



netwrix

Netwrix Auditor

Vollständige Sichtbarkeit von Hybrid-Cloud-IT-Umgebungen



netwrix.com | netwrix.com/social

01

Produktüberblick

Netwrix Auditor Plattform

Netwrix Auditor ist eine Plattform für Sichtbarkeit und Steuerung, mit der die Kontrolle über Änderungen, Konfiguration und Zugriffe für Hybrid-Cloud-IT-Umgebungen unterstützt wird, um unstrukturierte Daten unabhängig vom Speicherort zu schützen. Die Plattform ermöglicht Sicherheitsanalysen für die Erkennung von ungewöhnlichem Benutzerverhalten und die Untersuchung von Bedrohungsmustern, noch bevor eine Datenschutzverletzung auftritt.



**Erkennen Sie
Bedrohungen der
Datensicherheit** —
Lokal und in der Cloud.

**Bestehen Sie
Compliance-Audits**
mit weniger Aufwand
und Kosten.

**Verbessern Sie die
Produktivität** Ihrer
Sicherheits- und
Betriebs-Teams.

02

Anwendungen

Netwrix Auditor Anwendungen

Netwrix Auditor beinhaltet Anwendungen für Active Directory, Exchange, Office 365, Windows Dateiserver, EMC Speichergeräte, NetApp File Appliances, SharePoint, SQL Server, VMware und Windows Server. Die Plattform ist mit RESTful API und Videoaufzeichnung von Benutzeraktivitäten ausgestattet und bietet eine einheitliche Sichtbarkeit und Steuerung für all Ihre IT-Systeme, egal ob lokal oder in der Cloud.



Netwrix Auditor for
Office 365



Netwrix Auditor for
NetApp



Netwrix Auditor for
EMC



Netwrix Auditor for
Active Directory



Netwrix Auditor for
File Servers



Netwrix Auditor for
Windows Server



Netwrix Auditor for
VMware



Netwrix Auditor for
Exchange



Netwrix Auditor for
SQL Server



Netwrix Auditor for
SharePoint

03

Vorteile

Erkennen Sie Bedrohungen der Datensicherheit — Lokal und in der Cloud

Netwrix Auditor schließt die Lücke in der Sichtbarkeit durch Sicherheitsanalysen bei kritischen Änderungen, dem Status von Konfigurationen und Datenzugriffen in Hybrid-Cloud-IT-Umgebungen und unterstützt die Untersuchung von verdächtigem Benutzerverhalten. Die Plattform ermöglicht außerdem eine Alarmierung bei Vorgängen, welche die Sicherheitsvorschriften des Unternehmens verletzen und auf mögliche Bedrohungen durch Insider hinweisen.

Bestehen Sie Compliance-Audits mit weniger Aufwand und Kosten

Netwrix Auditor liefert die Nachweise, die erforderlich sind, um zu beweisen, dass das IT-Sicherheitsprogramm Ihrer Organisation alle Standards wie PCI DSS, HIPAA, HITECH, SOX, FISMA/NIST800-53, COBIT, ISO/IEC 27001 und andere einhält. Außerdem wird der einfache Zugriff auf Compliance-Berichte über einen Zeitraum von mehr als 10 Jahren gewährleistet.

Verbessern Sie die Produktivität von Sicherheits- und Betriebs- Teams

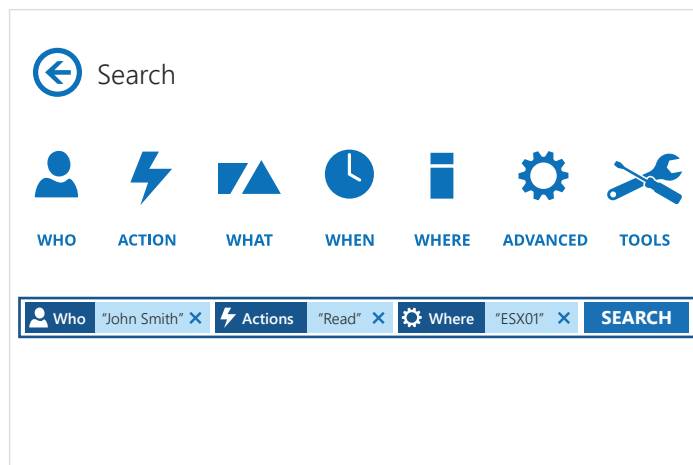
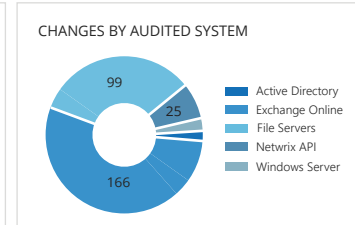
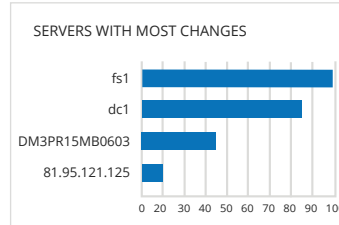
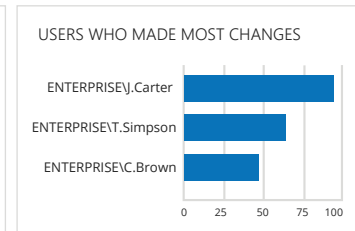
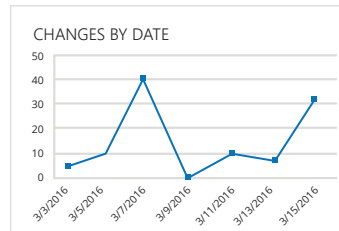
Mit Netwrix Auditor besteht keine Notwendigkeit zum Durchforsten von Wochen an Log-Daten, um Fragen zu beantworten, wie zum Beispiel: wer hat was geändert, wann und wo wurde die Änderung durchgeführt oder wer hat worauf Zugriff. Die Plattform stellt Audit-Daten, auf die reagiert werden kann, für alle Mitarbeiter Ihrer Organisation zur Verfügung, die diese benötigen.

04

In Aktion: Erkennen Sie Bedrohungen der Datensicherheit

Erkennen Sie frühzeitig verdächtige Insider-Aktivitäten

Verschaffen Sie sich mithilfe von Enterprise Overview-Dashboards einen Überblick über die Aktivitäten von Mitarbeitern in Ihrer IT-Infrastruktur. Erkennen Sie, wie oft Änderungen durchgeführt werden, welche Benutzer verdächtige Aktionen durchführen, welche Systeme betroffen sind und mehr.



Untersuchen Sie ungewöhnliches Benutzerverhalten

Wann immer Sie eine Änderung oder einen Datenzugriffsversuch erkennen, der die Sicherheitsrichtlinien Ihres Unternehmens verletzt, können Sie die Google-ähnliche Suche verwenden, um zu untersuchen, warum und wie es passierte, um ähnliche Vorfälle in der Zukunft zu verhindern.

05

In Aktion: Erkennen Sie Bedrohungen der Datensicherheit

Verhindern Sie das Herausfiltern von Daten

Stellen Sie sicher, dass nur die berechtigten Mitarbeiter Ihrer Organisation Zugriff auf kritische Ressourcen haben, indem Sie sich ein Gesamtbild der gültigen Berechtigungen und Dateiaktivitäten auf Ihren Dateiservern und NAS verschaffen.

Object Permissions by Object

Shows accounts with their inherited or explicitly assigned basic permissions allowing them to access folders and subfolders, results are grouped by object path.

Folder path: \\fs1\Management\Finance

User Account	Permissions	User Permissions Inheritance
ENTERPRISE\Administrators	List folder/ read data Read attributes Read extended attributes Read permissions Change permissions	Explicit
ENTERPRISE\J.Smith	List folder/ read data Read attributes Read extended attributes Read permissions Change permissions	Inherited

Failed Read Attempts

Shows unauthorized file access attempts. This report can be used for compliance audit 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	9/26/2015 3:03:08 PM
Where:	ENTWKS0412			
■ Read (Failed Attempt)	File	\\fs1\Finance\Accounting\Statement0313.xlsx	ENTERPRISE\S.Hernandez	9/26/2015 3:05:38 PM
Where:	ENTWKS0524			
■ Read (Failed Attempt)	File	\\fs1\HR\NewHire\SalaryList.xlsx	ENTERPRISE\K.Davis	9/26/2015 3:07:23 PM
Where:	172.17.4.34			

Überwachen Sie den Zugriff auf unstrukturierte Daten

Egal ob Ihre Dateien Daten von Karteninhabern, medizinische Aufzeichnungen oder Finanzberichte enthalten, Netwrix Auditor zeigt auf, wer (mit oder ohne Erfolg) versucht hat, auf die Dateien zuzugreifen, und wann bzw. wo der Versuch stattfand.

06

In Aktion: Erkennen Sie Bedrohungen der Datensicherheit

Sperren Sie den Zugriff auf unzureichend gesicherte Daten

Erkennen Sie unnötige Zugriffsberechtigungen auf unstrukturierte Daten, um diese zu sperren und das Risiko von Privilegienmissbrauch zu verringern.

Excessive Access Permissions

Shows accounts with permissions for infrequently accessed files and folders. Use this report for spotting unnecessary permissions and preventing data leaks.

Object: \\fs1\shared (Permissions: Different from parent)

Action	Permissions	Means Granted	Times Accessed
ENTERPRISE\Administrator	Full Control	Group	258
ENTERPRISE\B.Atkins	Read (Execute, List folder content)	Group	14280
ENTERPRISE\H.Malicious	Read (Execute, List folder content)	Group	1745
ENTERPRISE\K.Smith	Read (Execute, List folder content)	Group	10020

Object: \\fs1\shared\Finance (Permissions: Same as parent)

Action	Permissions	Means Granted	Times Accessed
ENTERPRISE\B.Atkins	Modify (Read, Write, Execute)	Group	8680
ENTERPRISE\H.Malicious	Full Control	Directly	966

Changes to Admin Group Memberships

Enable

Description:

Alert on changes to the Domain Admins and Enterprise Domain Admins groups Edit...

Alert Filters

Specify filters for the changes that must trigger alerts:

- Addition to Enterprise Admins Group
- Removal from Enterprise Admins Group
- Addition to Domain Admins Group
- Removal from Domain Admins Group

Add... Remove Edit...

Notifications

Recipient	Type	Format
Administrator@enterprise.com	Email	Html

Add...

Lassen Sie sich bei Bedrohungsmustern alarmieren

Lassen Sie sich über nicht autorisierte Änderungen alarmieren, während diese stattfinden, damit Sie Sicherheitsverletzungen verhindern können. Sie können sich beispielsweise benachrichtigen lassen, wenn jemand zur Enterprise Admins-Gruppe hinzugefügt wird oder wenn ein Benutzer auf zu viele Dateien gleichzeitig zugegriffen hat.

07

In Aktion: Erkennen Sie Bedrohungen der Datensicherheit

Erkennen Sie, was sonst nicht zu erkennen ist


Verschaffen Sie sich Einsicht in alle Systeme und Anwendungen, auch wenn diese keine Log-Daten erzeugen, indem Sie Videoaufzeichnungen der Bildschirmaktivitäten von Benutzern erstellen. Sie können die Aufzeichnungen durchsuchen und abspielen, um genau festzustellen, welche Aktionen durchgeführt wurden.

Activity Records

Generate a summary of video records

Date 9/25/2014

Computer	User	Start Time	End Time	Duration
dc1.enterprise.com	ENTERPRISE\J.Smith	9/25/2015 4:12 PM	9/25/2015 4:17 PM	00:05:15
dc1.enterprise.com	ENTERPRISE\J.Smith	9/25/2015 5:12 PM	9/25/2015 5:13 PM	00:01:15





Long Term Archive

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

Location and retention settings

Modify...

Write audit data to: C:\ProgramData\Netwrix Auditor\Data

Keep audit data for: 24 months

Archivieren Sie Daten von Sicherheitsanalysen über Jahre

Die zweistufige AuditArchive™ Abspeicherung (dateibasiert + SQL-Datenbank) ermöglicht die Aufbewahrung von Big Data über mehr als 10 Jahre, um historische Vorgänge elektronisch aufzudecken oder Sicherheitsuntersuchungen durchzuführen.

08

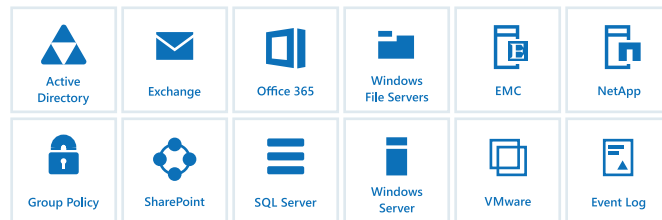
In Aktion: Bestehen Sie Compliance-Audits

Verschaffen Sie sich die Kontrolle über Sicherheitsrichtlinien

Netwrix Auditor unterstützt das breiteste Spektrum an IT-Systemen, egal ob lokal oder in der Cloud, und ermöglicht damit Compliance-Überprüfungen der gesamten IT-Infrastruktur und dient als einziger Zugangspunkt zu Prüfprotokollen.

Welcome to Netwrix Auditor

Click the tile below to create a Managed Object to define the auditing scope.



Who	Object type	Action	What	Where	When
ENTERPRISE\ J.Smith	Group	Modified	\enterprise\Users\ Domain Admins	dc1.enterprise.com	4/28/2015 1:05:34 PM
Security Global Group Member: -Added: "\enterprise\Users\George Moore"					
ENTERPRISE\ G.Davis	Group	Modified	\enterprise\Users\ Accountants	dc1.enterprise.com	4/29/2015 11:25:36 AM
Security Global Group Member: -Added: "\enterprise\Users\Roy Taylor"					

Beantworten Sie Fragen von Auditoren schneller

Liefen Sie schnell Antworten auf die Fragen von Auditoren, beispielsweise welche Änderungen an der Gruppe Enterprise Domain Admins im vergangenen Jahr stattfanden oder wer diese Änderungen durchgeführt hat. Mit Netwrix Auditor kann jetzt in Minuten erledigt werden, was früher Wochen dauerte.

09

In Aktion: Bestehen Sie Compliance-Audits

Nutzen Sie vordefinierte Compliance-Berichte

Auditoren möchten bewiesen haben, dass bestimmte Prozesse und Kontrollen vorhanden sind und dies auch in der Vergangenheit waren. Beweisen Sie Ihre Compliance anhand von vordefinierten Berichten, die den Anforderungen von Compliance-Kontrollen entsprechen.

The screenshot shows the 'Reports' section of the Netwrix Auditor interface. It features a navigation menu with 'ALL REPORTS' and 'COMPLIANCE' tabs. A search bar is present above a list of compliance categories: FISMA Compliance, HIPAA Compliance, ISO/IEC 27001 Compliance, PCI DSS v3.0, and SOX Compliance. To the right, a list of specific audit events is displayed, including 'User Accounts Group Membership', 'User Accounts Last Logon Time', 'All Group Policy Changes by Group', 'Account Policy Changes', 'Audit Policy Changes', 'Interactive Logon Settings Changes', 'Password Policy Changes', and 'Restricted Groups Policy Changes'. Below this, a detailed view for a specific event is shown for the group '\Enterprise\Users\Domain Users'. The event table is as follows:

Action	Who	What	When
Added	ENTERPRISE\J.Brown	Audit Object Access Policy	4/30/2015 2:29:11 AM
Where:	dc1.enterprise.com		
Workstation:	172.17.34.23		

The screenshot shows the 'AuditIntelligence' settings page. It includes a sub-header 'AuditIntelligence' and a description: 'Default Audit Database settings required to take advantage of AuditIntelligence provided by the Netwrix Auditor client.' Below this, the 'Database Retention' section is visible, showing that 'Database retention enabled' is set to 'Yes' and 'Store audit data in the database for' is set to '180 days'. A 'Modify...' button is located to the right of the retention settings.

Speichern Sie Ihre Prüfprotokolle, und greifen Sie noch nach Jahren darauf zu

Viele Compliance-Vorschriften verlangen, dass Organisationen ihre Prüfprotokolle über längere Zeiträume aufbewahren. Netwrix Auditor gibt Ihnen die Möglichkeit, Ihre Prüfprotokolle im komprimierten Format mehr als 10 Jahre lang aufzubewahren, wobei sichergestellt ist, dass jederzeit auf einfache Weise auf die Daten zugegriffen werden kann.

10

In Aktion: Verbessern Sie die Produktivität von IT-Teams

Bleiben Sie auf dem Laufenden darüber, was sich in Ihrer Umgebung ändert

Erkennen Sie, wann eine bestimmte Änderung durchgeführt wurde, wer sie vorgenommen hat und was geändert wurde, einschließlich der Werte vor und nach der Änderung. Diese detaillierten Informationen sind für alle Änderungen Ihrer IT-Systeme verfügbar, egal ob lokal oder in der Cloud.

All Changes by User

Shows all changes across the entire IT infrastructure grouped by the users who made the changes.

Who Changed: ENTERPRISE\F.Wilson

Audited System: Active Directory

Action	Object Type	What	When
Modified	User	\enterprise\Users\Glen Williams	9/09/2015 4:31:49 PM

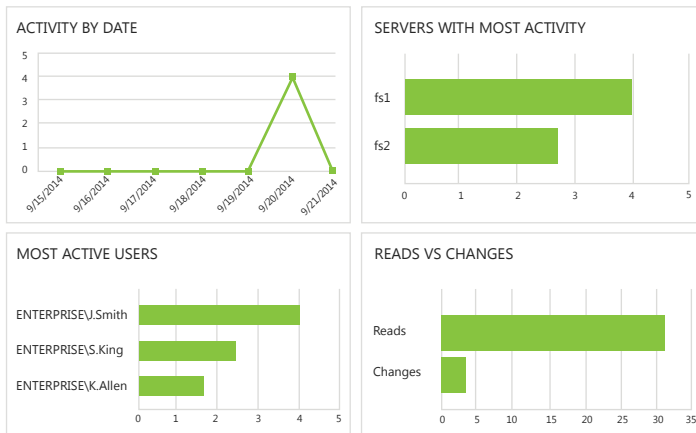
Where: ex1.enterprise.com
Principal Name set to "Glen.Williams@enterprise.com"

Audited System: VMware

Action	Object Type	What	When
Removed	VirtualMachine	\ha-folder-root\ha-datacenter\vm1	9/11/2015 3:11:41 PM

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

File Servers Overview



Vereinfachen Sie das Berichtswesen

Netwrix Auditor beinhaltet mehr als 200 vordefinierte Berichte und Dashboards, die einfach mit integrierten Filter-, Gruppierungs- und Sortierfunktionen angepasst werden können. Sie können die Daten als PDF, XLS und in anderen Formaten exportieren, E-Mail-Benachrichtigungen aufsetzen und vieles mehr.

11

In Aktion: Verbessern Sie die Produktivität von IT-Teams

Beschleunigen Sie die Berichtserstellung

Eliminieren Sie langsame, manuelle Berichtserstellungsverfahren, bei denen Benutzer die benötigten Berichte bei IT anfordern und lange darauf warten müssen. Mit Netwrix Auditor können berechtigte Personen regelmäßig erstellte Berichte abonnieren oder mithilfe des Netwrix Auditor Client bei Bedarf Berichte generieren.



Active Directory Object Restore

Select Rollback Source

Restore from state-in-time snapshots

This option allows restoring deleted AD objects down to their attribute level based on the state-in-time snapshots made by Netwrix Auditor.

Monitored domain:

Select a state-in-time snapshot

Restore from AD tombstones

This option provides partial AD objects restore based on the information retained on deleted AD objects tombstones. Use this option if no state-in-time snapshots are available for the selected period.

Audited domain:

Minimieren Sie Systemausfälle

Wenn eine nicht autorisierte Änderung durchgeführt wird, welche die Systemverfügbarkeit beeinträchtigt, können Sie diese schnell auf den vorherigen Status zurücksetzen, ohne Ausfallzeiten oder das Zurückladen von Backup-Daten.

12

In Aktion: Verbessern Sie die Produktivität von IT-Teams

Konzentrieren Sie sich auf die wirklich wichtigen Dinge

Verwenden Sie Alarme, um sicherzustellen, dass Sie über kritische Systemkonfigurationsänderungen informiert werden, während diese stattfinden. Sie können die spezifischen Änderungsvorgänge auswählen, bei denen Sie alarmiert werden möchten, wie beispielsweise Änderungen bei den Mitgliedern der Domain Admins-Gruppe.

Real-time Alert

Changes to Admin Group Membership

Severity	Critical
Domain	ENTERPRISE.COM
Change Type	Modified
Object Type	Group
When Changed	7/6/2015 4:58:53 AM
Who Changed	ENTERPRISE\J.Smith
Where Changed	dc1.enterprise.com
Object Name	\enterprise\Users\Domain Admins
Details	Security Global Group Member: • Added: "\enterprise\Users\Nick White"

All Group Policy Changes

Shows all changes to Group Policy objects, settings, GPO links and permissions with the name of the originating workstation from which a user made the change.

Action	What	Who	When
■ Modified	Security Policy	ENTERPRISE\J.Smith	7/23/2015 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	Modified Policy: Maximum password age; Setting: 20 days -> 200 days; Modified Policy: Minimum password length; Setting: 7 characters-> 4 characters;		

Beschleunigen Sie die Fehlersuche

Wenn ein Problem auftritt, liefert Ihnen Netwrix Auditor nicht Berge von Rohdaten, die Sie durchsuchen müssen, sondern sinnvolle Einsichten, auf die sie reagieren können und mit denen Sie schnell die Abläufe untersuchen und die zugrundeliegende Ursache des Problems erkennen können.

13

Adressieren Sie die Herausforderungen Ihres Bereichs und Ihres Unternehmen in Bezug auf IT-Audits

System Administrator

Erzeugen und liefern Sie Audit- und Compliance-Berichte schneller als je zuvor

Untersuchen Sie verdächtiges Benutzerverhalten, bevor eine Sicherheitsverletzung entsteht.

IT Manager

Übernehmen Sie die Kontrolle über Ihre IT-Infrastruktur und bestehen Sie Ihren nächsten Compliance-Audit ohne unnötigen Stress.

MSP

Steigern Sie Ihren Umsatz, indem Sie gemanagte Umgebungen transparent machen und Compliance als Service anbieten.

IT

Sicherheits-Administrator

Verhindern Sie Datenschutzverletzungen und minimieren Sie die Compliance-Kosten.

CIO/CISO

Berichterstattung durch Analysten



Gartner

„...Werkzeuge für das Auditing unterstützen bei der Analyse von Konfigurationen in Bezug auf Best Practices und helfen bei der Einführung von Konfigurationsstandards und der Einhaltung von Richtlinienanforderungen...“



Redmond
MAGAZINE

„...Audits sind im Allgemeinen eine schwierige Aufgabe, insbesondere, wenn sie manuell durchgeführt werden. Netwrix Auditor kümmert sich um all die vielen Details, die Sie beachten und deren Einhaltung Sie überwachen müssen...“



Windows IT Pro

„...4 Jahre hintereinander bestes Active Directory/Group Policy Produkt und bestes Auditing/Compliance Produkt...“



Petri
IT Knowledgebase

„...volle fünf von fünf möglichen Sternen und Empfehlung an alle, die eine AD-Umgebung haben, das Produkt unter die Lupe zu nehmen...“

Implementierungsoptionen

Lokal, virtuell oder in der Cloud – implementieren Sie Netwrix Auditor, wo immer Sie ihn benötigen

Lokal

Volle Unterstützung auf der **Microsoft Windows Server** Plattform

Virtuell

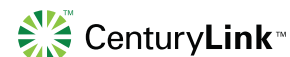
Verfügbar als Appliance für **VMware und Microsoft Hyper-V**

Cloud

Volle Unterstützung und getestet unter **Microsoft Azure**

Volle Unterstützung unter **AWS Marketplace**

Volle Unterstützung unter **CenturyLink Cloud Marketplace**



RESTful API — grenzenlose Integrations-, Auditing- und Berichtsmöglichkeiten



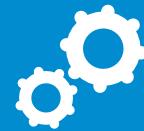
Zentralisieren Sie Auditing und Berichtswesen

Netwrix Auditor sammelt die Audit-Daten aller Anwendungen, egal ob lokal oder in der Cloud, und speichert sie an einem sicheren zentralen Ort, wo sie durchsucht und für Berichte genutzt werden können.



Nutzen Sie Ihre Investitionen in SIEM optimal

Netwrix Auditor führt Ihrer HP Arcsight, Splunk, QRadar oder anderen SIEM-Lösung granulare Daten zu und erhöht damit den Anteil nutzbarer Daten, um die SIEM-Lösung optimal nutzen zu können.



Automatisieren Sie IT-Arbeitsabläufe

Sie können die Audit-Daten von Netwrix Auditor an andere wichtige IT-Funktionen weiterleiten, wie beispielsweise das Änderungsmanagement oder die Service-Funktion, um Arbeitsabläufe zu automatisieren und optimieren.

Die Netwrix Auditor-Architektur wurde für IT-Umgebungen beliebiger Größe entwickelt und unterstützt das Wachstum Ihrer Organisation



**Luftfahrt & Verteidigung,
45.000 Mitarbeiter**

L-3 Communications setzt Netwrix ein, um Änderungen an Active Directory und Group Policy nachzuverfolgen und damit SOX-Compliance-Anforderungen zu erfüllen.

**american
career
college**

**Bildung,
5500 Mitarbeiter**

American Career College sorgt für Datensicherheit auf dem Campus mit Netwrix Auditor für Active Directory.



**Technologie,
1300 Mitarbeiter**

Auch bei IT-Erweiterungen kontrolliert Belkin Änderungen in Active Directory und Exchange Server mit Netwrix.



**Bank-und Finanzwesen,
100 Mitarbeiter**

Heritage Bank nutzt Netwrix Auditor, um die Einhaltung wichtiger Sicherheits- und Compliance-Richtlinien sicherzustellen.



Nächste Schritte

Kostenlose Testversion: Richten Sie Ihre eigene Testumgebung ein netwrix.com/freetrial

Test: virtuelles POC, Test in einem bei Netwrix gehosteten Testlabor netwrix.com/testdrive

Live-Demo: Produktvorstellung durch einen Netwrix-Experten netwrix.com/livedemo

Kontaktieren Sie den Vertrieb für weitere Informationen netwrix.com/contactsales

Awards



Corporate Headquarters:

300 Spectrum Center Drive, Suite 1100, Irvine, CA 92618

Netwrix Deutschland: +49 711 899 89 187 **Schweiz:** +41 43 508 34 72 **Österreich:** +43 72 0775872

Vertreten durch unseren Partner:

UBM GmbH Austria
Aschau Dorf 36
A-6365 Kirchberg in Tirol
austria@ubm-global.com
Tel: +43 (0) 5357 7110
Fax: +43 (0) 5357 7111

UBM GmbH Germany
Siemensstrasse 24
D-85716 Unterschleissheim
germany@ubm-global.com
Tel: +49 (0) 89 3215 2810
Fax: +49 (0) 89 3215 2811

UBM GmbH Switzerland
Friedeggstrasse 13
CH-3400 Burgdorf
switzerland@ubm-global.com
Tel: +41 (0) 34 427 1065
Fax: +41 (0) 34 427 1066



netwrix
reseller gold

netwrix.com/social

