netwrix

Netwrix Data Security

Protégez vos données en toute simplicité.

www.netwrix.fr

Présentation du produit

La sécurité des données par Netwrix

Les solutions Netwrix vous permettent d'identifier avec précision les informations sensibles, réglementées et critiques et d'appliquer des contrôles d'accès de manière cohérente quel que soit l'endroit où elles sont stockées. Vous pouvez minimiser les risques de violation des données et assurer la conformité réglementaire en réduisant l'exposition des données sensibles et en détectant rapidement les infractions aux politiques et les comportements suspects des utilisateurs.

Identifier

Sachez quelles données ont besoin d'être protégées et à quel point elles sont exposées.

Protéger

Minimisez les risques de violation de données.

Détecter

Détectez rapidement les menaces envers la sécurité des données.

Réagir

Prenez des décisions plus rapides et plus éclairées en matière d'intervention sur d'incident.

Récupérer

Facilitez la récupération des données essentielles et tirez les leçons des incidents passés.

Se conformer

Assurez et prouvez la conformité réglementaire.

Avantages

01 | Sachez quelles données ont besoin d'être protégées et à quel point elles sont exposées

Identifiez et classez les données sensibles, structurées et non structurées, ainsi que les risques liés à l'infrastructure qui pourraient compromettre la sécurité des données.

02 | Minimisez les risques de violation de données

Découvrez qui a accès à quoi et remédiez de manière proactive à la surexposition des données sensibles, réglementées et stratégiques.

03 | Détectez rapidement les menaces envers la sécurité des données

Repérez les comportements anormaux des utilisateurs et les infractions aux politiques qui menacent la sécurité des données.

04 | Prenez des décisions plus rapides et plus éclairées en matière d'intervention sur d'incident

Réduisez le temps moyen de réponse aux menaces envers la sécurité des données et limitez les incidents.

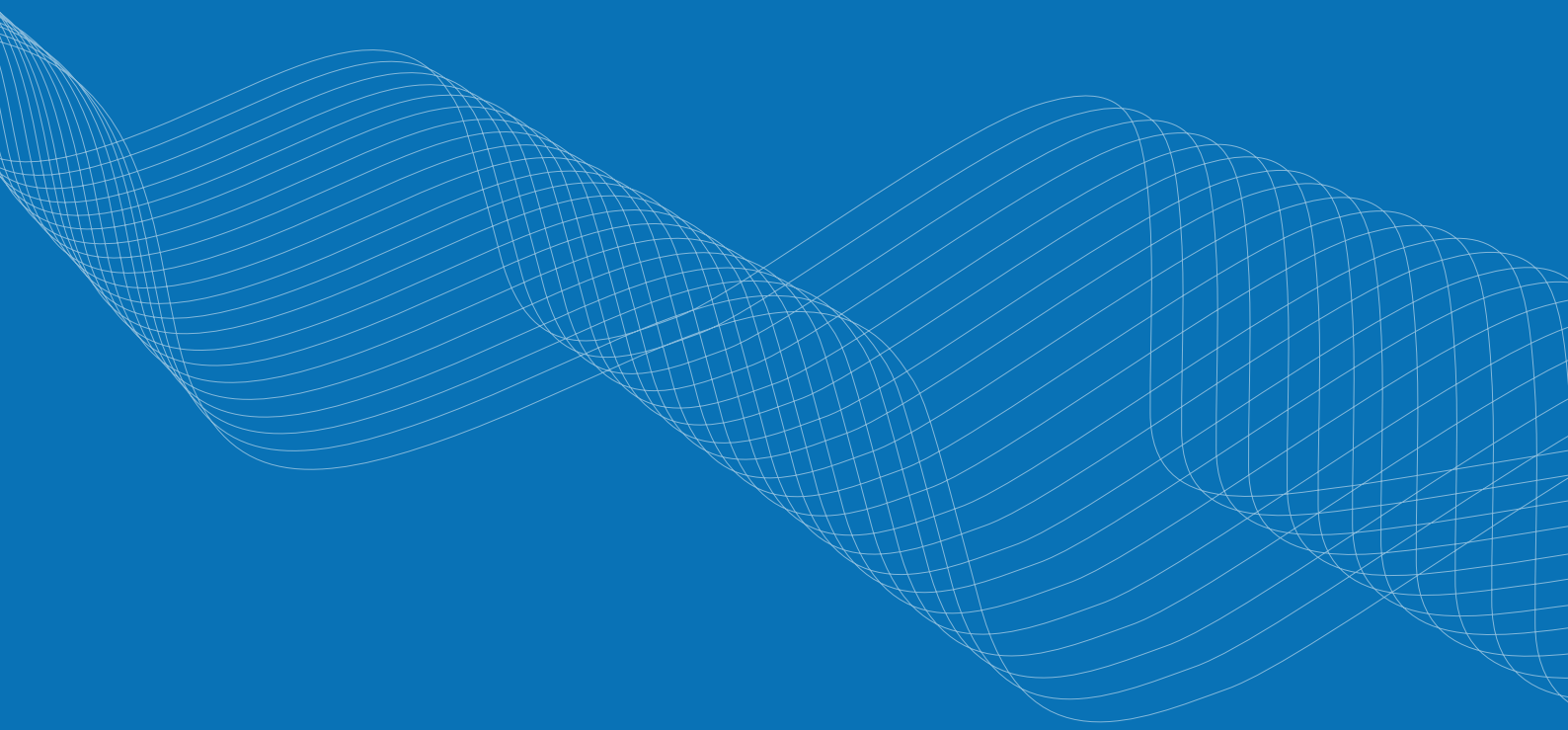
05 | Facilitez la récupération des données essentielles et tirez les leçons des incidents passés

Examinez tous les détails concernant la façon dont un incident de sécurité s'est produit et les données affectées.

06 | Assurez et prouvez la conformité réglementaire

Évaluez de manière proactive l'efficacité de vos contrôles de sécurité des données et prouvez votre conformité aux auditeurs avec des preuves tangibles.

01 | Sachez quelles données ont besoin d'être protégées et à quel point elles sont exposées



Hiérarchisez la sécurité des données sensibles dans plusieurs silos de données

Classez et étiquetez les données structurées et non structurées indépendamment de leur emplacement afin de hiérarchiser la sécurité des informations sensibles. Appliquez les politiques de sécurité de manière cohérente dans plusieurs dépôts de données.

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
\\fs1\Accounting	GDPR	1300
	PCI DSS	585
\\fs1\Finance	GDPR	715
	HIPAA	1085
	PCI DSS	952
\\fs1\HR	GDPR	1500
	HIPAA	250
\\fs1\Public	PCI DSS	15

Overexposed Files and Folders

Shows sensitive files and folders accessible by the specified users or groups, based on the combination of folder and share permissions. Clicking the "Object path" link opens the "Sensitive File and Folder Permission Details" report. Use this report to identify data at high risk and plan for corrective actions accordingly.

Group Name: Everyone

Object path	Categories
\\fs1\Accounting\Contractors	GDPR
	PCI DSS
	PII
\\fs1\Accounting\Payroll	GDPR
	PCI DSS
\\fs1\Accounting\Invoices	GDPR
	PCI DSS

Identifiez les données sensibles surexposées

Constatez quelles données sensibles sont les plus exposées afin d'établir un ordre de priorité pour la remédiation à ces risques. Découvrez les informations sensibles qui sont exposées à un grand nombre d'utilisateurs sans véritable nécessité ou qui sont stockées dans un endroit non sécurisé.

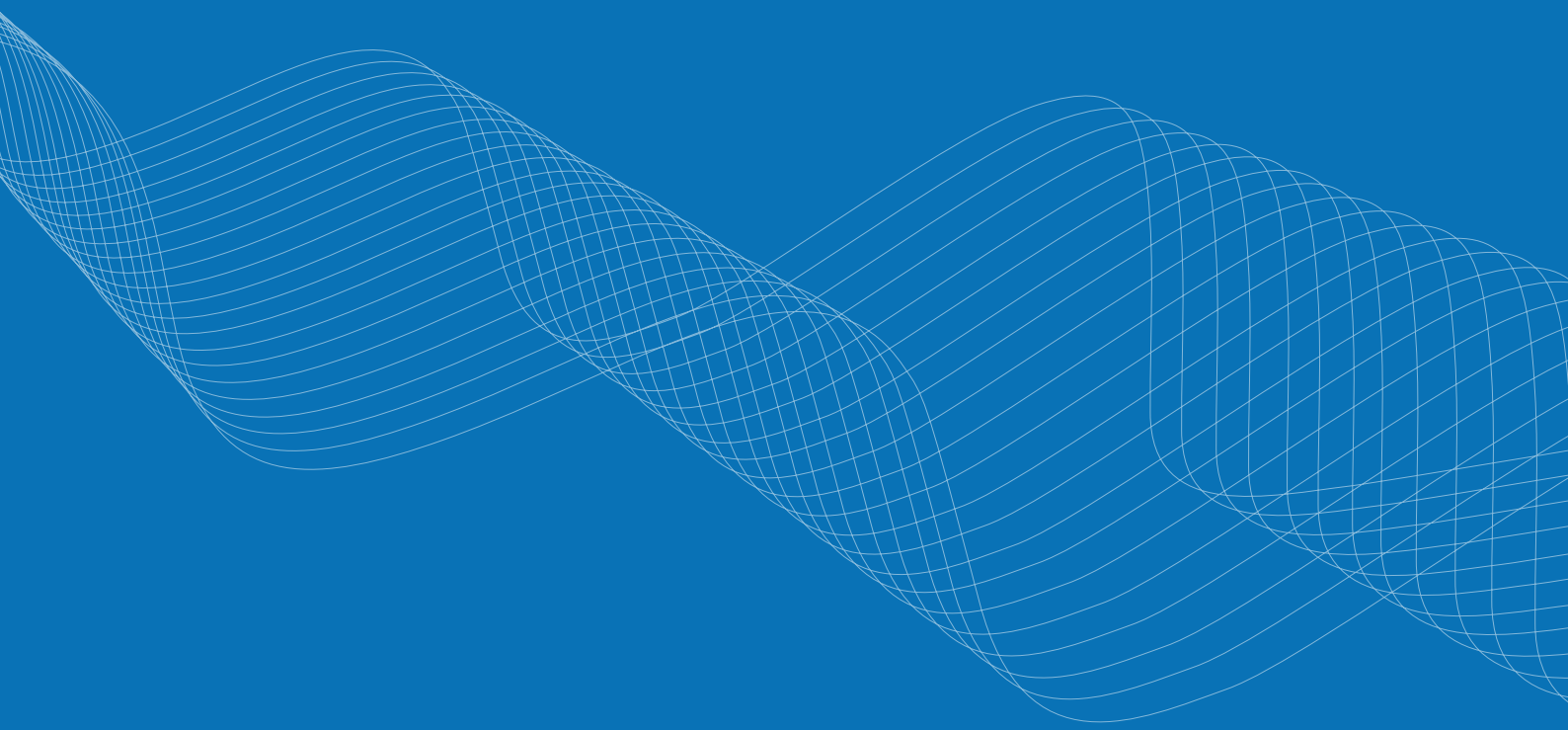
Évaluez les risques pour la sécurité des données et de l'infrastructure

Identifiez les lacunes en matière de sécurité des données et de l'infrastructure, telles qu'un grand nombre d'autorisations directement attribuées ou un trop grand nombre de comptes d'utilisateur inactifs. Évaluez continuellement ces critères de sécurité et concentrez-vous sur ce qui est le plus important.

Risk Assessment – Overview

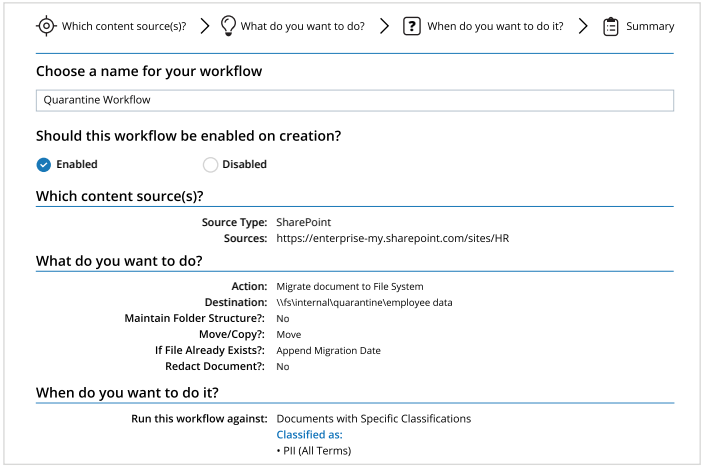
Risk name	Current value	Risk level
Users and Computers		
User accounts with Password never expires	2	Medium (1-4)
User accounts with Password not required	0	Low (0)
Disabled computer accounts	0% (0 of 20)	Low (0)
Inactive user accounts	10% (3 of 30)	High (1% - 100%)
Inactive computer accounts	20% (4 of 20)	High (3% - 100%)
Permissions		
User accounts with administrative permissions	20% (6 of 30)	High (3% - 100%)
Administrative groups	12% (6 of 50)	High (3% - 100%)
Empty security groups	6% (3 of 50)	High (2% - 100%)
Data		
Shared folders accessible by Everyone	14% (2145 of 15321)	High (5% - 100%)
File names containing sensitive data	2	High (2 - unlimited)

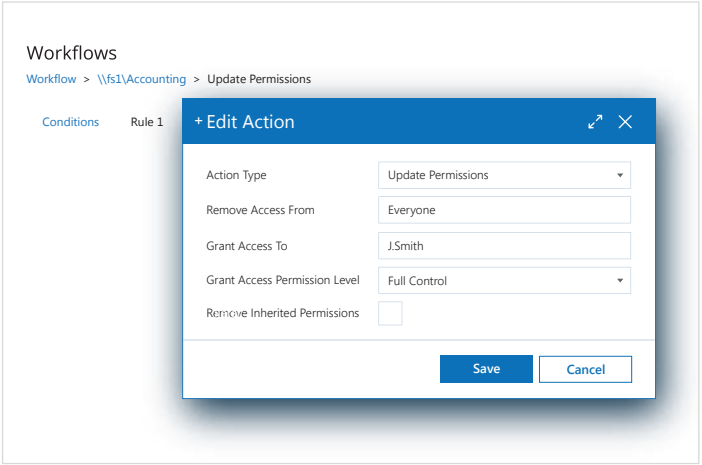
02| Minimisez les risques de violation de données



Mettez automatiquement en quarantaine les données sensibles afin de réduire le risque de violation ou de perte

Si un fichier sensible est découvert à un endroit inattendu, déplacez-le automatiquement dans une zone de quarantaine jusqu'à ce que vous puissiez déterminer où il doit être stocké et qui doit y avoir accès.





Verrouillez immédiatement les données sensibles surexposées

Si les contrôles d'accès aux données sensibles ne sont pas adaptés aux risques, supprimez automatiquement tous les droits de lecture ou de modification de ces informations pour les groupes d'accès globaux (par exemple «Tout le monde»).

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. Si tel n'est pas le cas, retirez les autorisations excessives pour appliquer le principe du moindre privilège et maintenir le risque à un niveau acceptable.

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, vie either group membershir or direct assignment. Reveal sensitive content that has permissions different from the parent folder.

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

Categories: GDPR, PCI DSS

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

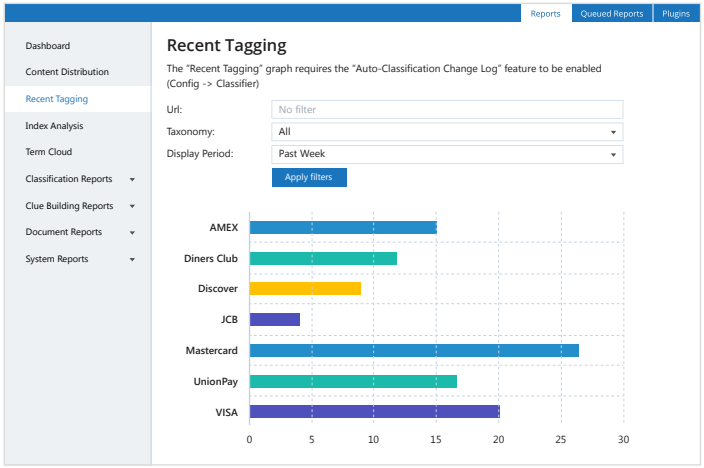
Object: \\fs1\Accounting\Europe (Permissions: Different from parent)

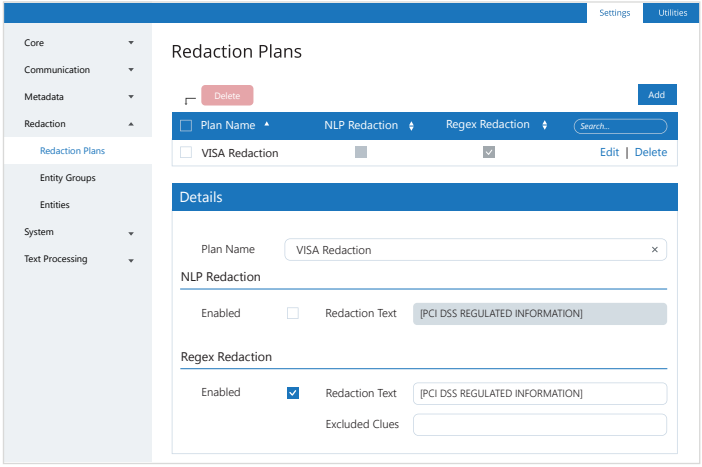
Categories: GDPR

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

Augmentez la précision de votre solution DLP

Les éléments non sensibles étiquetés par erreur n'ont pas besoin de protection. Optimisez vos efforts en matière de sécurité des données en augmentant la précision de votre outil de prévention des pertes de données (DLP) grâce aux balises de classification de haute précision écrites par Netwrix.

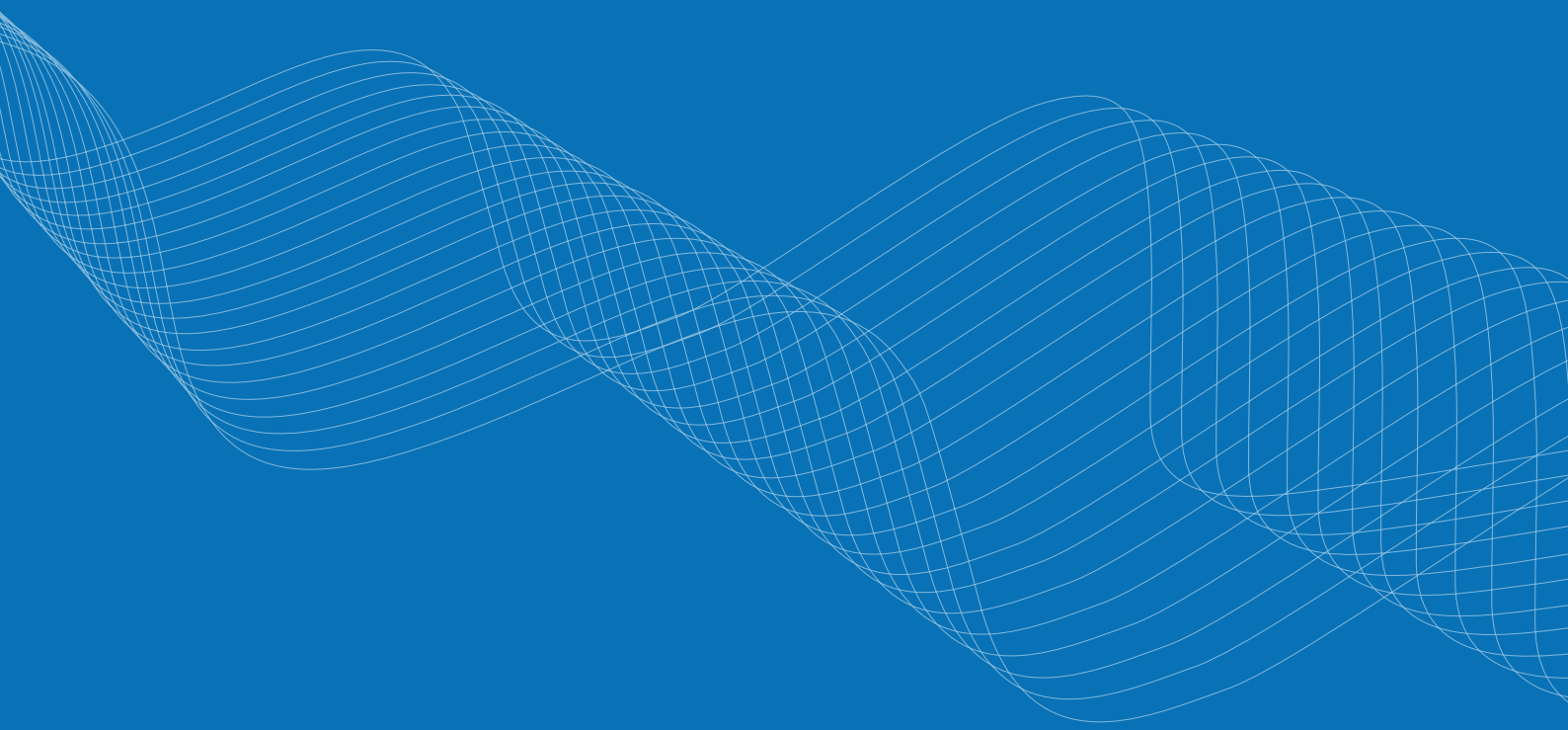




Expurgez les informations sensibles selon la politique de l'entreprise

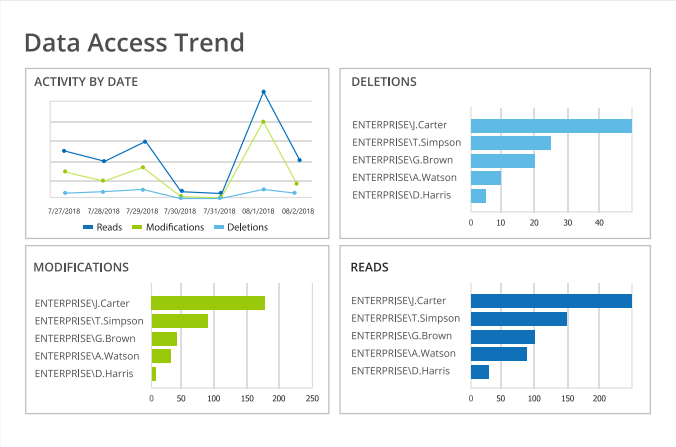
Réduisez le risque d'exposition des informations confidentielles en supprimant automatiquement les contenus sensibles des documents si leur présence ne constitue pas un impératif métier. Préservez la productivité en conservant le reste du document intact.

03 | Détectez rapidement les menaces envers la sécurité



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 pour accéder, modifier ou supprimer des données sensibles en toute impunité.



Administrative Group Membership Changes

Shows changes to membership of the Domain Admins, Enterprise Admins, Schema Admins, Account Operators, and other administrative groups.

Group name: \ENTERPRISE\Users\Domain Admins

Action	Member	Who	When
Added Where:	\ENTERPRISE\Users\Jack Falcon dc1.enterprise.com	ENTERPRISE\ R.Ferrano	9/17/2018 6:57:32 PM

Group name: \ENTERPRISE\Users\Domain Admins

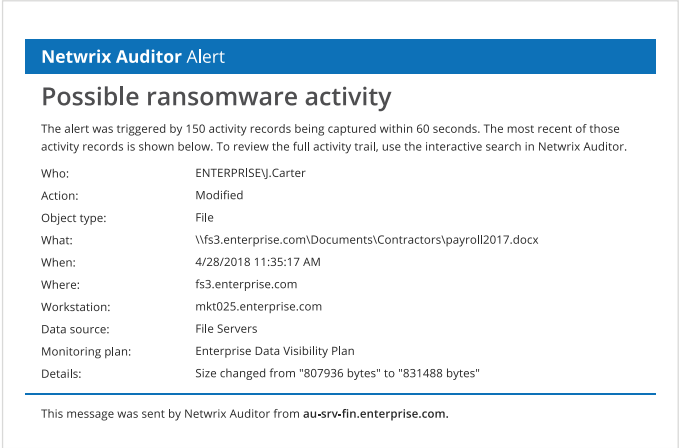
Action	Member	Who	When
Added Where:	\ENTERPRISE\Users\Liza Lee dc1.enterprise.com	ENTERPRISE\ P.Jackson	9/16/2018 7:07:18 PM

Soyez informé des augmentations de privilèges

Détectez toute modification des droits d'accès ou de l'appartenance à un groupe afin de pouvoir évaluer si les autorisations d'accès aux données sensibles ont été modifiées sans motif légitime.

Détectez les attaques de rançongiciels en cours

Soyez alerté des signes d'une éventuelle activité de rançongiciel, par exemple un grand nombre de modifications de fichiers dans un laps de temps très court. Isolez rapidement le compte utilisateur responsable pour empêcher le logiciel de chiffrer tous les fichiers auxquels ce compte a accès sur votre réseau.



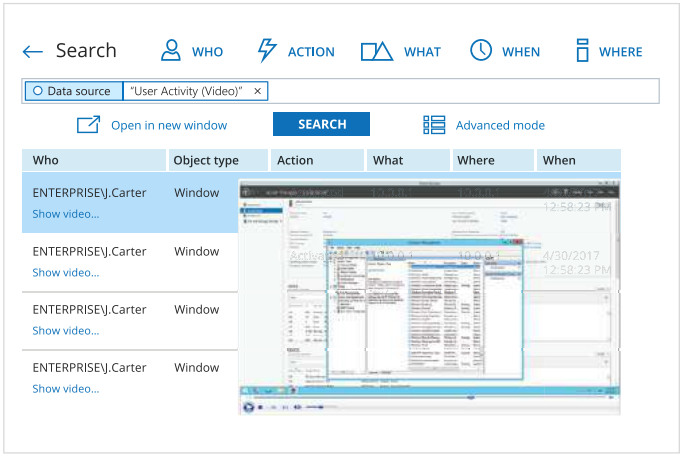
Netwrix Auditor Alert

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:	4/28/2018 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.**

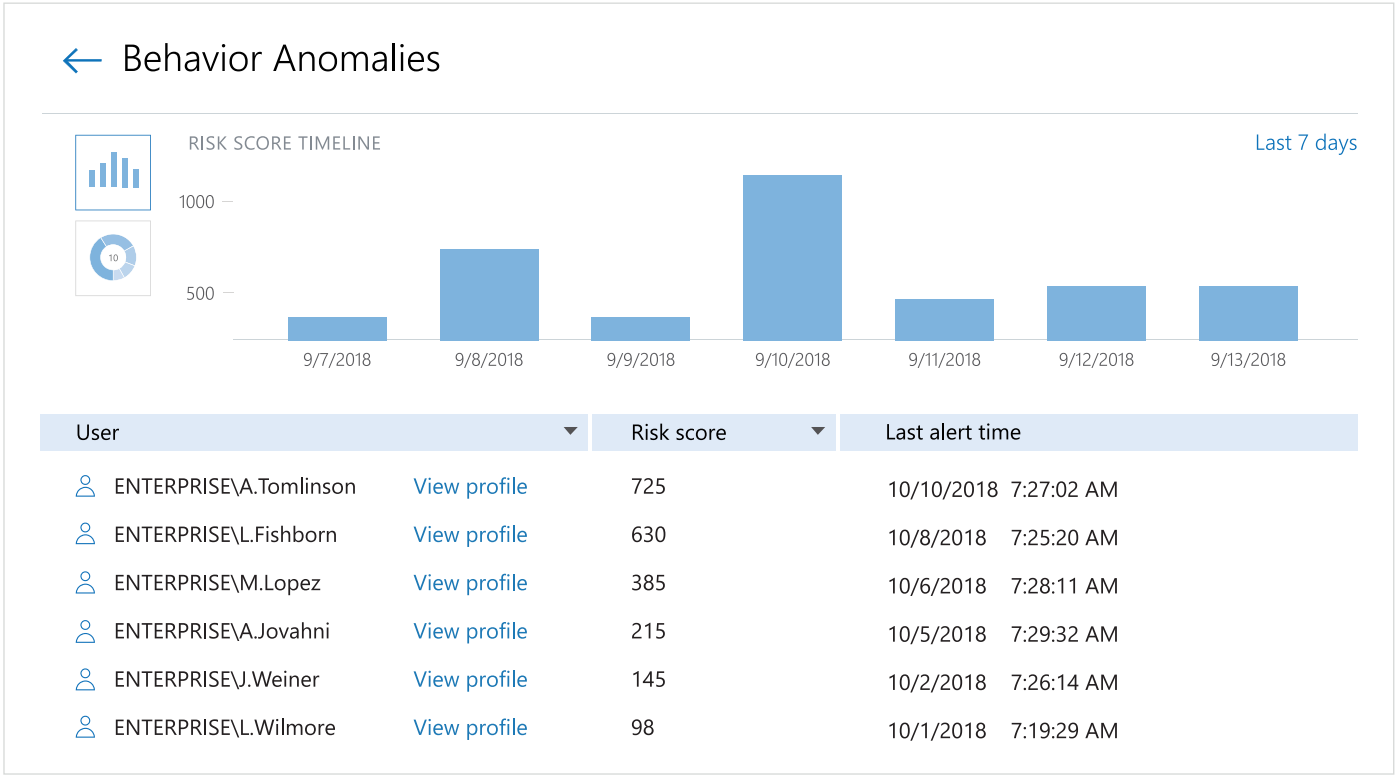


Surveillez de près les activités des tiers

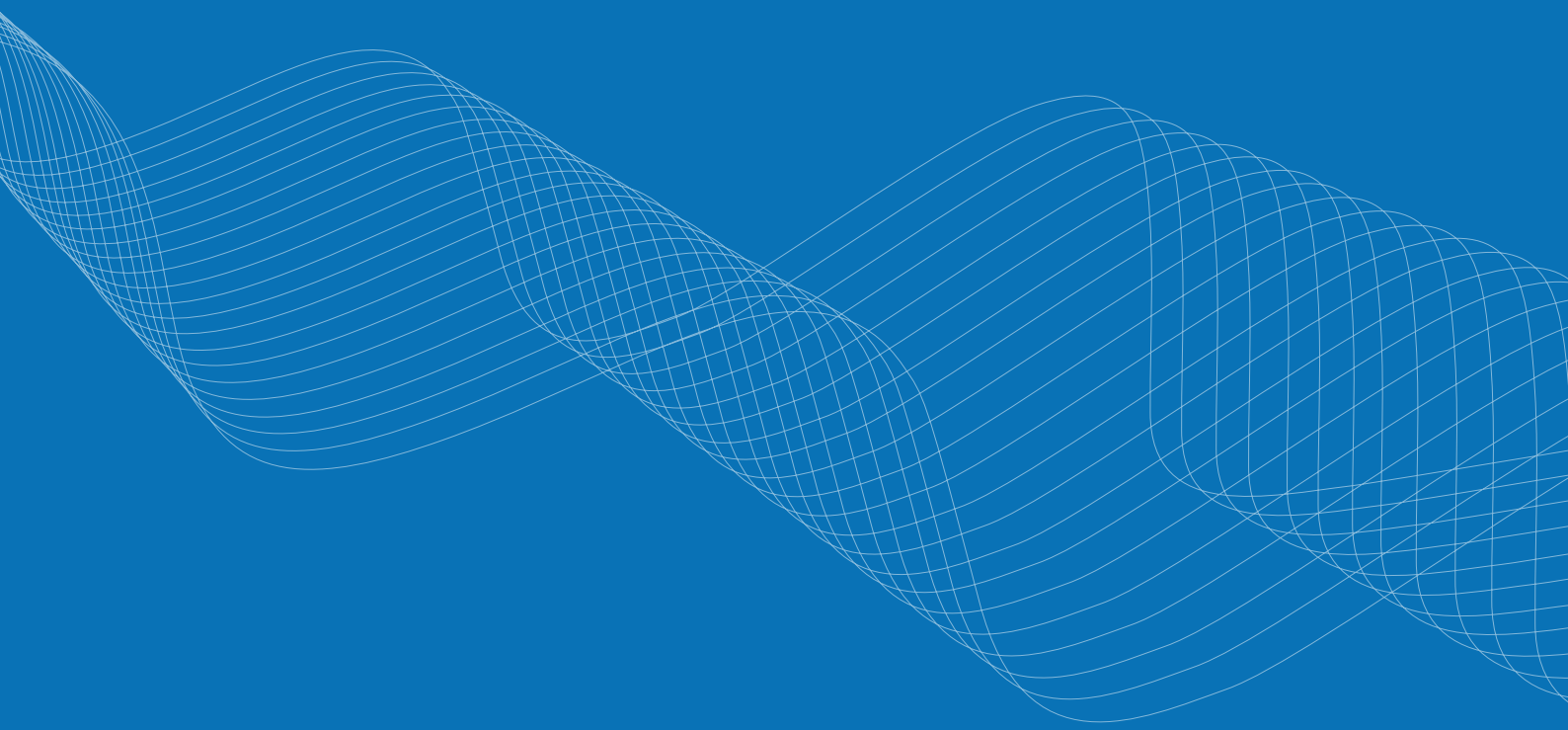
Surveillez attentivement l'activité des comptes d'utilisateur tiers dans tout système ou toute application, même si ceux-ci ne produisent pas de journaux, afin d'établir les responsabilités. Soyez averti chaque fois qu'un fournisseur fait quelque chose qui ne relève pas de son domaine d'activité, car ses actions non autorisées pourraient mettre vos données en péril.

Détectez les comptes compromis et les utilisateurs internes malveillants

Détectez rapidement les moindres signes d'éventuelles menaces en cours pour la sécurité des données, telles que des connexions inhabituelles ou des utilisateurs accédant à des données sensibles auxquelles ils n'ont jamais accédé auparavant. 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.

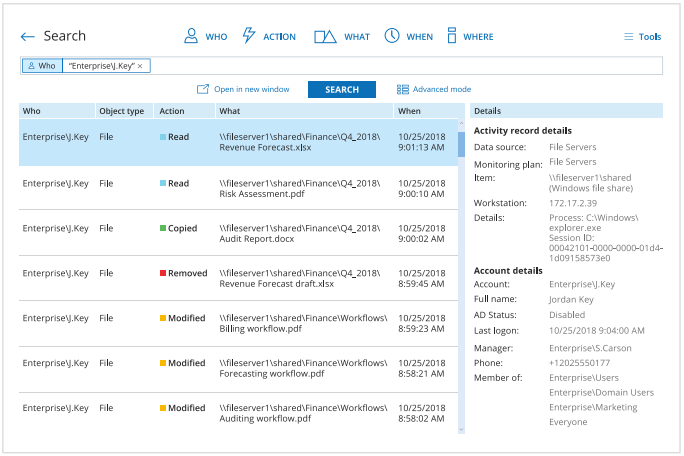


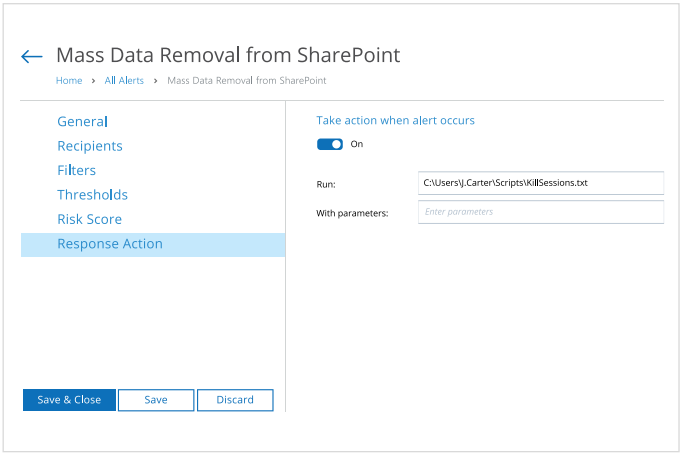
04 | Prenez des décisions plus rapides et plus éclairées en matière d'intervention sur d'incident



Rationalisez les enquêtes sur incident

Faites rapidement la lumière sur les incidents impliquant des données sensibles : comprenez exactement ce qui s'est passé, comment c'est arrivé, qui était derrière cela et quels éléments d'information ont été affectés. Servez-vous de ce contexte pour formuler la meilleure réponse possible à l'incident.





Réagissez plus 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 cas d'incident, accélérez les enquêtes et améliorez leur précision en intégrant Netwrix à votre processus SecOps.

Déterminez et signalez la gravité d'une violation de données

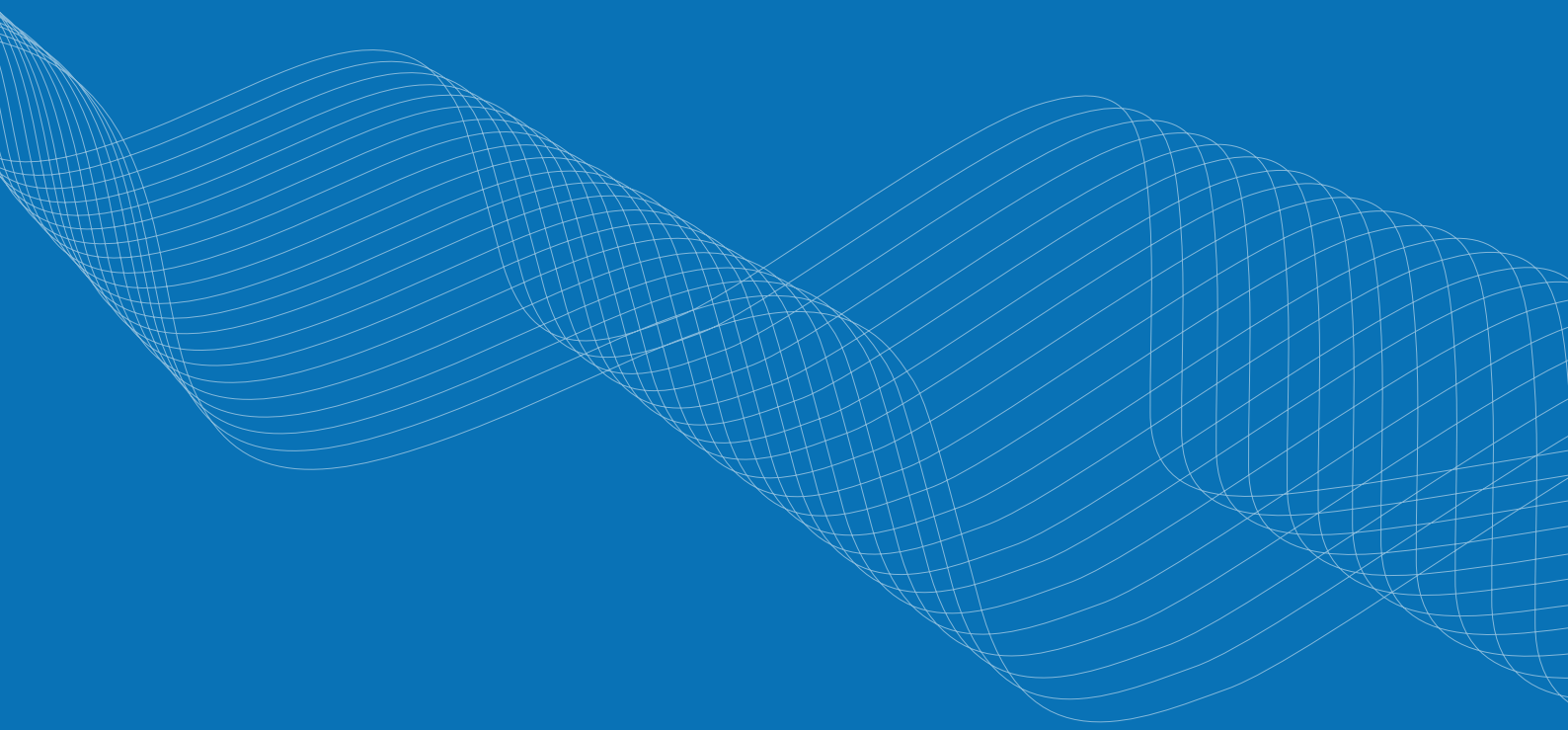
Analysez la quantité de données auxquelles un utilisateur interne malveillant ou un compte compromis a eu accès et quelles données ont été réellement consultées, modifiées ou supprimées. Utilisez ces renseignements pour déterminer si vous devez signaler l'incident et, si nécessaire, aviser toutes les parties concernées et prendre d'autres mesures appropriées.

Activity Related to Sensitive Files and Folders

Shows all access attempts (failed and successful changes, and successful and failed read attempts) to files and folders that contain certain categories of sensitive data.

Action	Object type	What	Who	When
Read (Failed Attempt) Where: Workstation: Categories:	Folder fs1 192.168.77.25 PCI DSS	\\fs1\Accounting\Payroll	ENTERPRISE\ M.Smith	3/12/2018 9:25:49 AM
Read Where: Workstation: Categories:	Folder fs1 192.168.77.25 PCI DSS	\\fs1\Accounting\Payroll	ENTERPRISE\ M.Smith	3/12/2018 9:25:55 AM

05 | Facilitez la récupération des données essentielles et tirez les leçons des incidents passés



Comprenez la valeur et la sensibilité des données lors de la planification des processus de récupération des informations

Faites l'inventaire de vos données et voyez où se trouvent les données les plus sensibles ou les plus précieuses. Créez des plans de récupération des informations qui établissent un ordre de priorité pour la restauration de ces données.

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
\\fs1\Accounting	GDPR	1300
	PCI DSS	585
\\fs1\Finance	GDPR	715
	HIPAA	1085
	PCI DSS	952
\\fs1\HR	GDPR	1500
	HIPAA	250
\\fs1\Public	PCI DSS	15

Activity Related to Sensitive Files and Folders

Shows all access attempts (failed and successful changes, and successful and failed read attempts) to files and folders that contain certain categories of sensitive data.

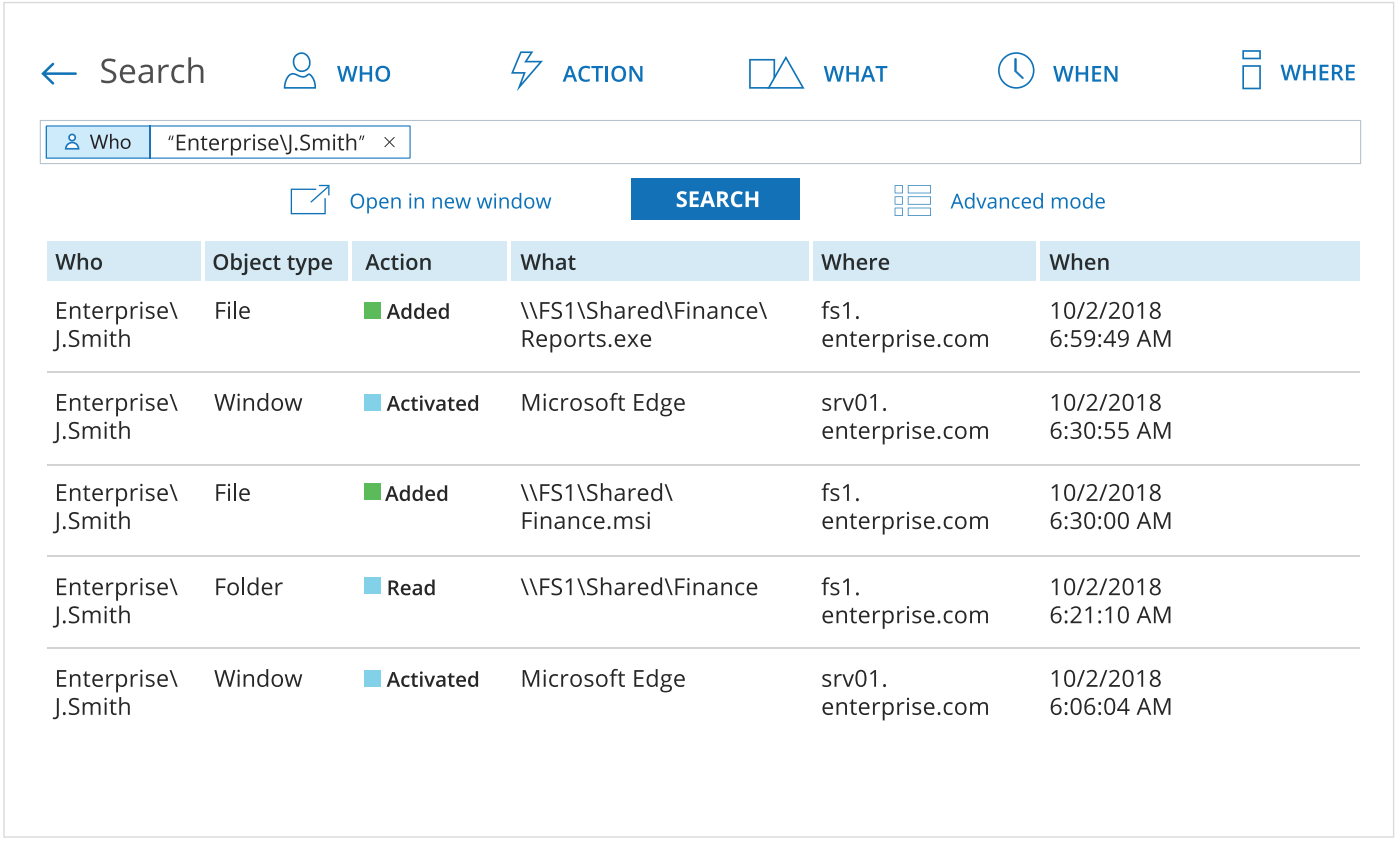
Action	Object type	What	Who	When
Removed	File	\\fs1\Finance\Revenue2018.xlsx	ENTERPRISE\ T.Simpson	12/22/2018 4:30:33 PM
Where: fs1 Workstation: 192.169.55.34 Categories: PCI DSS Date created: "1/24/2018 10:11:42 AM"				
Removed	File	\\fs1\Finance\Revenue2017.xlsx	ENTERPRISE\ T.Simpson	12/22/2018 4:35:47 PM
Where: fs1 Workstation: 192.169.55.34 Categories: PCI DSS Date created: "1/23/2017 11:34:54 AM"				

Accélérez la reprise en définissant des priorités pour la récupération des données essentielles

Déterminez quelles données sensibles, confidentielles ou stratégiques ont été corrompues pendant une attaque et établissez un ordre de priorité pour leur récupération. Découvrez qui a eu quel accès à ces documents, pour permettre à vos utilisateurs professionnels de reprendre le travail le plus rapidement possible.

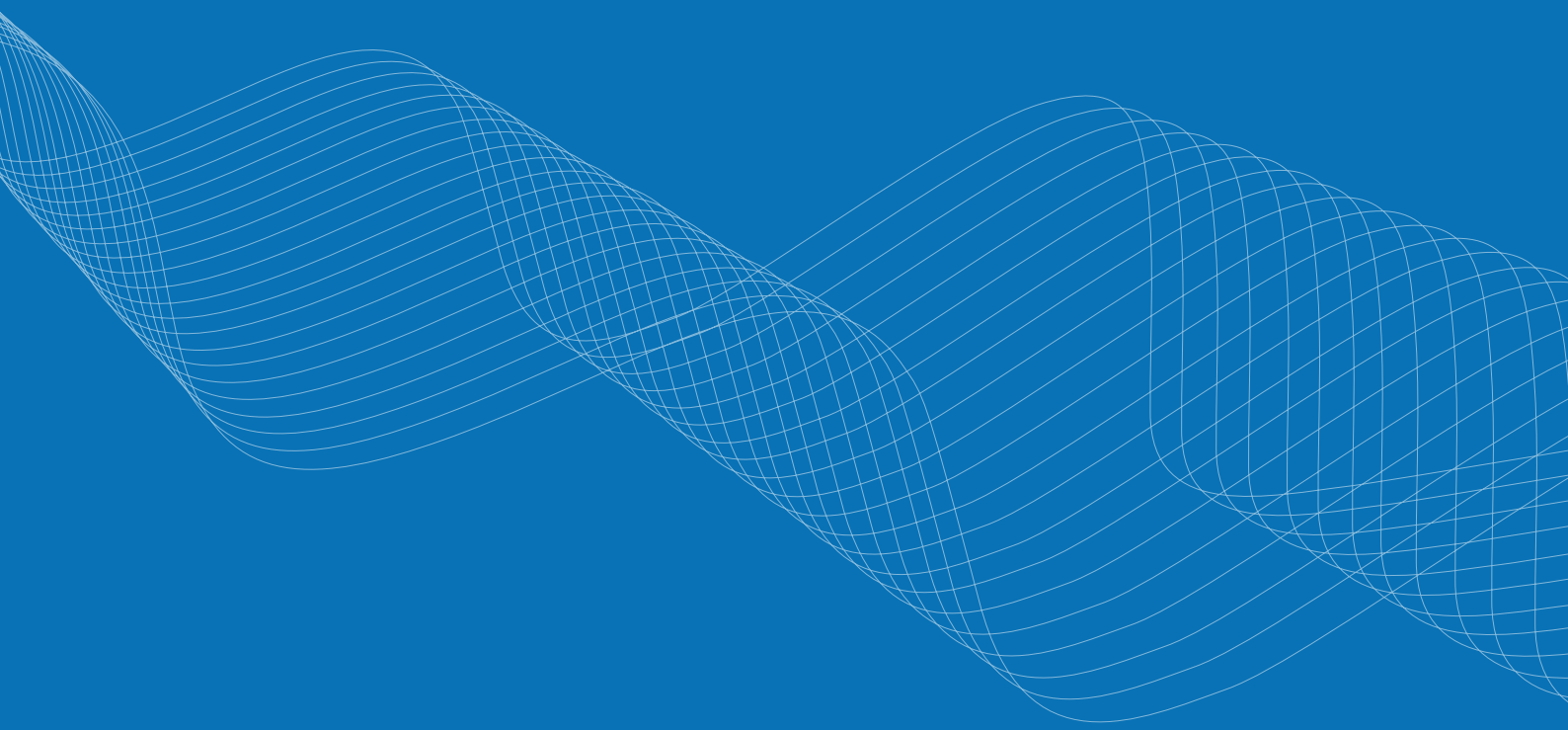
Intégrez les leçons tirées de l'expérience dans votre stratégie de sécurité des données

Analysez précisément la manière dont un incident de sécurité s'est produit et utilisez ces informations pour améliorer votre stratégie de sécurité des données et prévenir des incidents similaires à l'avenir.



Who	Object type	Action	What	Where	When
Enterprise\ J.Smith	File	Added	\\FS1\Shared\Finance\ Reports.exe	fs1. enterprise.com	10/2/2018 6:59:49 AM
Enterprise\ J.Smith	Window	Activated	Microsoft Edge	srv01. enterprise.com	10/2/2018 6:30:55 AM
Enterprise\ J.Smith	File	Added	\\FS1\Shared\ Finance.msi	fs1. enterprise.com	10/2/2018 6:30:00 AM
Enterprise\ J.Smith	Folder	Read	\\FS1\Shared\Finance	fs1. enterprise.com	10/2/2018 6:21:10 AM
Enterprise\ J.Smith	Window	Activated	Microsoft Edge	srv01. enterprise.com	10/2/2018 6:06:04 AM

06| Assurez et prouvez la conformité réglementaire



Évaluez l'efficacité de vos contrôles de sécurité des données

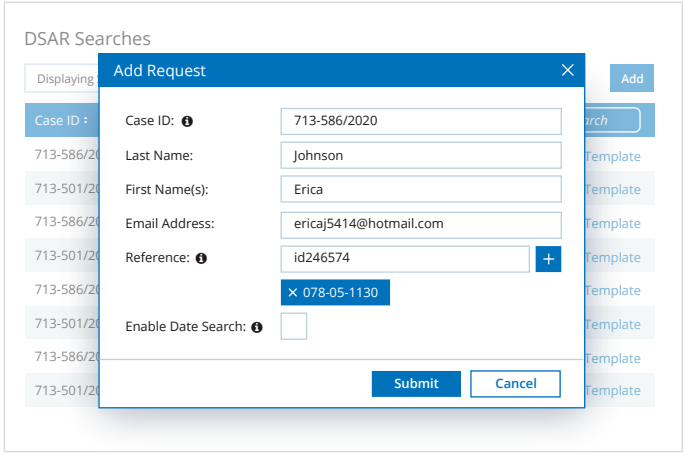
Mettez en œuvre des contrôles de conformité dans toute votre infrastructure et évaluez régulièrement leur bon fonctionnement. Si les politiques de sécurité écrites diffèrent des mesures en place, vous pouvez remédier à vos contrôles de sécurité défaillants avant que les auditeurs ne les découvrent.

Account Permissions

Shows accounts with permissions granted on files and folders (either directly or via group membership). Use this report to see who has access to files and folders and ensure these settings comply with your policies.

Group name: Everyone

Object Path	Permissions	Means Granted
\\pdc\shared\Accounting	Read (Execute, List folder content)	Directly
\\pdc\shared\Customer Data	Full Control	Directly
\\pdc\shared\Orders	Read (Execute, List folder content)	Directly
\\pdc\shared\Finance	Read (Execute, List folder content)	Directly
\\pdc\shared\Internal	Full Control	Directly
\\pdc\shared\Sales	Full Control	Directly

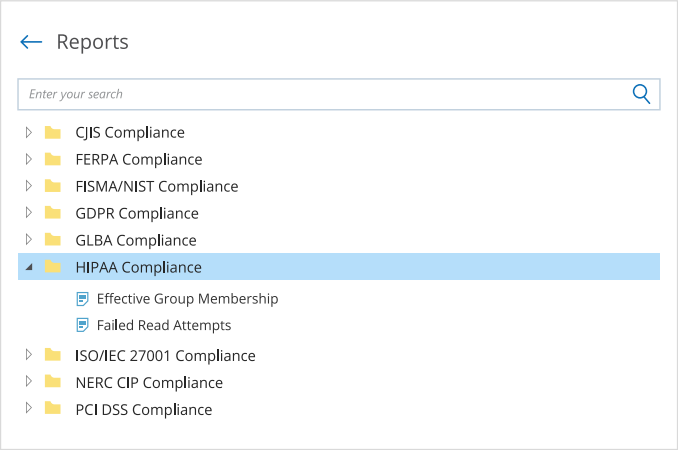


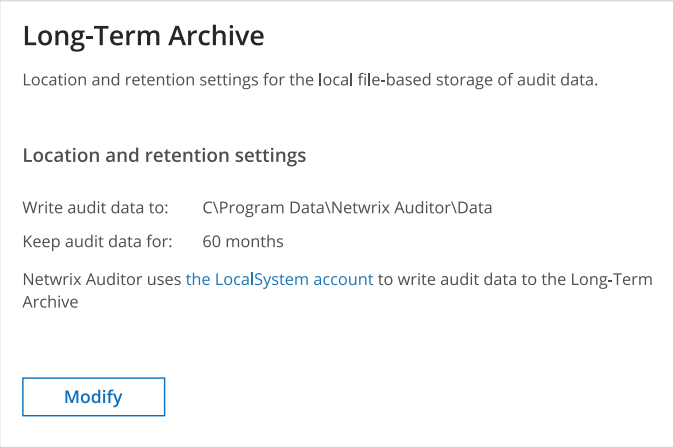
Satisfaites les demandes d'accès

Trouvez facilement toutes les données que vous stockez sur un sujet de données particulier lorsque celui-ci exerce ses droits à la confidentialité selon le RGPD, CCPA ou d'autres réglementations modernes. Fournissez-lui une liste de ces informations ou supprimez-les si le sujet retire son consentement.

Gagnez du temps dans la préparation de la conformité et les audits

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.





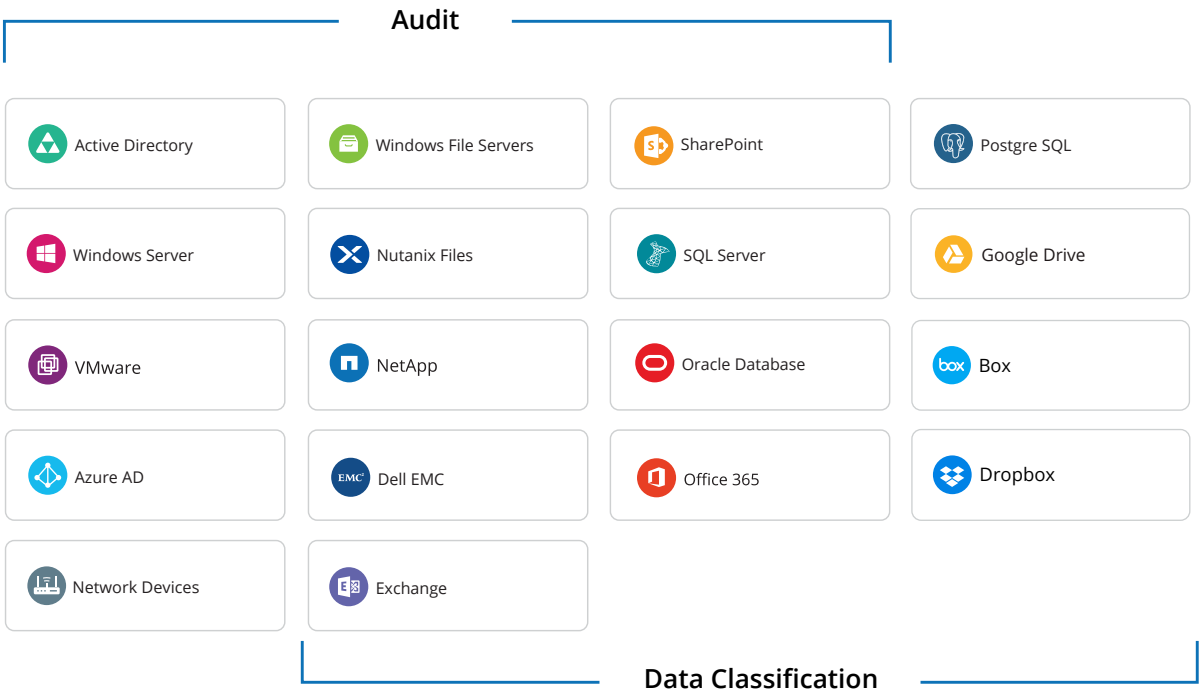
Stockez et accédez à votre piste d'audit pendant des années

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.

Systèmes pris en charge

Systèmes pris en charge par Netwrix

Les plateformes Netwrix prennent en charge une vaste gamme de systèmes, qui fournissent une vue d'ensemble de ce qui se passe dans les **systèmes de stockage de données** et les **systèmes informatiques dorsaux**. Ces connaissances permettent aux entreprises de savoir où se trouvent leurs données sensibles, quels risques les concernent et quelles activités menacent leur sécurité.



Profitez de capacités d'intégration infinies pour une meilleure sécurité des données

Centralisez les audits et le reporting

Netwrix 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

En alimentant en données d'audit granulaires vos solutions HP Arcsight, Splunk, IBM QRadar ou autres solutions SIEM, Netwrix augmente le rapport signal/bruit et maximise la valeur du SIEM.

Automatisez les flux de travail informatiques

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

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

Qu'est-ce qui nous differencie ?

Retour sur investissement rapide

Obtenez de la valeur dès le départ et rentabilisez votre investissement en quelques jours, et non en quelques mois.

Un conseiller de confiance

Choisissez un partenaire stratégique plutôt qu'un simple fournisseur, et profitez d'un partenariat fiable et à long terme.

Une assistance de première classe

Vos problèmes sont définitivement résolus par le service à la clientèle basé aux États-Unis, avec un taux de satisfaction de 97 %.

Conçu pour les environnements informatiques de toutes tailles, l'architecture de Netwrix prend en charge la croissance de votre entreprise

Synergia

Santé

Le Groupe Synergia assure sa conformité RGPD et jugule une attaque ransomware en une heure.

WILLIAM WOODS UNIVERSITY

Éducation

L'Université William Woods utilise Netwrix pour réduire le risque d'exposition des données et améliorer la posture de sécurité.

JOHNSON COUNTY KANSAS

Gouvernement

Le comté de Johnson au Kansas simplifie la détection des événements suspects et les enquêtes à leur sujet avec Netwrix

PIKE CONSTRUCTION

Énergie

Pike Electric résout plus rapidement les problèmes de sécurité et assure la continuité des opérations grâce à Netwrix.

À propos de Netwrix

Netwrix est un éditeur de logiciels qui permet aux professionnels de la sécurité et de la gouvernance de l'information de reprendre le contrôle des données sensibles, réglementées et stratégiques, quel que soit leur emplacement. Plus de 10 000 organisations du monde entier s'appuient sur les solutions Netwrix pour sécuriser leurs données sensibles, tirer pleinement parti des contenus d'entreprise, réussir les audits de conformité en déployant moins d'efforts et en dépensant moins et améliorer la productivité de leurs équipes informatiques et de leurs travailleurs du savoir.

Pour plus d'information, visitez www.netwrix.fr.

Étapes suivantes

Essai gratuit — Essayez Netwrix Auditor dans votre propre environnement de test : netwrix.fr/freetrial

Calculatrice de retour sur investissement – Découvrez comment les solutions Netwrix peuvent réduire votre exposition financière en cas de violation des données : netwrix.fr/roi

Démonstration individuelle — Programmez une présentation personnalisée du produit : netwrix.fr/one-to-one

Demande de tarifs — Obtenez un devis sur mesure : netwrix.fr/buy

Awards

Siège social :

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

Tél : + 33 9 75 18 11 19 **Gratuit :** 888-638-9749

netwrix.com/social

Copyright © Netwrix Corporation. Tous droits réservés. Netwrix est une marque de commerce de Netwrix Corporation et/ou d'une ou plusieurs de ses filiales et peut être enregistrée dans le Bureau des brevets et marques aux États-Unis et dans d'autres pays. Toutes les autres marques de commerce et marques déposées appartiennent à leurs propriétaires respectifs.