

Injecting **visibility**
into your IAM program for
greater confidence

Table of contents

Executive summary	3
1. Prior to IAM implementation	4
Understanding the challenges	4
Discovering your existing workflows	5
Revising you current workflows	7
Cleaning up Active Directory	8
2. At the IAM implementation stage	11
Controlling integrator activities	11
Gaining visibility into IAM results so you can improve them	13
Ensuring regulatory compliance	15
3. After IAM implementation	18
Improving security by quickly detecting threats	18
Streamlining preparation for audits	19
Improving data governance	20
Maximizing the value of security investments	20
Ensuring secure, cost-effective storage of audit data for years	21
About Netwrix	22

Executive summary

Many organizations today are making heavy investments in identity and access management (IAM) technologies. IAM tools promise to not only improve information security, but also optimize workflows, reduce errors and even deliver cost savings.

But an IAM rollout, like almost any other project of similar scale, is not without serious challenges, and the inability to address those challenges proactively and effectively is the main reason why these projects are so often a failure.

This eBook explains a number of critical challenges that organizations commonly face during the planning and implementation stages of an IAM project, and details how gaining visibility into your critical systems using Netwrix Auditor can help you tackle them effectively and keep your IAM project on track. Specifically, you will learn:

- How lack of visibility into your existing processes and environment puts your IAM program at risk, and exactly what insights Netwrix Auditor delivers to reduce these risks
- Why a clean directory is vital for a successful IAM implementation, and how Netwrix Auditor delivers the actionable information you need to clean it up
- Why you have to be especially watchful shortly after initial IAM implementation, and how Netwrix Auditor's out-of-the-box reports can help you spot threats you might otherwise miss
- How Netwrix Auditor can help you evaluate whether your IAM solution is actually doing its job and give you the information you need to fine-tune it for maximum value
- How Netwrix Auditor can help you be agile in managing situations that could otherwise put you in violation of compliance requirements

In addition, chapter 3 explains how your organization can continue to receive value from Netwrix Auditor long after you've successfully finalized your IAM implementation project by enabling you to:

- Quickly detect information security threats
- Streamline compliance processes
- Improve data governance
- Maximize the value of your other security investments
- Store your audit data for years, securely and cost effectively

1. Prior to IAM implementation

Understanding the challenges

Before you implement an IAM solution or replace your current solution with a new one, it's essential to understand your existing security and access models and bring order to your existing business processes. Even the most advanced, expensive and recognized IAM solution cannot deliver the outcomes you require if you cannot feed it clear and accurate roles and business rules. Instead, your project will almost certainly fail to meet expectations, which in turn can lead to business disruptions and even financial losses.

Why is this preparation so important? If your organization is like most, you have hundreds or thousands of users who perform a wide range of roles that require different sets of privileges. In some cases, the same individual may even hold multiple different roles, and many users' responsibilities change over time. It's critical that each person can access the resources they need to do their job, nothing more, nothing less. You probably also have multiple IT systems, and while some of them rely on Active Directory for authentication and authorization, others have their own systems for that.

Over time, all this complexity takes its toll, and organizations find that their user, administrative, service, system and guest accounts have turned into a mess that hurts both security and productivity. Many users have incorrect privileges — in fact, the same person might have access to resources they shouldn't see and, at the same time, lack access rights to resources they do need. Accounts are not deprovisioned in a timely manner, and provisioning new users is slow and inaccurate. The IT team is in no position to answer basic questions such as "Does this new user have the right privileges to do her job?", let alone the broader governance question, "Who has what privileges to access which systems, and why were those privileges granted?"

You know this; it's probably why you're investing in an IAM solution or upgrading to a new one in the first place. But setting up your new IAM solution demands that you be able to answer exactly these kinds of questions. You need to understand your current IAM workflows, establish access baselines, codify business roles and authorities, and revise access policies to meet your business requirements before you ever launch your IAM implementation project. While much of the information you need is available in the audit logs across your IT infrastructure, collecting and aggregating the data manually is feasible only in the context of a small number of IT systems and users, and cast-iron discipline will be required to handle the task even in that small-scale scenario. If your organization is any larger, you need a specialized visibility solution to achieve these critical goals and be ready to implement your IAM solution properly.

Netwrix Auditor is just such a solution. With Netwrix Auditor, prior to IAM implementation, you can:

- Discover your existing workflows and determine whether they comply with your corporate policies
- Revise your current workflows to improve both security and user productivity
- Clean up your Active Directory

Discovering your existing workflows

To set up the proper roles and business rules in your new IAM solution, you need to uncover what role models and rules you currently have in place, so you can revise and fine-tune them as you implement the new solution.

Many organizations use automated or semi-automated scripts to help with common tasks such as user provisioning and deprovisioning, changing user profiles and user privileges in their various IT systems, managing passwords, and more. However, quite often, they lack the ability to say how exactly these scripts work and what the results of their execution are. In particular, when script authors leave the company or lose interest in their scripts due to a change of seats in the organizational hierarchy, the people who inherit the scripts have problems understanding them and the ideas behind them.

Netwrix Auditor can help you track down script execution outcomes and draw a larger picture of existing workflows. It delivers complete visibility into changes, configurations and access across multiple IT systems in your environment in a unified way. Understanding how scripts change security groups, user and computer accounts, group membership, Group Policy objects (GPOs) and other directory entities becomes an easy task with Netwrix Auditor.

Security Group Changes

Shows changes to security groups (permissions, membership, descriptions, etc.), and affected parent groups.

Who: ENTERPRISE\I.Baldwyn

Action	What	Scope	When
<div> <div></div> Modified </div>	\Enterprise\Users\Domain Admins Where: dc1.enterprise.com Security Global Group Member: <ul style="list-style-type: none"> Added: "\Enterprise\Users\Ricardo Olvarez" 	Security Global Group	8/22/2016 1:13:26 PM
<div> <div></div> Modified </div>	\Enterprise\Users\Domain Admins Where: dc1.enterprise.com Security Local Group Member: <ul style="list-style-type: none"> Removed: "\Enterprise\Users\Jessie Rico" 	Security Domain Local Group	8/20/2016 4:15:41 PM

If you previously implemented an IAM solution and are now replacing it, you can benefit from the enterprise-wide visibility delivered by Netwrix Auditor in similar way. Simply use the older tool to perform a common task, such as user provisioning and access rights delegation. Netwrix Auditor will reveal exactly what alterations the solution effected in the IT environment, and you can use that information to evaluate your existing workflows, including whether they are complying your corporate policies, both logical and effective.

Security Settings Changes

Shows changes to policy settings grouped under the Security Settings node, such as Account Policies, Local Policies, and Event Log.

Action	What	Who	When
■ Modified	Default Domain Policy	ENTERPRISE\tsimpson	1/12/2017 3:27:53 PM
Where:	dc1.enterprise.com		
Path:	Computer Configuration (Enabled)/Policies/Windows Settings/ Security Settings/Account Policies/Account Lockout Policy		
Removed	Policy: Account lockout duration; Setting: 30 minutes;		
Removed	Policy: Account lockout threshold; Setting: 7 invalid logon attempts;		
Removed	Policy: Reset account lockout counter after; Setting: 30 minutes;		

Perhaps your organization has always relied on manual processes to manage users and access, and now you need to automate these processes with a new IAM solution. That requires translating every aspect of your manual procedures into a set of clear identity governance and access request management rules for the new solution. In a situation like this, mere verbal communication with your administrators is unlikely to be enough; a visual demonstration of test cases will probably be required. Netwrix Auditor will be invaluable because it can document the output of each action performed, in a form that is easy to read, analyze, store and refer back to.

Account Policy Changes

Shows changes to account policies and their settings.

Action	What	Who	When
■ Added	New group policy	ENTERPRISE\G.Graham	5/13/2017 3:46:08 PM
Where:	dc1.enterprise.com		
Path:	Computer Configuration (Enabled)/Policies/Windows Settings/ Security Settings/Account Policies/Account Lockout Policy		
Added	Policy: Account lockout duration; Setting: 30 minutes;		
Added	Policy: Account lockout threshold; Setting: 3 invalid logon attempts;		
Added	Policy: Reset account lockout counter after; Setting: 30 minutes;		
■ Modified	Default Domain Policy	ENTERPRISE\Administrator	5/13/2017 3:29:16 PM
Where:	dc1.enterprise.com		
Path:	Computer Configuration (Enabled)/Policies/Windows Settings/ Security Settings/Account Policies/Password Policy		
Modified	Policy: Password must meet complexity requirements; Setting: Enabled -> Disabled;		

In addition to providing deep visibility into changes, Netwrix Auditor also makes it far easier to verify your current configurations. It includes a number of state-in-time reports that enable you to quickly see who has access and who doesn't.

User Accounts - Group Membership

Shows user accounts, with the group membership, group path, and type (Security, Local, Global, Builtin, etc.) for each account.

User Path: \com\enterprise\Managers\Anna Watson

Group Path	Group Type
\com\enterprise\Users\Domain Admins	Security Global Group
\com\enterprise\Users\Domain Users	Security Global Group

User Path: \com\enterprise\Production\Diana Harris

Group Path	Group Type
\com\enterprise\Users\Domain Admins	Security Global Group

Revising the current workflows

Discovering your current procedures for user lifecycle management is the lion's share of preparation. However, you can also use that information to further facilitate smooth implementation of your IAM program. After all, your current situation is not necessarily the desired state. Even when account administration and access delegation are performed according to policy, they might still be far from optimal.

In particular, many organizations do not have adequate procedures for revoking access privileges. Over time, employees gradually acquire access rights, like ships grow barnacles. In two or three years, no one can really tell why users got those privileges and whether they still need them. Similarly, the accounts of employees who leave the company may not be deprovisioned in a timely manner, or at all. These shortcomings put your security at risk.

Netwrix Auditor provides the information you need to improve the efficacy and security of your workflows and policies. Based on the behavioral profiles of users, you can make recommendations for future corrections and cultivate a least-privilege access model. Netwrix Auditor can show you where too much access is provided and which of those permission were granted directly, so you can implement the best practice of granting access rights only through group membership. It also details your data usage patterns, identifies your most active users, reports on who has made failed attempts to perform specific actions, and much more.

Excessive Access Permissions

Shows accounts with permissions for infrequently accessed files and folders. Use this report for spotting unnecessary permissions and preventing data leaks. Track permissions assigned to accounts directly or by group membership.

Object: \\fs1\Circuit Layouts (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

You can also identify potential data owners by seeing which users frequently access files in a given folder. This information can also be used as a rationale for revoking the access privileges of employees who are not active in the same file repository.

Potential Data Owners by Folders

Shows users who frequently access files in a given folder. Use this report to identify factual data owners and analyze usage patterns.

Folder: \\fs1\Shared\Finance

Owner: ENTERPRISE\S.Coleman

Who	Changes	Reads
ENTERPRISE\S.Coleman	164	207
ENTERPRISE\A.Dowson	43	118
ENTERPRISE\E.Swift	4	17

Cleaning up Active Directory

Many contemporary IAM technologies are based on LDAP directories. If your directory is a mess, your new IAM solution won't be able to properly provision access and enforce proper security measures. Unfortunately, Active Directory hygiene is less than stellar at most organizations. There are often user and computer accounts and groups that were created for no apparent purpose, accounts with generic names, duplicate accounts, an unreasonably large number of administrative accounts, lingering inactive accounts, and improper group membership — all of which represent a clear risk to the security of your sensitive assets.

Before you implement your new IAM solution, you want exactly the opposite — clarity about the status, purpose and relevance of each user and computer account and user group, with all redundant entities removed or deactivated. A clean house with no mess significantly reduces the risk of running into significant problems implementing your IAM solution, and increases the ultimate value of the resulting directory-based IAM ecosystem.

Netwrix Auditor provides you with the high-quality, identity-related information you need to clean up your Active Directory. Its predefined state-in-time reports give you the information you need to clean up your group membership and user and computer accounts. Historic snapshots enable you to see the state of things at present or at a particular moment in the past.

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

A clear listing of all inactive user and computer accounts makes it easy to find obsolete accounts that can and should be removed. Even better, Netwrix Auditor can spare you the work of manually handling those accounts by automatically disabling them, assigning them random passwords, moving them to a designated OU or deleting 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)

Netwrix Auditor will also inform you of the total number of expired accounts in your directory and provide details about each one, including the path and expiration date, so you can decide whether to re-activate them or delete them.

User Accounts - Expired

Shows expired user accounts, their paths, logon names and expiration dates.

Total Count: 5

Path	Name	Logon Name	Expiration Date
com\enterprise\Inactive Users\Lisa Evans	Lisa Evans	L.Evans	11/3/2016
\com\enterprise\Inactive Users\Tom Allen	Tom Allen	T.Allen	10/15/2016
\com\enterprise\Inactive Users\Caron Hall	Caron Hall	C.Hall	8/22/2016
\com\enterprise\Inactive Users\Donald King	Donald King	D.King	7/12/2016
\com\enterprise\Inactive Users\Mark Perez	Mark Perez	M.Perez	6/18/2016

Similarly, you can use Netwrix Auditor to review your existing groups and verify group membership. Being able to retrieve this information quickly and have it in a human-readable form simplifies the otherwise monumental task of cleaning up your Active Directory. With far less time and effort, you'll be able to have an AD in which each user and computer account and group is justified by a business need, and group membership is in strict accordance with role requirements. Having this normalized Active Directory will significantly reduce the amount of work needed to define role models and access assignment rules, and will help ensure a proper implementation of identity and access management.

Group Members

Shows members of the specified groups, with the type (user, group, computer, etc.) and status (enabled or disabled) for each member.

Security Builtin Local Group: \com\enterprise\Builtin\Administrators

Member Path	Type	Status
\com\enterprise\Users\Administrator	user	Disabled
\com\enterprise\Users\Domain Admins	group	N/A
\com\enterprise\Users\Enterprise Admins	group	N/A

Security Builtin Local Group: \com\enterprise\Builtin\Guests

Member Path	Type	Status
\com\enterprise\Users\Domain Guests	group	N/A
com\enterprise\Users\Guests	user	Disabled

2. At the IAM implementation stage

Netwrix Auditor does far more than help you prepare for IAM implementation; it continues to deliver value throughout the project to help ensure its success. In particular, the solution enables you to:

- Keep a close eye on the IAM vendor staff helping you integrate the solution
- Evaluate how the new solution is performing and fine-tune it to meet your requirements
- Ensure regulatory compliance and pass audits

Controlling integrator activities

Whether you choose a full-featured IAM solution or a simpler option with limited functionality, you're likely to require system integration and consulting services from your vendor. System integrators will join your team for up to a year, helping to integrate the new components into your environment, solve automation problems, troubleshoot issues and fine-tune the new technology to accomplish the goals you set for it.

These temporary team members will need access privileges — probably even some high-level privileges. Unless you can exercise proper oversight over their activities, your sensitive corporate and customer data will be at risk throughout the project.

Netwrix Auditor provides rich auditing and investigation capabilities to keep your IAM consultants under constant vigilance. You will be alerted whenever they act against agreed-upon or implied norms. You will be able to review privileged access to systems and data with full details; analyze behavior patterns; investigate incidents; and file documented evidence if anyone steps away from their contractual assignments. This deep insight into what contractors do is vital for creating proper working conditions and establishing trust without jeopardizing security.

In particular, Netwrix Auditor enables you to capture the screen activity of privileged users in specific applications, shares, production databases and other sensitive or critical IT systems. This functionality is an effective deterrent of improper behavior: People who know they are being monitored are far more likely to act with careful consideration and follow protocols and security policies. If deviations from prescribed behavior still occur, the video records will show exactly what was done, providing the evidence you need to respond appropriately.

← Search
WHO
ACTION
WHAT
WHEN
WHERE

Data source
"User Activity (Video)"

Open in new window
SEARCH
Advanced mode

Who	Object type	Action	What	Where	When
ENTERPRISEJ.Carter	Window				
Show video...					
ENTERPRISEJ.Carter	Window				
Show video...					
ENTERPRISEJ.Carter	Window				
Show video...					
ENTERPRISEJ.Carter	Window				
Show video...					

Netwrix Auditor also enables you to keep a complete trail of what contractors do, either across your entire IT infrastructure, within a particular IT system or even within a specific part of one system. Multiple predefined reports provide detailed information about all system configuration changes, as well as all attempts to access information systems and structured or unstructured data.

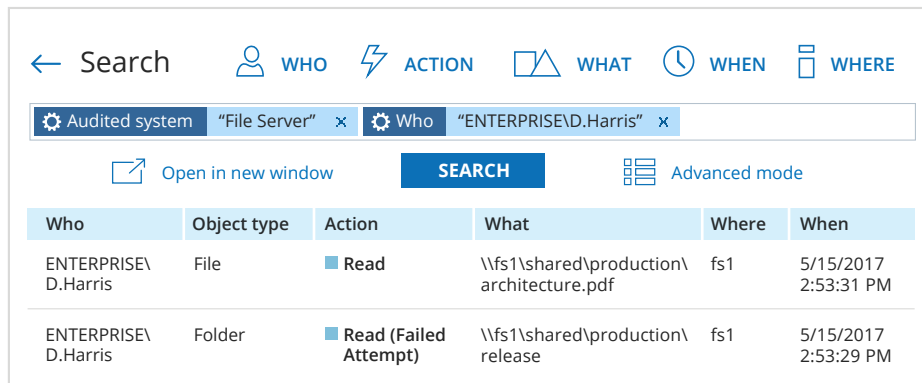
All Active Directory Changes by User

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

Who: ENTERPRISEJ.Carter

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

Netwrix Auditor facilitates investigation of incidents involving contractors by providing easy cross-system search of any activities by any actors within any time period. The simplicity of the Interactive Search GUI makes it easy to hone in on the exact audit information you need.



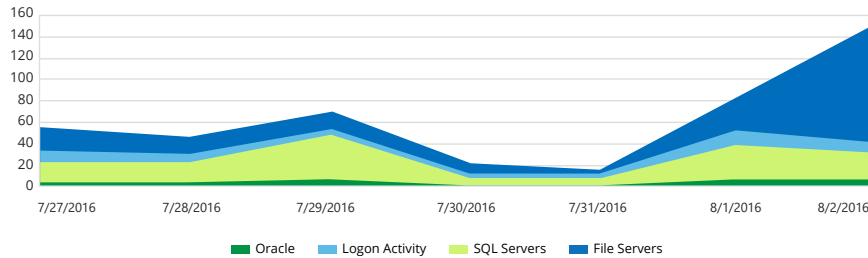
Gaining visibility into IAM results so you can improve them

To ensure security and business continuity and minimize user frustration, you need to carefully observe how your IAM solution performs for some time after implementation. Even if you were meticulous in defining roles, cleaning up your directory and improving procedures during the planning stage, you probably missed some things. You need to be able to spot instances of improper issuing and recalling of privileges, discrepancies in how business rules apply in different scenarios and other lapses of prescribed IAM functioning. And you need to be able to relate those specific activities and events to specific rules and configurations in your IAM solution. By continuously identifying and analyzing arising issues, you will be able to fine-tune your IAM tool and ensure its correct functioning.

Netwrix Auditor is a handy tool for this critical job. It enables you to see in detail into how your new IAM solution performs in every business scenario — whether it ensures proper user authentication or causes login failures; whether it grants user access based on employee job function or provides either excessive or insufficient privileges; whether Group Policy changes and new policies become effective in a timely manner; whether it launches the required scripts or delivers only user account provisioning; and so on. This deep visibility into what is actually changing in your environment upon execution of the IAM program is essential for validating that your new IAM solution is actually a benefit, rather than a security or productivity gap.

For example, a lot of failed activity might indicate the need to reconfigure IAM to grant more access privileges. The Netwrix Auditor overview dashboards visualize failed activity trends, enabling you to see how the situation changed after new IAM started functioning. You can drill down into the graph for more granular predefined reports that provide valuable details about each type of failed activity detected in your environment.

Failed Activity Trend



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

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

You can also evaluate whether your IAM solution is making logins to systems and applications easier by analyzing logon activity. You can review both successful and failed user logons using Netwrix Auditor's predefined reports and graphical dashboards.

Interactive Logons

Shows interactive logon attempts. Use this report to analyze user activity and validate compliance.

Action	What	Who	When
<div>Successful Logon</div> <div>Where: wks035.enterprise.com</div> <div>Workstation: wks035.enterprise.com</div>	wks035.enterprise.com	ENTERPRISE\T.Simpson	6/13/2017 6:27:41 PM
<div>Successful Logon</div> <div>Where: dc1.enterprise.com</div> <div>Workstation: wks076.enterprise.com</div>	wks076.enterprise.com	ENTERPRISE\J.Carter	6/13/2017 6:20:18 PM
<div>Failed Logon</div> <div>Workstation: wks061.enterprise.com</div> <div>Cause: pre-authentication information was invalid: usually means bad password. This entry represents 2 matching events occurring within 10 seconds.</div>	N/A	ENTERPRISE\P.Anderson	6/13/2017 5:59:34 PM

By reviewing changes to group membership, accounts and account policies that occurred over a specific period of time, you will get a better understanding of how your current IAM configuration settings reverberate in your environment.

Security Group Membership Changes

Shows changes to the membership of security groups.

Group name: \com\enterprise\Users\Accounting

Action	Member	Who	When
■ Added	enterprise.com/Users/George Black	ENTERPRISE\j.carter	4/25/2017 12:39:26 PM
Where:	dc1.enterprise.com		

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

Action	Member	Who	When
■ Added	enterprise.com/Users/George Black	ENTERPRISE\j.carter	4/25/2017 12:38:15 PM
Where:	dc1.enterprise.com		

Ensuring regulatory compliance

One of the primary drivers of IAM initiatives is the need to establish, maintain and demonstrate compliance with regulations and industry standards. Even organizations that are not required by law to demonstrate compliance often do so to beat the competition in the fight for customers. There's no doubt that IAM can help you achieve compliance, but until your IAM solution is fine-tuned and matured, it can make demonstrating more, rather than less, complicated a task.

In such situations, it's critical to have tools that provide visibility into and control over every aspect of your IT environment. The tool also needs to help you be agile in managing situations that could put you in violation of compliance requirements. And you need to be able to satisfy auditors by demonstrating your ability to address flaws they identify immediately. Netwrix Auditor delivers all this and more.

Netwrix Auditor features a flexible alerting mechanism that allows you to specify which events are high risk and should trigger an alert, such as changes to security groups in Active Directory, permissions in Exchange or roles in Oracle Database. These alerts enable you to respond to incidents quickly and report them in a timely manner. Moreover, alerts are available across multiple audited systems. You can also choose to turn on the threshold-based alerting if needed.

Netwrix Auditor Alert

Possible privilege abuse

Who: ENTERPRISE\J.Carter
 Action: Modified
 Object type: Farm
 Item: http://sp.enterprise.com:4755 (SharePoint farm)
 What: http://sp.enterprise.com:4755
 When: 5/3/2017 6:16:26 AM
 Where: http://sp.enterprise.com:4755
 Data source: SharePoint
 Monitoring plan: Enterprise Data Visibility Plan
 Details: Managed Accounts:
 - Added: "ENTERPRISE\T.Simpson"

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

After implementing of any major new system — and an IAM solution certainly qualifies — it's critical to pay due attention to the conduct of users, some of whom might try to take advantage of the overall disarray. The Netwrix Auditor Data Access Surges report is a good way to stay informed about users who start attempting to access data they almost never accessed before. You can easily drill down and see full details about each user's activity in your various systems.

Data Access Surges

Shows users who have accessed sensitive data they almost never accessed before (by default, the inactivity threshold is set to 2 actions). The report highlights previously inactive users who performed more actions within a short period of time (by default, 7 days) than during a considerably longer preceding period (by default, 30 days).

Path	User Name	Attempts
\\fs1\Engineering\Circuits\Utility.psd	ENTERPRISE\J.Smith	19
http://spenterprise/Documents/Projects/ConstructionBudgets.xlsx	ENTERPRISE\G.Johnson	11
\\emcfs2\HR\Contractors\NewHires2017.xlsx	ENTERPRISE\J.Rosenberg	6
http://spenterprise/Documents/PowerPlans/Research/2017.docx	ENTERPRISE\J.Rosenberg	3
\\nf1\Sales\NorthAmerica\Q12017.xlsx	ENTERPRISE\D.Harris	2

Auditors will likely be very interested in seeing what has been happening to user accounts over a certain period. Given that user accounts are in the focus of almost any IAM tool, staying in control of account changes throughout the implementation stage is a must. Netwrix Auditor enables you to stay current on any such changes with a number of reports, such as 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
<div>■ Locked</div> <div>Domain Controller: dc1.enterprise.com</div> <div>Workstation: WIN-46OJH7MQNFT</div>	\Enterprise\Users\Domain Admins	8/22/2016 1:13:26 PM
<div>■ Locked</div> <div>Domain Controller: dc1.enterprise.com</div> <div>Workstation: WIN-74HTEGDHOYE</div>	\com\enterprise\Users\Guest	10/14/2016 3:36:00 PM
<div>■ Enabled</div> <div>Domain Controller: dc1.enterprise.com</div>	\com\enterprise\Users\Gabriel Molls	8/29/2016 5:47:26 PM

3. After IAM implementation

Even after your IAM project is complete and your new solution is effectively automating your critical identity management and access provisioning processes, you will continue to reap significant value from your Netwrix Auditor investment. Read on to see how this visibility solution can help you:

- Efficiently control and mitigate modern cybersecurity risks
- Demonstrate compliance with far less time and effort
- Maximize the value of your IT security ecosystem through easy integration using a RESTful API

Netwrix Auditor is a truly unified, industry-leading visibility platform for user behavior analysis and risk mitigation. It enables you to gain visibility into what's going on in your most critical IT systems — both on-premises and in the cloud. Its easy-to-read intelligence will help you close visibility gaps, improve your breach detection capabilities, respond to cyber threats faster, and dramatically reduce the time and effort required for security and compliance processes.

Improving security by quickly detecting threats

Netwrix Auditor includes many prebuilt reports designed specifically to help you discover security incidents, attacks in progress and aberrant employee behavior in a timely manner. Here are just a few:

- Logons by Single User from Multiple Endpoints
- Activity Outside Business Hours
- Potentially Harmful Files on File Shares
- Temporary Users in Privileged Groups
- All Exchange Server Non-Owner Mailbox Access Events

Logons by Single User from Multiple Endpoints

Shows users who logged on from several endpoints within a short period of time. Such occurrences may indicate that the account's password was stolen or compromised. Use this report to detect suspicious user activity and prevent data breaches.

Who: **ENTERPRISEJ.Carter** (First Attempt: 7/27/2016 2:02:26 PM)

Endpoint	Logon Attempts
172.17.6.36	2
ENTWKS0376	6
WST055	12
192.168.1.1	1

Streamlining preparation for audits

Netwrix Auditor also features out-of-the-box compliance reports mapped to the specific provisions of FISMA/NIST, GDPR, GLBA, HIPAA, ISO/IEC 27001, PCI DSS, SOX and other regulatory mandates. These reports enable your IT staff to 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.

← Reports

ALL REPORTS

COMPLIANCE

Enter your search

Q

▸ CJS Compliance

▸ FERPA Compliance

▸ FISMA/NIST Compliance

▸ GDPR Compliance

▸ GLBA Compliance

▸ HIPAA Compliance

▾ ISO/IEC 27001 Compliance

▸ NERC CIP Compliance

Files and Folders Deleted

Security Group Membership Changes

Improving data governance

Netwrix Auditor also enables better data governance. For instance, its file analysis reports deliver detailed information on overexposed data and data ownership, data usage and data volumes, stale data, and duplicate files. These reports include:

- Empty Folders
- Files and Folders by Owners
- Potential Data Owners
- Top Owners by Total Files Size
- Largest Files
- Creation of Files with Sensitive Data
- Potentially Harmful Files

Creation of Files with Sensitive Data

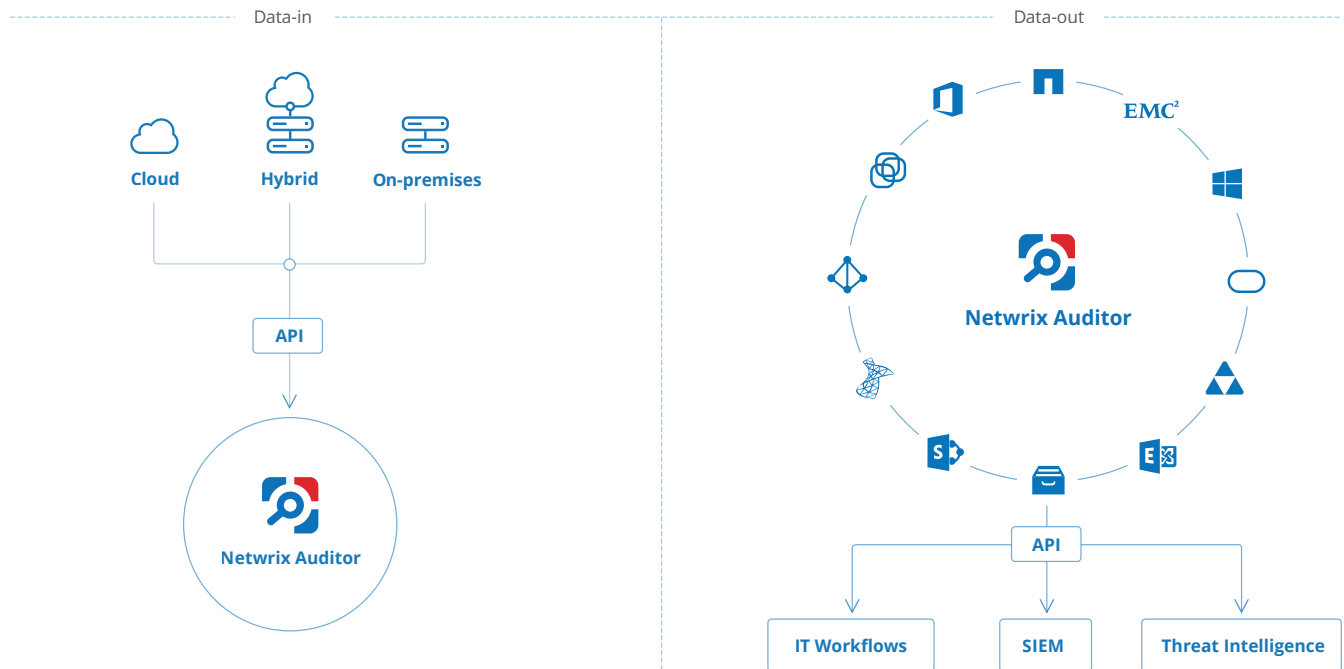
Shows users who created files with names that suggest they contain sensitive data (e.g., MyPasswords.docx). Run this report regularly to promptly identify users with files that disclose confidential data. The following words are disallowed by default: password, social security number, credit card, cardholder, payment, payroll, ssn, pwd.

What	User Name	Actions	When Created
\\fs1\Users\PASSWORDS.docx Where: fs1.enterprise.com	ENTERPRISE\ G.Brown	1	1/17/2017 7:37:18 PM
http://sharepoint/Documents/ ALL SOCIAL SECURITY NUMBERS.xlsx Where: http://sharepoint	ENTERPRISE\ D.Harris	1	1/16/2017 12:20:24 PM
\\fs1\Documents\CARDHOLDER INFO.csv Where: fs1.enterprise.com	ENTERPRISE\ T.Simpson	2	1/15/2017 3:13:09 PM

Maximizing the value of security investments

Additionally, Netwrix Auditor offers a RESTful API that enables seamless, bi-directional integration with any of your existing on-premises and cloud applications, enabling you to leverage your IT security ecosystem to the full. Both “Data-in” and “Data-out” integration scenarios are supported. A number of integration add-ons have

already been created and tested by Netwrix; they are available for free from the [Netwrix Auditor Add-on Store](#).



Ensuring secure, cost-effective storage of audit data for years

Netwrix provides a cost-effective and reliable approach to storing audit data for historical reporting, incident investigations and compliance audits. Your audit trail is simultaneously preserved in a SQL database and in a file storage in a compressed file format. This reliable two-tiered storage system ensures you can maintain proper speed of access to audit data for review during compliance checks, security investigations or troubleshooting, with no risk of increase in associated costs, while also keeping all your audit data securely and cost-effectively for 10 years or longer.



These and other Netwrix Auditor features will add a new layer of transparency across the key elements of your IT infrastructure, thereby enhancing both your organization's security posture and your ability to pass compliance audits.

About Netwrix




Netwrix Corporation was first to introduce visibility platform for user behavior analysis and risk mitigation in on-premises, hybrid and cloud IT environments. 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 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 the RESTful API and user activity video recording, the platform delivers visibility and control across all of your on-premises or cloud-based IT systems in a unified way.

More than 160,000 IT departments worldwide rely on Netwrix Auditor to detect insider threats on premises and in the cloud, pass compliance audits with less expense, and increase the productivity of IT security and operations teams.

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 200, Irvine, CA 92618

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



netwrix.com/social