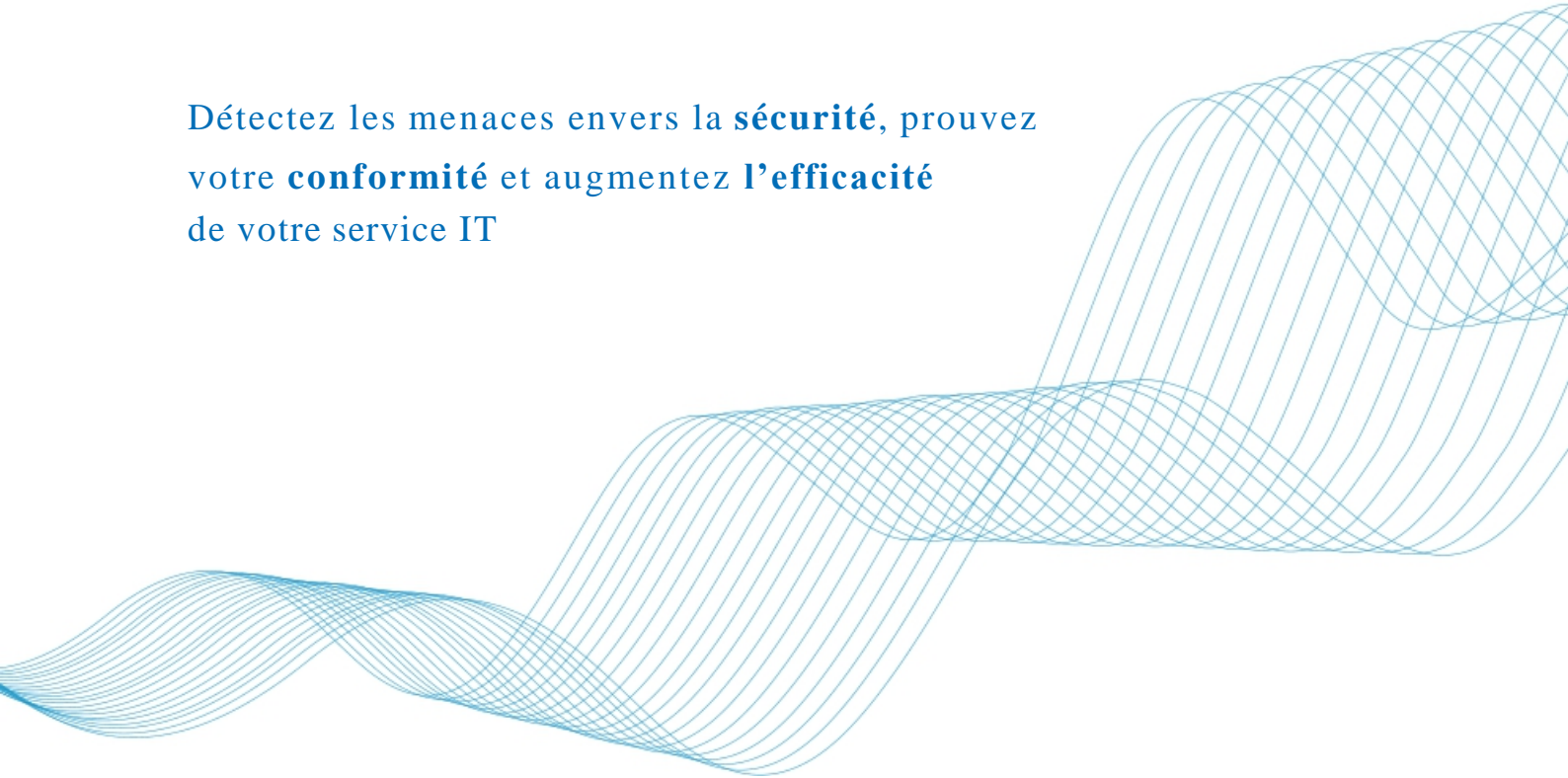




# Netwrix Auditor

Déterminez les menaces envers la **sécurité**, prouvez  
votre **conformité** et augmentez l'**efficacité**  
de votre service IT



# 01

## Présentation du produit

# Simplifiez les audits IT

Les audits informatiques internes comme externes viennent s'intégrer au quotidien d'un nombre croissant d'organisations. Après tout, non seulement ils sont essentiels pour la sécurité et la conformité réglementaire, mais ils contribuent également à trouver et à éliminer les inefficacités dans les processus opérationnels. Malheureusement, la conduite de ces audits réguliers est généralement beaucoup plus fastidieuse et chronophage que nécessaire.

Avec Netwrix Auditor, vous pouvez alléger ce fardeau et atteindre vos objectifs en déployant beaucoup moins d'efforts. Ses capacités de renseignement prêtes à l'emploi vous permettent d'automatiser un grand nombre de tâches liées à la sécurité, à la conformité et aux opérations informatiques qui nécessitaient auparavant des heures de travail, si bien que vous pouvez satisfaire les impératifs de votre organisation sans être constamment surchargé.



*« Nous n'aimons pas les fournisseurs, nous aimons les partenaires. Netwrix fait désormais pratiquement partie de notre équipe. Avec Netwrix Auditor, notre service informatique gagne un temps précieux, ce qui accroît l'efficacité de notre organisation dans la réalisation de nos objectifs pour le comté. »*

**John Adams**, DSI, Comté de Washington, Arkansas, USA



# 02

## Présentation du produit



### Détectez plus rapidement les menaces pour éviter de faire les gros titres

Réduisez l'exposition de vos ressources critiques en identifiant vos principaux risques de sécurité et en durcissant les autorisations. Détectez suffisamment tôt les menaces et intervenez en conséquence, en configurant des alertes et des actions automatisées, et en menant des enquêtes plus rapidement et de manière plus pertinente.



### Gagnez du temps et de l'argent lors des audits de conformité

Assurez, prouvez et maintenez la conformité au prix de moins d'efforts et de dépenses en réduisant jusqu'à 85 % le temps de préparation des audits. Ne perdez plus de temps à passer la piste d'audit au peigne fin chaque fois que vous devez répondre à des questions spécifiques des auditeurs.



### Améliorez l'efficacité de votre équipe informatique sans compromettre l'équilibre entre vie professionnelle et vie privée de ses membres

Donnez les moyens à votre équipe informatique de faire plus avec moins et d'atteindre des indicateurs clés de performance élevés sans pour autant travailler tard tous les soirs. Résolvez les problèmes critiques avant que les utilisateurs ne soient frustrés ou que l'entreprise ne soit affectée, et fournissez les informations requises par les différents acteurs plus rapidement que vous ne pourriez le faire en recourant à des processus manuels.

# 03

## Déterminez plus rapidement les menaces pour éviter de faire les gros titres

### Évaluez et atténuez les risques informatiques

Identifiez et corrigez les lacunes relatives à la sécurité des données et de l'infrastructure dans votre environnement informatique, par exemple des autorisations directement attribuées en masse ou un trop grand nombre de comptes d'utilisateurs inactifs, afin de réduire votre surface d'attaque.

#### Risk Assessment – Overview

Risk name	Current value	Risk level
Users and Computers		
User accounts with Password never expires	2	Medium (1-4)
User accounts with Password not required	0	Low (0)
Inactive user accounts	10% (3 of 30)	High (1% - 100%)
Inactive computer accounts	20% (4 of 20)	High (3% - 100%)
Permissions		
User accounts with administrative permissions	20% (6 of 30)	High (3% - 100%)
Empty security groups	6% (0 of 50)	Low (0)
Data		
Shared folders accessible by Everyone	11% (1685 of 15321)	Medium (5% - 15%)
File names containing sensitive data	2	High (2 - unlimited)
Potentially harmful files on file shares	0	Low (0)
Direct permissions on files and folders	21% (10759 of 51237)	High (5% - 100%)

#### Sensitive Files Count by Source

Shows the number of files that contain specific categories of sensitive data. Clicking the "Categories" or "Source" link narrows your results down to a certain file in this report. Use this report to estimate amount of your sensitive data in each category, plan for data protection measures and control their implementation.

Content source	Categories	Files count
\\fs I\Accounting	GDPR	1300
	PCIDSS	585
\\fs I\Finance	GDPR	715
	HIPAA	1085
	PCIDSS	952
\\fs I\HR	GDPR	1500
	HIPAA	250
\\fs I\Public	PCIDSS	15

### Acquérez une connaissance approfondie de vos données sensibles

Localisez et classez les informations sensibles, y compris les données de cartes bancaires, les dossiers médicaux et autres informations personnelles identifiables, et repérez celles qui apparaissent dans des endroits non sécurisés, pour minimiser les risques de violation.

# 04

## Déterminez plus rapidement les menaces pour éviter de faire les gros titres

### Rationalisez les attestations régulières de privilèges

Sachez qui a accès à quelles données sensibles et comment ces personnes ont obtenu ces accès, et donnez la possibilité aux propriétaires de données de vérifier régulièrement que ces droits correspondent aux besoins métier.

#### Sensitive Data Object Permissions

For each SharePoint object (site, list or document) listed, this report shows the user accounts that have access to this object, their effective permissions and how those permissions were granted. Use this report to control access to SharePoint objects that contain sensitive data.

**Object path:** <http://sp.enterprise.com/sites/HR/Shared/Candidates> **Info 2019.xlsx**

**Categories:** PII

**Total accounts count:** 5

User account	Permissions	Means granted
ENTERPRISE\J.Carter	Full Control	Zone: Default (policy), Web application pool account
ENTERPRISE\T.Simpson	Full Control	Zone: Default (policy), Web application pool account
ENTERPRISE\A.Brown	FullControl	Farm Account
ENTERPRISE\B.Richter	Read	Permission level, Site collection administrator
ENTERPRISE\J.London	Contribute	Farm Account

#### User Sessions

Use this report to identify suspicious user sessions on Windows servers. Find out which users were active on critical or terminal servers and the total time during a day when their activity on the servers was monitored by Netwrix Auditor.

**When:** 4/23/2019

**Who:** ENTERPRISE\J.Carter

Where	Active time
audit.enterprise.com	3:05
dc1.enterprise.com	0:14

**Who:** ENTERPRISE\T.Simpson

Where	Active time
audit.enterprise.com	0:09
dc1.enterprise.com	0:32

### Établissez une responsabilité stricte en ce qui concerne l'utilisation des comptes privilégiés

Surveillez en permanence l'activité des utilisateurs privilégiés sur tous les systèmes, afin de vous assurer qu'ils respectent les politiques internes et n'abusent pas de leurs privilèges.

# 05

## Déterminez plus rapidement les menaces pour éviter de faire les gros titres

### Soyez le premier informé des activités suspectes

Déterminez les menaces de sécurité, telles qu'une activité de SQL Server en dehors des heures de bureau ou une vague de modifications des fichiers qui pourrait indiquer une attaque par rançongiciel, afin de réagir avant que des dommages importants ne soient causés.

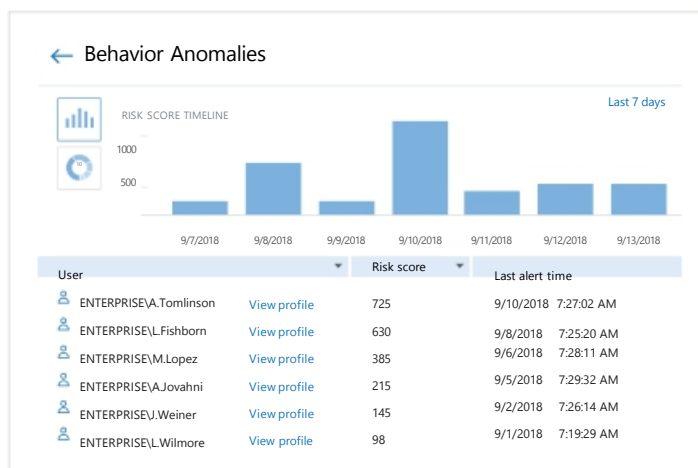
#### Netwrix Auditor Alert

#### 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.

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  
Details: Size changed from "807936 bytes" to "831488 bytes"

This message was sent by Netwrix Auditor from [au-srv-fin.enterprise.com](mailto:au-srv-fin.enterprise.com).



### Déterminez les comptes compromis et les utilisateurs internes malveillants

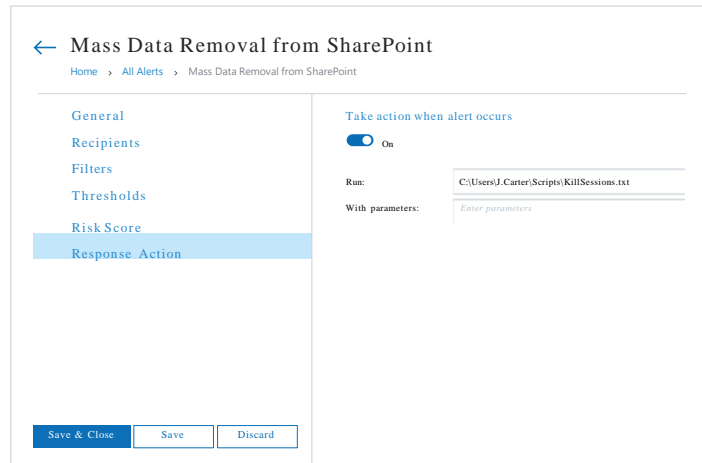
Repérez les signes subtils de menaces potentielles envers la sécurité, tels que des connexions inhabituelles ou un accès distant non autorisé à votre réseau. Identifiez facilement les utilisateurs qui présentent le plus de risques et enquêtez sur eux grâce à une vue agrégée de l'activité anormale de chaque utilisateur.

# 06

## Déterminez plus rapidement les menaces pour éviter de faire les gros titres

Réagissez rapidement aux menaces en automatisant la réponse aux incidents anticipés

Réagissez plus rapidement aux menaces pour la sécurité des données en automatisant la réponse aux incidents anticipés. Fournissez un premier support en intégrant Netwrix Auditor à votre processus SecOps.



The screenshot shows the search results interface. At the top, there are navigation tabs: WHO, ACTION, WHAT, WHEN, and WHERE. The search criteria are "Who" and "ENTERPRISE\J.Key". Below the search bar, there are options for "Open in new window", "SEARCH", and "Advanced mode". The main content is a table with the following data:

Who	Object type	Action	What	When
ENTERPRISE\J.Key	File	Read	\\fileserv1\shared\Finance\Q4_2018\Revenue Forecast.xlsx	10/25/2018 9:01:13 AM
ENTERPRISE\J.Key	File	Read	\\fileserv1\shared\Finance\Q4_2018\Risk Assessment.pdf	10/25/2018 9:00:10 AM
ENTERPRISE\J.Key	File	Copied	\\fileserv1\shared\Finance\Q4_2018\Audit Report.docx	10/25/2018 9:00:02 AM
ENTERPRISE\J.Key	File	Removed	\\fileserv1\shared\Finance\Q4_2018\Revenue Forecast draft.xlsx	10/25/2018 8:59:45 AM
ENTERPRISE\J.Key	File	Modified	\\fileserv1\shared\Finance\Workflows\Billing workflow.pdf	10/25/2018 8:59:23 AM

## Rationalisez les enquêtes sur incident

Faites rapidement la lumière sur les incidents impliquant des données sensibles grâce à la recherche de type Google : comprenez exactement ce qui s'est passé, comment c'est arrivé, qui était derrière cela et quels éléments d'information ont été affectés.

# 07

## Gagnez du temps et de l'argent lors des audits de conformité

Assurez-vous que vos contrôles de sécurité sont efficaces

Mettez en œuvre des contrôles de conformité dans toute votre infrastructure et évaluez régulièrement leur bon fonctionnement. Si les politiques de sécurité écrites diffèrent des mesures en place, remédiez à vos contrôles de sécurité défectueux avant que les auditeurs ne les découvrent.

### Sensitive File and Folder Permissions Details

Shows permissions granted on files and folders that contain certain categories of sensitive data. Use this report to see who has access to a particular file or folder, via either group membership or direct assignment. Reveal sensitive content that has permissions different from the parent folder.

**Object:** \\fs1\Accounting (Permissions: Different from parent)

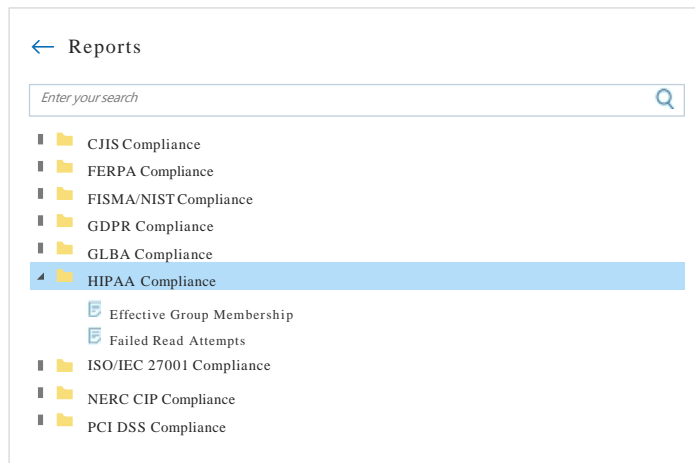
**Categories:** GDPR

Account	Permissions	Means granted
ENTERPRISE\J.Carter	Full Control	Group Directly
ENTERPRISE\T.Simpson	Full Control	Group
ENTERPRISE\A.Brown	Full Control	

**Object:** \\fs1\Accounting\Contractors (Permissions: Different from parent)

**Categories:** GDPR

Account	Permissions	Means granted
ENTERPRISE\M.Smith	Full Control	Group
ENTERPRISE\A.Gold	Full Control	Group



## Gagnez du temps dans la préparation de la conformité

Préparez-vous à la masse de requêtes des auditeurs en tirant parti des rapports prêts à l'emploi adaptés aux contrôles de conformité RGPD, HIPAA/HITECH, PCI DSS ou d'autres réglementations courantes.

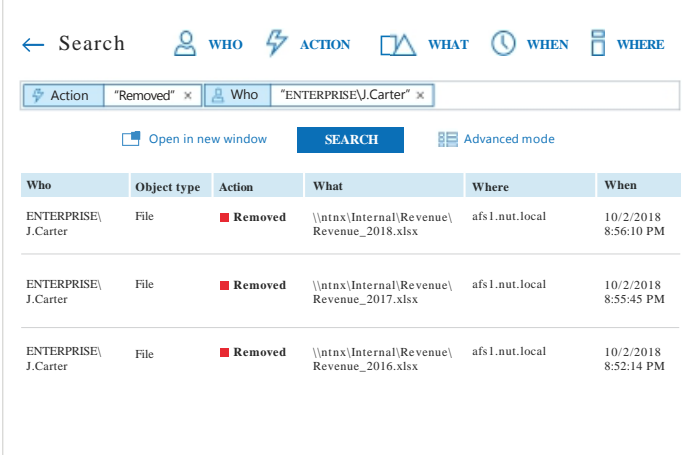


# 08

## Gagnez du temps et de l'argent lors des audits de conformité

### Répondez aux questions spécifiques des auditeurs

Si des questions inattendues surviennent en cours d'audit, servez-vous de la recherche de type Google pour trouver immédiatement les informations demandées.



The screenshot shows the Netrix Auditor search interface. At the top, there are navigation icons for WHO, ACTION, WHAT, WHEN, and WHERE. Below these is a search bar with filters for Action (set to "Removed"), Who (set to "ENTERPRISE\J.Carter"), and a SEARCH button. Below the search bar is a table with the following columns: Who, Object type, Action, What, Where, and When.

Who	Object type	Action	What	Where	When
ENTERPRISE\J.Carter	File	Removed	\\ntnx\Internal\Revenue\Revenue_2018.xlsx	afs1.nut.local	10/2/2018 8:56:10 PM
ENTERPRISE\J.Carter	File	Removed	\\ntnx\Internal\Revenue\Revenue_2017.xlsx	afs1.nut.local	10/2/2018 8:55:45 PM
ENTERPRISE\J.Carter	File	Removed	\\ntnx\Internal\Revenue\Revenue_2016.xlsx	afs1.nut.local	10/2/2018 8:52:14 PM

### 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\Netrix Auditor\Data

Keep audit data for: 60 months

Netrix Auditor uses the [LocalSystem account](#) to write audit data to the Long-Term Archive

[Modify](#)

### Stockez et accédez à votre piste d'audit pendant des années

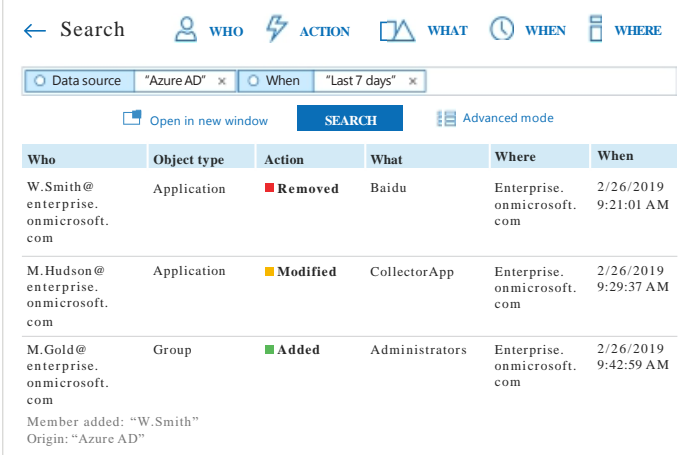
Archivez votre piste d'audit dans un format compressé pendant plus de 10 ans, comme l'exigent de nombreuses réglementations, tout en vous assurant que toutes les données d'audit sont facilement accessibles à tout moment par les utilisateurs autorisés.

# 09

## Améliorez l'efficacité de votre équipe IT

Résolvez les difficultés des utilisateurs avant qu'elles ne deviennent de véritables problèmes

Chaque fois que des utilisateurs veulent savoir pourquoi leur fichier a disparu et comment ils peuvent le récupérer ou pourquoi ils ne peuvent pas accéder à une machine virtuelle exécutant une application critique, obtenez la réponse en quelques clics et permettez-leur de se remettre au travail.



Who	Object type	Action	What	Where	When
W.Smith@enterprise.onmicrosoft.com	Application	Removed	Baidu	Enterprise.onmicrosoft.com	2/26/2019 9:21:01 AM
M.Hudson@enterprise.onmicrosoft.com	Application	Modified	CollectorApp	Enterprise.onmicrosoft.com	2/26/2019 9:29:37 AM
M.Gold@enterprise.onmicrosoft.com	Group	Added	Administrators	Enterprise.onmicrosoft.com	2/26/2019 9:42:59 AM

Member added: "W.Smith"  
Origin: "Azure AD"

### Netwrix Auditor Alert

A SQL Server database has been deleted

Who: ENTERPRISEJ.Smith  
Action: Removed  
Object type: Database  
What: Database/Main/Customers  
When: 4:57:40 PM 4/24/2019 4:57:40 PM  
Where: sql1  
Workstation: mkt023.enterprise.com  
Data source: SQL Server  
Monitoring plan: SQL Server Monitoring

This message was sent by Netwrix Auditor from [au-srv-fin.enterprise.com](mailto:au-srv-fin.enterprise.com).

Réagissez rapidement aux événements susceptibles de provoquer des indisponibilités

Soyez informé à temps des événements tels que la suppression d'une unité d'organisation ou d'une base de données contenant des informations sur les clients, et remédiez rapidement à la situation avant que les activités de l'entreprise ne soient affectées.

# 10

## Améliorez l'efficacité de votre équipe IT

Faites-vous une idée précise de ce qui a été modifié

Gardez un œil sur les modifications apportées à vos systèmes informatiques locaux et Cloud afin de pouvoir repérer et résoudre les problèmes avant qu'ils ne nuisent à l'activité de l'entreprise et à la productivité des utilisateurs. Ainsi, vous pouvez fournir des services informatiques sans interruption et satisfaire de manière cohérente vos accords de niveau de service et les attentes des utilisateurs.

### Sharing and Security Changes

Shows changes to security group membership, policies, and sharing settings, such as promoting a user to site collection administrator or sharing data with external users.

Action	Object Type	What	Who	When
■ Modified	Group	GroupName1	T.Simpson @enterprise. onmicrosoft.com	9/1/2018 8:56:10 AM
		<b>Where:</b> <a href="https://enterprise-my.sharepoint.com/sites/Test_Do_Not_Delete">https://enterprise-my.sharepoint.com/sites/Test_Do_Not_Delete</a>		
		<b>Workstation:</b> 81.09.21.122		
■ Modified	List	<a href="https://enterprise-my.sharepoint.com/Lists/Customers">https://enterprise-my.sharepoint.com/Lists/Customers</a>	T.Simpson @enterprise. onmicrosoft.com	9/1/2018 8:35:44 AM
		<b>Where:</b> <a href="https://enterprise-my.sharepoint.com">https://enterprise-my.sharepoint.com</a>		
		<b>Workstation:</b> 81.09.21.122		
		<b>Permissions:</b> <ul style="list-style-type: none"><li>• Added: "User Account Administrator (Edit)"</li></ul>		

### Windows Server Configuration Details

Provides review of Windows server configuration. For a server, the following details are reported: its OS, antivirus, local users and groups, files shares, installed programs, and services. You can apply baseline filters to highlight security issues, such as outdated operating system or improper antivirus. Use this report to examine server configuration details and proactively mitigate risks in your environment.

#### Category: General

Server	OS Name	OS Version	Antivirus Status
audit.enterprise.com	Microsoft Windows Server 2012 R2 Standard	6.3.9600	Issues Detected

#### Category: Software

ObjectType	ObjectName	Properties
Software	Microsoft OneDrive	Available: ENTERPRISE\M.Peterson, Version: 17.3.4604.0120
Software	Trojan	Available: All users, Version: 6.9.5.2956
Software	Google Chrome	Available: All users, Version: 66.0.3359.139
Software	uTorrent	Available: ENTERPRISE\J.Hanson, Version: 3.5.3.44396

Examinez la configuration de vos systèmes et repérez les écarts par rapport à une référence fiable et connue

Déterminez l'état courant de vos ressources critiques plus rapidement que vous ne pourriez le faire avec des processus manuels, et vérifiez ainsi que vos configurations correspondent à une référence fiable et connue. Dans le cas contraire, corrigez les problèmes afin d'éviter les indisponibilités système et les perturbations pour les utilisateurs.

# 11

## Améliorez l'efficacité de votre équipe IT

Répondez aux questions en quelques minutes, et non en quelques heures

Chaque fois que des parties prenantes vous demandent des informations, par exemple une liste des personnes ayant accès à un dossier particulier ou la preuve qu'il n'y a pas d'utilisateurs inactifs dans l'environnement informatique, répondez rapidement en présentant des rapports prêts à l'emploi et clairement lisibles.

### Folder and File Permission Details

Shows permissions granted on a shared folder, its subfolders and files (either directly or via group membership). Use this report to see who has access to a particular folder and its contents, and reveal objects that have permissions different from their parent. Clicking the group link opens the "Group Membership by User" report.

**Object:** \\fs1\Accounting\Contractors (Permissions: Different from parent)

Account	Permissions	Means Granted
ENTERPRISE\J.Carter	Full Control	<a href="#">Group</a>
ENTERPRISE\T.Simpson	Read (Execute, List folder content)	<a href="#">Group</a> Directly
ENTERPRISE\J.Smith	Full Control	<a href="#">Group</a> Directly
ENTERPRISE\A.Tompson	Full Control	
ENTERPRISE\M.Brown	Full Control	

Name	Type	Status	Mode	Recipients	Schedule
Administrative Group and Role Changes	Search	✓ Completed	<input type="checkbox"/> Off	sysadmins@enterprise.com	Daily
J.Carter's Activity	Search	✓ Scheduled	<input checked="" type="checkbox"/> On	T.Simpson@enterprise.com	Weekly
Subscription to the 'Windows Server Configuration Details' report	Report	✓ Scheduled	<input checked="" type="checkbox"/> On	sysadmins@enterprise.com	Weekly
Subscription to the 'Overexposed Files and Folders' report	Report	✓ Scheduled	<input checked="" type="checkbox"/> On	J.Phillips@enterprise.com	Daily
Subscription to the 'Sensitive File and Folder Permissions Details' report	Report	✓ Scheduled	<input checked="" type="checkbox"/> On	J.Phillips@enterprise.com	Daily

Ne soyez plus un goulot d'étranglement en matière de reporting

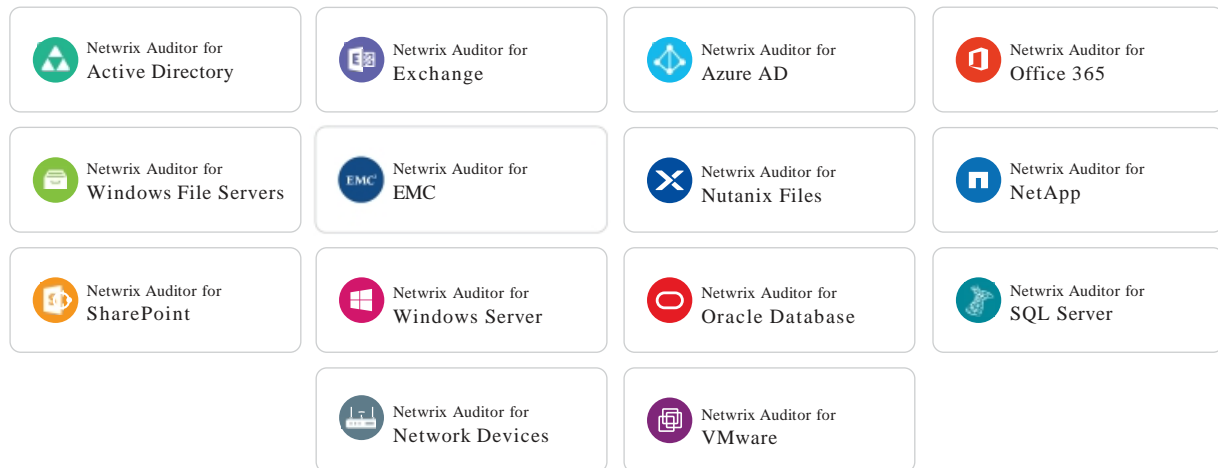
Envoyez automatiquement aux parties prenantes les informations qu'elles demandent, au rythme qu'elles préfèrent. Alternativement, offrez-leur un accès granulaire à Netwrix Auditor afin qu'elles puissent obtenir les informations dont elles ont besoin quand elles le souhaitent.

# 12

## Applications Netwrix Auditor

# Auditez vos systèmes IT les plus importants depuis une plateforme centrale

Ne jonglez plus avec de multiples outils pour collecter les informations d'audit de tous vos systèmes locaux et Cloud, laissez Netwrix Auditor fournir les informations utiles de manière unifiée et cohérente.



# 13

## API d'intégration de Netwrix Auditor

### Profitez des possibilités illimitées d'intégration, d'audit et de reporting



#### Centralisez les audits et le reporting

Netwrix Auditor collecte les traces d'activité de toutes les applications sur site ou dans le Cloud et les stocke dans un dépôt central sécurisé, disponibles pour les contrôles d'historique et les enquêtes de conformité.



#### Tirez le meilleur parti de votre investissement SIEM

Obtenez des résultats plus clairs de votre SIEM et accélérez vos enquêtes grâce aux données lisibles et exploitables collectées par Netwrix Auditor.



#### Automatisez les flux de travail informatiques

Netwrix Auditor s'intègre aux autres outils de sécurité informatique, de conformité et de gestion des données, permettant ainsi d'automatiser et d'améliorer des flux de travail informatiques.

UNIX®



splunk>



now



Visitez la boutique en ligne de modules complémentaires pour Netwrix Auditor à l'adresse [netwrix.com/go/add-ons](https://netwrix.com/go/add-ons) et trouvez des modules complémentaires gratuits conçus pour intégrer Netwrix Auditor à votre écosystème informatique.

# 14

## Pourquoi Netwrix Auditor ?

### Découvrez ce qui pousse les clients à choisir Netwrix Auditor



#### Gain rapide

Obtenez de la valeur dès le départ et bénéficiez d'un retour sur investissement en quelques jours, non en quelques mois. Ne payez pas des services professionnels coûteux et ne perdez pas de temps avec un long processus de déploiement.



#### Prix raisonnable

Profitez d'une solution à prix raisonnable assortie de frais de fonctionnement transparents et prévisibles. Réalisez de multiples objectifs en matière de sécurité, de conformité et d'opérations informatiques sans dépenser une fortune pour des outils disparates.



#### Architecture non intrusive

Évitez d'avoir à composer avec des agents intrusifs et des méthodes de collecte de données non documentées.



#### Support technique de première classe

Vos problèmes sont rapidement résolus par notre support technique exceptionnel, avec un taux de satisfaction de 97 %.



« Netwrix Auditor présente le meilleur rapport qualité-prix, sans contestation. »

Un DSI du secteur financier 