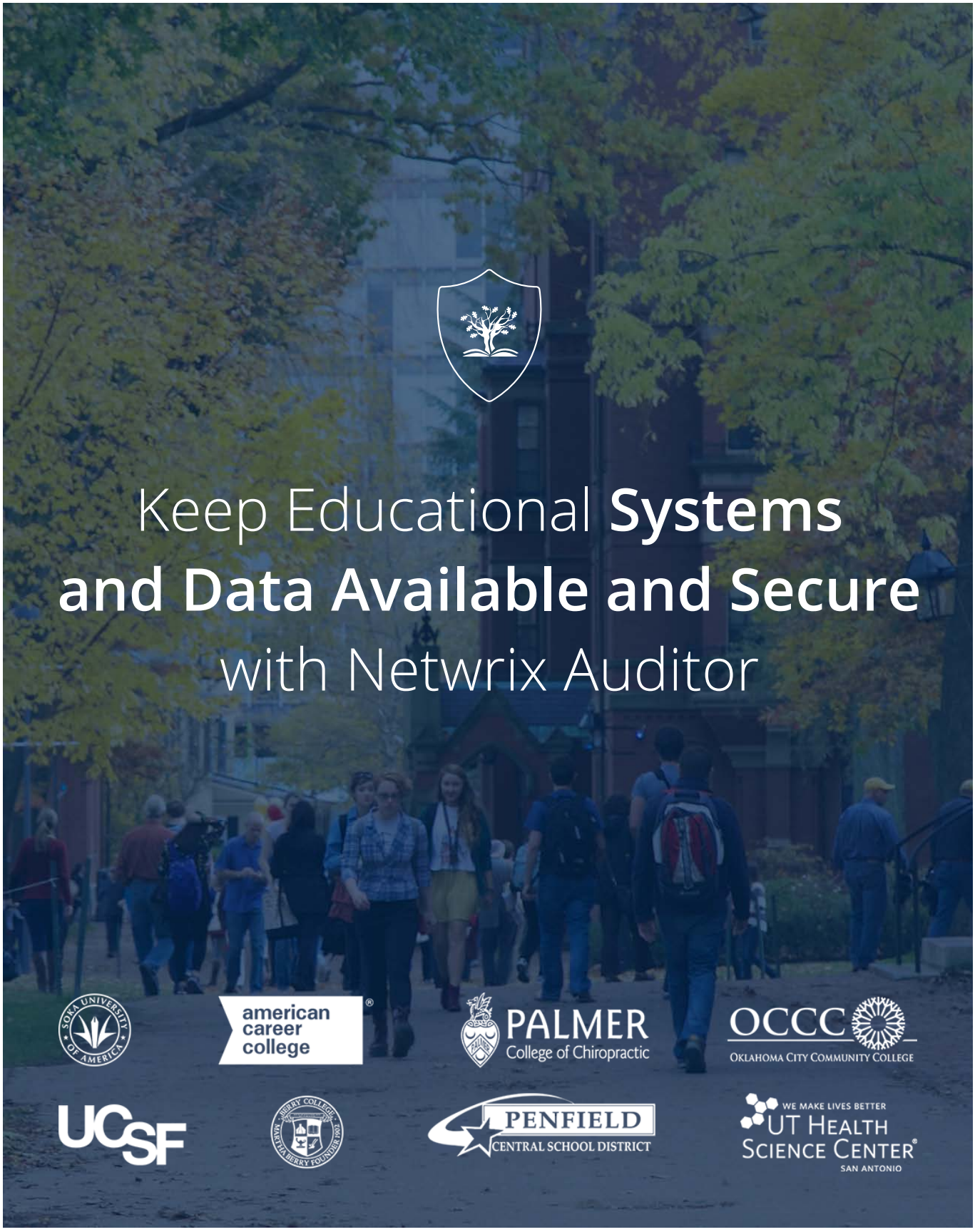
netwrix



Keep Educational **Systems and Data Available and Secure** with Netwrix Auditor

SOKA UNIVERSITY OF AMERICA

american career college

PALMER College of Chiropractic

OCCC Oklahoma City Community College

UCSF

ABERRY COLLEGE

PENFIELD CENTRAL SCHOOL DISTRICT

WE MAKE LIVES BETTER UT Health Science Center SAN ANTONIO

Table of Contents

Executive Summary

School districts, colleges, universities and other academic institutions have to handle many types of sensitive data, including students' academic records and PII. Safeguarding that data against both internal threats and external attacks is a top priority for IT departments. However, their IT teams are frequently understaffed and underfunded, while the environments they have to control are often extremely dynamic, highly populated and geographically dispersed.

In addition to protecting sensitive data, educational institutions also need to comply with FERPA, HIPAA and a variety of other laws and regulations — which keep growing in both number and complexity as technology advances and the deluge of data accelerates. An organization's inability to demonstrate compliance might not only damage their reputation and consequently their admission numbers, but also lead to fines and budget cuts.

In addition, given the important role that IT systems play in educational processes today, IT teams must also be keenly focused on ensuring ongoing system availability. An expired or locked-out account, a missing file, or an unavailable application interrupt the work of students or faculty. Repeated availability issues can lead to a bad reputation, not just for the IT department but for the educational institution in general.

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 560 K-12 and higher education organizations worldwide already use to minimize risks to their sensitive information and ensure uninterrupted educational process. You can, too.

This eBook details how Netwrix Auditor can help your educational institution become more resilient to the cyber threats that endanger the **highly sensitive information** that students entrust you with — and also help you ensure system and data availability. Specifically, the eBook answers the following critical questions:

- How can you reduce the risk of privilege misuse in a dynamic and highly populated environment?
- How can you honor your obligation to ensure the security of student data by quickly identifying insider and external attacks?
- How can you cut the time and effort required to prepare for and pass regulatory audits?
- How can you make sure that educational processes are never interrupted by maintaining system and data availability?
- How can you improve the efficiency of your IT team so they can do all this with their limited staff and budget?

1. Mitigate the insider threat by cleaning up accounts and controlling groups and permissions

Maintaining a secure and compliant IT environment in a school, college, university or other educational institution can be a challenge, even for the most experienced IT staff. Students come and go every year, and so do professors and other staff. Some are gone for only a month or two while others will never return, and the IT is usually the last to know. In these highly populated and dynamic environments, user and computer accounts, group membership, and permissions can quickly fall into disarray, diminishing your chances of detecting an active threat to your sensitive data and increasing the risk of unsanctioned information access and data manipulation. For instance, if accounts of expelled students are not disabled promptly, disgruntled pupils may still be able to use their credentials to access protected resources or their accounts might be hacked by malicious actors, putting data confidentiality, integrity and availability at risk. Without proper monitoring, accountability and control over accounts, groups and permissions, you may not know about account hijacking or privilege abuse until it's too late and you find yourself in a situation you'd rather not be in.

Netwrix Auditor makes it easy — even for understaffed IT teams — to control accounts, groups, group membership and permissions, as well as monitor any activity related to them. Comprehensive reporting functionality and alerts on threat patterns enable you to maintain a clean environment, identify potential security holes and quickly detect suspicious activity.

> Netwrix Auditor lets us see our Active Directory changes and get notifications when user and computer accounts are changed, added, removed, etc. This helped us find a security hack at one point, and due to the instant email alerts, we were able to rectify the problem immediately! This central console software solution has helped us on many occasions and gives us a great peace of mind on our security and accounts.

EMSD37
East Moline School District 37

1.1 Reduce the risk of account misuse by cleaning up your Active Directory

Educational institutions tend to have large numbers of accounts. The inability to keep track of them and control the sprawl leaves blind spots in your security that malicious actors can use to get into your environment. Of particular concern are people who are familiar with your network, such as current and former employees (including administrators and other power users) and students. 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.

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

With students coming and going every semester and many professors working on a transient basis, your Active Directory can easily get flooded with inactive accounts. Netwrix Auditor alerts you when an account has been idle for a specified number of days and also allows you to take a look at the state of user accounts at any moment in the past by choosing a historical snapshot. It can even automatically disable these inactive accounts, assign them random passwords, move them to a designated OU or delete them, saving you the trouble of dealing with them manually.

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)

1.2 Avoid abuse of excessive privileges by taking charge of groups and group membership

In large and dynamic environments where a significant number of users come and leave several times in a year, user provisioning and group membership assignment can become a huge burden for IT staff. Moreover, without proper visibility into Active Directory, it's all too easy to make mistakes that can severely hurt the productivity of end users, who might not have access to the resources required for their job, as well as overall security, because users might see and read files that they are not supposed to. Netwrix Auditor helps you tidy up your Active Directory and make it more secure by simplifying routine review and validation of groups and group membership with predefined detailed 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

You should also be on the lookout for certain changes to privileged groups that 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 one or more privileged groups; this can indicate a rogue employee or an outsider trying to obtain extended privileges and cover their tracks. In addition to reporting on all administrative group additions and removals, Netwrix Auditor also enables you to monitor threats such as temporary users in privileged groups.

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				

If an existing account is added into the Domain Admin group without proper authorization it might be a sign that someone is actively trying to corrupt or steal data or otherwise inflict damage. Netwrix Auditor enables you to stay on top of such incidents and respond quickly by providing both predefined reports and automated alerts on the most critical Active Directory changes and threat patterns.

Changes to Admin Group Membership

Severity	Critical
Domain	ENTERPRISE.COM
Change Type	Modified
Object Type	Group
When Changed	18/2/2016 4:58:53 AM
Who Changed	ENTERPRISE\Administrator
Where Changed	dc1.enterprise.com
Object Name	Enterprise\Users\Domain Admins
Details	Security Global Group Member: • Added: "Enterprise\Users\Nick Key"

1.3 Tighten up file server permissions and limit your attack surface

Many educational institutions fail to follow a critical security best practice: delegation of access rights based on a least-privilege model and in accordance with segregation of duties. This failure puts sensitive data at increased risk of disclosure or destruction by the insiders, and it also increases the potential damage from ransomware and other attacks. 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 for the ever-changing environments of educational institutions. Students often change courses, move departments and participate in different projects, but the information they need — and nothing more — should always be available to them. The same goes for professors and administrative staff. 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 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

Another way you can limit the potential damage from ransomware and other attacks is by identifying stale data in your environment. Netwrix Auditor enables you to spot data that has not been used for a specified number of days, so that you can either move it to a protected archive or encrypt it. This not only prevents data loss during an attack, but also saves you money because this data can be moved to a cheaper storage.

Stale Files

Shows files with no recent changes. This report's data set is pre-filtered by the "Stale Data by Folder" report.

Size (MB)	Owner	Path	Created	Modified
10.32	BUILTIN \Administrators	\\stateuniversity\shared \Planned Expenditures.xls	3/21/2016 3:31:47 PM	3/21/2016 3:23:19 PM
27.78	ENTERPRISE \J.Carter	\\stateuniversity\shared \Faculty Members 2015.pdf	8/11/2016 5:33:09 PM	8/11/2016 5:33:31 PM
19.96	ENTERPRISE \T.Simpson	\\stateuniversity\shared \All Curriculum 2014.rtf	11/10/2015 2:58:12 PM	11/10/2015 2:58:36 PM

2. Combat data security threats and streamline investigations with complete visibility

As the volume of unstructured data grows ever larger on your files shares, securing that data is becoming as difficult as it is important. After all, disclosure of a student's academic records might jeopardize their career prospects; exfiltration of Social Security numbers or other PII might lead to identity theft. At the same time, your IT team has to ensure the availability of the data to facilitate learning and research. That is why having 360-degree visibility into what happens in your IT environment and being able to investigate any incident are critical to identifying, measuring and minimizing risks to your highly sensitive data.

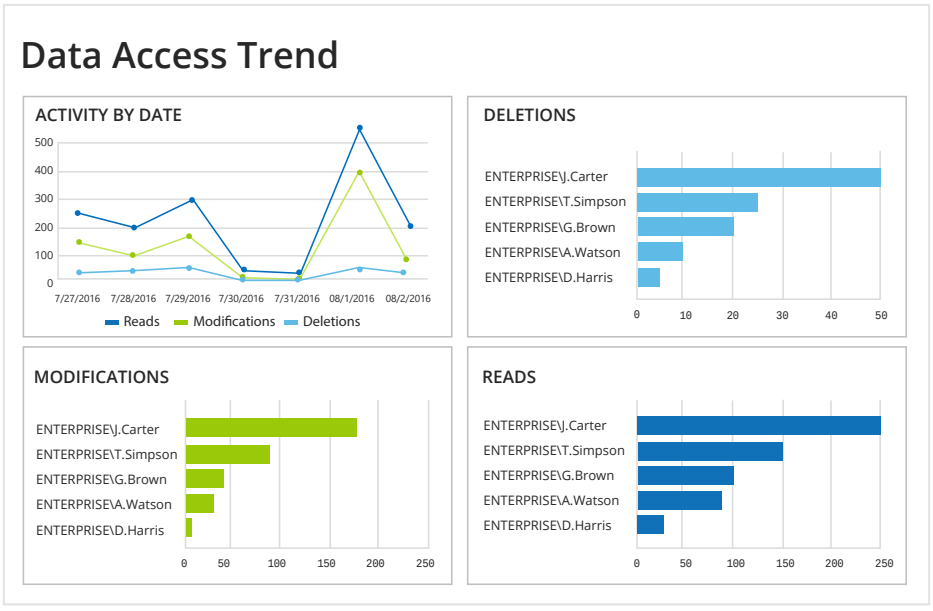
Netwrix Auditor offers an extensive feature set that hundreds of educational institutions all over the world use to keep track of everything that's happening across their core systems, establish user accountability, investigate incidents and assess IT security risks. User Behavior and Blind Spot Analysis functionality simplifies the detection of potentially malicious activity and weaknesses in your data protection, while Interactive Search enables the reconstruction of any security incident step-by-step to find out what exactly happenned.

> We work for three school districts, and we have a huge shared folder with thousands of files, many of which contain PII of students and employees. It is our major goal to protect them both from insider misuse and from hackers who could use the data to steal somebody's identity. Netwrix Auditor empowers us with the knowledge of what is happening in our shared folder, including who deletes, modifies or reads files. It makes routine security work so much easier for our small IT team.

COLTON REDLANDS YUCAIPA
REGIONAL OCCUPATIONAL PROGRAM
Inspiring Possibilities

2.1 Detect threats to sensitive student data early by tracking activity across all your data storage locations

Students and faculty trust educational institutions like yours to ensure the security of their PII, their research results and other sensitive information. You need to be proactive about security risks and be able to spot the earliest signs of active threats. Netwrix Auditor provides security analytics that give you complete visibilty into what is happening on your sensitive file shares. You can get a holistic overview of file-related activity and also drill down to the most specific who, what, when and where details.



Data deletions require special attention, since a single deleted file or folder can stymie the work of hundreds or thousands of people in your educational institution. Netwrix Auditor keeps track of all data deletions, modifications and creations on your file systems and databases, helping you establish accountability and quickly remediate issues, whether the changes were caused by ransomware, a malicious insider or an inadvertent mistake.

Files and Folders Deleted

Shows removed files and folders with their attributes.

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

2.2 Safeguard student PII by promptly detecting aberrant user behavior

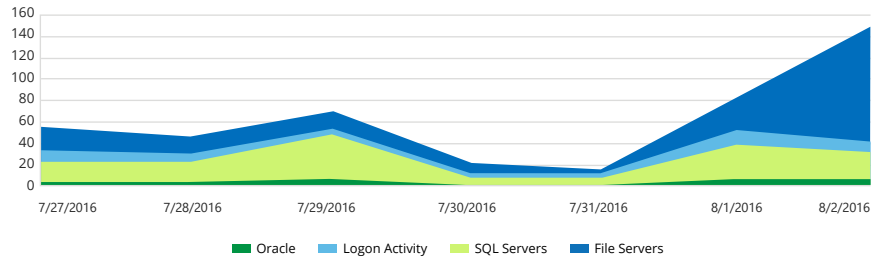
Not being able to efficiently analyze user behavior greatly increases the chance that attacks on your environment will go unnoticed, possibly wreaking havoc in your systems and leading to leaks of sensitive data. Netwrix Auditor helps you close this security gap by providing a set of security analytics 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 has been active outside of business hours, who tried to log in from multiple endpoints within a short time period and much more.

All Logon Activity

Action	Logon Type	What	Who	When
Successful Logon **Where**: dc1.enterprise.com **Workstation**: pl.enterprise.com	Interactive	pl.enterprise.com	ENTERPRISE\J.Carter	7/5/2016 3:57:28 AM
Failed Logon **Where**: dc1.enterprise.com **Workstation**: 192.168.10.7 **Cause**: User logon with misspelled or bad password.	Non-Interactive	N/A	ENTERPRISE\L.Fletcher	7/6/2016 10:59:59 AM

Sudden bursts of failed activity are especially concerning and might signify improper user behavior or an automated attack. Netwrix Auditor allows you to establish a baseline for failed activity in your environment so that you can quickly react to an abnormal spike in the number of failed logons or unsuccessful attempts to access, alter, copy or remove data on file shares and in databases. The overview dashboards help you quickly see failed activity trends, and predefined reports provide valuable details about each type of failed activity 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 Tie evidence together into a coherent whole and hold individuals accountable

Once you detect aberrant behavior or start to suspect a certain user is jeopardizing the security of sensitive student data, you need to investigate the incident from every possible angle to get as much context as possible and determine the full scope of the incident. The Interactive Search available in Netwrix Auditor enables you to quickly sort through audit data and find definitive information about any particular event or string of events to determine the true seriousness of an issue.

Search WHO ACTION WHAT WHEN WHERE

Audited system "File Server" Who "ENTERPRISE\D.Harris" SEARCH

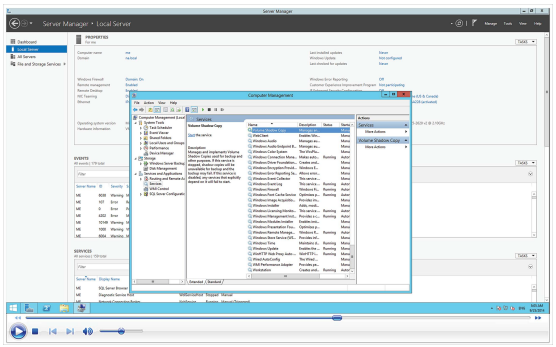
Who	Object type	Action	What	Where	When
ENTERPRISE\ D.Harris	File	Read	\\fs1\shared\ Faculty\pwd.rtf	fs1	6/15/2016 2:53:31 PM
ENTERPRISE\ D.Harris	Folder	Read	\\fs1\shared\faculty	fs1	6/15/2016 2:53:31 PM
ENTERPRISE\ D.Harris	Folder	Read (Failed Attempt)	\\fs1\shared\ University Board	fs1	6/15/2016 2:53:29 PM

You can't fully guarantee the security of critical systems and applications that your students and staff rely on if you don't have a way to monitor the activity of privileged IT staff and hold them accountable for their actions. Netwrix Auditor can capture the screen activity of users in any application, 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. Streamline compliance audit preparation and demonstrate the effectiveness of your security controls

Educational institutions need to maintain strong data security and be able to prove the maturity and effectiveness of their data protection programs to regulators. Highly demanding compliance auditors are never satisfied with a simple declaration of your commitments; they require you to demonstrate your security policies in action. Without proper tools, providing evidence of compliance can be quite costly and time consuming.

Netwrix Auditor helps understaffed IT teams establish and maintain full control over their environments to ensure the security of PII and other sensitive data. Empowered by out-of-the-box compliance reports and a variety of additional compliance features, 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.

> Our internal auditor recommended that we enhance visibility into Active Directory and audit all changes. Netwrix Auditor simply does what we need it to do. I also like the breadth of reporting capabilities as well as the real-time alerting. Before Netwrix, we would not even attempt to find the root cause of some incidents. With Netwrix, it just takes a couple of minutes to pull the report.

WE MAKE LIVES BETTER
UT HEALTH SCIENCE CENTER®
SAN ANTONIO

3.1 Minimize the challenge of getting started with compliance

If your educational institution is only just starting with compliance, you might feel overwhelmed by complex regulatory requirements and unsure about how you can implement them. Don't worry; Netwrix Auditor has you covered. Our solution comes with a report mapping for each of the major compliance standards, including FERPA, FISMA and HIPAA, providing easy-to-read guidelines and best practices for implementing specific requirements.

Mapping of Processes and Report Categories to FERPA Regulations Based on 34 CFR Part 99 Subpart D

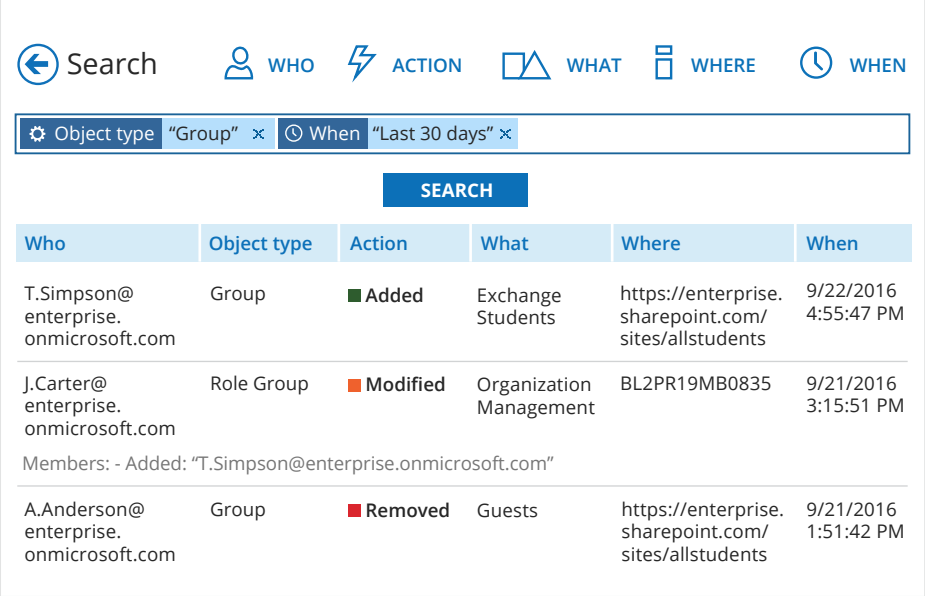
The following mapping is divided into two parts, depending on the subject that holds students' education records. The first part is tailored specifically for an educational agency or institution to ensure all the needed technological controls are validated for security and compliance.

Part I: Requirements for Educational Agencies or Institutions

Procedure	How to Comply?	Processes and Report Categories
§99.31 (a)(ii) An educational agency or institution must use reasonable methods* to ensure that school officials obtain access to only those education records in which they have legitimate educational interests.	Audit all user access to designated locations in information systems where education records are stored, including successful and failed read attempts, to ensure no unauthorized access has taken place.	**ACCESS CONTROL** System Access Data Access Data Integrity **DATA GOVERNANCE** Data Integrity Data Access Permission States

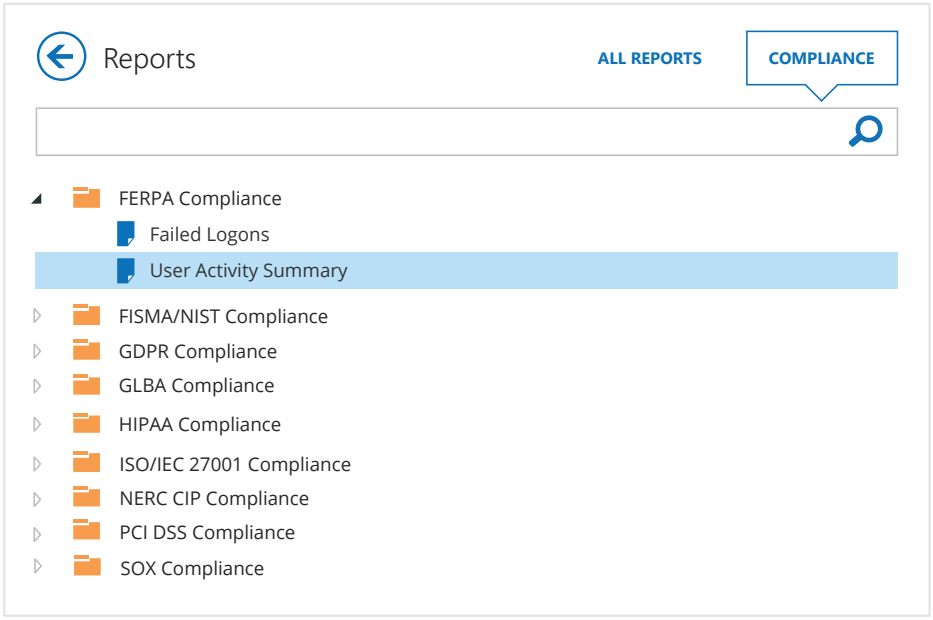
3.2 Streamline preparation for internal audits and external compliance checks

Multiple regulatory bodies place many requirements on educational institutions to ensure the security of student data, and your next attestation always seems to be looming around the corner. Preparing for internal and external assessments can be quite stressful and take a big chunk out of your day. But it doesn't have to. 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 from auditors' checklists, and you can save those reports for immediate access during actual assessments.

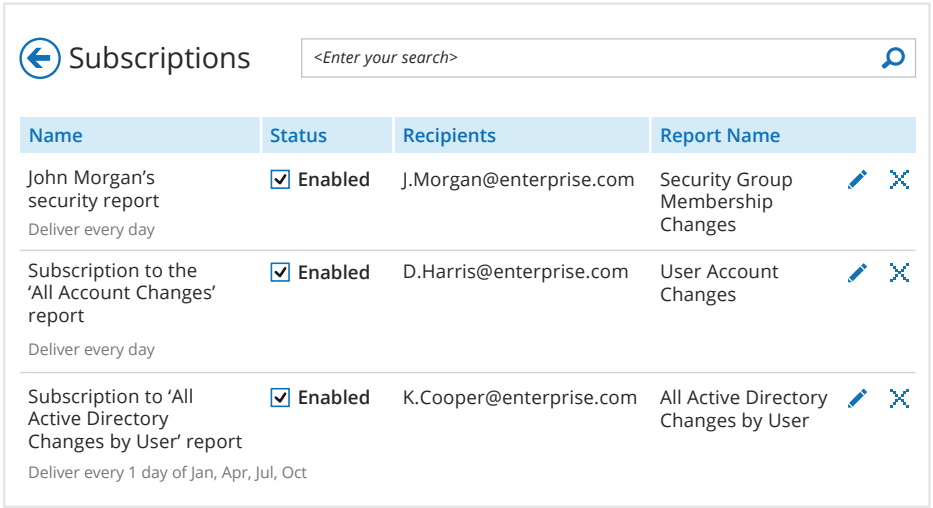


3.3 Meet auditors' expectations with far less effort

Long story short, you really don't want to fail a compliance audit. A failure can lead to even more in-depth assessments in the future, people might lose their jobs and your educational institution might face significant fines. To help you avoid this, Netwrix Auditor offers a wide variety of compliance features that can help you effectively tackle many of the specific requirements your organization is subject to. For instance, the FERPA compliance report pack includes multiple security reports that help you demonstrate that you continuously monitor access to education records and that you have taken adequate measures to ensure data integrity and privacy.



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.



4. Unburden your IT staff and ensure continuous access to educational resources

IT teams in educational institutions are often understaffed. Without an efficient and easy-to-use solution, it is impossible to control a large, dynamic and geographically dispersed environment and ensure normal operations while simultaneously handling numerous helpdesk calls. Addressing this challenge is critical, since IT systems play a pivotal role in educational processes today and if any system is down or network resource is unavailable, it causes a lot of user frustration.

Netwrix Auditor greatly simplifies IT routines that can otherwise be overwhelming. It enables IT teams to 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 makes troubleshooting more straightforward, while various specific features reduce the number of tickets users submit. Plus, the tool enables heads of other departments to take on some functions themselves, relieving IT staff.

> Netwrix Auditor met our initial requirements very quickly. Because we are a small team here, we have spent a lot of time documenting changes made to Active Directory, much longer than we expected. Now the response time to system configurations issues has decreased from an average of 8 hours to 1 hour, which is very important to our employees, students, and tech department.

american career college®

4.1 Proactively troubleshoot issues and minimize user frustration

Because IT staff in educational institutions often have to wear multiple hats and support a large number of users, they can easily get overwhelmed, which eventually affects the quality of service they provide. 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 have 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\Physics Professors\Alex Terry	Alex Terry	A.Terry
\com\enterprise\Management students\Andrew Wiggin	Andrew Wiggin	A.Wiggin
\com\enterprise\Inactive Users\Mike Harris	Mike Harris	M.Harris

More often than not, your students and staff have more important things on their mind than their expiring passwords. However, you know how important a strong password policy is for IT security. With the help of Netwrix Auditor, you can prevent disruptions to the educational process by keeping up with user accounts whose passwords are about to expire. The solution also helps 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 Efficiently deal with helpdesk calls for missing files

How often do you have to deal with helpdesk calls about missing data from your students and staff? When somebody's group project or curriculum file has been deleted or moved and they don't have a backup, you have to find it for them using whatever incomplete details they manage to provide. With Netwrix Auditor, you can maintain data integrity and find out what happened to missing files and folders in minutes. Moreover, you can subscribe someone from each department to receive scheduled reports on file activity on their respective file shares, so that many of these issues can be handled without the IT team.

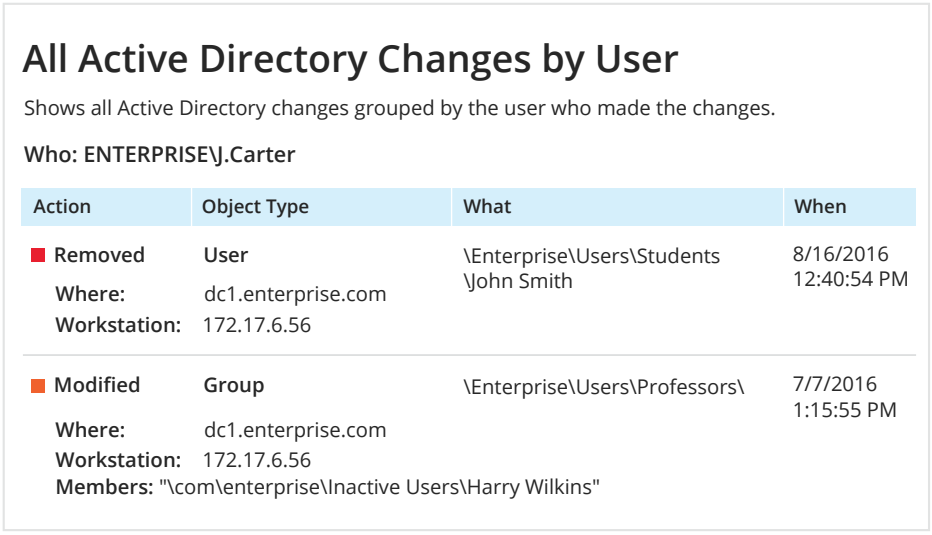
All File Server Activity

Shows activity (changes, failed modifications, reads and failed attemps) on all audited file servers.

Action	Object Type	What	Who	When
Removed Where:	File fs1	\\fs1\Department of Physics\LabProjects \VelocityGraph.png	ENTERPRISE\J.Brown	2/15/2016 1:20:39 PM
Added Where:	Folder fs1	\\fs1\Department of Physics\LabProjects \Astrophysics Projects	ENTERPRISE\J.Brown	2/15/2016 2:11:41 PM
Modified Where:	File fs1	\\fs1\Department of Physics\Academic Performance\2016 Records.xls	ENTERPRISE\N.King	2/15/2016 2:20:14 PM

4.3 Stay aware of critical configuration changes across your geographically dispersed environment

When an educational institution has multiple facilities or campuses, chances are that each one is administered by a separate team or a dedicated specialist. Ensuring communication and accountability can be a struggle. For example, you might see that a change broke something in the environment and you need to investigate it, or you might just want to check whether a particular action was authorized. Netwrix Auditor gives you a way to control your entire environment from a single location.



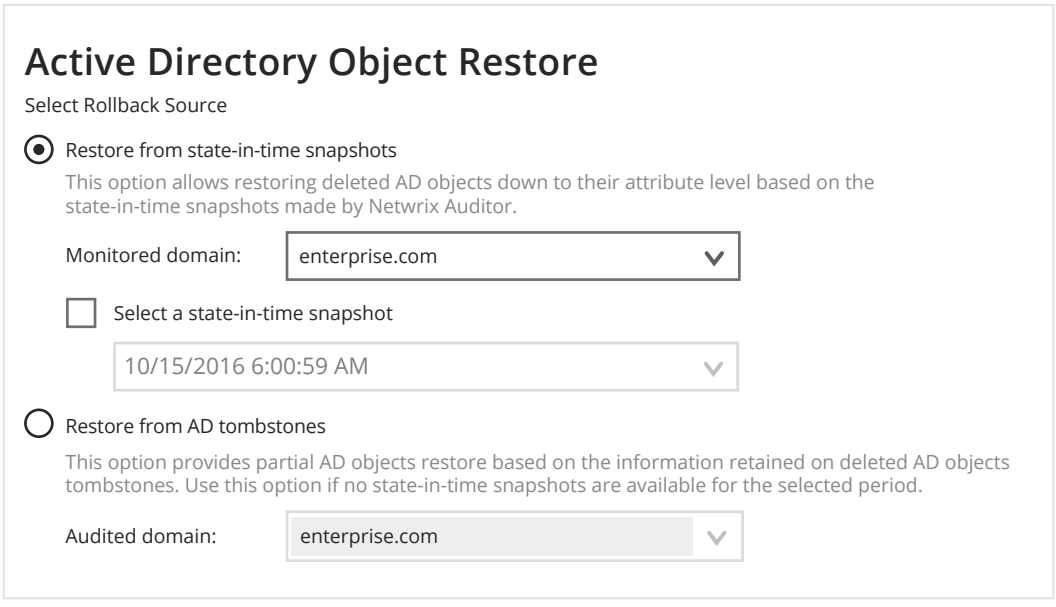
All Active Directory Changes by User

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\Students \John Smith	8/16/2016 12:40:54 PM
Modified **Where:** dc1.enterprise.com **Workstation:** 172.17.6.56 **Members:** "\com\enterprise\Inactive Users\Harry Wilkins"	Group	\Enterprise\Users\Professors\	7/7/2016 1:15:55 PM

In particular, if a certain Active Directory modification has caused system downtime, not only will Netwrix Auditor help you establish accountability for this event, you can use it to restore Active Directory objects in order to quickly resume normal service.



Conclusion

Most IT teams in educational institutions face a common set of serious challenges: lack of budget to hire more staff, a large number of users to support, multiple remote facilities and strict regulatory requirements for data confidentiality. As a result, despite their expertise and dedication, they are often overwhelmed, which limits the quality of service they can provide, which in turn hurts both educational processes and the security of the sensitive data that the institutions handle.

By automating and optimizing IT processes, you can address all of these challenges. Netwrix Auditor can streamline IT workflows across your entire infrastructure and lift significant burdens from the shoulders of IT staff. Over 500 educational establishments around the world, including universities, colleges and school districts already rely on Netwrix Auditor to minimize risks to their sensitive information, more easily pass regulatory audits and ensure uninterrupted educational processes.

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 security gaps in your environment and active threats, 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 or see the solution in action right away at www.netwrix.com/one-to-one.html

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