Netwrix Auditor

Visibility Platform for User Behavior Analysis and Risk Mitigation in Hybrid IT Environments
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 intelligence to identify security holes, detect anomalies in user behavior and investigate threat patterns in time to prevent real damage.

Detect data security threats, both on premises and in the cloud.

Pass compliance audits with less effort and expense.

Increase the productivity of IT security and operations teams.

#completevisibility
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.

#completevisibility
Detect data security threats, both on premises and in the cloud

Netwrix Auditor bridges the visibility gap by delivering security intelligence about critical changes, data access and configurations in hybrid IT environments. Organizations can use this data to continuously assess and proactively mitigate security risks. The platform identifies users with the most anomalous activity over time, and alerts on behavior patterns that indicate a possible insider threat or account takeover. And it makes it easy to investigate any suspicious action or security policy violation so you can quickly determine the best response.

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/HITECH, SOX, GLBA, FISMA/NIST800-53, FERPA, CJIS, NERC CIP, ISO/IEC 27001, GDPR and other standards. It also ensures easy access to your complete audit trail 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 or when and where a change was made. Nor do you need to painstakingly write, maintain and run PowerShell scripts to identify inactive users, report on effective user permissions or perform software inventory tasks. The platform delivers actionable audit data to anyone in your organization who needs it.
In Action: Detect Data Security Threats

Continuously assess and mitigate data security risks

Identify high-risk configurations, such as excessive access permissions for the “Everyone” group or an abundance of directly assigned permissions, that need your immediate attention. Adjust your policy settings or permissions as necessary to minimize the ability of intruders and insiders to cause damage.

Prevent privilege abuse and data breaches

Get a complete picture of effective user permissions in Active Directory and file servers. Lock down overexposed data and make sure that only eligible employees have access to critical resources. Stay aware of any modifications that affect user privileges so you can respond immediately.

#completevisibility
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. Spot surges in anomalous activity, see which users are most active and determine which systems are most affected.

Spot abnormal user behavior that would otherwise go unnoticed

Quickly identify subtle signs of possible threats, 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 reports, no malicious activity can slip under your radar.

#completevisibility
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 many files in a short period of time, which could indicate a ransomware attack.

**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.

**Behavior Anomalies**

<table>
<thead>
<tr>
<th>User</th>
<th>Risk score</th>
<th>Last alert time</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTERPRISE\Tomlinson</td>
<td>725</td>
<td>10/10/2017 7:27:02 AM</td>
</tr>
<tr>
<td>ENTERPRISE\Fishborn</td>
<td>630</td>
<td>10/8/2017 7:25:20 AM</td>
</tr>
<tr>
<td>ENTERPRISE\Lopez</td>
<td>385</td>
<td>10/6/2017 7:28:11 AM</td>
</tr>
<tr>
<td>ENTERPRISE\Jovahni</td>
<td>215</td>
<td>10/5/2017 7:29:32 AM</td>
</tr>
<tr>
<td>ENTERPRISE\Weiner</td>
<td>145</td>
<td>10/2/2017 7:26:14 AM</td>
</tr>
<tr>
<td>ENTERPRISE\Wilmore</td>
<td>98</td>
<td>10/1/2017 7:19:29 AM</td>
</tr>
</tbody>
</table>

Identify high-risk user accounts

Improve the detection of rogue insiders and accounts compromised by external attackers with a single aggregated view of anomalous activity by each individual. Use the associated risk scores to prioritize incidents so you can investigate and determine the best response.

#completevisibility
07
In Action: Detect Data Security Threats

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.

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.

#completevisibility
Centralize IT security monitoring with API-enabled integrations

Centralize security monitoring and reporting by feeding Netwrix Auditor data from other on-premises or cloud applications. You can also use the actionable security intelligence from Netwrix Auditor to augment the output data of your SIEM solution.

**Netwrix Auditor Alert**

**Network routing rule modification**

<table>
<thead>
<tr>
<th>Who</th>
<th>Carter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Modified</td>
</tr>
<tr>
<td>Object type</td>
<td>Configuration</td>
</tr>
<tr>
<td>What</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>When</td>
<td>4/09/2017 12:58:23 PM</td>
</tr>
<tr>
<td>Where</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>Workstation</td>
<td>188.243.82.139</td>
</tr>
<tr>
<td>Monitoring plan</td>
<td>Cisco ASA Visibility Plan</td>
</tr>
<tr>
<td>Details</td>
<td>Raw Message changed from &quot;&quot; to &quot;&lt;165&gt;Apr 30 2017 12:58:23: %ASA-5-111010: User 'Carter', running 'ASDM' from IP 188.243.82.139, executed 'route enterprise 192.169.12.101 255.255.255.255 192.170.10.1 1'&quot;&quot;</td>
</tr>
</tbody>
</table>

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

**Modify Database Retention Settings**

Set a database retention period to clear stale data

- **On**

Store audit data in the database for 180 days

**Archive security analytics data for years**

The two-tiered (file-based + SQL database) AuditArchive™ storage enables you to keep your big data archived for historic e-discovery or security investigations for more than 10 years.

#completevisibility
Enable control over security policies

By supporting the broadest variety of IT systems, Netwrix Auditor helps you implement compliance controls across your entire infrastructure. It serves as a single point of access to the audit trail and enables you to easily provide proof that your security policies are enforced.

In Action: Pass Compliance Audits

New Monitoring Plan
Get ready to monitor your environment. Choose a data source or pick a specific area of interest.

<table>
<thead>
<tr>
<th>Active Directory</th>
<th>Azure AD</th>
<th>Windows File Servers</th>
<th>Exchange</th>
<th>Exchange Online</th>
<th>Share Point</th>
<th>Share Point Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Database</td>
<td>SQL Server</td>
<td>Windows Server</td>
<td>Group Policy</td>
<td>VMware</td>
<td>EMC</td>
<td>NetApp</td>
</tr>
<tr>
<td>Logon Activity</td>
<td>User Activity</td>
<td>Integration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Risk</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folders with &quot;Everyone&quot; group access</td>
<td>■ Acceptable</td>
</tr>
<tr>
<td>File names containing sensitive data</td>
<td>■ Acceptable</td>
</tr>
<tr>
<td>Potentially harmful files on file shares</td>
<td>■ Pay attention</td>
</tr>
<tr>
<td>Direct permissions on files and folders</td>
<td>■ Take action</td>
</tr>
</tbody>
</table>

Demonstrate a proactive approach to risk mitigation

Visualize your security posture and impress auditors with interactive risk assessment dashboards. Use them to prove your ability to continuously evaluate and reduce risks to protected data.

#completevisibility
Slash preparation time for audits and prove your compliance using out-of-the-box reports aligned with the compliance controls of FISMA, GDPR, HIPAA/HITECH, PCI DSS, SOX and many other common regulations.

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

Slash preparation time for audits and prove your compliance using out-of-the-box reports aligned with the compliance controls of FISMA, GDPR, HIPAA/HITECH, PCI DSS, SOX and many other common regulations.

Prove that compliance controls are — and have always been — in place

Demonstrate to auditors that group membership, effective user permissions and other configurations in your environment have always been in line with security policies. Easily compare current and past configurations to prove that no unauthorized changes took place.

#completevisibility
In Action: Pass Compliance Audits

Address auditor’s questions faster

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

Long-Term Archive

Location and retention settings for the local file-based storage of audit data.

Location and retention settings

- Write audit data to: C:\Program Data\Netwrix Auditor\Data
- Keep audit data for: 60 months
- Netwrix Auditor uses the LocalSystem account to write audit data to the Long-Term Archive

Store and access your audit trail for years

Many compliance regulations require organizations to retain their audit trails for extended periods. Netwrix Auditor enables you to keep your audit trail archived in a compressed format for more than 10 years, while ensuring that all audit data can easily be accessed by authorized users at any time.

#completevisibility
In Action: Increase the Productivity of IT Teams

Keep tabs on what’s happening in your environment

Monitor all changes across your on-premises and cloud-based IT systems. See when a specific change was made, who made it, and what was changed, with the before and after values. Use this information to verify the purpose of each change and revert unwanted modifications before they turn into a problem.

<table>
<thead>
<tr>
<th>Action</th>
<th>What</th>
<th>Who</th>
<th>When</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where:</td>
<td>dc1.enterprise.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workstation:</td>
<td>172.17.35.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path:</td>
<td>Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/ Account Policies/Password Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modified</td>
<td>Policy: Enforce password history; Setting: 24 passwords remembered -&gt; 3 passwords remembered;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modified</td>
<td>Modified Policy: Maximum password age; Setting: 20 days -&gt; 200 days;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modified</td>
<td>Modified Policy: Minimum password length; Setting: 7 characters-&gt; 4 characters;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Maintain good IT hygiene

Create a cleaner and more manageable environment using Netwrix Auditor’s state-in-time reports. Regularly review your identity and access configurations, and easily verify that they match a known good state.

Account Permissions in Active Directory

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

<table>
<thead>
<tr>
<th>Object Name</th>
<th>Object Type</th>
<th>Means Granted</th>
</tr>
</thead>
<tbody>
<tr>
<td>\com\enterprise\Computers</td>
<td>container</td>
<td>Directly</td>
</tr>
<tr>
<td>\com\enterprise</td>
<td>domainDNS</td>
<td>Group</td>
</tr>
<tr>
<td>\com\enterprise\Builtin</td>
<td>builtinDomain</td>
<td>Group</td>
</tr>
<tr>
<td>\com\enterprise\Builtin\Account Operators</td>
<td>group</td>
<td>Group</td>
</tr>
<tr>
<td>\com\enterprise\Builtin\Administrators</td>
<td>group</td>
<td>Group</td>
</tr>
<tr>
<td>\com\enterprise\Builtin\Backup Operators</td>
<td>group</td>
<td>Group</td>
</tr>
</tbody>
</table>

#completevisibility
In Action: Increase the Productivity of IT Teams

Simplify reporting routines

Netwrix Auditor supplies more than 200 predefined reports and dashboards that are easy to narrow down using built-in filtering, grouping and sorting. You can also easily address any specific security and compliance concerns by building custom reports using the Interactive Search feature.

![Data Access Trend](image)

**Activity by Date**

**Deletions**

**Modifications**

**Reads**

Netwrix Auditor 9.5

Visibility Platform for User Behavior Analysis and Risk Mitigation

- **Quick Start**
  - New Active Directory Plan
  - New Windows File Servers Plan
  - New Windows Server Plan
  - New SQL Server Plan
  - New Exchange Plan
  - New Exchange Online Plan
  - New Azure AD Plan
  - All data sources

- **Intelligence**
  - Search
  - Behavior anomalies
  - Failed activity trend
  - User account status changes
  - Activity outside business hours
  - Logs by single user from multiple endpoints
  - Administrative group and role changes
  - AD or Group Policy modifications by administrator

- **Configuration**
  - Monitoring Plans
  - Alerts
  - Subscriptions
  - Integration
  - Health log
  - Settings

Speed report delivery

Netwrix Auditor can automatically generate reports on the schedule you specify and either email them to stakeholders or save them in a dedicated file share for easy reference. Alternatively, you can give stakeholders access to Netwrix Auditor so they can generate the reports they need on demand.

#completevisibility
Minimize system downtime

If an unauthorized or inappropriate change is made to your environment, you can quickly turn back the clock by reverting the settings to a previous state — without any downtime or having to restore from backup.

**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.

**Focus on what’s really important**

Regularly run risk assessments to pinpoint the areas that need your immediate attention. Use alerts to stay aware of actions you consider critical, such as the deletion of business-critical files or changes to your SQL Server configuration.
Addressing the Security and Compliance Challenges of Your Department and Your Business

**CIO/IT Director**
Keep your IT environment clean, manageable and secure.

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

**System Administrator**
Generate and deliver security and compliance reports faster.

**CISO**
Prevent data breaches and minimize compliance costs.

**Security Analyst**
Identify security gaps and investigate suspicious user activity in time to prevent real damage.

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

#completevisibility
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

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

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

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

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

Copyright © Netwrix Corporation. All rights reserved. Netwrix is trademark of Netwrix Corporation and/or one or more of its subsidiaries and may be registered in the U.S. Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are the property of their respective owners.