netwrix

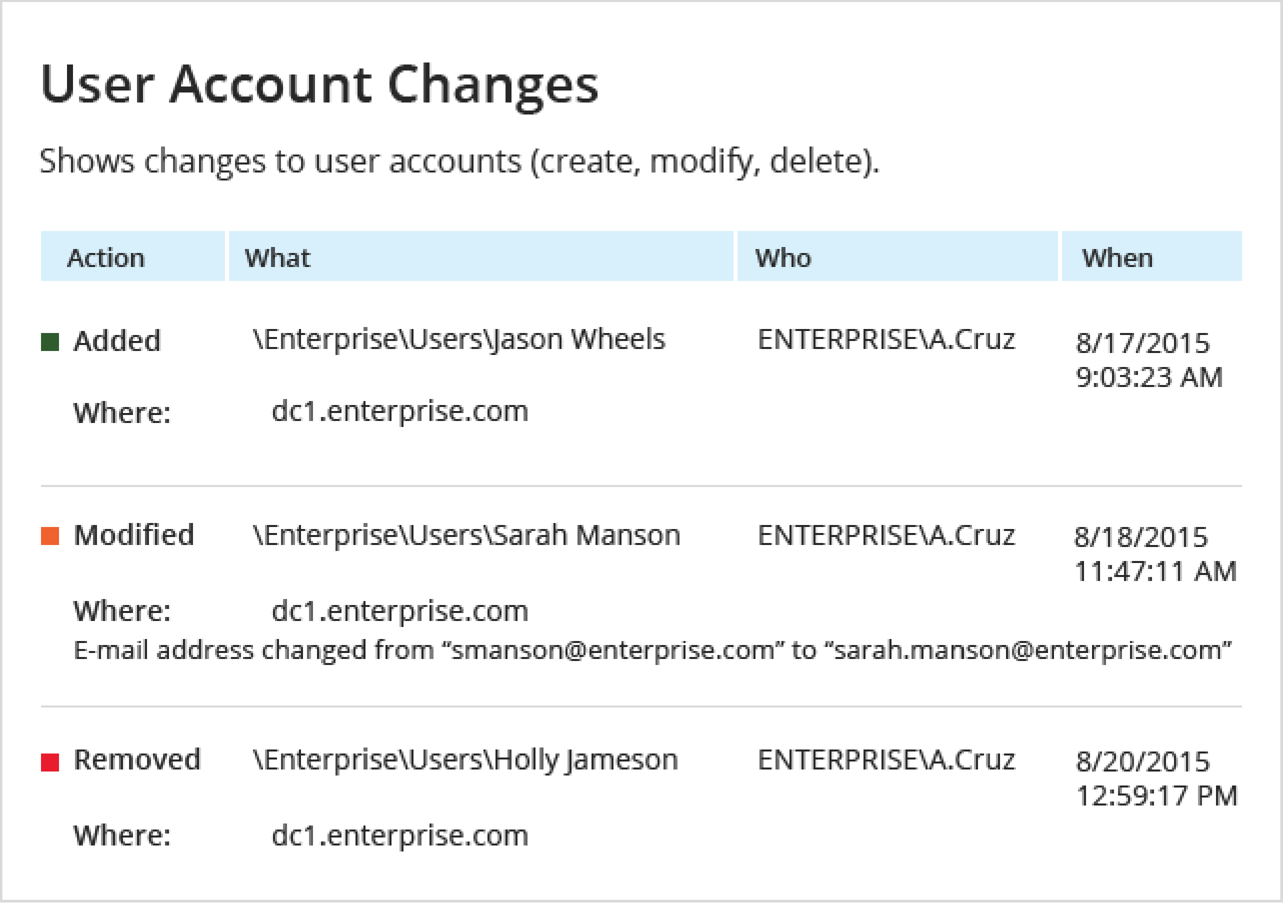
Top 5 Active Directory Incidents You Need Visibility Into

Table of Contents

#1: User Account Changes

Any unauthorized modification to an AD user account can be a sign of malicious activity that might result in a data breach. Therefore, timely detection and investigation of user account changes is essential. Netwrix Auditor shows all newly created, deleted or modified user accounts and helps answer the following questions:

- **What** changes were applied to which user accounts?
- **Who** performed each change?
- **When** was each change made?
- **In which domain** was each change made?



User Account Changes

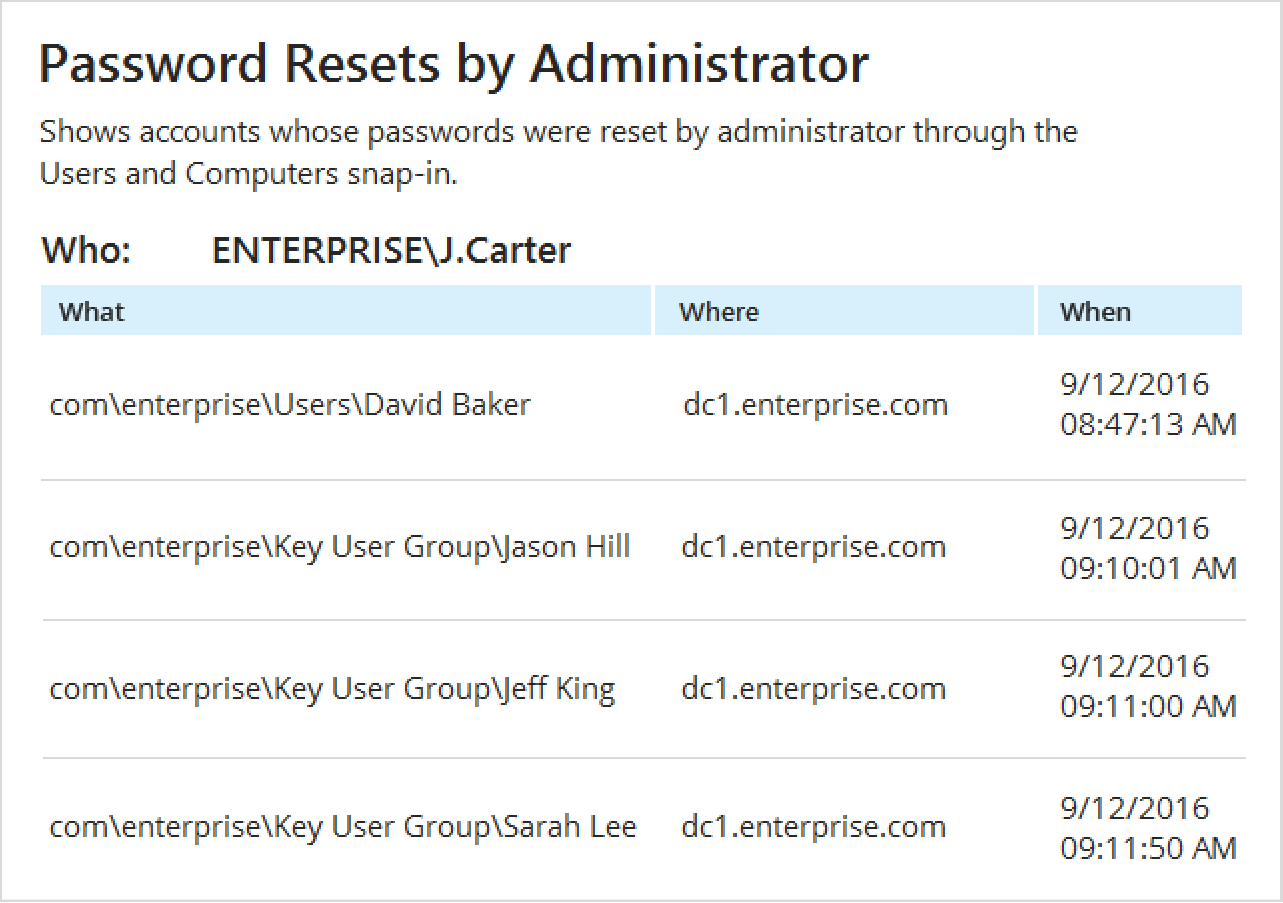
Shows changes to user accounts (create, modify, delete).

Action	What	Who	When
🟩 Added Where:	\Enterprise\Users\Jason Wheels dc1.enterprise.com	ENTERPRISE\A.Cruz	8/17/2015 9:03:23 AM
🟧 Modified Where:	\Enterprise\Users\Sarah Manson dc1.enterprise.com E-mail address changed from “smanson@enterprise.com” to “sarah.manson@enterprise.com”	ENTERPRISE\A.Cruz	8/18/2015 11:47:11 AM
🟥 Removed Where:	\Enterprise\Users\Holly Jameson dc1.enterprise.com	ENTERPRISE\A.Cruz	8/20/2015 12:59:17 PM

#2: Password Resets by Administrator

Monitoring password resets performed by IT administrators is critical because unfamiliar password reset activity can be a sign that the administrative account has been compromised. Netwrix Auditor tracks all password resets performed by administrators and helps answer the following questions:

- **Which user** account passwords were reset?
- **Which IT** administrator reset each user account password?
- **In which domain** was each password reset performed?
- **When** was each password reset?



Password Resets by Administrator

Shows accounts whose passwords were reset by administrator through the Users and Computers snap-in.

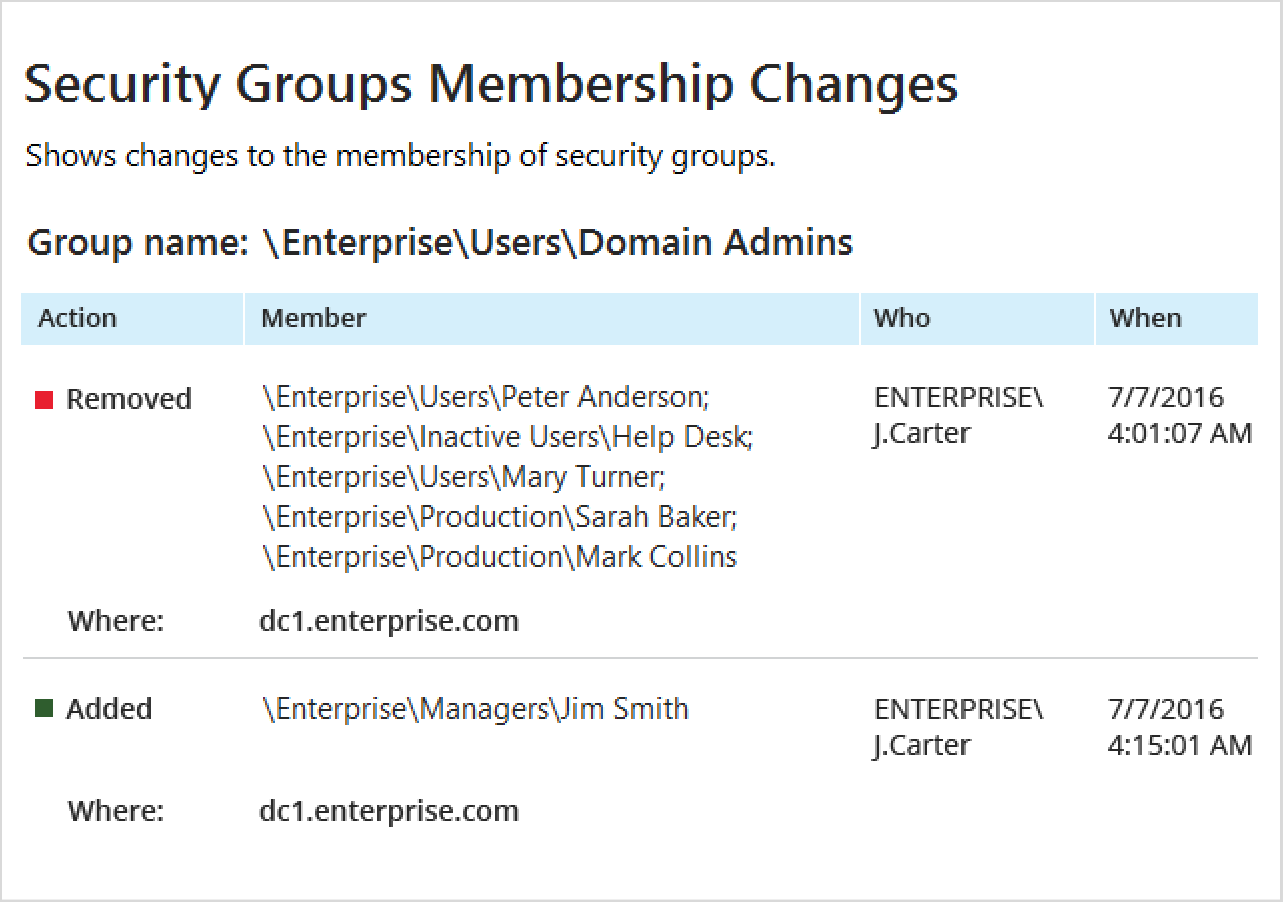
Who: ENTERPRISE\J.Carter

What	Where	When
com\enterprise\Users\David Baker	dc1.enterprise.com	9/12/2016 08:47:13 AM
com\enterprise\Key User Group\Jason Hill	dc1.enterprise.com	9/12/2016 09:10:01 AM
com\enterprise\Key User Group\Jeff King	dc1.enterprise.com	9/12/2016 09:11:00 AM
com\enterprise\Key User Group\Sarah Lee	dc1.enterprise.com	9/12/2016 09:11:50 AM

#3: Security Group Membership Changes

Security groups should be under close control in case a user, maliciously or by mistakes, is added to one of these groups and therefore is granted unwarranted rights to access, modify or remove sensitive data. Netwrix Auditor tracks all security group membership changes and helps answer the following questions:

- **Who** was added to or removed from a security group?
- **Who** made each change to a security group?
- **Which domain** was the changed security group in?
- **When** was each change to a security group made?



Security Groups Membership Changes

Shows changes to the membership of security groups.

Group name: \Enterprise\Users\Domain Admins

Action	Member	Who	When

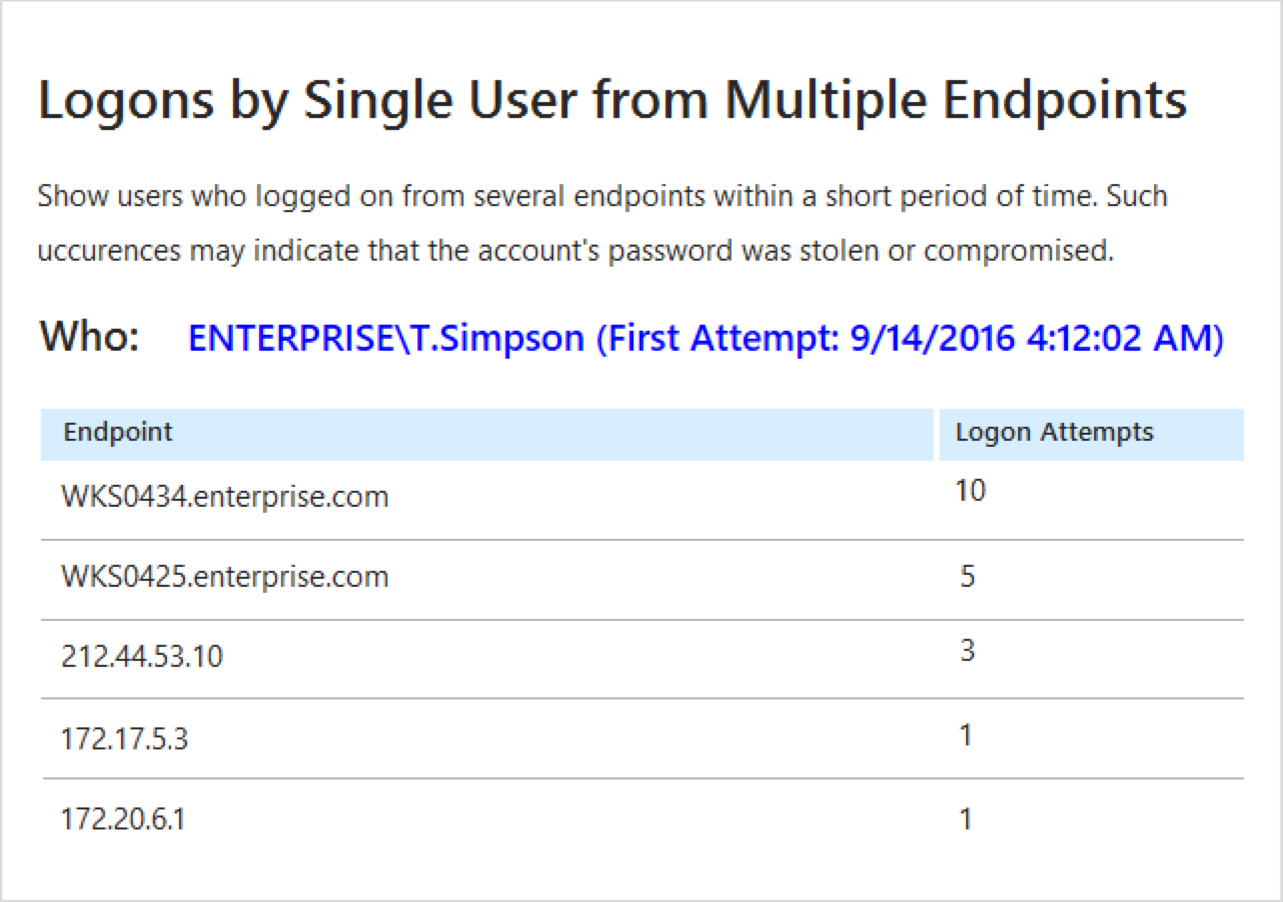
🟥 Removed	\Enterprise\Users\Peter Anderson;
	\Enterprise\Inactive Users\Help Desk;
	\Enterprise\Users\Mary Turner;
	\Enterprise\Production\Sarah Baker;
	\Enterprise\Production\Mark Collins
		ENTERPRISE\ J.Carter	7/7/2016 4:01:07 AM

Where:	dc1.enterprise.com		
🟩 Added	\Enterprise\Managers\Jim Smith	ENTERPRISE\ J.Carter	7/7/2016 4:15:01 AM
Where:	dc1.enterprise.com		

#4: Logons by a Single User from Multiple Endpoints

Numerous logons by a single user from different endpoints can indicate that this user account has been compromised and therefore the security of your systems is at risk. Netwrix Auditor shows accounts that performed successful logons from several endpoints within a short period of time and helps answer the following questions:

- **Which account** was used to log on from multiple endpoints?
- **What endpoints** were used to log on to the system?
- **How many logon** attempts were made from each endpoint?
- **When** was the first logon attempt performed?



Logons by Single User from Multiple Endpoints

Show users who logged on from several endpoints within a short period of time. Such uccurences may indicate that the account's password was stolen or compromised.

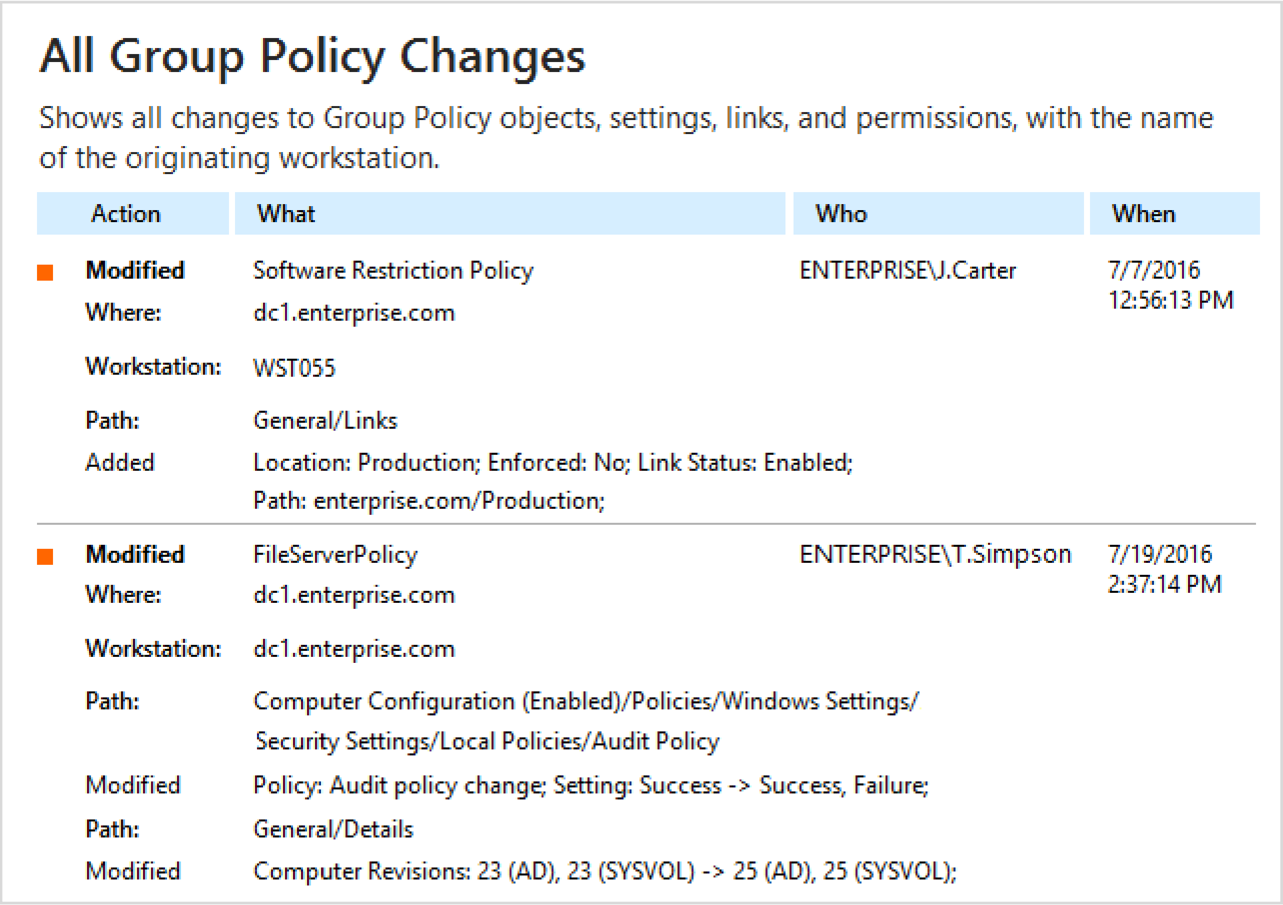
Who: ENTERPRISE\T.Simpson (First Attempt: 9/14/2016 4:12:02 AM)

Endpoint	Logon Attempts
WKS0434.enterprise.com	10
WKS0425.enterprise.com	5
212.44.53.10	3
172.17.5.3	1
172.20.6.1	1

#5: Group Policy Changes

Lack of visibility into what's going on in your Group Policy can lead to late detection of malicious activity and put your data security at risk. Netwrix Auditor monitors all Group Policy changes and gives detailed answers to the following questions:

- **What type** of changes were made to your Group Policy?
- **What** exactly was changed and how?
- **Who** performed each change?
- **When** each change was made?



All Group Policy Changes

Shows all changes to Group Policy objects, settings, links, and permissions, with the name of the originating workstation.

	Action	What	Who	When
■	**Modified**	Software Restriction Policy	ENTERPRISE\J.Carter	7/7/2016 12:56:13 PM
	Where:	dc1.enterprise.com		
	Workstation:	WST055		
	Path:	General/Links		

	Added	Location: Production; Enforced: No; Link Status: Enabled;
		Path: enterprise.com/Production;		

■	**Modified**	FileServerPolicy	ENTERPRISE\T.Simpson	7/19/2016 2:37:14 PM
	Where:	dc1.enterprise.com		
	Workstation:	dc1.enterprise.com		
	Path:	Computer Configuration (Enabled)/Policies/Windows Settings/ Security Settings/Local Policies/Audit Policy		
	Modified	Policy: Audit policy change; Setting: Success -> Success, Failure;		
	Path:	General/Details		
	Modified	Computer Revisions: 23 (AD), 23 (SYSVOL) -> 25 (AD), 25 (SYSVOL);		

About Netwrix Auditor

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 unified platform provides security analytics for detecting anomalies in user behavior and investigating threat patterns before a data breach occurs.

Netwrix Auditor includes applications for Active Directory, Azure AD, Exchange, Office 365, Windows file servers, Dell data storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware and Windows Server. Empowered with a RESTful API, Netwrix Auditor provides **endless integration, auditing and reporting capabilities** for security and compliance.

Unlike other vendors, Netwrix focuses exclusively on providing complete visibility and governance for hybrid cloud security. The sharp focus enables us to offer much more robust functionality than legacy change auditing solutions. Netwrix Auditor has been already honored with more than **100 awards** and recognized by almost **160,000 IT departments** worldwide.

Deploy Netwrix Auditor Wherever You Need It

- Free 20-Day Trial for On-Premises Deployment: netwrix.com/freetrial
- Free Virtual Appliance for Hyper-V and VMware Hypervisors: netwrix.com/go/appliance

netwrix.com/social

Netwrix Corporation, 6160 Warren Parkway, Suite 100, Frisco, TX, US 75034

Toll-free: 888-638-9749
Int'l: +1 (949) 407-5125
EMEA: +44 (0) 203-318-0261