



Maintain high-quality public service and data integrity with Netwrix Auditor



Table of Contents

Executive summary	3
1. Reduce the risk of privilege misuse by cleaning up accounts and controlling groups and permissions	4
1.1 Reduce the risk of account misuse by keeping close track of accounts and minimizing sprawl	5
1.2 Mitigate privilege abuse by verifying groups and controlling group membership	7
1.3 Limit potential damage by implementing privilege attestation and restricting permissions	8
2. Deter aberrant behavior and streamline investigations with enterprise-wide visibility	9
2.1 Protect sensitive data by tracking activity across all your data storage locations	10
2.2 Establish proper control across your environment with flexible reporting	11
2.3 Safeguard data by promptly detecting abnormal user activity	12
2.4 Tie evidence together into a coherent whole and hold individuals accountable	13
3. Meet security mandates and excel at passing compliance audits	14
3.1 Prepare for internal audits and external examinations effectively	15
3.2 Meet auditors' expectations with far less effort	16
3.3 Minimize the complexity and stress of getting started with compliance	17
4. Meet quality service commitments and unburden your IT staff	18
4.1 Proactively troubleshoot issues and ensure uninterrupted public service	19
4.2 Deal with the information demand when IT teams are undermanned or geographically dispersed	20
Conclusion	22
About Netwrix	23

Executive Summary

Federal and regional public sector organizations have to handle many types of sensitive data as they pursue their missions to serve the general public and businesses, observe and defend citizens' rights, and improve public safety. Safeguarding that data against both internal and external threats is necessarily a high priority, but it can be a daunting challenge. In particular, IT departments in local-level agencies are often understaffed and constrained by tight budgets, while federal-level organizations usually have geographically distributed networks because they have offices and personnel scattered across the country.

In addition to protecting sensitive data, public sector organizations also need to comply with a variety of laws and regulations — which keep growing in both number and complexity as technology advances and the deluge of data accelerates. Government agencies and other public sector organizations that fail to demonstrate their compliance to regulatory authorities may have their budgets cut and be exposed to public censure.

Having a specialized technical solution can help organizations address these challenges effectively. **Netwrix Auditor** is a visibility and governance platform for hybrid cloud security that over 700 public sector organizations worldwide already use to minimize risks to their sensitive information and successfully pass regulatory audits. You can, too.

This eBook details how Netwrix Auditor can help your government organization become more resilient to the cyber threats that endanger the **highly sensitive information** that the public entrusts you with — and also help you prepare for and successfully pass regulatory compliance audits. Specifically, this eBook will answer the following critical questions:

- How can you reduce the risk of privilege misuse when you must deal with multiple contractors, temporary projects and numerous employees?
- How can you honor your commitments and obligations to citizens by quickly identifying malicious attacks that threaten data integrity?
- How can you cut the time and effort required to prepare for and pass regulatory audits?
- How can you deliver better services to citizens and your own employees by making your IT processes more efficient?

1. Reduce the risk of privilege misuse by cleaning up accounts and controlling groups and permissions

Government agencies and other public sector organizations frequently interact with contractors, suppliers and other third parties. In addition, temporary staff members are often involved in projects. As a result, user accounts, groups, group membership and permissions can very quickly fall into disarray — increasing the risk of unauthorized data access and data manipulation and impairing your threat detection capabilities. For example, if accounts are not promptly disabled, your past contractors may still be able to use their login credentials or share them with other parties, like their own sub-contractors, who aren't supposed to directly access your protected resources. Without proper monitoring, accountability and control over accounts, groups and permissions, you may not know about account misuse, privilege abuse and data integrity breaks until it's too late and you find yourself in a situation you'd rather not be in.

Netwrix Auditor simplifies the task of keeping user and computer accounts, groups, group membership and permissions properly configured, and it also makes it easy to track any activity related to them. The product provides comprehensive reporting that enables you to maintain a clean environment, identify potential security holes and quickly detect malicious activity.



Cleaning up user accounts, verifying user permissions and closing security gaps is a monumental task. Netwrix Auditor makes it far easier. It can trace down issues; it tells us who has access and who doesn't; and it lets us know when access permissions may have changed.



1.1 Reduce the risk of account misuse by keeping close track of accounts and minimizing sprawl

Allowing user accounts of uncertain purpose to linger in your environment creates opportunities for imposters to break into your network. Of particular concern are people who are familiar with your network, such as former employees (including power users and administrators), contractors and partners. Netwrix Auditor helps you reduce these risks by reporting on all enabled and disabled accounts with critical details like path, status and last logon time, so you can clean up unneeded accounts and prevent their misuse. You can also check the state of user accounts at any particular moment in the past by choosing a historical snapshot.

User Accounts

Shows user accounts, their paths, logon names, statuses (enabled or disabled), and last logon time.

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	23/10/2016 7:56:44 AM
\\com\enterprise \Users\Anna Watson	Anna Watson	A.Watson	Enabled	28/11/2016 10:12:32 AM
\\com\enterprise \Users\Administrator	Administrator	Administrator	Disabled	30/09/2016 11:05:17 AM

In addition, Netwrix Auditor keeps you aware when accounts become dormant. You will receive detailed alerts based on the inactivity criteria that you configure. Netwrix Auditor even spares you the work of manually dealing with the accounts: It can automatically disable inactive accounts, assign them random passwords, move them to a designated OU or delete them.

Inactive Users in Active Directory Report

The following accounts are no longer active:

Account Name	Account Type	E-Mail	Inactivity Time	Account Age
A.Kowalski	User	A.Kowalski@enterprise.com	33 day(s)	307 day(s)
S.Parker	User	S.Parker@enterprise.com	37 day(s)	311 day(s)
D.Lopez	User	D.Lopez@enterprise.com	40 day(s)	77 day(s)
R002312	User	None	21 day(s)	400 day(s)

Certain types of user activity are red flags that someone might be attempting to corrupt or steal data or otherwise inflict damage. Keeping a close eye on specific indicators of account misuse can help you identify such misuse and policy violations promptly. Netwrix Auditor provides predefined reports like Temporary User Accounts and Recently Enabled Accounts to help you see those indicators.

Temporary User Accounts

Shows user accounts that were deleted soon after they were created in on-premises Active Directory or Azure AD. Use this report to detect intruders attempting to hide malicious activity.

Object Path	When Created	Who Created	When Removed	When Removed	Actions on User
\com\enterprise \Users\William Lewis User Name: W.Lewis	9/28/2016 1:00:16 PM	ENTERPRISE \T.Simpson	9/28/2016 4:30:12 PM	ENTERPRISE \T.Simpson	4
\com\enterprise \Users\Adam Jets User Name: A.Jets	9/28/2016 1:01:38 PM	ENTERPRISE \T.Simpson	9/28/2016 4:30:05 PM	ENTERPRISE \T.Simpson	7
\com\enterprise \Users\Alan Tompson User Name: A.Tompson	9/28/2016 1:00:55 PM	ENTERPRISE \T.Simpson	9/28/2016 4:30:21 PM	ENTERPRISE \T.Simpson	5

Any unwarranted changes to an account's status can be a sign of malicious attempts to use it for sabotage or other abusive activity. Netwrix Auditor enables you to stay current on any such changes with the User Account Status Changes report.

User Account Status Changes

Shows changes to user accounts status (enabled, disabled, locked, unlocked).

Total Count: 32

Who: ENTERPRISE\DC1\$

Action	What	When
Locked Domain Controller: dc1.enterprise.com Workstation: WIN-46OJH7MQNFT	\Enterprise\Users\Domain Admins	8/22/2016 1:13:26 PM
Locked Domain Controller: dc1.enterprise.com Workstation: WIN-74HTEGDHOYE	\com\enterprise\Users\Guest	10/14/2016 3:36:00 PM
Enabled Domain Controller: dc1.enterprise.com	\com\enterprise\Users\Gabriel Molls	8/29/2016 5:47:26 PM

1.2 Mitigate privilege abuse by verifying groups and controlling group membership

In large or dynamic environments, groups and group membership can easily get messy. This can hurt the productivity of end users because they might not be able to access resources they need, and it can also negatively impact security, because some people might be able to access resources they should not be able to use. Netwrix Auditor helps you improve Active Directory hygiene by making routine review and validation of groups and group membership much easier with reports like Effective Group Membership and Administrative Group Members.

Effective Group Membership

Lists user and computer accounts that belong to a specified group, the status (enabled, disabled) for each account, and whether the account was explicitly named as a member of the group or was included implicitly through group membership.

Name	Member Through	Type	Status
Administrator	Explicit	user	Disabled
Anna Kowalski	Explicit	user	Disabled
Anna Watson	Explicit	user	Enabled
Danny Johnson	Explicit	user	Enabled
Elena Anderson	Explicit	user	Enabled
Garry Brown	Explicit	user	Disabled

Certain changes to privileged groups signal a very likely threat to the safety of your sensitive data. In particular, it is unusual for a user account to be deleted soon after it was created and added to privileged groups; this can indicate a rogue employee or an outsider trying to obtain extended privileges and cover their tracks. Netwrix Auditor enables you to spot such threats with the Temporary Users in Privileged Groups report.

Temporary Users in Privileged Groups

Shows user accounts deleted soon after they were created and added to privileged groups, such as Domain Admins, Enterprise Admins, Schema Admins, Account Operators, and other groups you specified. Use this report to detect intruders attempting to hide malicious activity.

Name	When Created	Who Created	When Removed	Who Removed
enterprise.com /Garry Smith	1/12/2016 1:27:58 AM	ENTERPRIS \J.Carter	1/12/2016 1:29:34 AM	ENTERPRIS \J.Carter
Group Name: \com\enterprise\Users\Domain Admins				
enterprise.com /Richard Smith	1/12/2016 1:30:13 AM	ENTERPRIS \J.Carter	1/12/2016 1:32:42 AM	ENTERPRIS \J.Carter
Group Name: \com\enterprise\Users\Domain Admins				

1.3 Limit potential damage by implementing privilege attestation and restricting permissions

Two important security best practices that too many public sector organizations fail to follow are the temporary assignment of high-level permissions, and delegation of access rights based on a least-privilege model and in accordance with segregation of duties. This puts sensitive data at increased risk of disclosure or destruction. Netwrix Auditor helps you keep your access policies under tight control by making it easy to find users with excessive access permissions.

Excessive Access Permissions

Shows accounts with permissions for infrequently accessed files and folders.

Object: \\fs1\Elected Officials (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

Putting permissions back in order should be a continuous process because users can change seats in an organization, projects start and end, and sensitive data can migrate from one resource to another. Many organizations fail to settle into this important routine because of inefficient processes or lack of technical capabilities. Netwrix Auditor provides an easy way to see who can access specific sensitive shares and folders, what permissions those users have, and whether their access rights were inherited or explicitly assigned. Historic snapshots enable you to see permissions at a particular moment in the past and compare them with the current setup or your established baselines.

Object Permissions by Object

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

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

Account	Permissions	Means Granted
ENTERPRISE\A.Kowalski	Full Control	Group
ENTERPRISE\A.Watson	Full Control	Group
ENTERPRISE\Administrator	Full Control	Group
ENTERPRISE\G.Brown	Full Control	Group
ENTERPRISE\J.Carter	Read (Execute, List folder content)	Directly
ENTERPRISE\P.Anderson	Full Control	Group
ENTERPRISE\T.Simpson	Full Control	Directly

2. Deter aberrant behavior and streamline investigations with enterprise-wide visibility

Government agencies and other public sector organizations have to maintain the integrity and privacy of data belonging to citizens, since disclosure of such information could jeopardize someone's ability to be hired for job, impact someone's health or private life, or even endanger public safety. Having 360-degree visibility into what happens in your IT environment and being able to produce a record of employee activity are critical to identifying, measuring and minimizing risks to your highly sensitive data.

Netwrix Auditor offers an extensive feature set to help you see everything happening across the core systems in your organization, establish user accountability, investigate incidents and assess risks. The intelligence that the platform provides is easy-to-read, consistent and full of details, which enables you to get to the what you need quickly. In particular, the User Behavior and Blind Spot Analysis reports simplify the task of detecting potentially malicious user behavior and weaknesses in your data protection, enabling you to be proactive in addressing known and unknown security threats.

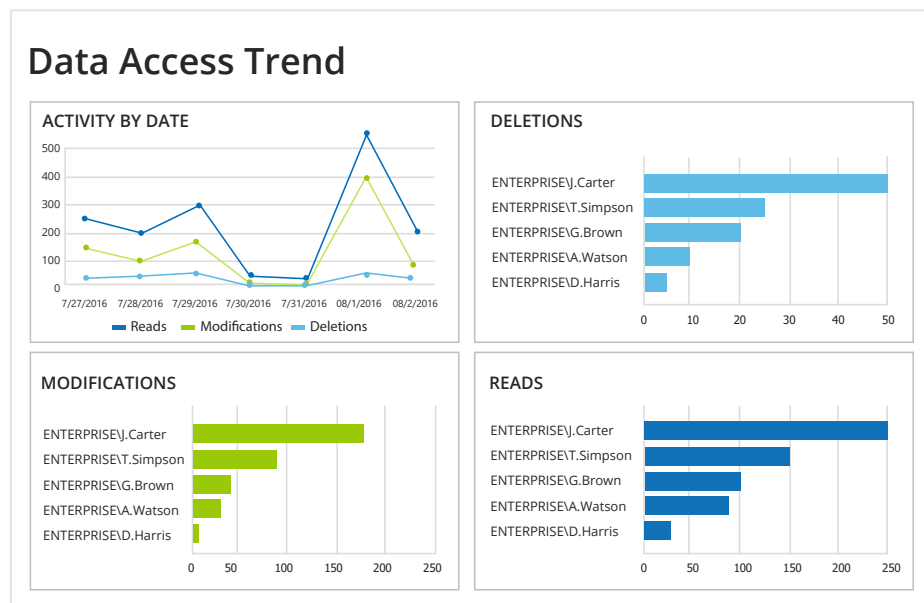


Netwrix Auditor has a winning combination of features to look after privileged users. We benefit from video recording capabilities to monitor user activity on specific servers and can immediately find and resolve issues attributed to user configuration errors.



2.1 Protect sensitive data by tracking activity across all your data storage locations

As a provider of governmental services, you have to ensure that the data citizens entrust you with is accurate and is not changed while in rest or in motion. Therefore, you need to be able to catch signs of active threats. Netwrix Auditor provides predefined reports and overview dashboards with security analytics about what's happening with your sensitive file shares and structured data repositories.



Data deletions are potential incidents, any way you slice it. These events need your immediate attention because they can mean an active breach or malware infection is in progress; they can hinder employees from doing their jobs; and they can definitely become hiccups along the way to compliance. Netwrix Auditor provides reports that help you stay aware of any deletions of data from your file systems and SQL and Oracle databases. Other reports help you keep an eye on data modifications and additions so you can ensure that sensitive data is not processed outside of proper workflows.

Files and Folders Deleted

Shows removed files and folders with their attributes.

Action	Object Type	What	Who	When
Removed	File	\\fs1\Contractors \Projects\ConstructionPlans.rtf	ENTERPRISE\ J.Carter	7/18/2016 5:02:02 PM
Removed	File	\\fs1\Suppliers\Payments \WesternCapital.rtf	ENTERPRISE\ J.Carter	7/18/2016 5:02:03 PM
Removed	File	\\fs1\Budgets\Statistics \Forecast_spring_03.01.2016.xlsx	ENTERPRISE\ J.Carter	7/18/2016 5:02:04 PM

2.2 Establish proper control across your environment with flexible reporting

Certain areas in your environment require constant vigilance. Netwrix Auditor simplifies the task of establishing proper control over the most critical elements of your IT infrastructure by providing organization level reports. It is easy to filter these reports by activity type, user, IT system, object or time frame. This flexibility allows you to be efficient in detecting vulnerabilities in your defenses, policy violations, account misuse and other activities you want to be aware of.

All Activity with Review Status

Action	Object Type	What	Who	When
■ Modify	computer	\com\enterprise\Computers \WIN-JH0E07LUN83	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

Failed actions need your thorough review as they can be the result of improper user behavior or automated attacks. Netwrix Auditor helps you safeguard your valuable data by providing visibility into any failed attempts to access, alter, copy or remove data on your protected databases and network drives. The overview dashboards help you quickly see failed activity trends, and predefined reports provide valuable details about all questionable activities detected on your network.

Failed Activity Trend

Date: 8/2/2016 (Attempts: 90)

Who	Attempts
ENTERPRISE\D.Harris	78
ENTERPRISE\G.Brown	7

2.3 Safeguard data by promptly detecting abnormal user activity

The inability to analyze behavior for signs of illicit actions creates opportunities for cyber adversaries to corrupt your systems and acquire your sensitive data. Netwrix Auditor helps you close this security gap by providing a set of security analytics reports that help you spot threats in your environment, such as activity surges, signs of identity theft and potentially malicious files. For instance, you can see how active users are, who is active outside of business hours, who tries to log in from multiple endpoints within a short time period and much more.

User Activity Summary

Shows the most active users. Use this report to detect suspicious user activity such as high numbers of failed access attempts or file reads.

Who	Changes	Reads	Failed Attempts	Deletions
ENTERPRISEJ.Carter	0	12	0	1
ENTERPRISEM.Spenser	0	18	0	0
ENTERPRISEV.Ramirez	4	20	1	0
ENTERPRISEY.Chong	124	346	569	134
ENTERPRISEI.Franko	5	19	1	1

Attackers or rogue employees — as well as employees who are simply gullible or insufficiently trained — can add and run executables of rootkits, viruses and other malicious software. Netwrix Auditor enables you to be proactive in detecting these dangerous files that shouldn't sit on your drives, and helps you track any actions related to them with the Potentially Harmful Files on File Shares and Potentially Harmful Files — Activity reports.

Potentially Harmful Files – Activity

Shows the creation, modification, and deletion of potentially harmful files, such as executables, installers, scripts, and registry keys on your file shares and SharePoint sites.

Audited System: File Servers

Action	What	Who	When
■ Read	\\fs1\shared\Dev\isass.inf	ENTERPRISEJ.Carter	08/26/2016 6:31:59 AM
■ Added	\\fs1\shared\Managers\nvcpl.exe	ENTERPRISEI.Simpson	08/24/2016 2:56:49 PM
■ Read	\\fs1\shared\Managers\nvcpl.exe	ENTERPRISEI.Simpson	08/23/2016 3:10:45 PM

2.4 Tie evidence together into a coherent whole and hold individuals accountable

When you detect suspicious events that might jeopardize the security of your sensitive data, you need to examine those events from every angle with as much relevant context as possible so you can respond properly. Netwrix Auditor eliminates blind spots and overcomes the problem of fragmented visibility. It provides a powerful search engine that facilitates the process of determining the true scope and seriousness of an issue.

← Search
WHO
ACTION
WHAT
WHEN
WHERE

⚙ Audited system
“Oracle Database” x
“SQL Server” x
Admin

SEARCH

Who	Object type	Action	What	Where	When
ENTERPRISE\ J.Carter	Login	■ Modified	Security\Logins\ [Enterprise]\J.Carter]	sql1. enterprise.com	11/7/2016 03:50:04 AM
Server Roles: - Added: “securityadmin;serveradmin;setupadmin;processadmin”					
ENTERPRISE\ J.Carter	Server Role	■ Modified	Security\Server Roles\ serveradmin	sql1. enterprise.com	11/7/2016 03:50:04 AM
Role Members: - Removed: “ENTERPRISE\Simpson”					

Securing your systems, applications and data requires keeping your business users, highly privileged IT staff and contractors accountable for their actions. Netwrix Auditor can capture the screen activity of users in any applications, including those that do not generate logs. This capability helps you deter abusive insider activity, detect unauthorized actions and improve accountability.

Activity Records

Generate a summary of video records

Date 9/25/2016

Computer	User	Start Time	End Time	Duration
dc1.enterprise.com	ENTERPRISE\J.Smith	9/25/2016 4:12 PM	9/25/2016 4:17 PM	00:05:15
dc1.enterprise.com	ENTERPRISE\J.Smith	9/25/2016 5:12 PM	9/25/2016 5:13 PM	00:01:15

3. Meet security mandates and excel at passing compliance audits

Government agencies and other public sector companies need to ensure data integrity — and they also need to be able to demonstrate the maturity and adequacy of their data protection programs and processes to regulators. Compliance auditors nearly always require demonstrating security policies in action and are rarely satisfied with a simple declaration of your commitments. Without proper tools, providing evidence of compliance can be quite taxing and time consuming.

Netwrix Auditor helps IT staff respond more efficiently to questions from auditors' checklists by enabling the vigilance required to manage risks to sensitive data. It provides extensive compliance reports out of the box, along with a variety of additional compliance features. As a result, IT staff can be more effective, both when they prepare evidence of compliance before audits and during the actual evaluation periods. This results in faster and less painful checks and improved scores with regulators.



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.



3.1 Prepare for internal audits and external examinations effectively

Regulations place a wide range of requirements on organizations in the public sector, and you have to be prepared for a full-blown attestation. In fact, more often than not, the next assessors' visit seems to be right around the corner. Netwrix Auditor simplifies the task of preparing for approaching audits, making it a less time-consuming and stressful process. The Interactive Search feature can help you create custom reports that answer potential questions in your auditors' checklists, and you can save those reports for immediate access during actual assessments.

← Search
WHO
ACTION
WHAT
WHERE
WHEN

⚙ Object type "Group" ×
🕒 When "Last 30 days" ×

SEARCH

Who	Object type	Action	What	Where	When
T.Simpson@enterprise.onmicrosoft.com	Group	■ Added	HR	https://enterprise.sharepoint.com/sites/PRportal	9/22/2016 4:55:47 PM
J.Carter@enterprise.onmicrosoft.com	Role Group	■ Modified	Organization Management	BL2PR19MB0835	9/21/2016 3:15:51 PM
Members: - Added: "T.Simpson@enterprise.onmicrosoft.com"					
A.Anderson@enterprise.onmicrosoft.com	Group	■ Removed	Guests	https://enterprise.sharepoint.com/sites/PRportal	9/21/2016 1:51:42 PM

3.2 Meet auditors' expectations with far less effort

Failing audits can flag your organization for more in-depth assessments later. To help you avoid this, Netwrix Auditor offers you a wide variety of compliance features that can help you effectively tackle many of the specific requirements that your organization is subject to. For instance, the FISMA compliance report pack includes multiple security reports that help you demonstrate that you continuously monitor that your security principles and policies are observed, and that you have taken adequate measures to ensure data integrity and privacy.

The screenshot shows the 'Reports' section of the Netwrix Auditor interface. At the top, there are buttons for 'ALL REPORTS' and 'COMPLIANCE'. Below is a search bar. A list of compliance categories is shown, with 'FISMA/NIST Compliance' expanded to show sub-items: 'Activity Outside Business Hours' and 'Administrative Group Membership Changes' (which is highlighted).

Demonstrate to auditors that your Information Security team members and other appropriate staff stay updated with security intelligence on a regular basis through subscriptions to scheduled reports and email alerts.

The screenshot shows the 'Subscriptions' page in Netwrix Auditor. It features a search bar and a table of active subscriptions. The table has four columns: Name, Status, Recipients, and Report Name. Each row includes a 'Deliver every' frequency and edit/delete icons.

Name	Status	Recipients	Report Name
John Morgan's security report Deliver every day	<input checked="" type="checkbox"/> Enabled	J.Morgan@enterprise.com	Security Group Membership Changes
Subscription to the 'All Account Changes' report Deliver every day	<input checked="" type="checkbox"/> Enabled	D.Harris@enterprise.com	User Account Changes
Subscription to 'All Active Directory Changes by User' report Deliver every 1 day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec	<input checked="" type="checkbox"/> Enabled	K.Cooper@enterprise.com	All Active Directory Changes by User

3.3 Minimize the complexity and stress of getting started with compliance

Netwrix Auditor can help you make your security program more solid right as you begin building it by telling you how to address the complex regulatory requirements you face. The product provides out-of-the-box compliance reports that help you ensure you implement the necessary controls, and Netwrix provides easy-to-understand information about best practices for meeting specific requirements.

Mapping of Processes and Report Categories to NIST Controls

Based on NIST Special Publication 800-53 rev.4

§ 164.308 Administrative safeguards. (HIPAA Security Rule)

Control	How to Comply?	Processes and Report Categories
AC-1 Access Control Policy and Procedures	Netwrix Auditor is designed to assist with establishment of organization-defined Access Control procedures.	ACCESS CONTROL Policy States Policy Changes
AC-2 Account Management	Audit information system accounts for compliance with organization-defined procedures and conditions.	ACCOUNT MANAGEMENT Account Changes Account States
AC-3 Access Enforcement	Audit authorization and access procedures for discrepancies.	ACCESS CONTROL System Access Data Access
AC-5 Separation of Duties	Monitor activities and verify that only the authorized individuals can use information systems.	ACCESS CONTROL System Access ACCOUNT MANAGEMENT Account States
AC-6 Least Privilege	Validate that only users and processes necessary for accomplishing assigned tasks in accordance with organizational missions and business functions are present in information systems.	ACCESS CONTROL Group Membership States Group Membership Changes ACCOUNT MANAGEMENT Account States
AC-7 Unsuccessful Logon Attempts	Audit failed logon activities.	ACCESS CONTROL System Access
AC-8 System Use Notification	Utilize User Activity Video Recording custom notification feature.	INTEGRITY MONITORING User Activity

4. Meet quality service commitments and unburden your IT staff

Understaffed IT teams are common in public companies. Often, these undermanned groups have to ensure normal business operations for a large number of internal departments and personnel across geographically distributed office locations. Addressing these challenges effectively is critical to the consistent delivery of high-quality services to citizens and internal workers.

Netwrix Auditor dramatically enhances efficiency across different IT silos. IT staff can proactively detect critical system configuration changes, user password changes, account lockouts, account expirations and other issues that could interfere with daily operations. The detailed information that Netwrix Auditor provides simplifies troubleshooting, while various specific features help reduce the number of submitted tickets. Plus, the tool allows heads of other departments to take on some functions themselves, relieving IT staff.



Because our admin team is distributed all over the country, staying on top of all admin activity has always been an issue for us. Netwrix Auditor relieves us greatly by giving us the visibility we need. For instance, when our admin in Portland, Oregon, makes some critical Active Directory changes, we quickly find out about it here at the main office.



4.1 Proactively troubleshoot issues and ensure uninterrupted public service

IT staff who have to wear multiple hats and support a large number of users can soon get overwhelmed, which eventually affects the quality of service. The pity is that much of their work could be automated or streamlined with the right tools, but too often that investment is last on the priority list. Netwrix Auditor provides a variety of state-in-time and change reports that enable IT administrators to address user issues proactively. For example, they can see which user accounts have become locked or expired, so they can tackle the problem before users even have a reason to submit a support ticket.

User Accounts - Locked

Shows locked user accounts, their paths and logon names.

Total Count: 3

Object Path	Name	Logon Name
\com\enterprise\Inactive Users\Alex Terry	Alex Terry	A.Terry
\com\enterprise\Inactive Users\Andrew Wiggin	Andrew Wiggin	A.Wiggin
\com\enterprise\Inactive Users\Mike Harris	Mike Harris	M.Harris

Administrators can prevent business disruptions by keeping up with user accounts whose passwords are about to expire. The Netwrix Auditor report provides all the necessary details. Netwrix Auditor can also reduce the number of helpdesk calls by automatically notifying users that they need to reset their passwords in X number of days.

Password Expiration Report

Passwords and accounts of the following users are about to expire:

User name	Email	Expires in
A.Wiggin	A.Wiggin@enterprise.com;	4 day(s): password
D.Galaher	D.Galaher@enterprise.com;	4 day(s): password
K.Miller	K.Miller@enterprise.com;	4 day(s): password
N.Key	N.Key@enterprise.com;	4 day(s): password
T.Allen	T.Allen@enterprise.com;	4 day(s): password

4.2 Deal with the information demand when IT teams are undermanned or geographically dispersed

Controlling the problems that often result from administrative activity when administrators are separated by distance or even different time zones can be difficult. Netwrix Auditor enables you to keep abreast of what power users do within specific time frames. You can run the required reports on demand or subscribe to them and receive detailed information via email on the schedule you choose. Report filtering options make it easy to narrow the scope of reports to just what's of interest to you.

All Active Directory Changes by User

Shows all Active Directory changes grouped by the user who made the changes.

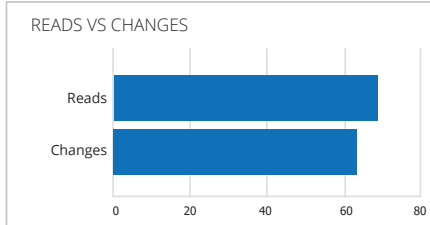
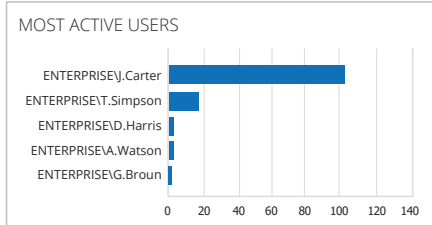
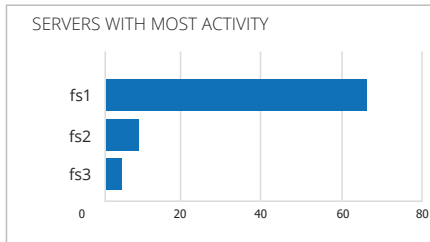
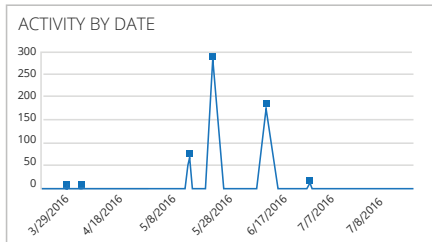
Who: ENTERPRISE\J.Carter

Action	Object Type	What	When
■ Removed Where: dc1.enterprise.com Workstation: 172.17.6.56	User	\Enterprise\Users\John Smith	8/16/2015 12:40:54 PM
■ Modified Where: dc1.enterprise.com Workstation: 172.17.6.56 Security Global Group Member: <ul style="list-style-type: none"> • Added: "\Enterprise\Users\Harry Johnson" 	Group	\Enterprise\Users\Managers	8/16/2015 12:45:11 PM

Non-IT managers are often concerned with data integrity or abnormal activity in the areas they are responsible for. If your IT team is not big enough to always perform that control for them, you can let those managers do the reviews themselves. Heads of departments can be subscribed to the Overview Dashboards or any other reports to enable them to track the things they care about daily, weekly or according to other specific schedule, so they keep abreast of critical events in a timely fashion. Alternatively, managers can be given full access to the information via the Netwrix Auditor client.

File Servers Overview

Shows consolidated statistics on all activity across all audited file servers in the specified time period.



Conclusion

Most IT teams in the public sector face a common set of serious challenges: lack of budget to hire more staff, a large number of internal and external business users to support, multiple office locations, and strict requirements for data confidentiality mandated by numerous laws and enforced by regulatory bodies. As a result, despite their expertise and dedication, they are often overworked, which can eventually start affecting the quality of service they provide to internal and external customers, the security of organizational resources, and even public safety.

By automating and optimizing IT processes, you can address all of these challenges. Netwrix Auditor can streamline IT workflows across your multiple silos and lift significant burdens from the shoulders of IT staff. Many government agencies and public sector businesses around the world already rely on Netwrix Auditor to minimize risks to their sensitive information and help them successfully pass regulatory audits.

With Netwrix Auditor, you can easily collect and consolidate audit data from all the critical systems across your IT organization, both on premises and in the cloud. You don't have to pore through multiple logs and try to piece together disparate and incomplete data: Netwrix Auditor provides actionable information in easy-to-understand dashboards and comprehensive reports, so you can easily detect both vulnerabilities in your environment and threats in progress, and respond quickly and effectively. It simplifies investigations with the powerful capabilities of its Interactive Search. Moreover, Netwrix Auditor slashes the time and effort required to prepare for regulatory compliance audits and helps you pass them with flying colors.

We invite you to learn more — including how you can get Netwrix Auditor up and running in your environment in just 15 minutes — at www.netwrix.com




About Netwrix

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

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 or cloud-based IT systems in a unified way.

For more information, visit www.netwrix.com

 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 NetwrixAuditor in the Cloud netwrix.com/go/cloud
--	---	--

Corporate Headquarters:

300 Spectrum Center Drive, Suite 1100, Irvine, CA 92618

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



netwrix.com/social