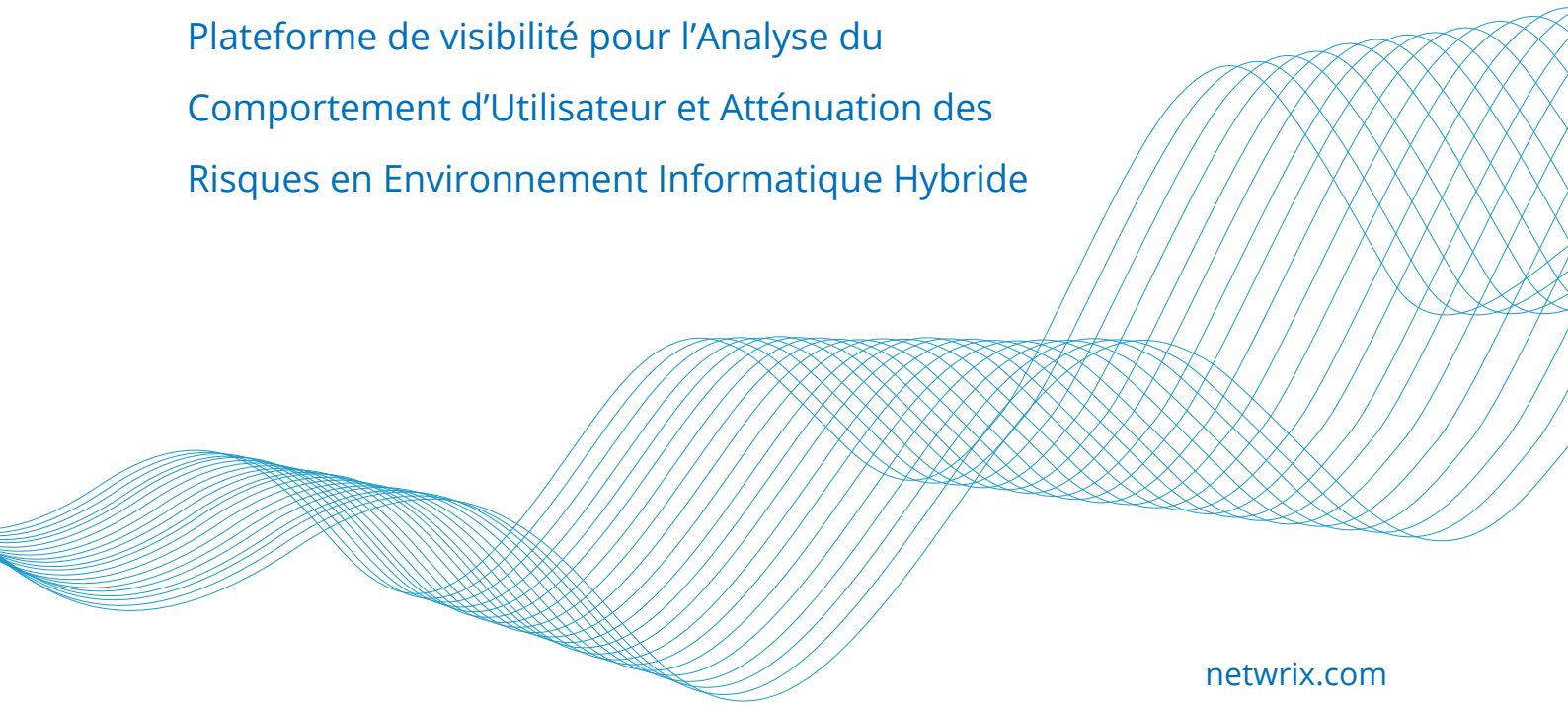
netwrix

Netwrix Auditor

Plateforme de visibilité pour l'Analyse du Comportement d'Utilisateur et Atténuation des Risques en Environnement Informatique Hybride

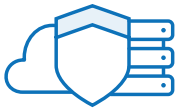


netwrix.com

01
Vue d'ensemble du produit

Plateforme Netwrix Auditor

Netwrix Auditor est une plateforme de visibilité pour l'analyse des comportements des utilisateurs et l'atténuation des risques qui permet de contrôler les modifications, les configurations et les accès aux environnements informatiques hybrides, pour protéger les données quel que soit leur emplacement. La plateforme fournit des renseignements de sécurité pour identifier les failles de sécurité, détecter des anomalies dans le comportement d'utilisateur et étudier des modèles de menace à temps pour éviter des dommages réels.



Détecte les menaces de sécurité aux données, à la fois sur site et dans le Cloud.

Passer les vérifications de conformité avec moins d'efforts et de charges.

Augmenter la productivité des équipes de sécurité informatiques et d'opérations.

02
Applications

Applications Netwrix Auditor

Netwrix Auditor comporte des applications pour Active Directory, Azur AD, Exchange, Office 365, les serveurs de fichiers Windows, les périphériques de stockage EMC, les appareils de stockage de fichiers NetApp, SharePoint, les Bases de données Oracle, Serveur SQL, VMware et Serveurs Windows. Renforcée par une API RESTful et l'enregistrement vidéo de l'activité d'utilisateur, la plate-forme offre, de manière intégrée, visibilité et contrôle sur l'ensemble des systèmes informatiques sur site et dans le Cloud.

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

03
Avantages

Détecter les menaces à la sécurité des données, sur Site et dans le Cloud

Netwrix Auditor comble l'écart de visibilité en fournissant des renseignements de sécurité sur les modifications critiques, l'accès aux données et les configurations dans les environnements informatiques hybrides. Les organisations peuvent utiliser ces données pour évaluer en permanence et atténuer les risques de façon proactive. La plateforme identifie les utilisateurs ayant l'activité la plus anormale au fil du temps et alerte sur les profils de comportement qui indiquent une possible menace interne ou de prise de contrôle de compte. Et elle facilite l'analyse de toute action suspecte ou violation de la politique de sécurité vous permettant de déterminer rapidement la meilleure réponse.

Passer les audits de conformité avec moins d'effort et de charges

Netwrix Auditor fournit la preuve exigée pour démontrer que le programme de sécurité de votre organisation informatique adhère au PCI DSS, HIPAA, HITECH, SOX, FISMA/NIST800-53, COBIT, ISO/IEC 27001 et autres normes. Netwrix Auditor assure également un accès facile à vos traces d'audit archivées pendant plus de 10 ans.

Augmenter la productivité des équipes de sécurité informatique

Avec Netwrix Auditor, il n'y a pas besoin de farfouiller dans des semaines d'enregistrements de données pour répondre aux questions à propos de qui a changé quoi ou quand, et où une modification a-telle été effectuée, ou qui a accès à quoi. Et de plus, vous n'avez plus besoin d'écrire, de maintenir et d'exécuter laborieusement des scripts PowerShell pour identifier les utilisateurs inactifs, signaler les autorisations effectives d'utilisateur ou effectuer des tâches d'inventaire logiciel.

04

En Action : Détecter les menaces à la sécurité des données

Atténuer les risques de sécurité des données

Ajustez les autorisations en fonction des besoins pour réduire au minimum la capacité des intrus et des employés à causer des dommages.

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

Total risk level for Data: Take action

Risk	Level
Shared folders accessible by Everyone	Take action

Total risk level for Users and Computers: Pay attention

Risk	Level
User accounts with Password never expires	Pay attention

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

Prévenir les violations de données

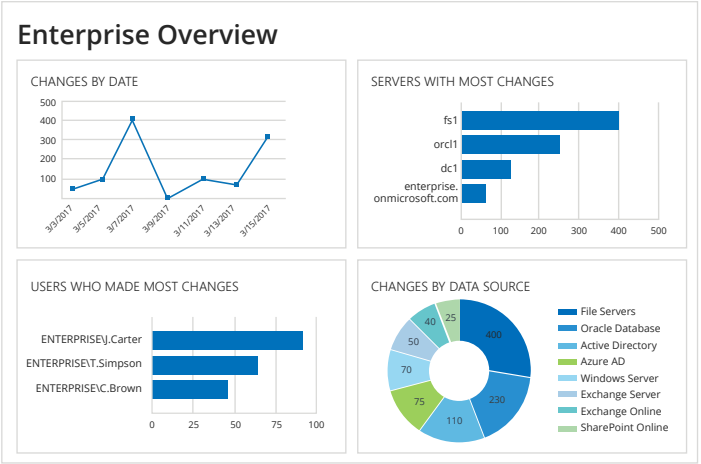
Obtenir une image complète des autorisations utilisateur réels dans Active Directory et les serveurs de fichiers. Verrouiller les données surexposées et s'assurer que seuls les employés autorisés ont accès aux ressources critiques. Restez au courant des modifications qui affectent les privilèges de l'utilisateur.

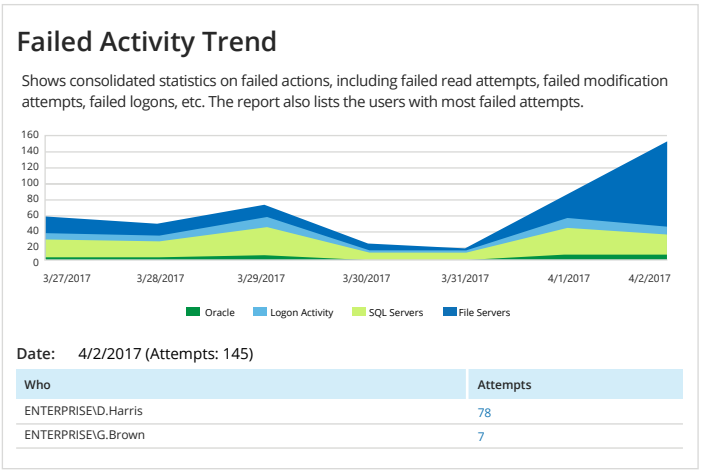
05

En Action Détecter les menaces à la sécurité des données

Avoir une vision globale de l'activité dans l'ensemble de l'IT

Avoir un aperçu large de ce qui se passe dans votre infrastructure informatique hybride avec le tableau de bord Enterprise Overview. Repérer les pointes d'activité anormales, voir quels utilisateurs sont les plus actifs et déterminer quels systèmes sont les plus touchés.





Détecter les comportements anormaux d'utilisateur

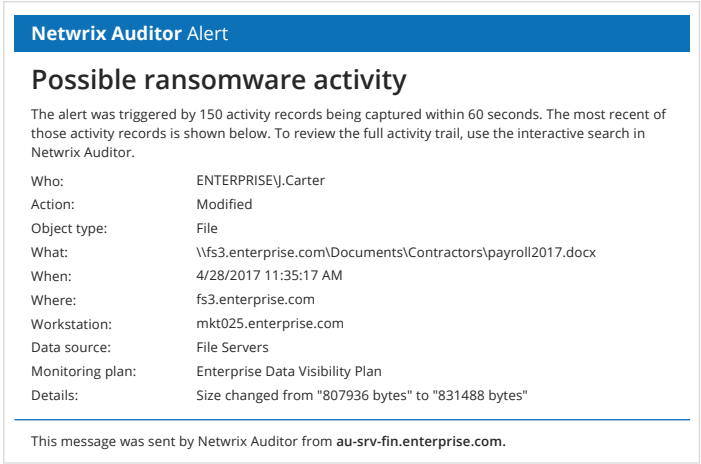
Identifiez rapidement les incidents de sécurité potentiels, tels que des ouvertures de sessions inhabituelles pouvant indiquer une usurpation d'identité d'utilisateur ou un utilisateur privilégié mécontent qui essaie de cacher son activité derrière des comptes temporaires.

06

En Action Détecter les menaces à la sécurité des données

Recevoir des alertes sur des modèles de menace

Utilisation des alertes pour être informé sur l'activité non autorisée dès qu'elle se produit. Par exemple, vous pouvez choisir d'être averti chaque fois qu'une personne a été ajoutée au groupe Administrateurs de l'Entreprise ou qu'un utilisateur a modifié de nombreux fichiers dans un court laps de temps, ce qui pourrait indiquer une attaque de ransomware.



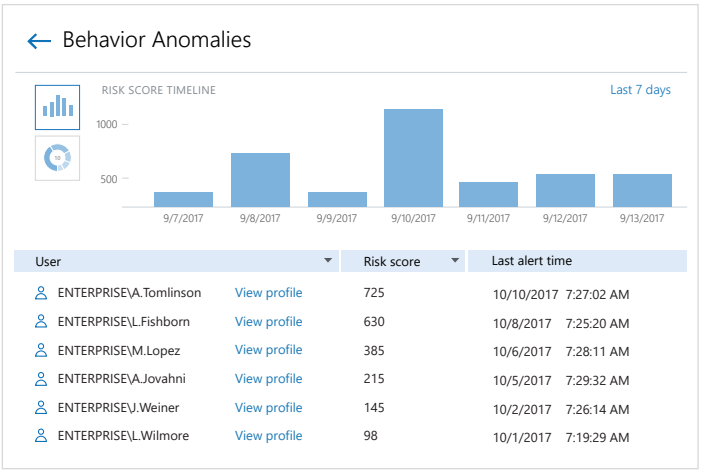
Netwrix Auditor Alert

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.**



Identifier les comptes d'utilisateurs à haut risque

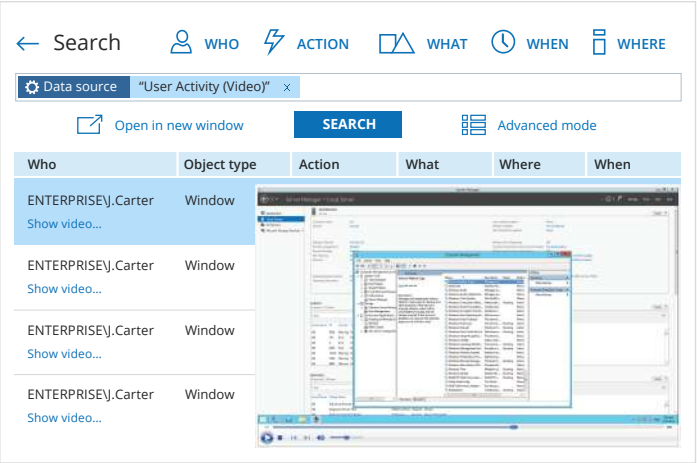
Améliorer la détection des employés voyous et des comptes mis en danger par des attaquants externes avec une seule vue 'ensemble de l'activité anormale de chaque individu. Utilisez les scores de risques associés pour prioriser les incidents afin de pouvoir étudier et déterminer la meilleure réponse.

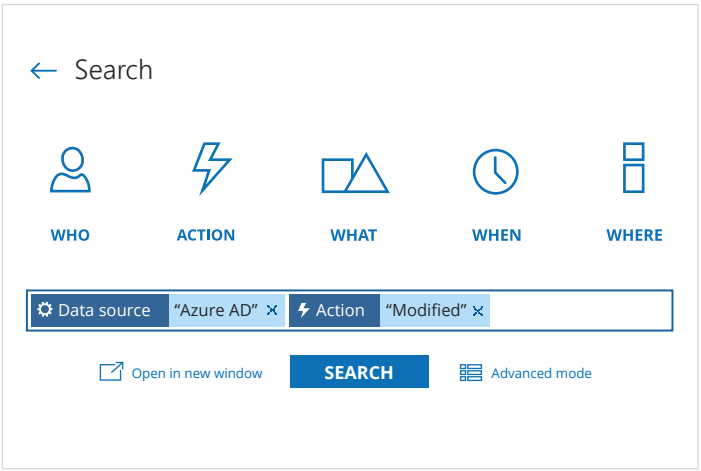
07

En Action Détecter les menaces à la sécurité des données

Détecter l'indétectable

Gagner en visibilité dans n'importe quel système ou application, même si elle ne produit pas de journaux, grâce à l'enregistrement vidéo de l'activité de l'utilisateur sur son écran. Vous pouvez rechercher et relire les enregistrements pour déterminer exactement quelles actions ont été effectuées.





Analyser les anomalies dans les comportements d'utilisateurs

Dès que vous détectez une modification ou une tentative d'accès aux données qui viole la politique de sécurité votre entreprise, utilisez notre recherche interactive de type Google pour reconnaître pourquoi et comment c'est arrivé de manière à prévenir les incidents semblables à l'avenir.

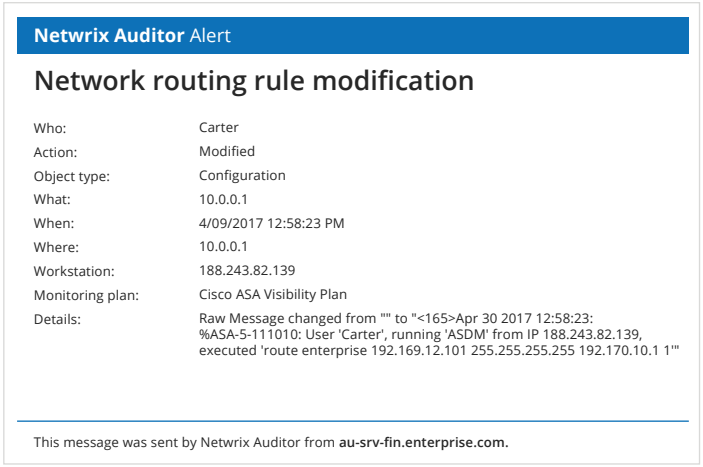
visibilité complète

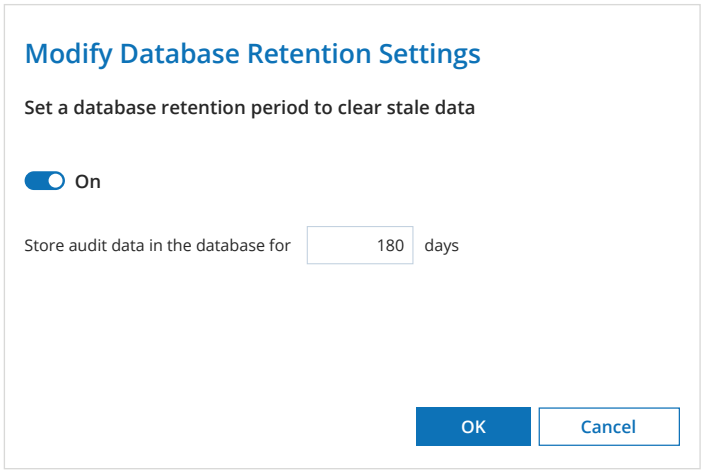
08

En Action Détecter les menaces à la sécurité des données

Automatiser les flux de travail de gestion des incidents

Centraliser le contrôle de la sécurité et des rapports en donnant à Netwrix Auditor des données d'autres applications locales ou dans le Cloud. Vous pouvez également utiliser Netwrix Auditor pour élargir la quantité de données produites par votre solution SIEM.





Archivez les données de de sécurité pendant des années

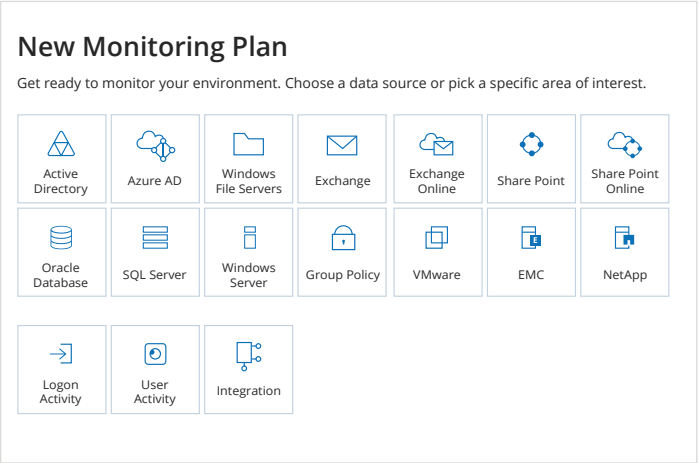
Le stockage AuditArchive™ à deux niveaux (fichier + base de données SQL) vous permet de conserver vos données importantes archivées pour exploitation électronique de l'historique ou les enquêtes de sécurité pendant plus de 10 ans.

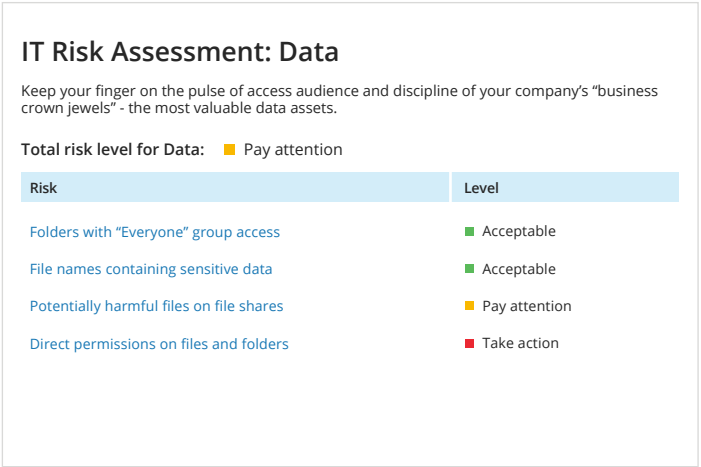
09

En Action : Passer les vérifications de conformité

Activez le contrôle sur les politiques de sécurité

Netwrix Auditor vous aide à mettre en œuvre des contrôles de conformité sur l'ensemble de votre infrastructure. Il sert de point unique d'accès à la piste d'audit et vous permet de facilement prouver que vos stratégies de sécurité sont mises en œuvre.





Recensez et hiérarchisez les risques

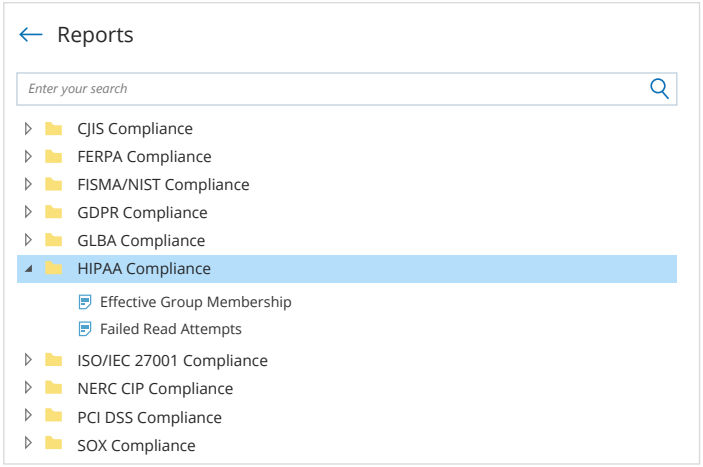
Visualisez votre position de sécurité et impressionnez les auditeurs avec tableaux de bord interactifs d'évaluation des risques. Utilisez-les pour prouver votre capacité à continuellement évaluer et réduire les risques aux données protégées.

10

En Action : Passer les vérifications de conformité

Mettez à profit les rapports de conformité prêts à l'emploi

Réduisez les temps de préparation des audits et prouvez votre conformité à l'aide de rapports préconçus selon les contrôles de conformité FISMA, PIBR, HIPAA/HITECH, PCI DSS, SOX et de nombreux autres règlements communs.



Members of Local Administrators Group

Shows Windows servers, with members of the local Administrators group for each server. You can apply baseline filter to highlight servers with security issues, e.g., those where the Administrators group include users not in your baseline list. Use this report to prevent rights elevation and exercise security control over your organization.

Server	Members	Status
fs1.enterprise.com	Administrator, fs1local, ENTERPRISE\Domain Admins	Issues Detected
sql01.enterprise.com	Administrator, J.Carter, ENTERPRISE\Domain Admins	Issues Detected
srv01.enterprise.com	Administrator, T.Simpson, ENTERPRISE\Domain Admins	Issues Detected
srv02.enterprise.com	Administrator, ENTERPRISE\Domain Admins	OK
srv03.enterprise.com	Administrator, ENTERPRISE\Domain Admins	OK
srv04.enterprise.com	Administrator, ENTERPRISE\Domain Admins	OK

Prouvez que les contrôles de conformité ont toujours été mis en œuvre

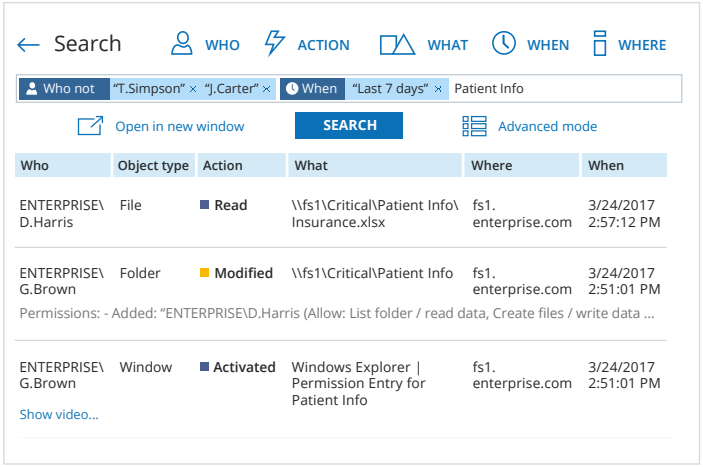
Montrez aux auditeurs que l'appartenance à un groupe, les autorisations utilisateur efficace et les autres configurations dans votre environnement ont toujours été conformes aux politiques de sécurité.

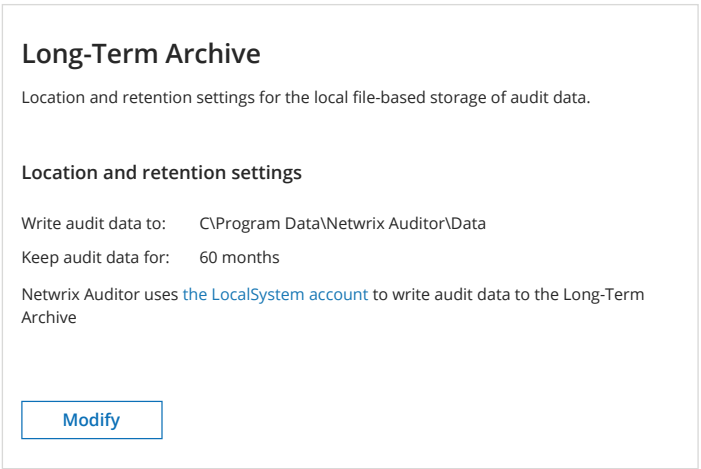
11

En Action : Passer les vérifications de conformité

Répondez plus vite aux questions des auditeurs

Donnez des réponses aux questions inattendues des auditeurs, telles que : qui a accédé à un fichier sensible, ou comment les droits d'accès à un dossier protégé ont été modifiés et qui effectué ces changements. Avec Netwrix Auditor, ce qui prenait autrefois des semaines s'effectue maintenant en quelques minutes.





Accédez aux traces de vos vérifications pendant des années

De nombreux règlements de conformité obligent les organisations à conserver les traces de leurs vérifications pendant une période prolongée. Netwrix Auditor vous permet de conserver les traces de vos vérifications archivées dans un format compressé pendant plus de 10 ans.

12

En Action : Augmenter la productivité des équipes IT

Gardez un œil sur ce qui se passe dans votre environnement

Surveillez toutes les modifications dans vos systèmes informatiques sur site et dans le Cloud. Voyez quand une modification spécifique a été apportée, qui l'a faite et ce qui a été modifié, grâce aux valeurs avant et après la modification.

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	Modified Policy: Maximum password age; Setting: 20 days -> 200 days; Modified Policy: Minimum password length; Setting: 7 characters-> 4 characters;		

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.

Account: \com\enterprise\Users\John Carter

Object Name	Object Type	Means Granted
\com\enterprise\Computers	container	Directly
\com\enterprise	domainDNS	Group
\com\enterprise\Builtin	builtinDomain	Group
\com\enterprise\Builtin\Account Operators	group	Group
\com\enterprise\Builtin\Administrators	group	Group
\com\enterprise\Builtin\Backup Operators	group	Group

Maintenir une bonne santé informatique

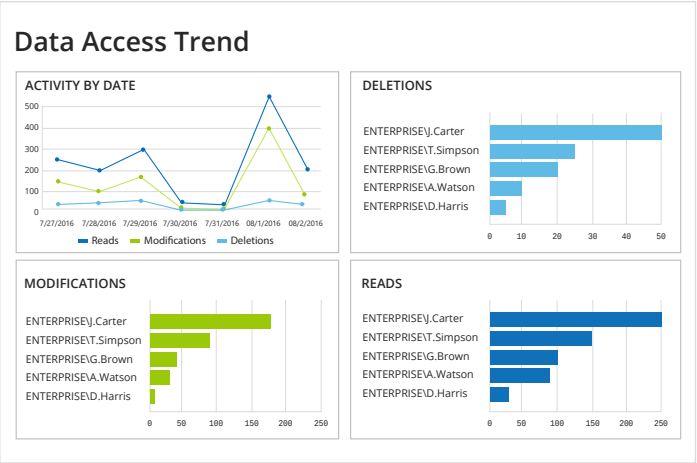
Créer un environnement plus propre et plus facile à gérer à l'aide des rapports à-un-moment-donné de Netwrix Auditor. Examinez régulièrement vos configurations d'identités et d'accès et vérifiez facilement qu'ils correspondent à un état correct connu.

13

En Action : Augmenter la productivité des équipes IT

Simplifiez les rapports de routine

Netwrix Auditor fournit plus de 200 rapports et tableaux de bord prédéfinis. Vous pouvez également facilement résoudre toutes préoccupations de sécurité spécifique et de conformité en établissant des rapports personnalisés à l'aide de la fonctionnalité de recherche Interactive.



Accélérez la remise des rapports

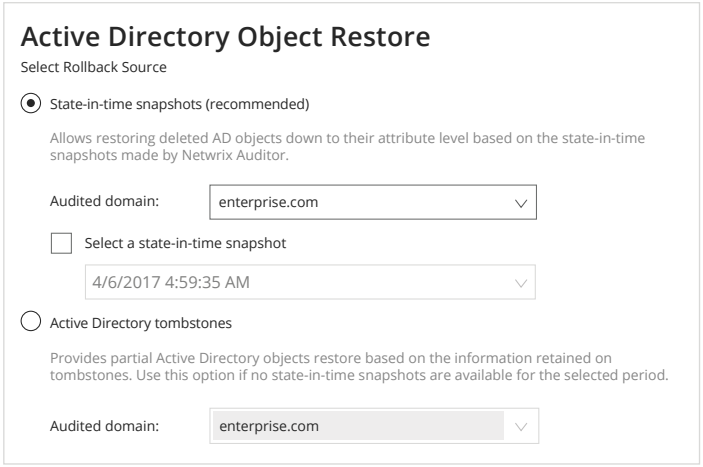
Netwrix Auditor peut générer automatiquement des rapports, puis les envoyer par e-mail aux intervenants ou les sauvegarder dans un fichier dédié. Vous pouvez également autoriser l'accès à Netwrix Auditor aux intervenants pour qu'ils puissent générer, à la demande, les rapports dont ils ont besoin.

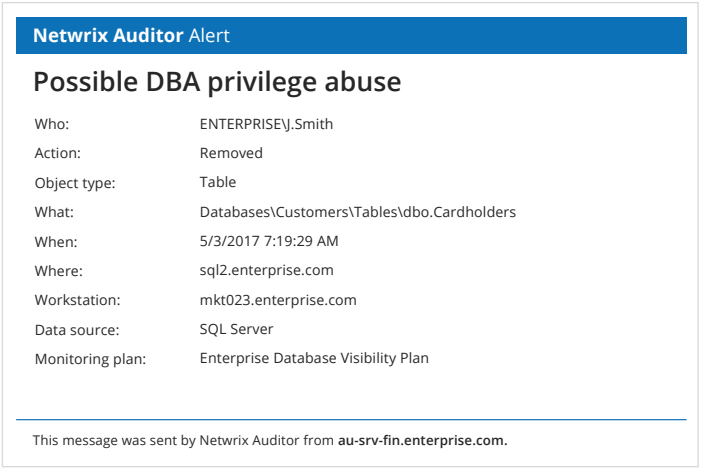
14

En Action : Augmenter la productivité des équipes IT

Réduire au minimum les indisponibilités du système

Dans le cas où une modification non autorisée ou inadéquate est faite à votre environnement, vous pouvez rapidement remonter le temps et rétablir l'état précédent — sans aucun temps d'arrêt ni le besoin de restaurer à partir d'une sauvegarde.





Concentrez-vous sur ce qui est vraiment important

Évaluez régulièrement les risques pour identifier les domaines qui nécessitent votre attention immédiate. Utilisez les alertes pour être au courant des actions que vous considérez critiques, comme la suppression de fichiers commerciaux critiques ou des modifications à votre configuration de SQL Server.

Relevez les Défis de Sécurité et de Conformité de Votre Service et de Votre Entreprise

Directeur Informatique

Gardez votre environnement informatique sécurisé, propre et facile à gérer.

Directeur de la sécurité informatique

Prévenez les violations de données et minimisez les coûts de conformité.

Directeur Informatique

Reprenez la maîtrise de votre infrastructure informatique et éliminez le stress de votre prochain audit de conformité.

Analyste de Sécurité

Identifiez les lacunes de sécurité et analysez l'activité suspecte d'utilisateur à temps pour éviter les dommages réels.

Administrateur Système

Générez et produisez plus vite les rapports de sécurité et de conformité.

MSP

Augmentez les bénéfices en favorisant la transparence des environnements gérés et en offrant la conformité comme un service.

Options de mise en oeuvre

Sur site, virtuel ou dans le Cloud — déployez Netwrix Auditor là où vous en avez besoin

On-premises

Entièrement pris en charge sur **la Plate-forme serveur Windows de Microsoft**

Virtual

Disponible dans les appareils pour **VMware et Microsoft Hyper-V**

Cloud

Totalement pris en charge et testé dans **Microsoft Azure**

Entièrement pris en charge sur **AWS Marketplace**

Windows Server

Microsoft Hyper-V

Microsoft Azure

vmware READY

awsmarketplace

visibilité complète

Des API rESTful — capacités infinies d'intégration pour améliorer la visibilité et simplifier les rapports

Centralisez les audits et les rapports

Netwrix Auditor recueille les traces d'activité de toute application ou stockage existant sur site ou dans le Cloud dans un référentiel central sécurisé, prêt pour les recherches et les rapports.

Profitez au maximum de votre investissement SIEM

En insérant des données d'audit plus granulaires dans votre HP Arcsight, Splunk, IBM QRadar ou autre solution SIEM, Netwrix Auditor augmente le rapport signal-bruit et maximise la valeur SIEM.

Automatisez les flux informatiques

Vous pouvez entrer les données depuis Netwrix Auditor dans d'autres processus informatiques critiques tels que la gestion des modifications, ou service bureau, pour automatiser et améliorer les flux de travail.

Visitez Add-on Store de Netwrix Auditor sur **www.netwrix.com/netwrix_addons** pour trouver des compléments gratuits conçus pour intégrer Netwrix Auditor avec votre écosystème Informatique.

Conçu pour les environnements informatiques de toutes tailles, Netwrix Auditor favorise la croissance de votre organisation

HERITAGE BANK

Banque et Finance, 100 employés

Heritage Bank s'appuie sur Netwrix Auditor pour administrer les sécurité essentielles et les politiques de conformité.

DONOHOE

Construction, 1,4K employés

Donohoe Companies a installé Netwrix Auditor pour résoudre les défis de la sécurité de ses données et de sa responsabilité.

american career college

Éducation, 5,5K employés

American Career College confie la sécurité des données du campus à Netwrix Auditor pour Active Directory.

Maine.gov

Gouvernement, 25K employés

L'État du Maine se conforme aux directives de sécurité de l'État et Fédérales avec Netwrix Auditor.

netwrix

Étapes suivantes

Essai gratuit : installez le programme dans votre propre environnement de test

- Sur Site : **netwrix.com/freetrial**
- Virtuel : **netwrix.com/go/appliance**
- Dans le Cloud : **netwrix.com/go/cloud**

Testez le produit : POC virtuel, essayez dans un laboratoire d'essais de Netwrix, **netwrix.com/testdrive**

Démo en direct : présentation du produit par un expert Netwrix **netwrix.com/livedemo**

Contact ventes : pour obtenir plus d'informations **netwrix.com/contactsales**

Récompenses

Siège social :

300 Spectrum Center Drive, Suite 200, Irvine, CA 92618

netwrix.com/social

Téléphone : 1-949-407-5125 **Numéro Gratuit :** 888-638-9749 **France :** 33-975-18-11-19