netwrix

What's New

Netwrix Auditor 9.5

Identify, Assess and **Reduce Risks** to Your **IT Infrastructure** and **Data**

Learn more: www.netwrix.com/auditor9.5

Risk Assessment

Close security holes by identifying and prioritizing risks

Minimize the ability of intruders and insiders to steal data or cause damage by proactively reducing your attack surface area. Enable continuous risk assessment with interactive risk dashboards that help you identify, prioritize and act on gaps in security and compliance best practices.

IT Risk Assessment: Data

Keep your finger on the pulse of access audience and discipline of your company's "business crown jewels" – the most valuable data assets.

Total risk level for Data: Pay attention

Risk	Level
Folders with "Everyone" group access	Acceptable
File names containing sensitive data	Acceptable
Potentially harmful files on file shares	Pay attention
Direct permissions on files and folders	Take action

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\Board Meetings

Account	Permissions	Means Granted
ENTERPRISE\Managers	Modify (Read, Write, Execute, List folder content)	Directly
ENTERPRISE\T.Simpson	Full Control	Directly
NT AUTHORITY\SYSTEM	Full Control	Directly

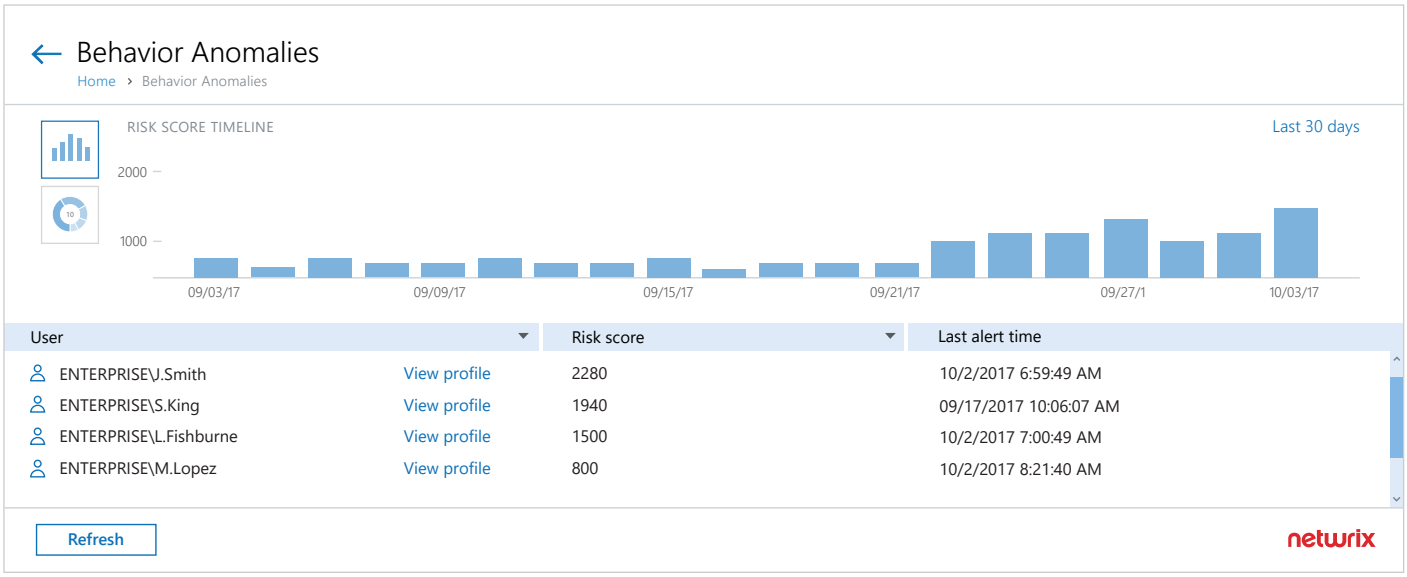
Object: \\fs1\shared\Human Resources

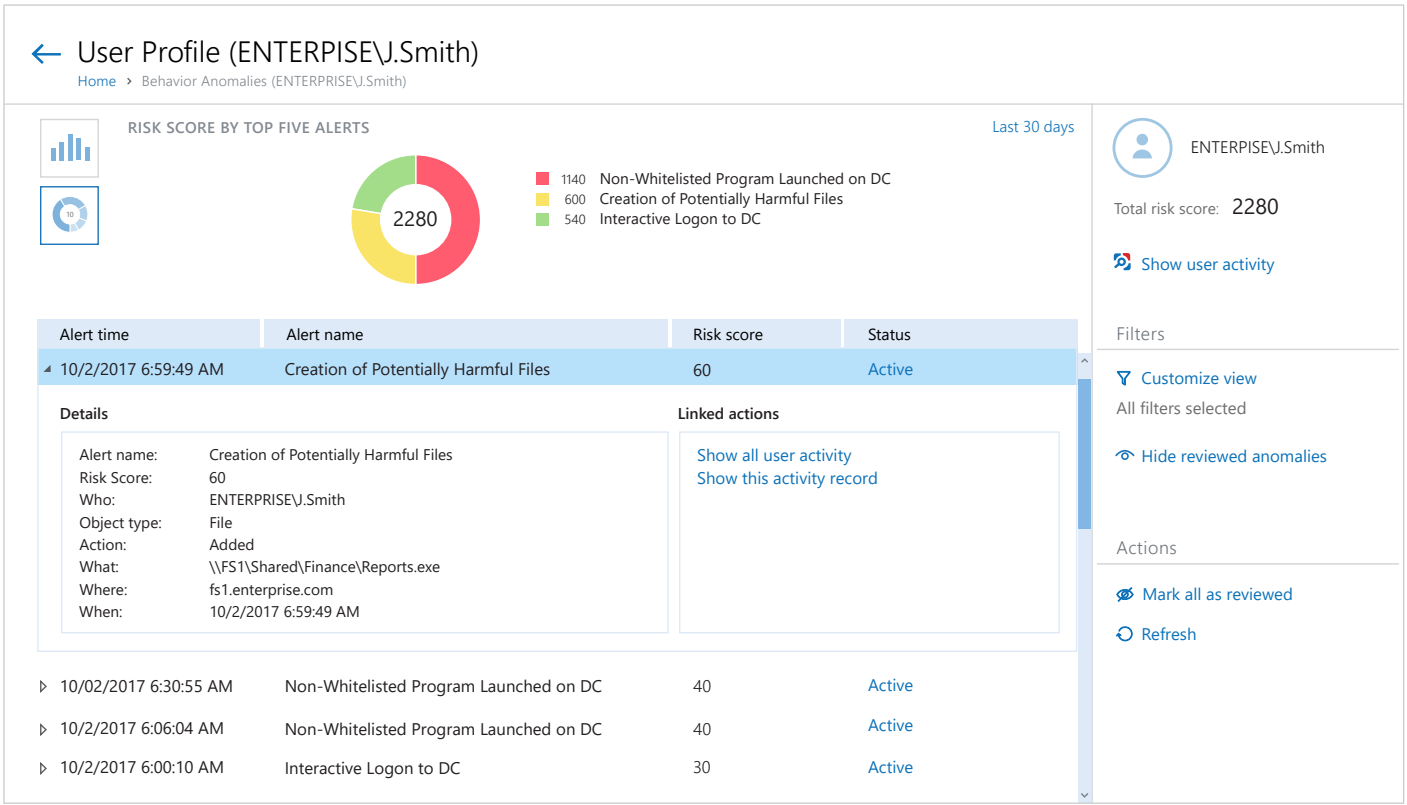
Account	Permissions	Means Granted
ENTERPRISE\HR	Full Control	Directly
ENTERPRISE\D.Harris	Read (Execute, List folder content)	Directly
NT AUTHORITY\SYSTEM	Full Control	Directly

Behavior Anomaly Discovery

Improve detection of malicious insiders and compromised accounts

Spot and investigate anomalies in user behavior in time to block external attackers who have compromised valid user accounts, as well as trusted insiders who have gone rogue.





Learn more: www.netwrix.com/auditor9.5

Permission Analysis

Scrutinize who has access to what

Analyze Active Directory effective permissions for important resources to spot unnecessary access rights. Remove them to mitigate the risk of privilege abuse and limit the damage that malware can inflict.

Object Permissions in Active Directory

Shows accounts with explicit or inherited permissions on a specific Active Directory object (either granted directly or through group membership). Use this report to see who has permissions to what in your Active Directory domain and prevent unnecessary rights elevation. The permissions are reported only for users that belong to the monitored domain.

Object Name: \Enterprise\Domain Controllers\DC1

Account Name	Account Type	Means Granted
\Enterprise\Users\Jack Carter	User	Group
\Enterprise\Users\Jon Smith	User	Group
\Enterprise\Users\Alex Terry	User	Directly
\Enterprise\Users\Susan Manson	User	Group

Stay informed about who has access to your critical servers by checking on local users and groups regularly. If you detect any deviations from your security policy or a known good baseline, quickly restrict access to minimize your attack surface.

Members of Local Administrators Group

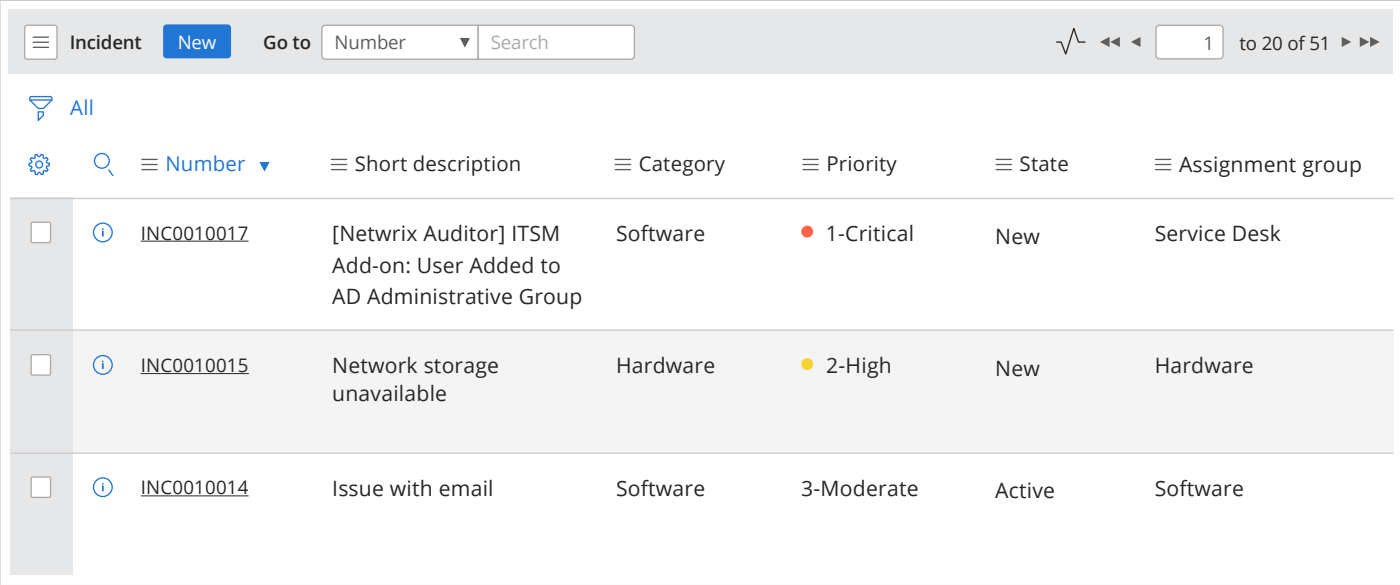
Shows Windows servers, with members of the local Administrators group for each server. You can apply baseline filter to highlight servers with security issues, e.g., those where the Administrators group include users not in your baseline list. Use this report to prevent rights elevation and exercise security control over your organization.

Server	Members	Status
fs1.enterprise.com	Administrator, fs1local, ENTERPRISE\Domain Admins	Issues Detected
sql01.enterprise.com	Administrator, J.Carter, ENTERPRISE\Domain Admins	Issues Detected
srv01.enterprise.com	Administrator, T.Simpson, ENTERPRISE\Domain Admins	Issues Detected
srv02.enterprise.com	Administrator, ENTERPRISE\Domain Admins	OK
srv03.enterprise.com	Administrator, ENTERPRISE\Domain Admins	OK
srv04.enterprise.com	Administrator, ENTERPRISE\Domain Admins	OK

Add-on for ServiceNow Incident Management

Streamline incident detection and response

Speed incident response and enable faster and more accurate incident investigation with this smart integration that uses information from Netwrix Auditor's alerts to automatically create detailed tickets in your ServiceNow ITSM and provide initial incident support.



Add-on for Privileged User Monitoring on Linux and Unix Systems

Identify and respond to improper behavior across your *nix systems

Enable full control over temporary privilege elevations via the SUDO command and OpenSSH remote sessions.

Add-on for Generic Linux Syslog

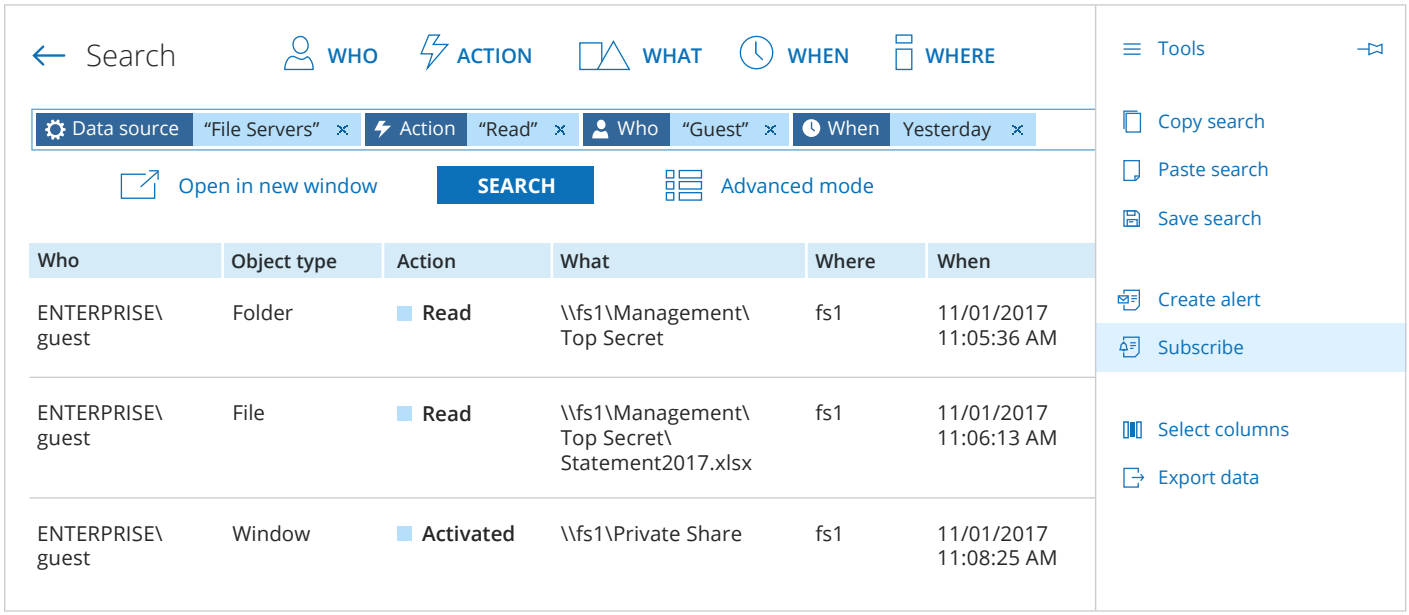
Spot and investigate threats to your Linux environment

Gain a single-pane view of what's happening across your Linux systmes and stay alert to risky behavior patterns, such as multiple authentication failures or failed attempts to run the SU command.

Custom Report Subscriptions

Stay informed about your specific security and compliance concerns

Easily ensure that your organization's specific security and compliance requirements are continuously met by creating custom reports using Interactive Search and having them sent to you or other stakeholders on a regular basis. Prove your compliance in minutes by simply having these custom reports saved in a particular folder and granting auditors access to that folder when they come.



How to upgrade to Netwrix Auditor 9.5 from previous versions?

www.netwrix.com/go/upgrade9.5