HR\Europe (Permissions: Different from parent)
Categories: GDPR

Account	Permissions	Means granted
ENTERPRISE\J.Miller	Full Control	Group
ENTERPRISE\A.Clark	Full Control	Group
ENTERPRISE\L.Adams	Full Control	Group
ENTERPRISE\P.Young	Full Control	Group

To demonstrate that you have an ongoing security audit process that involves key decision makers and security practitioners appropriately, go to the report subscriptions section and show that **security reports about changes**, **access** and other **activity** have the right filters configured and that they are delivered to appropriate recipients or stored in a designated folder on a regular basis. For reports that are sent to a folder, open the folder and show the stakeholder the reports that have been generated over time.



Prove that you have an effective early warning system for threat mitigation by showing auditors or stakeholders a list of your active **alerts**. Show that the right people are specified as the recipients for each alert.



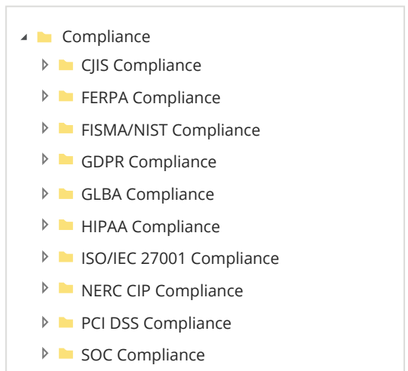
Demonstrate that you are efficient and flexible when conducting security investigations with the **Interactive Search**. Show how it enables you to search across all your audit data using any filtering criteria you want, so you can untangle even the most complex chain of events. Also show that you can save your searches as custom reports that you can access at any time and share with other security staff who might need them.

Also demonstrate that you have implemented **role-based access control (RBAC)** for use of Netwrix Auditor itself, so users are restricted in what they can do with the product in accordance with their job responsibilities. Make sure that the Configurator role is assigned to a trusted person in your organization, such as your chief system administrator or a security expert.

3.2 Streamline audit preparation

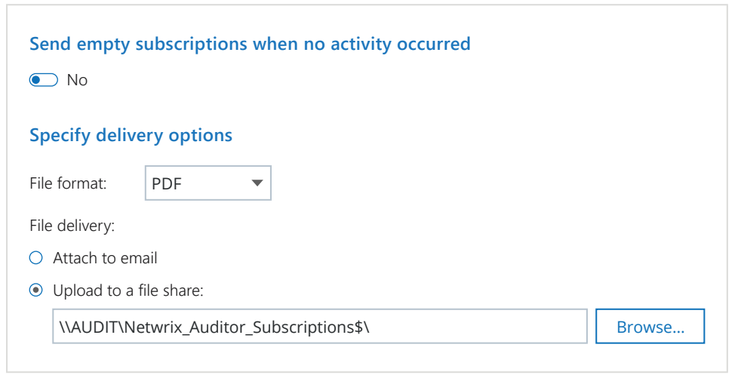
Preparing for audits often requires pulling IT staff away from their primary duties for weeks or even months. Netwrix Auditor makes the process much faster and less stressful by making it easy to locate, extract and prepare data that auditors are likely to request.

Start by seeing which controls Netwrix Auditor is likely to help you address. Simply click on the folder in the report tree that corresponds to the regulatory standard you're subject to:

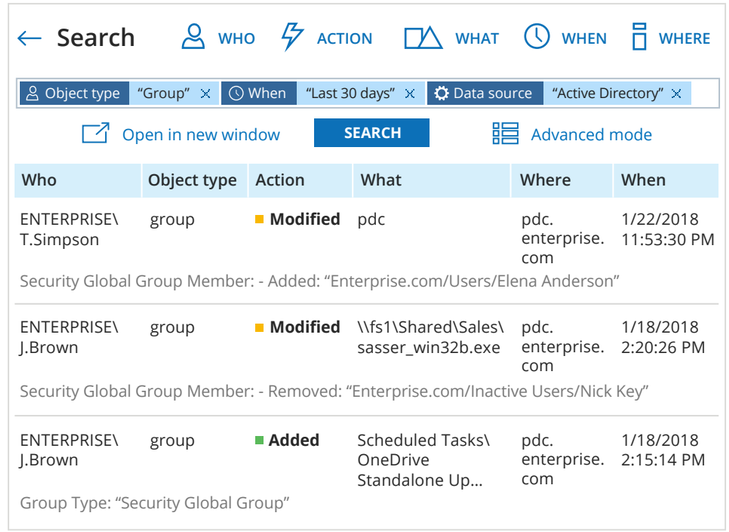


Then click the "View detailed mapping document" link in the upper right corner of the window to download a document that explains the purpose of the standard and maps its specific controls and requirements to specific Netwrix Auditor functionality. Study these mappings and adjust your preparation plan accordingly.

Identify the predefined reports that will be of most help during your upcoming audit and use the subscription feature to have them generated automatically on schedule and saved to a designated compliance folder. If auditors want proof that you've been generating and archiving all the appropriate reports, just show them that folder.



Easily supplement the predefined reports with custom reports tailored to your specific needs. With the **Interactive Search**, you can create a custom report in a matter of minutes or hours, rather than days or weeks. Make sure your search queries are fairly specific. Broad criteria are most useful during security investigations, when you're casting a wide net to find any indications of a compromise. Auditors, on the other hand, are likely to ask very specific questions, so you need to use focused filters to limit the reports to just the right amount of information required to provide clear answers. You can subscribe to custom reports just as you can to predefined reports.



With the automation provided by the report subscription feature and the flexibility of the Interactive Search, you can effectively prepare evidence of compliance in significantly less time and with much less effort than ever before.

3.3 Demonstrate your compliance during auditors' visits

When auditors come to your site, they usually demand that you demonstrate the effectiveness of your data protection controls in action, and they require those controls to remain effective long after the examination. Use Netwrix Auditor's compliance features to meet the most stringent demands from auditors and make audits less painful.

Right at the start of your audit, mention that instead of cryptic system logs, you rely on a visibility platform that transforms raw data into actionable intelligence, which improves your breach detection capabilities greatly. Also stress that this tool is a fully integrated, unified product that centralizes all security auditing and review processes in a single place, bolstering your efficiency. You don't have to operate multiple standalone tools, each with its own interface and report layouts, which invites mistakes.

Then show your auditor the contents of the appropriate compliance report pack. It will include multiple security reports that you can run on demand to demonstrate the adequacy of your internal controls.

Emphasize to the auditor that Netwrix Auditor includes snapshot technology that enables you to report on **system configuration states** (such as the state of your security groups, user accounts or object permissions) at present or any given moment in the past. These state-in-time reports will help you quickly answer questions such as "Who was a member of this security group three months ago?" and "What permissions did this critical share have a month ago and how do they compare to today's?"

User Accounts

Total Enabled: 9
Total Disabled: 23
Total Count: 32

Path	Name	Logon Name	Status	When
\com\enterprise\Inactive Users\Alex Terry	Alex Terry	A.Terry	Disabled	23/10/2018 7:56:44 AM
\com\enterprise \Users\Anna Watson	Anna Watson	A.Watson	Enabled	28/11/2018 10:12:32 AM
\com\enterprise \Users\Administrator	Administrator	Administrator	Disabled	30/09/2018 11:05:17 AM

To answer additional questions from auditors on the fly, turn to the **Interactive Search**. It makes it easy to answer questions such as "Who did what yesterday?", "What has been happening in this system since my last visit?" and "Prove that nothing happened to this sensitive folder over the past month." You might be able to just tweak the filters on one of the custom reports you created during the preparation phase; if not, you can easily create a new search query.

The auditor is also likely to demand a demonstration of your incident response process. Show the auditor the early warning system you have set up with Netwrix Auditor **alerts**, which ensures that appropriate employees are notified about changes that could signify an intruder or render a system vulnerable to attack. Show how these email notifications look.

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\payroll2018.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.**

Also demonstrate the report subscriptions you have in place to keep appropriate staff updated with security intelligence about potential threats in your IT environment. The reports are run and sent automatically, so the auditor will be assured you don't have to count on someone manually generating them on top of their core duties, illnesses, vacations, etc. Be sure to show the auditor that the right people are specified as the recipients of each report.

Active use of the compliance functionality of Netwrix Auditor will make you look prudent about risk mitigation in the eyes of the auditors.

3.4. Meet the requirements of new data protection regulations

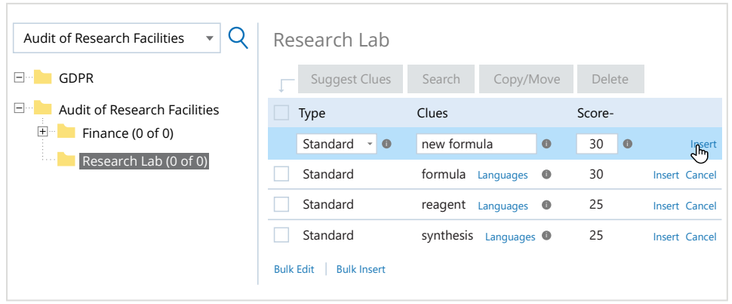
To comply with regulatory standards using your limited resources, you need to know a lot about the sensitive data stored in your organization: where it is, how critical it is, who has permissions to access it and how it is actually being used.

Use **Data Discovery and Classification** functionality to automate the data discovery process. Simply define rules for attributing sensitive data to specific categories and run the discovery regularly. Several taxonomies (rule sets for data categorization) are provided out of the box, so you can quickly see where regulated data of the most common types (such as Social Security, bankcard and Medicare numbers) is concentrated. Predefined reports make it easy to review who can access the data, what permissions each user has, who owns the data, and who is actually using it. This information will give you the proper level of control over sensitive resources as required by many regulatory standards, and tell you which resources require tighter security.

Sensitive Files Count by Source

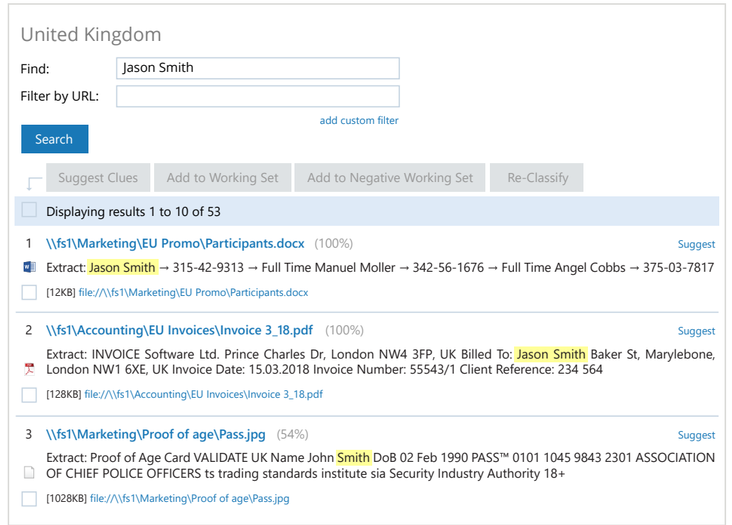
Content source	Categories	Files count
\\fs1\Accounting	GDPR PCI DSS	1300 585
\\fs1\Finance	GDPR PCI DSS	715 250 952
\\fs1\HR	GDPR PCI DSS	1500 1085

As both your business and the regulatory landscape change over time, you may need to protect additional types of data. The Data Discovery and Classification Collector console makes it easy to revise your taxonomies and create new rules for classification, so you can aptly address any new data protection requirements that arise in the future.



Many regulatory standards have data breach notification requirements. To report a breach to appropriate authorities and notify all affected parties as required, you need to be able to determine which data was affected. The **Activity Related to Sensitive Files and Folders** report shows all reads, modifications and deletions of classified data that occurred during a specified time period. If your security investigation reveals which account the attacker used, restrict the report to the actions taken by that account; this will reduce the time required to compile a complete list of folders and files that were compromised. This information will help you fulfill the data breach reporting requirements.

Some compliance standards also require you to revise or erase the personal data of any individual upon their request. Netwrix Auditor's web-based Data Discovery and Classification Collector console simplifies these tasks. Just enter the user's name or other identifying information, and the search functionality will find all documents, including images, that contain the words or phrases you are looking for.

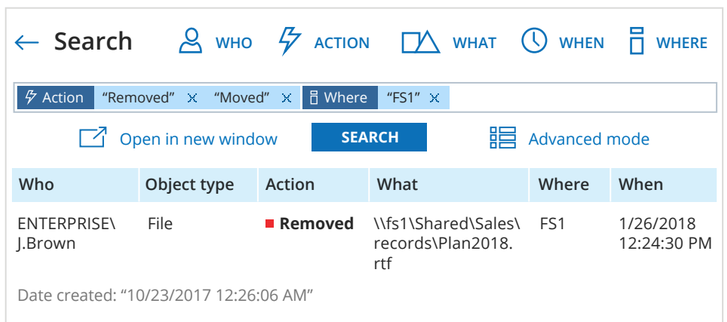


4. Meeting SLAs and Increasing the Efficiency of IT Teams

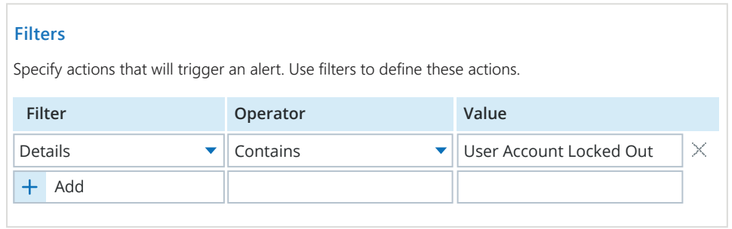
4.1 Detect and resolve user issues quickly

When something is not working properly in your environment, your ability to consistently deliver high-quality services to internal business users and external customers is jeopardized. Netwrix Auditor can help you proactively detect critical system configuration changes, user password changes, account lockouts, account expirations and other common issues that can interfere with daily operations.

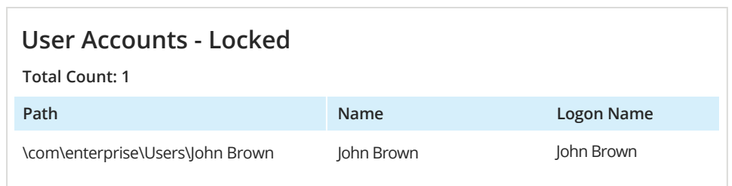
Use the **Interactive Search** to quickly discover the root cause of a problem causing user frustration. Suppose an important file is missing from its regular location. Interactive Search will quickly show you all recent file moves and deletions on your file shares or all document moves and deletions in SharePoint — it can even show you both at the same time. If the file was moved or deleted, you will know who is responsible.



Account lockouts are a frequent problem for users, and resolving them usually requires a call to the IT helpdesk. Use Netwrix Auditor's alerts to proactively notify helpdesk staff about account lockouts as soon as they occur, so they can resolve the issue — without the user even having to submit a ticket. You can choose to be alerted only when particular accounts are locked out.

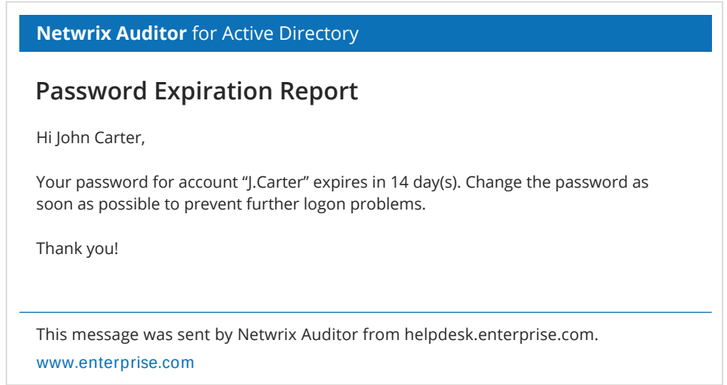


You can also use the **state-in-time report User Accounts – Locked** to keep an eye on lockouts, especially if your organization is huge and there are many such events waiting for resolution.



Password expiration is another frequent problem for users. Many people fail to change their passwords on time, and your helpdesk team has to constantly hustle to keep everyone productive.

Use Netwrix Auditor Password Expiration Notifier to automatically send out email reminders that tell users the number of days left before their passwords expire. With this functionality, you can reduce the time your support personnel spend resolving password-related support tickets and enable them to focus on more important tasks.



By resolving issues quickly, or even proactively, you will improve user productivity and satisfaction, and consistently meet your service-level agreements.

4.2 Increase the efficiency of your IT teams

When you have multiple IT teams working in geographically distributed office locations, wearing multiple hats and supporting a large number of business users, coordination and communication become huge challenges. Overcoming these challenges is critical to both the consistent delivery of high-quality services to internal users and the security of your systems and data. Netwrix Auditor can simplify the task of coordinating activities between members of different teams.

Many predefined Netwrix Auditor reports facilitate the change management process — and it's easy to keep everyone current on the status of each change. Simply click the "Click to update status" link to revise the status of a change (for instance, from "New" to "In Review"). Be sure to record all relevant details; for example, you can link a change to the corresponding ticket in your ticketing system.

All Activity with Review Status

Action	Object Type	What	Who	When
Modified	**computer**	\com\enterprise\Computers \WIN-JH0EO7LUN83	ENTERPRISE\ J.Carter	10/13/2016 5:48:30 PM
Where: dc1.enterprise.com Workstation: 192.168.10.28 Computer Account Enabled Review status: New				Click to update status
Added	**user**	\com\enterprise\Users \Paul Anderson	ENTERPRISE\ J.Carter	10/13/2016 2:46:59 PM
Where: dc1.enterprise.com Workstation: dc1.enterprise.com User Account Enabled Review status: New				Click to update status

Sometimes an IT team member will change a part of a system to address an immediate problem without understanding how that change could impact other people's work. Use the **Interactive Search** to track down what that person did, including which specific parameters were altered, so you can quickly get everything back to normal.

Use **alerts** to be notified about critical events that might severely impact business operations. The details in the alert will help you quickly restore the working configuration.

Netwrix Auditor Alert

Network routing rule modification

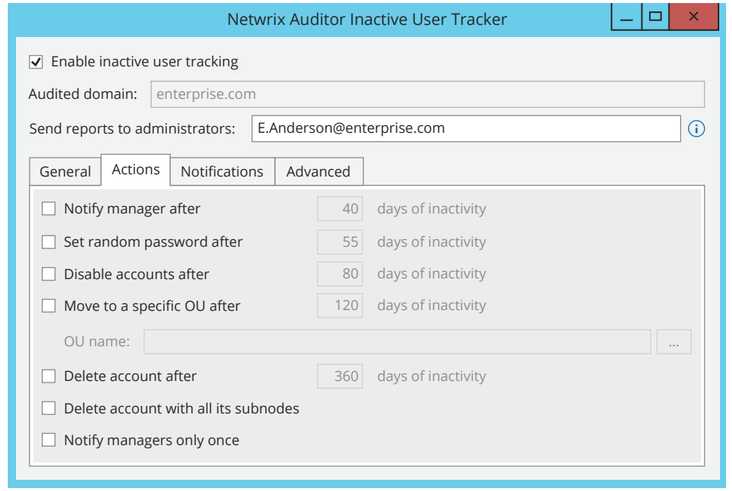
The alert was triggered by 150 activity records being captured within 60 seconds. The most recent of those activity records is shown below. To review the full activity trail, use the interactive search in Netwrix Auditor.

Who:	Carter
Action:	Modified
Object type:	Configuration
What:	10.0.0.1
When:	4/09/2017 12:58:23 PM
Where:	10.0.0.1
Workstation:	188.243.82.139
Monitoring plan:	Cisco ASA Visibility Plan
Details:	Raw Message changed from "" to "<165>Apr 30 2017 12:58:23: %ASA-5-111010: User 'Carter', running 'ASDM' from IP 188.243.82.139, executed 'route enterprise 192.169.12.101 255.255.255.255 192.170.10.1 1'"

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

Use Netwrix Auditor's **video recording** functionality to record all actions your highly privileged employees perform in critical IT systems or applications, such as production databases. The video recordings will help you understand not just what happened but also exactly how these people did what they did. You'll need this information to revert their changes or repair any damage. Furthermore, this evidence will help you establish user accountability if any actions prove to be malicious.

To automate routine user management and cleanup in Active Directory, use the Netwrix Auditor Inactive User Tracker. It will give you a clear listing of all inactive user and computer accounts in your directory, and even send alerts based on the inactivity criteria that you configure. Even better, it can spare you the work of manually handling inactive accounts by automatically disabling them, assigning them random passwords, moving them to a designated OU or deleting them.



Universal Guidelines

This section provides recommendations for using the Netwrix Auditor platform in keeping with best practices. These guidelines might not apply in every environment; however, they rest on Netwrix's expertise as a security vendor and the knowledge we have obtained from analysis of our clients' successful deployments.

These best practices are best reviewed in the order provided, and applied all at once as part of an iterative process. Accordingly, we have organized these guiding principles in the form of a process flowchart that depicts the major logical steps you need to take in order to reap the maximum possible value from your Netwrix Auditor investment.

General steps to identify, assess and reduce risks to your IT infrastructure and data more effectively using Netwrix Auditor

1 Assess your environment on a regular basis

- Understand what needs to be cleaned up or reconfigured using state-in-time reports on Active Directory, Group Policy and file servers.
- Discover high-risk configurations and understand how they impact overall security with IT Risk Assessment reports.
- Compare the current state of things to your organization's normal values using baseline reports on Windows Server.
- Locate and properly protect sensitive data with Data Discovery and Classification reports.

2 Establish activity baselines and remediate blind zones

Review User Behavior & Blind Spot Analysis reports regularly to:

- Stay current on what's normal for your environment — typical levels of data access, failed activity, activity outside business hours, etc. — so you can spot deviations going forward.
- Find, analyze and remediate security blind spots, including those that exist for only a brief time, like short-lived user accounts or a user who was a member of a privileged group for only a few hours.

3 Set up an early warning system to enable timely response to incidents

- Turn on selected predefined Netwrix Auditor alerts to ensure you will be notified about critical events in time to respond effectively.
- Set up custom alerts to get alerts about other events and behavior patterns you deem risky.
- Define the recipient list for each alert to include anyone who would benefit from notifications.
- Assign a risk score to each alert, for use in the Behavior Anomaly Discovery feature (see step 5).

4 Improve security governance through technology integrations

Use Netwrix Auditor's RESTful API and free add-ons to centralize auditing and extend the capabilities of solutions you already use:

- Reduce the noise input into your SIEM, so you get more meaningful and actionable information out.
- Centralize security auditing across your entire IT infrastructure, including network devices, RADIUS Server computers, and web services such as AWS.
- Simplify IT workflows such as change management and incident response.

5 Analyze user behavior across information systems

- Use overview dashboards to quickly understand the big picture.
- Ensure individual accountability and quickly pinpoint the root cause of each problem using reports, video recordings of user actions, Interactive Search and alerts.
- Prioritize your response to potential insider threats and external attacks with the Behavior Anomaly Discovery dashboard, which provides a consolidated view of anomalous activity based on the alerts generated in your environment.

6 Investigate incidents both deeply and broadly

- Thoroughly investigate suspicious incidents to understand how they occurred and prevent them from happening again. You can search for any activities performed by or related to any user, within any period, and across all or just several of your IT systems.
- Share your results with appropriate stakeholders and save your searches as custom reports for future use.
- Easily find the information you need to prove your compliance during audits.

1. Assess Your Environment on a Regular Basis

You need to be able to identify, analyze and prioritize your information security risks, so you can develop effective mitigation strategies. One of the critical first steps in managing risks is getting a complete and accurate understanding of the current state of things in critical systems like Active Directory, Windows Server and file storage. Your starting point here is information delivered through Netwrix Auditor's state-in-time reports, IT Risk Assessment reports, and Data Discovery and Classification reports.

Analyze the state of Active Directory, Group Policy and file servers

Active Directory, Group Policy and file server **state-in-time reports** help you understand what needs to be cleaned up or re-configured in those systems to tighten up overall security. Your objective when using these reports is to lock things down, eliminate disarray, and keep everything at the necessary minimum with no hanging unclear entities or unsecure configurations. The reports identify which accounts are stale and can be eliminated; whose access to shares can be removed because the users never use the resources; who has membership in your Active Directory security groups and whether those are direct or nested memberships; what password policies are currently applied; and whether there are any identical GPO settings that might explain why something is not working as it should.

Find deviations from baselines in Windows Server

Windows Server state-in-time reports help you assess your Windows Server environment: what servers exist; what operating systems they run (and whether they are outdated versions); whether appropriate antivirus software is installed; what other programs and services they have; and what local users, groups and file shares exist on each server. Most of these reports also enable you to compare the current configuration with your established baselines, so you can easily spot any servers that deviate from your company's security standard. And like all state-in-time reports, these reports enable you to compare the present configuration to any daily snapshot from the past.

Conduct IT risk assessment

IT Risk Assessment reports enable you to identify configuration gaps in your environment and understand the extent to which they could impact security and operations, including your mission, functions and reputation. For instance, they can spot chaotic privilege structures, "shadow" user and computer accounts, and improper content on your file shares. They clearly indicate which areas are acceptable from a security perspective, where you need to pay attention and where you should take immediate action. These reports are also snapshot-based, so you want to make sure the state-in-time functionality is enabled in Netwrix Auditor.

Define data categories and identify data residency

It's difficult to take effective measures to protect regulated or otherwise sensitive data if that data sprawls from designated network locations into unknown locations, or if you cannot distinguish highly sensitive files from the mass of less critical ones.

Data Discovery and Classification reports help you find exact locations where sensitive data resides within your file system; you can choose to see only the folders, or the exact files with their UNC paths. Netwrix Auditor automatically categorizes the data based on the taxonomies you choose using the web-based DDC Collector Console. You can use the supplied taxonomies as is, customize them to meet your needs, or provide new ones if you need to identify additional types of sensitive data. The reports help you determine how many sensitive files you have in each storage location, spot overexposed data accessible by improper users, see what permissions users have to specific data, find data owners and analyze actual data usage.

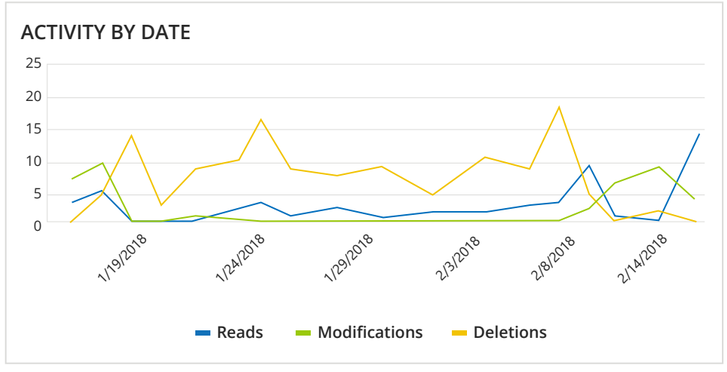
To reduce risk and ensure regulatory compliance, we suggest that you subscribe to the relevant state-in-time, IT Risk Assessment, and Data Discovery and Classification reports. You can choose to receive them in your inbox on a monthly basis, or even weekly if your environment is large and dynamic. This automation facilitates regular review for stronger security.

2. Establish Activity Baselines and Remediate Blind Zones

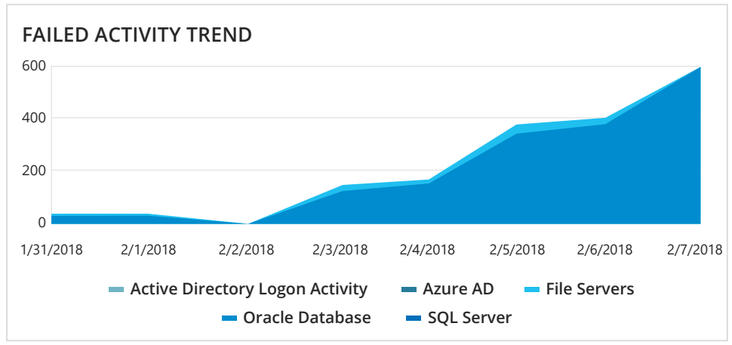
To spot unusual behavior that could be a threat, you need to know what level of activity is normal in your environment. And to ensure nothing important slips under your radar, you need to be able to spot security blind zones. You can achieve both of these goals using Netwrix Auditor's User Behavior and Blind Spot Analysis reports.

Spot abnormal behavior

Quite often, "malicious" means "different than normal" — so you need to establish an activity baseline to compare future behavior against. **User Behavior and Blind Spot Analysis reports** like **Data Access Trend** and **Failed Activity Trend** will show you the ordinary level of events over specific time period, and highlight any sudden bursts of activity or a steady growth of activity.



The visualizations enable you to instantly spot anything strange and quickly investigate. For instance, you can figure out whether an incident is of malicious nature or just the result of your recent experiments with access delegation. The graphs are adjustable and actionable, so you can change the time frame and click on the graph data to drill down into more details.



Remediate blind zones

Other security analytics reports in this report pack will help you uncover potential security blind zones. For example, in the space of just five minutes, a malicious insider could create a new user account, add it to the Domain Admins group to elevate its privileges, use it for unauthorized activity, and then remove it from both the group and the directory. Even if you audit your AD configuration on a daily basis, you'd never see that temporary user account or its momentary inclusion in the privileged group. To detect activity like this, regularly review the **Temporary User Accounts** and **Temporary Users in Privileged Groups** reports.

Temporary Users in Privileged Groups

Group: Domain Admins

Name	When Created	Who Created	When Removed	Who Removed
Enterprise.com/ Managers/Managers	1/22/2018 3:04:55 AM	ENTERPRISE\ I.Scur	1/22/2018 3:08:08 AM	ENTERPRISE\ I.Scur

Group Name: \com\enterprise\Users\Domain Admins

In a similar way, other reports will inform you about recently enabled accounts and who enabled them; files on your shares with names that suggest those files contain sensitive data (such as names with "password", "payroll" or other words you specify); and potentially harmful files on your shares, such as executables, installers and scripts.

The rest of the User Behavior and Blind Spot Analysis reports are focused on inherently suspicious user activity, such as activity outside business hours, non-owner mailbox access, data access surges, and logons by single user from multiple endpoints (or logons by multiple users from a single endpoint) in a short period of time.

Together, these security intelligence reports will ensure you don't miss potentially risky configurations that existed in your environment for only a very short period of time, and they will help you spot abnormal activity faster and with less effort. Furthermore, they will help you identify the risky users inside your environment, so you know who you should keep an eye on going forward.

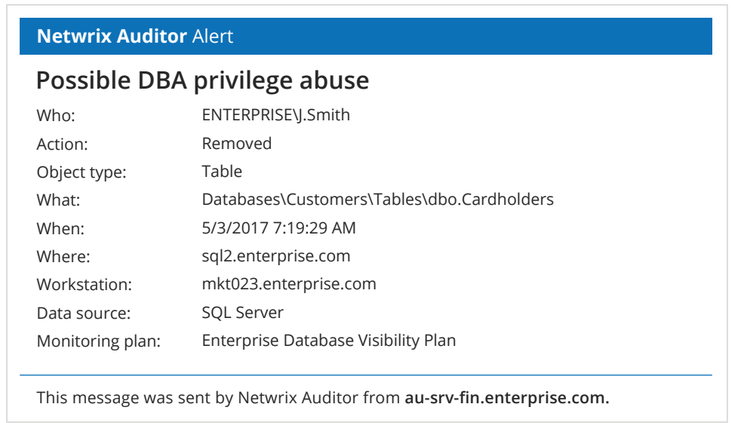
3. Set up an Early Warning System

Ensuring appropriate personnel are alerted to events that could lead to a breach or downtime is essential to security, compliance and business continuity. Netwrix Auditor will help you establish an effective early warning system.

Enable predefined alerts

Start by reviewing the predefined **alerts** supplied with Netwrix Auditor and enabling the ones that would be useful for your organization. For example, you might want to know right away if someone is added to a powerful group like Enterprise Admins. The alert **Group Membership Changes** is there for you right out of the box; you just need to turn it on. To maximize the effectiveness of any alert, make sure you choose the recipients carefully. You should also assign the alert a score that reflects the level of risk associated with it; that risk score will be used by the Behavior Anomaly Discovery feature in Step 5.

Whenever an event occurs that matches an alert's parameters, the recipients will receive an email notification.



Create custom alerts

If the predefined alerts do not cover everything you want, you can create custom alerts. Think hard about what you want each alert to achieve, and don't be surprised if getting there requires several rounds of fine tuning as you observe how it works. To make alert management easier, apply tags to your alerts so you can distinguish one alert from another, and create groups of similar alerts.

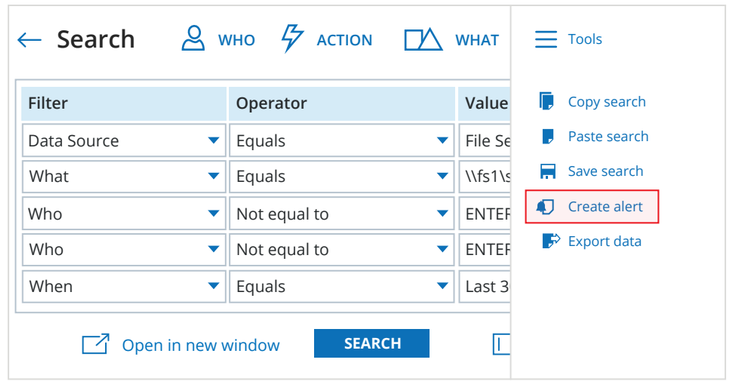
Use threshold-based alerts

Certain events signal a threat only if they occur repeatedly within a certain timeframe. For example, you wouldn't want to get an alert each time a user enters an incorrect password, but multiple failed logons within a short time could be a sign of a brute-force attack in progress — something you need to know about right away.

To be notified about these kinds of situations, use **threshold-based alerts**. Netwrix Auditor offers some threshold-based alerts out of the box, including **Multiple Failed Logons** and **Failed Access to Critical Assets.**

Create an alert from your Interactive Search query

You can also create **alerts based on your Interactive Search** queries. For example, suppose you perform a spot check on an admin's activity. Even if the search reveals no improper actions so far, you might want to keep a close eye on that user. You can quickly create a new alert based on your search criteria.



4. Improve Security Governance through Integrations

If your organization relies on a variety of third-party and custom information technology solutions, such as SIEMs and ticketing tools, in your day-to-day operations, you may be facing both security and efficiency challenges. For instance, employees might have to constantly switch from one program's interface to another to do their jobs, and manually resolve problems such as incompatible data formats. These issues can slow execution of tasks and increase the risk of human errors. By integrating Netwrix Auditor with one or several of the products you already use, you can improve both efficiency and security.

Netwrix Auditor provides a RESTful API for integrations, and a number of ready-to-use **free add-ons** are available to streamline the integration process.

Enhance SIEM efficiency

Integrate Netwrix Auditor with your SIEM (Splunk, IBM QRadar, Alien Vault, LogRhythm, etc.) to improve the quality of SIEM input data, resulting in more meaningful and actionable information in the output.

Netwrix Auditor improves SIEM input data and reduces its volume by merging multiple related events into a single, more meaningful activity record. As a result, you'll need fewer InfoSec personnel, and they'll be able to better detect incidents and recognize threat patterns, as well as establish the context around them, faster. This noise reduction and added intelligence increases the long-term viability of your SIEM solution, and makes it more cost-effective, too.

Furthermore, Netwrix Auditor will augment SIEM reporting with specific details that might be missing from the SIEM's log-based reporting. For instance, details about change to a Group Policy object's attributes or the delegation of organizational unit permissions to a user are not stored in security logs, but Netwrix Auditor will get this information and stream it into your SIEM for reporting.

Speed incident response

If your organization relies on ServiceNow® Incident Management to aggregate all enterprise activity into a single information hub for centralized review and management, you can **integrate it** with Netwrix Auditor to simplify incident discovery and speed the incident handling process.

After integration, tickets on incidents will be automatically opened in the ServiceNow ITSM based on Netwrix Auditor alerts about critical events across a wide range of IT systems. Important data about the incident will be filled in, and the ticket will automatically be assigned to the designated team or individual.

This integration will speed up the process of restoring normal business services, minimize the gap between incident detection and the start of a resolution process, automate incident handling, and reduce human errors that could impact service quality and security.

Centralize security auditing

The SIEM and ServiceNow integrations are examples of "data-out" scenarios, in which Netwrix Auditor performs the role of data provider. The API also supports "data-in" integrations where Netwrix Auditor receives audit data from other systems — for example cloud services (such as Amazon Web Services, Dropbox or Box), Unix-based operating systems (such as RedHat or Ubuntu), network devices (such as Cisco or Juniper) or business intelligence apps (such as SAP or Tableau).

All of this data is stored in a highly reliable and cost-efficient two-tiered storage, ready for search and reporting. That way, you centralize all your security auditing and reporting in one single location —the Netwrix Auditor platform — and gain visibility into everything that is happening across your entire hybrid IT environment.

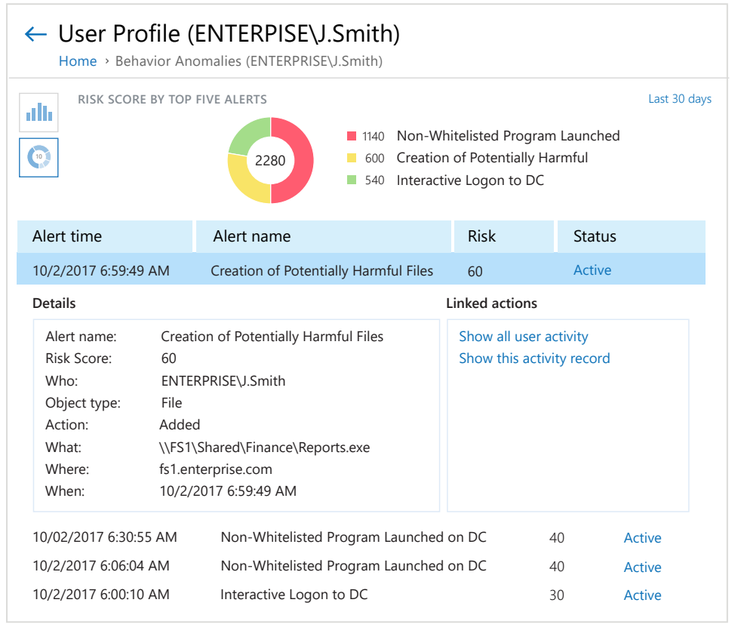
5. Analyze User Behavior across Key Systems

The first four steps of the Universal Guidelines focus on information security hardening measures for building a more layered and robust defense against internal and external threats. Once you have cleaned up your critical systems, set up alerts and report subscriptions, and integrated Netwrix Auditor with your other tools, you can concentrate on analyzing user activity to detect security threats.

Know which users merit close attention

Use **Behavior Anomaly Discovery** functionality and security intelligence reports to detect suspicious activity — even when malicious actors try to obfuscate their actions. First, use the Behavior Anomaly Discovery dashboard to see the users with highest risk scores across all your monitored systems, based on their cumulative risk scores from the alerts they triggered. You can see exactly what actions raised the alerts.

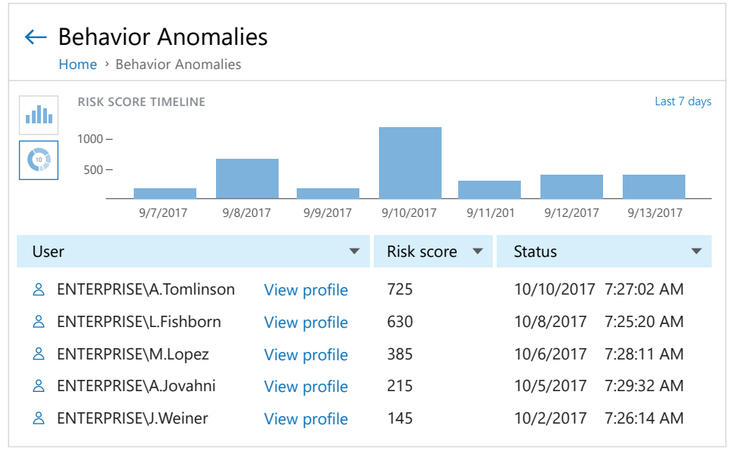
If you just recently started using Netwrix Auditor, you may find that you need to revise the original risk scores you assigned to various alerts in Step 3 in order to get the most value from this dashboard. That's normal; everyone needs to observe and experiment to figure out what values work best in their unique environment.



Spot spikes in suspicious activity

In addition to identifying risky users, you also need to watch for splashes of potentially dangerous activity across your systems, such as an unusually large number of user actions that triggered alerts on a given day.

Check the Behavior Anomaly Discovery risk score timeline daily to help ensure you detect troublesome activity early enough to prevent serious damage.



Work as a team

As you review and analyze the anomalies, use the status and comments fields to collaborate with other security specialists on your team and determine the best response to each incident.

Keep an eye out for other suspicious activity

In addition to Behavior Anomaly Discovery, be sure to take advantage of Netwrix Auditor's predefined activity reports, such as **"Potential Harmful Files – Activity"**, **"Creation of Files with Sensitive Data"** and **"All File Server Activity"**. They can further streamline incident detection and response, and the report subscription feature facilitates regular review.

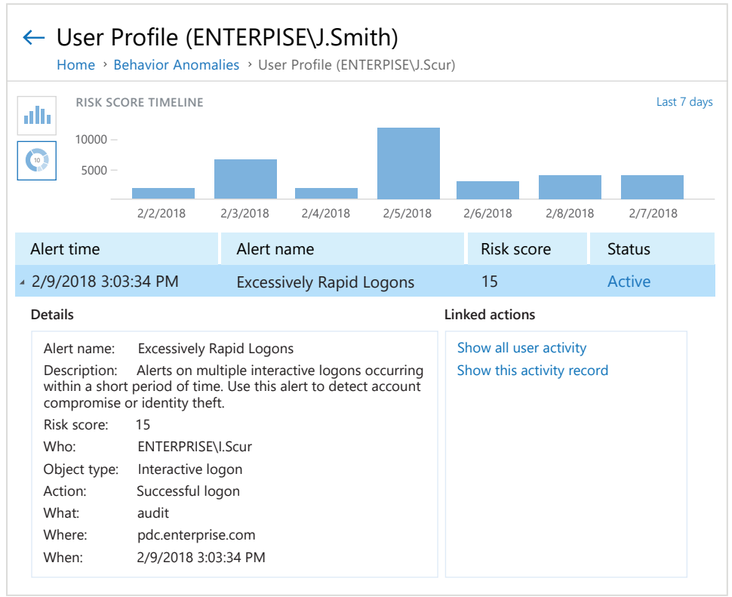
6. Investigate Incidents both Deeply and Broadly

Often, one particular event or anomaly is just the tip of the iceberg, with a broader problem hidden beneath the surface. Therefore, thorough investigation is essential to not only resolving immediate issues, but also minimizing the risk of recurrence.

Netwrix Auditor's **Interactive Search** can help you trace the entire chain of events that led to a specific problem, so you can be sure that the current matter is completely closed, hold the responsible individuals accountable, and also understand the incident in the broader context of organizational security. Even better, you can launch the Interactive Search directly from the **Behavior Anomaly Discovery** dashboard and the filtering criteria will be filled in for you.

Investigate anomalous events and actions

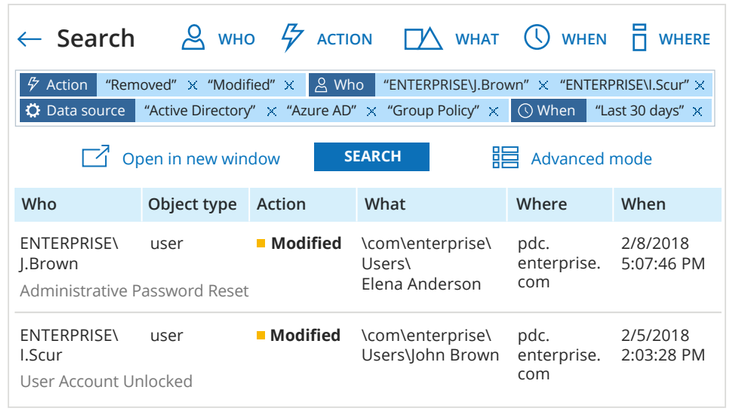
Start by investigating anomalous events and the activity of the users with highest risk scores. Simply click the "View Profile" link next to a user you want to investigate to see a list of the alerts triggered by that user; then double-click any alert record to see a detailed description of it.



Look into specific activity broadly or deeply

Next, you can use the options in the "Linked actions" section to either go broad and review all the activity of that risky user, or dig down into the action that triggered that particular alert. Clicking either link will launch the Interactive Search with the appropriate filtering criteria pre-selected, and you will be able to further investigate the user by adjusting the criteria as needed.

The Interactive Search is a powerful and very flexible instrument that simplifies your investigations. Suppose you need to see just specific kinds of actions that were performed by just two specific users across three specific systems within a given timeframe. You can do that easily do with the Interactive Search, and the findings will all be displayed in a single chart, so you won't have to jump between screen tabs or launch different applications.



Save and share the information you found

You will need to save the information you find to share with others or for formal reporting needs. Simply export your search results to a PDF or CSV file. You might also want to save specific search queries so you can use them again. You can turn any of your Interactive Search queries into a new custom report, which will be added in the Netwrix Auditor report tree. You can run or subscribe to custom reports just as you can with predefined reports.

Helpful Resources

- **Netwrix Auditor feature walkthrough videos**
  https://www.netwrix.com/netwrix_auditor_product_trainings.html

- **Netwrix Auditor Online Help Center**
  https://helpcenter.netwrix.com/Home.html

- **Netwrix Auditor product documentation**
  https://www.netwrix.com/documentation.html#guides

- **Product-related eBooks**
  https://www.netwrix.com/white_papers.html

- **"How-to" instructions**
  https://www.netwrix.com/how_to_guides.html

- **Cybersecurity best practice guides**
  https://www.netwrix.com/best_practices.html

- **How to secure Netwrix Auditor from unauthorized usage**
  https://www.netwrix.com/kb/2099

About Netwrix

Netwrix Corporation was the first vendor to introduce visibility and governance platform for on-premises, hybrid and cloud IT environments. More than 160,000 IT departments worldwide rely on Netwrix to detect insider threats on premises and in the cloud, pass compliance audits with less expense and increase productivity of IT security and operations teams. Founded in 2006, Netwrix has earned more than 100 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.

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.

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 a RESTful API and user activity video recording, the platform delivers visibility and control across all of your on-premises and cloud-based IT systems in a unified way.

For more information, visit **www.netwrix.com**

If you want to evaluate Netwrix Auditor in your environment, choose one of the deployment options below. To see Netwrix Auditor in action without having to download and install it, visit **netwrix.com/testdrive**.

On-Premises Deployment

Download a free 20-day trial

netwrix.com/go/freetrial

Virtual Appliance

Download our virtual machine image

netwrix.com/go/appliance

Cloud Deployment

Deploy Netwrix Auditor in the cloud

netwrix.com/go/cloud

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**