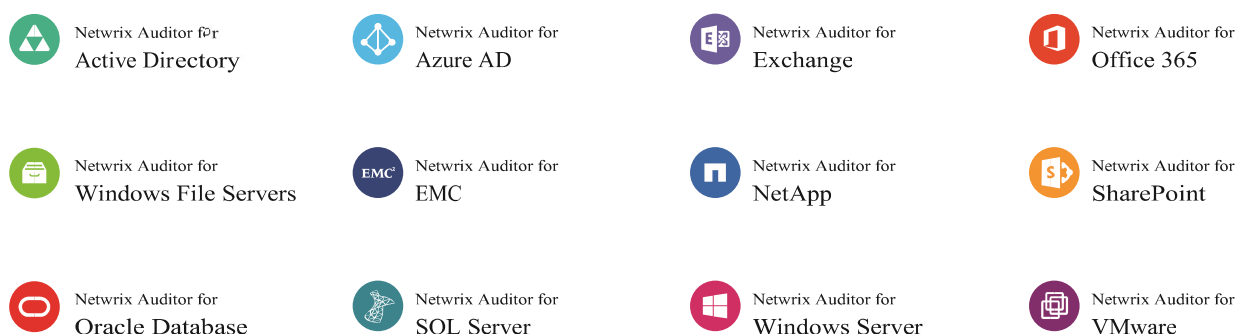


# Cosa è Netwrix Auditor?

**Netwrix Auditor** è una piattaforma di visibilità e di governance che permette di controllare modifiche, configurazioni e l'accesso in ambienti IT hybrid cloud per proteggere i dati indipendentemente da dove si trovino. La piattaforma fornisce analisi di sicurezza per rilevare anomalie nel comportamento degli utenti e indagare sulle minacce prima che si verifichi una violazione dei dati.

Netwrix Auditor include le applicazioni per 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. La piattaforma offre visibilità e controllo su tutti i tuoi sistemi IT on-premise o basati sul cloud in modo unificato.



# Cosa fa Netwrix Auditor ?

## Rileva minacce alla sicurezza dei dati – On Premises e nel Cloud

Netwrix Auditor offre visibilità, fornendo analisi di sicurezza sui cambiamenti critici, le configurazioni e l'accesso ai dati in ambienti IT hybrid cloud e consente di indagare su comportamenti sospetti degli utenti. La piattaforma fornisce inoltre alert su azioni che violano le policy di sicurezza aziendale e indicano una possibile minaccia insider.

## Permette di passare Audit di Compliance con meno sforzo e costi

Netwrix Auditor fornisce le prove necessarie per dimostrare che i programmi di sicurezza IT della propria organizzazione siano conformi a PCI DSS, HIPAA, SOX, GLBA, FISMA / NIST800-53, COBIT, FERPA, NERC CIP, ISO / IEC 27001, **GDPR**, DGL 196/03 e altri standard. Essa garantisce anche un facile accesso ai report di conformità per più di 10 anni.

## Aumenta la produttività dei team di Sicurezza e Operation

Con Netwrix Auditor, non c'è bisogno di cercare attraverso settimane di dati di log peraltro illeggibili e difficilmente interpretabili per rispondere alle domande su chi cambiato cosa, quando e dove un cambiamento è stato fatto, o chi ha accesso a cosa. La piattaforma fornisce dati di controllo fruibili a chiunque ne abbia necessità nella propria organizzazione.

**Identificare, valutare e ridurre i rischi per la tua Infrastruttura IT e i dati**



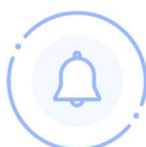
Copyright © Netwrix Corporation. All rights reserved. Netwrix is trademark of Netwrix Corporation and/or one or more of its subsidiaries and may be registered



### User Behavior e Blind Spot Analysis:

Netwrix Auditor consolida e correla i dati provenienti da più sistemi per individuare gli accessi sospetti, l'accesso insolito ai dati sensibili, attività fuori orario di lavoro, la creazione di account temporanei e altre minacce alla sicurezza. I report predefiniti ti permettono di identificare velocemente diritti d'accesso eccessivi, dati sovraesposti, e azioni sospette sui file. Determina chi possiede quali dati e quali file sono inutili o duplicati. Ottieni le risposte a domande come:

- Chi ha l'accesso a dati che non dovrebbe avere?
- C'è stata un'attività insolita che indica una minaccia ransomware?
- C'è stato un accesso anomalo ai dati sensibili?
- Ci sono attività anomale fuori dall'orario lavorativo?



### Alert personalizzabili su modelli di minacce - Alerts on Threat Patterns

Con Netwrix Auditor è possibile creare alert personalizzati su attività non autorizzate in tempo reale per prevenire violazioni alla sicurezza. Ad esempio, puoi scegliere di essere avvisato ogni volta che qualcuno è stato aggiunto al gruppo Enterprise Admins o un utente ha modificato troppi file in un determinato tempo, che potrebbe indicare un attacco ransomware in corso.

- Alert per tutti i sistemi
- Lista di avvisi predefiniti
- Alert personalizzabili
- Avvisi su soglia



### RESTful API - integrazione, capacità di auditing e report infiniti

**Data in:** Centralizza l'auditing e il reporting fornendo a Netwrix Auditor i dati di audit da qualsiasi applicazione esistente on premises o in cloud.

**Data out:** Puoi integrare i dati dettagliati di Netwrix Auditor ai processi critici per IT, come ad esempio change management o service desk, per l'eventuale trattamento automatizzato ed efficace.

Visita il nostro Add-on Store per vedere quali benefici puoi trarre da RESTful API con addons per **Linux, Unix, Cisco, ServiceNow, Amazon Web Services, Splunk, Alien Vault, IBM Qradar, Solarwinds, Intel, LogRhythm e HP ArcSight:** [www.netwrix.com/netwrix\\_addons.html](http://www.netwrix.com/netwrix_addons.html)



### On premises, in ambiente virtuale o in cloud - installa Netwrix Auditor ovunque ne hai bisogno

Oltre all'installazione tradizionale "on premises", Netwrix Auditor offre due opzioni di installazione che migliorano il "time-to-value" dando la possibilità di avviare lo strumento in soli 15 minuti:

**Ambiente virtuale:** Scarica il nostro virtual appliance, pronto per Microsoft Hyper-V e VMware hypervisor: [www.netwrix.com/virtual\\_appliances.html](http://www.netwrix.com/virtual_appliances.html)

**Cloud:** Visita i marketplace di Microsoft Azure, Amazon o CenturyLink per installare Netwrix Auditor in cloud.



### Controllo degli accessi basato sui ruoli

Assegna i ruoli di accesso alla piattaforma in maniera granulare in base alle esigenze ed alle competenze dei tuoi colleghi.

#### Netwrix Auditor ruoli:

- Reviewer
- Configurator
- Global Administrator



### Report per la compliance pronti all'uso

Migliora il tempo di preparazione dei controlli di audit del 50% o più

#### Report e documentazione disponibile pronta all'uso:

- GDPR
- ISO 27001
- PCI-DSS
- SOX
- HIPPA e molti altri



### Archiviazione e accesso ai dati per anni

Netwrix Auditor archivia in modo sicuro a due livelli il vostro audit trail in un formato compresso per più di 10 anni, consentendo di rispettare le policy interne e le normative esterne. Si può facilmente accedere ai dati di audit archiviati in qualsiasi momento, per analisi di sicurezza o indagini storiche





## IT Risk Assessment

Identifica e dai priorità ai rischi per prendere decisioni di sicurezza IT più intelligenti e colmare i buchi di sicurezza.

- Un set di dashboard interattive
- Intelligenza utilizzabile per identificare e colmare lacune di sicurezza
- Basato su dati State-in-Time

### IT Risk Assessment: Overview

Gives you a bird's eye view of risks in your organization. Control and mitigate your IT risks by continuously monitoring and addressing weak points in your environment, such as chaotically organized privilege structure, "shadow" user and computer accounts, and improper content on your file shares.

**Total risk level for Permissions:** ■ Acceptable

Risk	Level
User accounts with administrative privileges	■ Acceptable
Administrative groups	■ Acceptable
Empty security groups	■ Acceptable

**Total risk level for Data:** ■ Take action

Risk	Level
Shared folders accessible by Everyone	■ Take action
File names containing sensitive data	■ Take action
Potentially harmful files on file shares	■ Take action
Direct permissions on files and folders	■ Pay attention

**Total risk level for Users and Computers:** ■ Pay attention

Risk	Level
User accounts with Password never expires	■ Pay attention
User accounts with Password not required	■ Acceptable
Disabled computer accounts	■ Acceptable
Inactive user accounts	■ Acceptable
Inactive computer accounts	■ Acceptable



## Behavior Anomaly Discovery

Analizza tutte le attività anomale di un utente in una singola dashboard per migliorare il rilevamento delle attività degli insider e di account compromessi

### User Profile (ENTERPRISE\J.Smith)

Home > Behavior anomalies (ENTERPRISE\J.Smith)

RISK SCORE BY TOP FIVE ALERTS

2280

- 145 Non-Whitelisted Program Launched on DC
- 600 Creation of Potentially Harmful Files
- 540 Interactive Logon to DC

Total risk score: 2280

Show user activity

Alert time	Alert name	Risk score	Status
10/2/2017 6:59:49 AM	Creation of Potentially Harmful Files	60	Active
10/2/2017 6:30:55 AM	Non-Whitelisted Program Launched on DC	40	Active
10/2/2017 6:06:04 AM	Non-Whitelisted Program Launched on DC	40	Active
10/2/2017 6:02:10 AM	Interactive Logon to DC	30	Active

**Details:**

Alert name:	Creation of Potentially Harmful Files	<b>Linked actions:</b>	Show all user activity
Risk Score:	60		Show this activity record
Who:	ENTERPRISE\J.Smith		
Object type:	File		
Action:	Added		
What:	\\FS1\shared\finance\Report-Leve		
Where:	fs1.enterprise.com		
When:	10/2/2017 6:59:49 AM		



## Permission Analysis

Controlla e gestisci i diritti di accesso e revoca le autorizzazioni eccessive per mitigare il rischio di abuso di privilegi

### Preview Report

Home > Reports > Preview Report

Planning Plan: [dropdown] Snapshot Date: [Current Server] [dropdown]

Item: [Enterprise Users] Object Type: [Group]

Client Type: [Organizational Unit, User, Group] Account (DC Path): [Enterprise\Users\Administrator]

Show Inherited Permissions: [Yes] Names (Group): [Group, Group, Everyone, AuthN]

Permissions: [Inherit All permissions, Cache, Drop]

---

**Account Permissions in Active Directory**

Show: 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 domains and reverse rights elevation. The permissions are reported only for users that belong to the monitored domain.

Object Name	Object Type	Member Granted
\\com\enterprise	domainDNS	Group, AuthN, Authenticated Users
\\com\enterprise\Builtin	BuiltinDomain	Group
\\com\enterprise\Builtin\Access Control Assistance Operators	group	Group, Authenticated Users
\\com\enterprise\Builtin\Account Operators	group	Group
\\com\enterprise\Builtin\Administrators	group	Group
\\com\enterprise\Builtin\Backup Operators	group	Group
\\com\enterprise\Builtin\Cryptographic Operators	group	Group, Authenticated Users
\\com\enterprise\Builtin\Device Drivers	group	Group, Authenticated Users
\\com\enterprise\Builtin\Event Log Readers	group	Group, Authenticated Users
\\com\enterprise\Builtin\Guests	group	Group, Authenticated Users



## Software inventory

Report pronti all'uso ti permettono di avere sotto controllo tutti gli asset aziendali con inventario dei sistemi operativi, dei software installati e della loro versione

### Windows Server Inventory

Lists Windows servers in your organization, with the operating system name and version, and antivirus status for each server. You can apply baseline filters to highlight issues and aberrant servers with red color. Use this report to identify servers that merit your special attention.

Server	OS Name	OS Version	Antivirus Status
SQL1	Microsoft Windows Server 2012 R2 Standard	6.3.9600	OK
FS2	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	5.2.3790	Issues Detected
FS1	Microsoft Windows Server 2016 Standard	10.0.14393	Issues Detected

