netwrix

Netwrix Auditor

Visibility Platform for User Behavior Analysis and Risk Mitigation in Hybrid IT Environments

01
Product Overview

Netwrix Auditor Platform

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.

Detect data security threats — on premises and in the cloud.

Pass compliance audits with less effort and expense.

Increase productivity of IT security and operations teams.

02
Applications

Netwrix Auditor Applications

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.

- Netwrix Auditor for **Active Directory**
- Netwrix Auditor for **Azure AD**
- Netwrix Auditor for **Exchange**
- Netwrix Auditor for **Office 365**
- Netwrix Auditor for **Windows File Servers**
- Netwrix Auditor for **EMC**
- Netwrix Auditor for **NetApp**
- Netwrix Auditor for **SharePoint**
- Netwrix Auditor for **Oracle Database**
- Netwrix Auditor for **SQL Server**
- Netwrix Auditor for **Windows Server**
- Netwrix Auditor for **VMware**

03
Benefits

Detect data security threats – on premises and in the cloud

Netwrix Auditor bridges the visibility gap by delivering security analytics about critical changes, state of configurations and data access in hybrid IT environments and enables investigation of suspicious user behavior. The platform also provides alerts about patterns that violate corporate security policies and indicate a possible insider threat.

Pass compliance audits with less effort and expense

Netwrix Auditor provides the evidence required to prove that your organization's IT security program adheres to PCI DSS, HIPAA, SOX, GLBA, FISMA/NIST800-53, FERPA, CJIS, NERC CIP, ISO/IEC 27001, GDPR and other standards. It also ensures easy access to compliance reports for more than 10 years.

Increase the productivity of IT security and operations teams

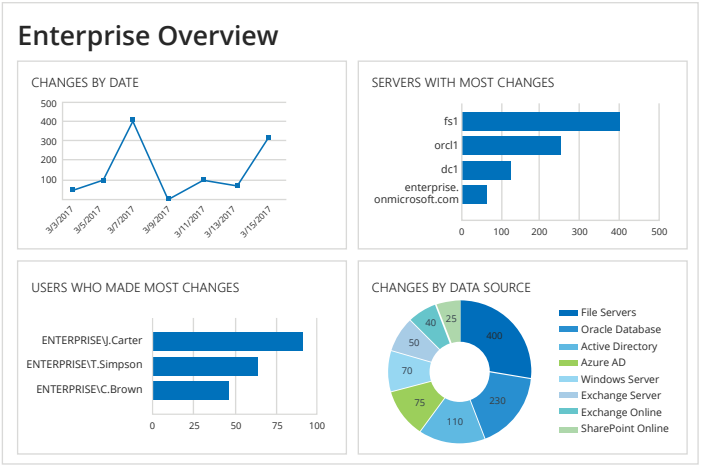
With Netwrix Auditor, there's no need to crawl through weeks of log data to answer questions about who changed what, when and where a change was made, or who has access to what. The platform delivers actionable audit data to anyone in your organization who needs it.

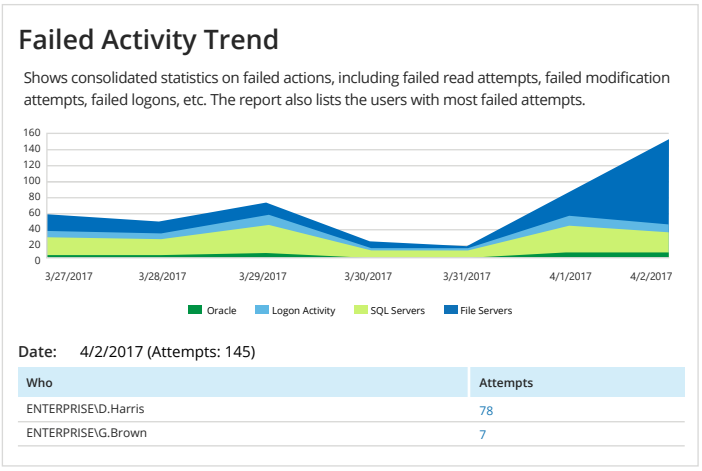
04

In Action: Detect Data Security Threats

Gain a bird's-eye view of activity across your IT environment

Get a high-level view of what's going on in your hybrid IT infrastructure with Enterprise Overview dashboards. Track trends in employee activity, such as how much activity is occurring, which users are most active and which systems are most affected.





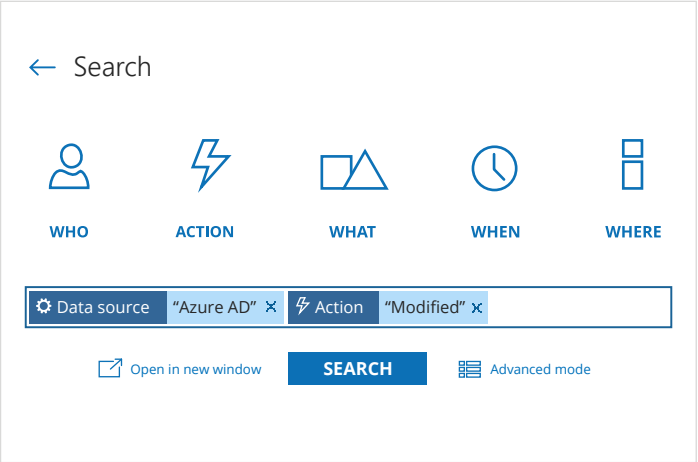
Spot abnormal user behavior that would otherwise go unnoticed

Quickly identify potential security incidents, such as unusual logons that might indicate user identity theft or a disgruntled privileged user trying to hide his or her activity behind temporary accounts. With the user behavior and blind spot analysis capability, no malicious activity can slip under your radar.

05
In Action: Detect Data Security Threats

Investigate anomalies in user behavior

Whenever you detect user activity that violates your corporate security policy, use our interactive Google-like search to investigate how it happened so you can prevent similar incidents from occurring in the future.



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\Finance (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	Full Control	Directly
ENTERPRISE\P.Anderson	Full Control	Group
ENTERPRISE\T.Simpson	Full Control	Directly
fs1\Administrator	Full Control	Group

Prevent data exfiltration

Make sure that only the eligible employees in your organization have access to critical resources by getting a complete picture of effective permissions and file activity on your file servers and NAS.

06

In Action: Detect Data Security Threats

Monitor access to unstructured data

Whether your files contain cardholder data, medical records or financial statements, Netwrix Auditor will show who attempted (successfully or unsuccessfully) to access those files, and when and where the attempt occurred.

Failed Read Attempts

Shows attempts to read files that failed due to lack of access rights. This report can be used during compliance audits to show that all unauthorized data access activities are traceable and easily auditable.

Action	Object Type	What	Who	When
Read (Failed Attempt)	File	\\fs1\Finance\Cardholders\Overview.xlsx	ENTERPRISE\B.Green	4/5/2017 3:07:08 PM
Where:	ENTWKS0412			
Read (Failed Attempt)	File	\\fs1\Finance\Accounting\Statement0313.xlsx	ENTERPRISE\S.Hernandez	4/5/2017 3:05:38 PM
Where:	ENTWKS0524			
Read (Failed Attempt)	File	\\fs1\HR\NewHire\SalaryList.xlsx	ENTERPRISE\K.Davis	4/5/2017 3:03:23 PM
Where:	172.17.4.34			

Excessive Access Permissions

Shows accounts with permissions to infrequently accessed files and folders (either directly or via group membership). Use this report to spot unnecessary permissions and thereby prevent data leaks.

Object: \\fs1\Accounting (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

Lock down overexposed data

Spot unnecessary permissions to unstructured data so you can lock down overexposed data and mitigate the risk of privilege abuse.

07
In Action: Detect Data Security Threats

Receive alerts on threat patterns

Be alerted about unauthorized activity as it happens so you can prevent security breaches. For example, you can choose to be notified whenever someone has been added to the Enterprise Admins group or a user has modified too many files at a time, which could indicate a ransomware attack in progress.

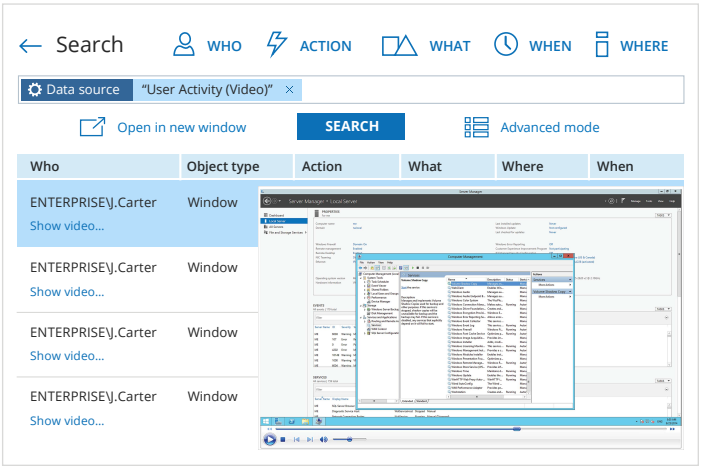
Netwrix Auditor Alert

Possible ransomware activity

The alert was triggered by 150 activity records being captured within 60 seconds. The most recent of those activity records is shown below. To review the full activity trail, use the interactive search in Netwrix Auditor.

Who:	ENTERPRISE\J.Carter
Action:	Modified
Object type:	File
What:	\\fs3.enterprise.com\Documents\Contractors\payroll2017.docx
When:	4/28/2017 11:35:17 AM
Where:	fs3.enterprise.com
Workstation:	mkt025.enterprise.com
Data source:	File Servers
Monitoring plan:	Enterprise Data Visibility Plan
Details:	Size changed from "807936 bytes" to "831488 bytes"

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



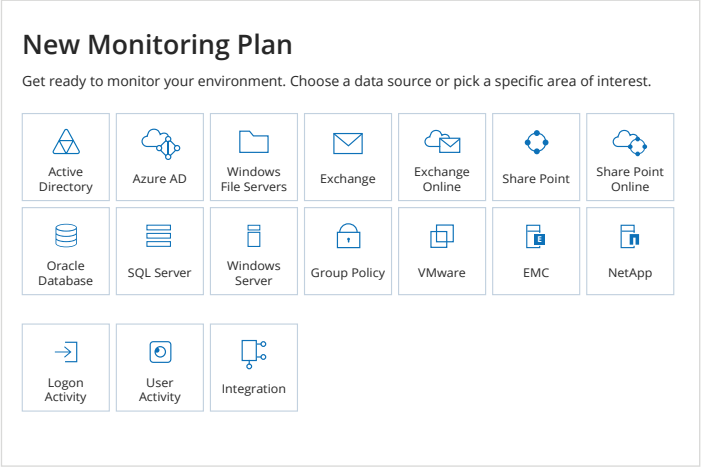
Detect the undetectable

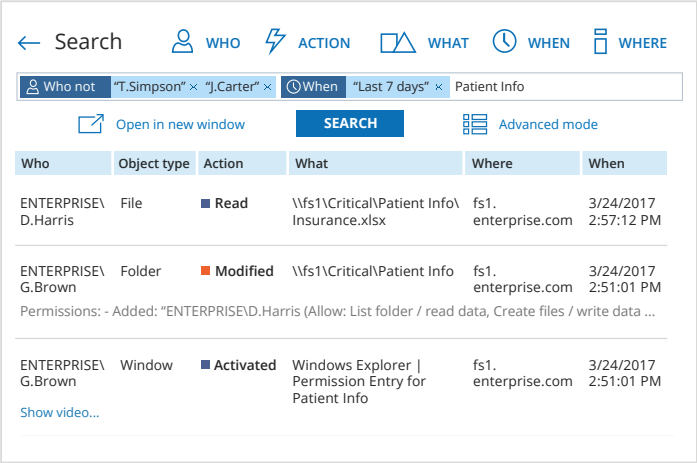
Gain visibility into any system or application, even if it doesn't produce any logs, by video recording a user's screen activity. You can search and replay the recordings to determine exactly what actions were performed.

08
In Action: Pass Compliance Audits

Enable control over security policies

By supporting the broadest variety of on-premises and cloud-based IT systems, Netwrix Auditor enables compliance controls across your entire IT infrastructure and serves as a single point of access to the audit trail.





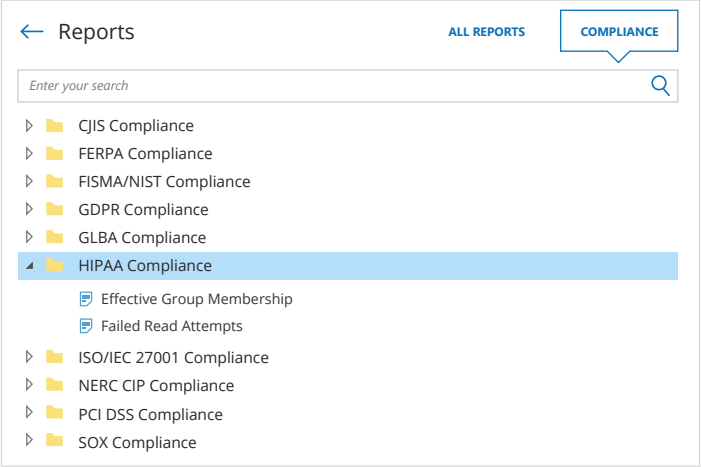
Address auditor's questions faster

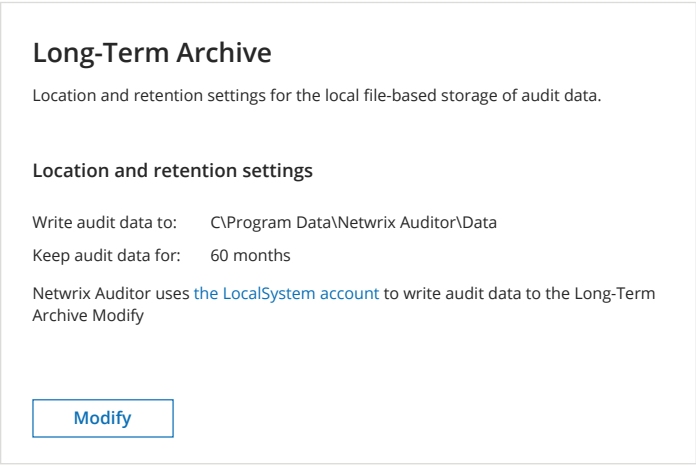
Quickly provide answers to auditors' questions, such as who has access to a protected folder or how access rights to this folder were modified during the past year and who made those changes. With Netwrix Auditor, what used to take weeks now takes minutes.

09
In Action: Pass Compliance Audits

Take advantage of out-of-the-box compliance reports

Auditors require proof that specific processes and controls are — and have always been — in place. Prove your compliance with out-of-the-box reports aligned with compliance controls.





Store and access your audit trail for years

Netwrix Auditor securely stores your audit trail in a compressed format for more than 10 years, enabling you comply with internal policies and external regulations. You can easily access the archived audit data at any time for security analytics, historic e-discovery or security investigations.

10

In Action: Increase the Productivity of IT Teams

Keep tabs on what's changing in your environment

See when a specific change was made, who made it, and what was changed, including the values before and after the change. This detailed information is available for every change in your on-premises and cloud-based IT systems.

All Changes by User

Shows all changes across the entire IT infrastructure, grouped by the user who made the change.

Who: ENTERPRISE\F.Wilson

Data Source: Active Directory

Action	Object Type	What	When
Modified	User	\enterprise\Users\Glen Williams	3/9/2017 4:31:49 PM

Where: ex1.enterprise.com
Principal Name set to "Glen.Williams@enterprise.com"

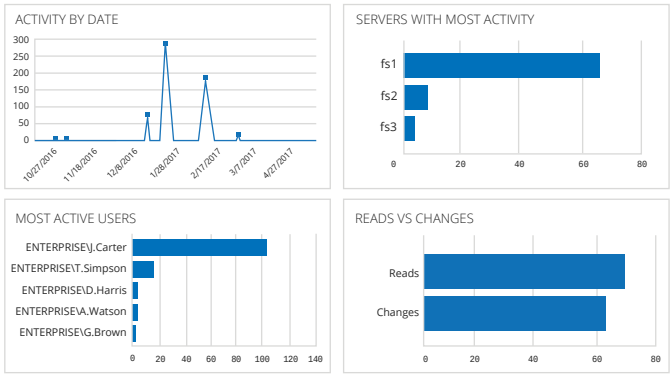
Data Source: VMware

Action	Object Type	What	When
Removed	VirtualMachine	\ha-folder-root\ha-datacenter\vm1	3/11/2017 3:11:41 PM

Where: https://vmhost1.enterprise.com:433

File Servers Overview

Shows consolidated statistics on all activity across all audited file servers.



Simplify reporting

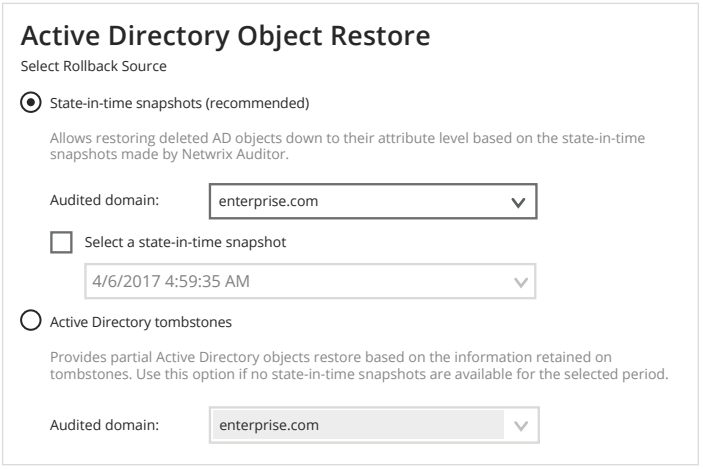
Netwrix Auditor supplies more than 200 predefined reports and dashboards that are easy to customize using built-in filtering, grouping and sorting. You can export the data to PDF, XLS and other formats, set up email subscriptions, and much more.

11

In Action: Increase the Productivity of IT Teams

Speed report delivery

Jettison slow, manual reporting processes that require users to request the reports they need from IT and wait their turn in the queue. With Netwrix Auditor, stakeholders can subscribe to scheduled reports or create reports on demand.



Minimize system downtime

In the event that an unauthorized change affecting system availability does occur, you can quickly turn back the clock by reverting the settings to a previous state — without any downtime or having to restore from backup.

12

In Action: Increase the Productivity of IT Teams

Focus on what's really important

Use alerts to ensure you are notified about critical actions as they happen. You can choose the specific types of activity you want to be alerted about, such as the deletion of business-critical files on a file server or changes to your SQL Server configuration.

Netwrix Auditor Alert

Possible DBA privilege abuse

Who:	ENTERPRISE\J.Smith
Action:	Removed
Object type:	Table
What:	Databases\Customers\Tables\dbo.Cardholders
When:	5/3/2017 7:19:29 AM
Where:	sql2.enterprise.com
Workstation:	mkt023.enterprise.com
Data source:	SQL Server
Monitoring plan:	Enterprise Database Visibility Plan

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

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	Security Policy	ENTERPRISE\J.Smith	3/23/2017 7:55:11 AM

Where:	dc1.enterprise.com
Workstation:	172.17.35.12
Path:	Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/ Account Policies/Password Policy
Modified	Policy: Enforce password history; Setting: 24 passwords remembered -> 3 passwords remembered;
Modified	Modified Policy: Maximum password age; Setting: 20 days -> 200 days;
Modified	Modified Policy: Minimum password length; Setting: 7 characters-> 4 characters;

Troubleshoot faster

When a problem arises, Netwrix Auditor delivers not mountains of raw data to pore through, but meaningful and actionable intelligence that enables you to quickly investigate the sequence of events involved and determine the underlying root cause of the issue.

13 Addressing the Security and Compliance Challenges of Your Department and Your Business

System Administrator

Generate and deliver security and compliance reports faster.

IT Security Administrator

Investigate suspicious user activity before it becomes a breach.

IT Manager

Take back control over your IT infrastructure and eliminate the stress of your next compliance audit.

CIO/CISO

Prevent data breaches and minimize compliance costs.

MSP

Increase revenue by enabling transparency of managed environments and offering compliance as a service.

Industry Recognition

Gartner

"...configuration auditing tools help you analyze your configurations according to best practices, enforce configuration standards and adhere to regulatory requirements... "

Redmond MAGAZINE

"...auditing is generally a rather difficult task, especially if done manually. All of the many details you need to consider and remember are taken care of by Netwrix Auditor..."

Windows IT Pro

"...best Active Directory/Group Policy product and Best Auditing/Compliance product 4 years in a row..."

Petri IT Knowledgebase

"...full five out of five stars and recommended to anyone with an AD environment give the product a whirl..."

Deployment Options

On-premises, virtual or cloud — deploy Netwrix Auditor wherever you need it

On-premises

Fully supported on **Microsoft's Windows Server** Platform

Virtual

Available in appliances for **VMware and Microsoft Hyper-V**

Cloud

Fully supported and tested in **Microsoft Azure**

Fully supported in **AWS Marketplace**

Windows Server

Microsoft Hyper-V

vmware READY

Microsoft Azure

awsmarketplace

RESTful API — endless integration capabilities for improved visibility and streamlined reporting

Centralize auditing and reporting

Netwrix Auditor collects activity trails from any existing on-premises or cloud applications and stores in a secure central repository, ready for search and reporting.

Get the most from your SIEM investment

By feeding more granular audit data into your HP Arcsight, Splunk, IBM QRadar or other SIEM solution, Netwrix Auditor increases the signal-to-noise ratio and maximizes SIEM value.

Automate IT workflows

You can feed audit data from Netwrix Auditor into other critical IT processes, such as change management or service desk, thereby automating and improving their workflows.

Visit the Netwrix Auditor Add-on Store at **www.netwrix.com/go/add-ons** to find free add-ons built to integrate Netwrix Auditor with your IT ecosystem.

Built for IT environments of all sizes, Netwrix Auditor architecture supports the growth of your organization

Maine.gov

Government, 25K employees
State of Maine meets state and federal security guidelines with Netwrix Auditor.

american career college

Education, 5,5K employees
American Career College ensures campus data security with Netwrix Auditor for Active Directory.

DONOHOE

Construction, 1,4K employees
The Donohoe Companies deployed Netwrix Auditor to solve its data security and accountability challenges.

HERITAGE BANK

Banking and Finance, 100 employees
Heritage Bank relies on Netwrix Auditor to govern essential security and compliance policies.

netwrix

Next Steps

Free Trial: setup in your own test environment

- On-premises: **netwrix.com/freetrial**
- Virtual: **netwrix.com/go/appliance**
- Cloud: **netwrix.com/go/cloud**

Test Drive: virtual POC, try in a Netwrix-hosted test lab **netwrix.com/testdrive**

Live Demo: product tour with Netwrix expert **netwrix.com/livedemo**

Contact Sales to obtain more information **netwrix.com/contactsales**

Awards

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