netwrix

Contrôles RGPD

et Mappage de Netwrix Auditor

À propos du RGPD

Le Règlement Général de la Protection des Données (RGPD) est un acte juridique du Parlement Européen et du Conseil (règlement (UE) 2016/679) qui a été adopté en avril 2016 et entrera en vigueur le 25 mai 2018. Le RGPD vise principalement à fournir des règles claires et unifiées sur la protection renforcée des données propres à l'ère du numérique, de donner aux individus un contrôle plus important de leurs renseignements personnels traitées par des entreprises, et à faciliter l'application de la loi. Le RGPD abrogera la loi actuelle (Directive 95/46/CE) adoptée en 1995, qui a été interprétée de manière incohérente par les différents états membres de l'Union Européenne.

En plus d'harmoniser la Loi de protection des données dans toute l'UE, la nouvelle réglementation affectera également les compagnies non européennes qui offrent des produits ou services, ou surveillent le comportement des résidents de l'Union Européenne, et donc traitent leurs données personnelles. Ceci se rapporte à l'application extraterritoriale de la Loi. En d'autres termes, les organisations de tous types dans toutes les industries qui sont établies en dehors de l'Union Européenne, mais y font des affaires seront soumises au respect du RGPD à compter du 25 mai 2018.

La compétence élargie du RGPD est sans doute la plus importante modification de la Directive de 1995. Les autres principes importants exprimés dans le RGPD sont les suivants :

- **Étendue des droits des personnes concernées** — Ceci comprend, entre autres, le droit d'accès, le droit à la portabilité des données et le droit à l'effacement des données.
- **Notification de violation de données sous 72 heures** — Dans le cas d'une violation de données personnelles, l'organisme concerné doit aviser l'autorité de surveillance au plus tard 72 heures après l'avoir constatée.
- **La vie privée dès la conception** — Les organismes doivent s'assurer que, tant dans la phase de planification des activités de transformation que dans la phase de mise en œuvre d'un nouveau produit ou service, les principes RGPD de protection des données et les sécurités appropriées sont abordés et mis en œuvre.
- **Responsabilité** — Un organisme doit assurer et démontrer la conformité avec les principes RGPD de protection de données.

Les amendes pour non-respect du RGPD dépendent de l'infraction. Dans le cas d'une violation de données à caractère personnel (définie comme une violation de sécurité menant à la destruction, la perte, l'altération, la divulgation ou les accès non autorisés, accidentels ou illicites, aux données à caractère personnel transmises, stockées ou traitées de toute autre manière), l'amende peut se monter jusqu'à 4 % du chiffre d'affaires mondial annuel de la société ou de € 20 millions, selon ce qui est le plus élevé. Pour les autres violations des dispositions du RGPD, l'amende est jusqu'à 2 % du chiffre d'affaires mondial annuel ou € 10 millions, selon ce qui est plus élevé.

Cartographie des processus et des catégories de rapports selon les dispositions des articles du RGPD

Le tableau suivant répertorie quelques-unes des principales dispositions du RGPD et explique comment Netwrix Auditor peut aider votre organisme à se conformer à ces dispositions. Veuillez prendre note que les efforts et les procédures requises pour satisfaire aux exigences du RGPD peuvent varier selon la configuration des systèmes des organismes, des procédures internes, de la nature de l'entreprise ainsi que d'autres facteurs. La mise en œuvre des procédures décrites ci-dessous ne garantit pas la conformité au RGPD, ni que tous les contrôles que Netwrix Auditor peut éventuellement prendre en charge, soient inclus. Ce mappage doit être utilisé comme un guide de référence pour vous aider à mettre en œuvre des politiques et des procédures adaptées à la situation particulière et aux besoins de votre organisme.

RGPD chapitre II		
Dispositions	**Comment faire ?**	**Processus et catégories de Reports**
Article 5. §1. Les données personnelles seront: **(f)** traitées d'une manière qui assure, par l'utilisation de mesures techniques ou organisationnelles appropriées ("intégrité et la confidentialité"), la sécurité des données personnelles, y compris la protection contre le traitement non autorisé ou illégal et contre la perte accidentelle, la destruction ou la détérioration.	Utilisez les abonnements du rapport pour définir un calendrier approprié pour l'examen des rapports qui montrent tous les comptes d'utilisateurs en l'état présent ou historique des autorisations sur les fichiers et les dossiers ; les appartenances présentes et passées aux groupe, les autorisations d'objets accordées aux comptes d'utilisateurs ; les autorisations d'accès excessives ; les permissions d'interruptions héritées ; et les changements dans les attributions de droits d'utilisateur. Utilisez les traces d'audit recueillies pour revoir les accès utilisateur au contenu et aux données sensibles dans SharePoint, Exchange, Exchange Online, les serveurs de fichiers Windows, les périphériques de stockage connectés au réseau, les bases de données et les autres systèmes informatiques. Servez-vous des rapports pour voir toutes les manipulations de données qui ont eu lieu sur un serveur SQL spécifié, y compris les modifications apportées aux clés, index, rôles de serveur, connexions et contenu de la base de données. Examinez les modifications apportées aux privilèges d'utilisateur, aux rôles, tableaux, vues et déclencheurs, ainsi que des tentatives réussies et échouées de modifier ou d'accéder à vos données structurées dans la Base de Données Oracle. Activez la détection, en temps réel, de toute action d'utilisateur qui viole votre politique de protection	**[Catégories de rapports]** États des Comptes États des Appartenances de Groupe Modifications des Appartenances de Groupe Contrôle des Accès Accès aux données Gouvernance des données Modifications des données Surveillance de l'Intégrité Intégrité des Données Modification de la Configuration Politique de Modification

	des données en vous abonnant aux rapports suivants : Fichiers et Dossiers Supprimés, Destructions de Données, Fichiers et Dossiers déplacés, Fichiers et Dossiers renommés et Fichiers Copiés.	
Article 5. §2. Le contrôleur est responsable de la conformité avec le paragraphe 1 (responsabilité) et doit être en mesure de la prouver.	Démontrez l'efficacité de vos contrôles de la protection des données au moyen d'une trace d'audit complète consolidée et maintenue fiable par Netwrix Auditor dans un système de stockage AuditArchive™ à deux niveaux (basé sur les fichiers + base de données SQL). Accédez facilement aux données archives d'audits chaque fois que cela est nécessaire pour l'évaluation de la sécurité, des analyses et procédures de conformité, des enquêtes et des processus de compatibilité. Obtenez des renseignements importants sur les actions de l'utilisateur et démontrez l'efficacité de vos contrôles à l'aide de tableaux de bord et des rapports prédéfinis. Créer des rapports personnalisés ou identifiez facilement des données spécifiques avec la Recherche Interactive.	**[Processus]** La collecte centralisée, la consolidation et l'archivage d'une trace complète d'audit sont possible par la fonction AuditArchive™ de Netwrix Auditor. **[Catégories de Rapports]** Trace d'Audit

RGPD chapitre IV		
Dispositions	**Comment se Conformer ?**	**Processus et Catégories de Rapport**
Article 24. §1. .. le contrôleur doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures doivent être revues et mises à jour lorsque c'est nécessaire.	Analysez les rapports de Netwrix Auditor exigés pour obtenir les informations appropriées du contexte concernant les modifications de configuration du système ainsi que les accès au système et aux données présentant des menaces sur les données à caractère personnel ; utilisez les rapports pour obtenir des renseignements précieux sur les contrôles existants afin de valider ces contrôles et établir la responsabilité de l'utilisateur	**[Catégories de Rapport]** Trace d'Audit
Article 25. §1. ... le contrôleur, tant au moment de la détermination des moyens de traitement et qu'au	Identifiez et évaluez l'efficacité de vos contrôles de la protection des données personnelles en utilisant la trace complète d'audit fournie par Netwrix Auditor et ses vastes fonctionnalités de suivi.	**[Catégories de rapports]** Gestion de la Configuration

moment du traitement lui-même, met en œuvre les mesures techniques et organisationnelles appropriées conçues pour mettre en œuvre les principes de protection des données et intégrer les protections nécessaires dans le traitement afin de répondre aux exigences du présent règlement et de protéger les droits des personnes concernées.	Analysez périodiquement les rapports qui produisent des informations, sur les événements critiques, faciles à lire dans vos journaux d'événements et dans Syslog. Analysez périodiquement les rapports qui produisent des détails sur toutes les installations et désinstallations d'applications logicielles ou de périphériques ; analysez les rapports qui indiquent la création de fichiers potentiellement dangereux Utilisez la fonctionnalité de recherche Interactive pour parcourir les traces d'audit consolidées et trouvez rapidement l'information exacte dont vous avez besoin. La recherche interactive vous permet de créer des rapports personnalisés facile-à-lire. En quelques clics, recherchez les données contextuelles et analysez les violations de données, simplifiant ainsi les enquêtes sur les incidents de sécurité ou les violations de données, et vous permettant de comprendre rapidement pourquoi et comment ces évènements sont survenus.	Intégrité du Système Modifications de sécurité Surveillance de l'Intégrité Accès au Système Intégrité des données Contrôle des Accès Accès à toutes les modifications de données Gestion des privilèges des Utilisateurs Modifications de Configuration **[Processus]** Recherchez les données contextuelles et analysez les violations de données avec la fonction de recherche Interactive de Netwrix Auditor.
Article 25. §2. Le contrôleur met en œuvre les mesures techniques et organisationnelles appropriées pour veiller à ce que, par défaut, seules les données personnelles nécessaires à chaque objectif spécifique du traitement soient utilisées. Cette obligation s'applique à la quantité de données personnelles collectées, à l'étendue de leur traitement, à la durée de leur stockage et à leur accessibilité. En particulier, de telles mesures veillent à ce que par défaut les données personnelles ne soient pas accessibles sans	Analysez périodiquement toutes les tentatives d'accéder à des ressources ou paramètres critiques, y compris les tentatives réussies et échouées. Abonnez-vous à des rapports quotidiens ou hebdomadaires montrant les modifications apportées aux autorisations utilisateur et l'appartenance à un groupe pour contrôler la délégation de privilège. Comparez des listes de comptes d'utilisateurs activés avec l'état actuel ou historique des autorisations pour valider que vos contrôles d'accès fonctionnent correctement. Analysez les autorisations excessives, les essais d'activité ayant échoué et les fichiers nouvellement créés qui peuvent contenir des données sensibles. Définissez un calendrier d'étude des rapports fournissant des détails sur les tentatives d'ouverture de session système réussies et échouées ; vérifier qu'il n'y a pas plusieurs cas d'accès. Surveillez les modifications apportées aux Objets de Stratégie de Groupe qui pourraient influer sur la politique de mot de passe, et vérifiez toutes les activités de mot de passe sur tous les	**[Catégories de Rapport]** Contrôle des Accès Accès au Système Politique de Modification des Mots de Passe d'accès aux données Gestion de Compte Conditions de Compte Modifications des Appartenance de Groupe Surveillance de l'Intégrité Activité d'Utilisateur

intervention de l'individu à un nombre indéterminé de personnes physiques.	systèmes d'informations pour confirmer la conformité aux politiques et aux procédures. Analysez périodiquement les rapports qui montrent les comptes d'utilisateurs activés, désactivés, expirés et bloqués. Analysez les rapports de la dernière connexion sur le compte d'utilisateur, et coordonnez avec votre département des ressources humaines, tous les statuts d'utilisateur. Utilisez Netwrix Auditor pour mettre en place une désactivation automatique des comptes d'utilisateurs après une certaine période d'inactivité. Activez l'enregistrement vidéo de l'activité d'utilisateur pour auditer les actions de l'utilisateur.	Intégrité des Données Gestion des Identifiants **[Processus]** Surveillez votre environnement informatique pour les utilisateurs inactifs avec la fonctionnalité utilisateurs inactifs de Netwrix Auditor
Article 32. §1. …. le contrôleur ainsi que le transformateur mettent en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité proportionné au risque, y compris : **(b)** la capacité d'assurer la confidentialité permanente, l'intégrité, la disponibilité et la résilience du traitement des systèmes et des services ; **(c)** la possibilité de restaurer la disponibilité et l'accès aux données personnelles en temps opportun dans le cas d'un incident technique ou physique; **(d)** un processus pour régulièrement tester, et évaluer l'efficacité des mesures techniques et organisationnelles mises en œuvre pour assurer la sécurité du traitement.	Utilisez des tableaux de bord pour obtenir une vue d'ensemble de ce qui se passe dans votre infrastructure INFORMATIQUE à un niveau élevé, y compris le nombre de fois où des modifications sont apportées, quels systèmes sont les plus touchés, et s'il y a des pics inhabituels dans le nombre de modifications et tentatives d'accès aux fichiers et dossiers. analysez les rapports prédéfinis requis pour obtenir une compréhension globale du contexte dans lequel les incidents de sécurité ont survenu ; les rapports d'audit fournissent des détails significatifs sur les activités de l'utilisateur pour vous aider à trouver rapidement la cause d'un problème et à établir la responsabilité de l'utilisateur. Utilisez Netwrix Auditor pour rétablir rapidement à une situation antérieure des modifications non autorisées ou accidentelles d'Active Directory et restaurer les objets effacés lorsque c'est nécessaire, sans immobilisation du contrôleur de domaine ou sans restauration à partir d'une sauvegarde.	**[Catégories de Rapports]** Traces d'Audit Toutes les modifications Contrôle d'Access aux mots de passe Politique de modifications. Politique de modifications de Configuration Accès au Système Gestion de la Configuration Intégrité du Système **[Processus]** Établissez et maintenez un contrôle continu des modifications d'infrastructure informatique, des configurations et des accès aux données avec Netwrix Auditor en utilisant toutes les catégories de rapports. **[Processus]** Restaurez une configuration de travail/sécurité d'Active Directory avec la fonctionnalité Active Directory Objet Restore de Netwrix Auditor.

Article 32. §2. Pour évaluer le niveau de sécurité approprié il faut tenir compte en particulier des risques présentés par le traitement, en particulier de la destruction accidentelle ou illicite, la perte, l'altération, la divulgation non autorisée, ou les accès aux données à caractère personnel transmises, stockées ou traitées autrement.	Analysez les rapports de Netwrix Auditor pour suivre toutes les modifications et tous les accès aux données dans un système particulier pour évaluer les risques à la confidentialité, l'intégrité et la disponibilité des données à caractère personnel. Activez la détection, en temps réel, de toute action d'utilisateur qui viole votre politique de protection des données en vous abonnant aux rapports suivants : Fichiers et Dossiers Supprimés, Destructions de Données, Fichiers et Dossiers déplacés, Fichiers et Dossiers renommés et Fichiers Copiés.	**[Catégories de Rapports]** Trace d'Audit de toutes les modifications Contrôle des Accès Data Groupe d'accès aux données Modifications d'appartenance Modifications d'autorisations Gestion des Privilèges d'Utilisateurs Intégrité des Données Gouvernance des Données Modifications des Données
Article 32. §4. Le contrôleur et l'opérateur informatique doivent prendre des mesures pour s'assurer que toute personne physique, agissant sous l'autorité du responsable du traitement ou de l'opérateur informatique, qui a accès aux données à caractère personnel ne les traite pas sauf sur instructions du contrôleur, à moins qu'il ou elle soit tenue de le faire sur demande s'un Syndicat ou par la Loi.	Abonnez-vous au rapport d'Activité Hors Horaires de travail pour savoir quels employés sont actifs sur le réseau alors qu'ils ne sont pas censés faire quoi que ce soit. Analysez périodiquement l'accès au rapport des Données d'Archivage pour détecter un nombre étrangement élevé de lectures de fichier dans votre espace de stockage d'archives, ce qui peut indiquer des activités malveillantes. Vérifiez périodiquement la pertinence de l'accès des utilisateurs en analysant les autorisations attribuées à chaque utilisateur pour les fichiers et classeurs par rapport au listing des employés de la DRH, et aux descriptions de fonctions en utilisant le rapport des Autorisations de Compte. Analysez le rapport des autorisations d'accès excessives pour vérifier qu'aucun droit d'accès excessif n'est attribué aux employés au-delà de celles nécessaires à leurs fonctions principales. Utilisez la capacité d'enregistrement vidéo de Netwrix Auditor pour capturer l'activité de l'écran des utilisateurs privilégiés dans les systèmes informatiques et les applications critiques (en particulier, ceux qui n'enregistrent pas d'événements) ; utilisez la fonctionnalité de	**[Catégories de Rapports]** Contrôle des Accès Accès au système Accès aux Données Activité Utilisateur Gestion de Compte Accès aux Données Conditions des autorisations

	notification d'enregistrement vidéo pour avertir les utilisateurs que leur activité peut être surveillée et enregistrée, ce qui favorise l'utilisation appropriée des systèmes et des données	
Article 33. §1. Dans le cas d'une violation de données à caractère personnel, le contrôleur doit sans retard injustifié et, lorsque cela est possible, au plus tard 72 heures après l'avoir identifiée, prévenir l'autorité de contrôle de la violation de données à caractère personnel …	Utilisez les alertes pré configurées pour répondre rapidement à des modèles de menace qui violent les politiques de sécurité de l'entreprise et indiquent les incidents de cyber-sécurité possibles, y compris la violation de données à caractère personnel. Les notifications, que vous pouvez personnaliser facilement, sont envoyées aux email spécifiés dès que les événements se produisent, vous permettant de rapidement réagir à une violation de données possible et informer promptement les autorités. Utilisez les abonnements aux rapports pour automatiser la délivrance de rapports d'audit critiques à un ensemble d'adresses de courrier électronique ou un dossier réseau désigné quotidiennement ou tout autre fréquence. Chaque rapport peut être délivré à plusieurs destinataires en même temps sans qu'il soit besoin de configurer chaque abonnement séparément.	**[Processus]** Mettez en place un système d'alerte précoce efficace grâce à la fonction d'alerte de Netwrix Auditor.. **[Processus]** Activez la surveillance continue des systèmes INFORMATIQUES critiques, et l'analyse des rapports grâce à la fonction d'abonnement de Netwrix Auditor.

Processus de Contrôle et Catégories de Rapports

Processus de Contrôle facilité par Netwrix Auditor

Du point de vue de la conformité, les opérations INFORMATIQUES peuvent être considérées et gérées comme un ensemble de processus de contrôle. Ces procédés permettent de concentrer les efforts d'organisation sur une zone informatique spécifique, renforçant certaines politiques et mettant en œuvre un ensemble de contrôles de conformité. Bien que les processus de contrôle puissent être considérés comme des entités distinctes dans le but de simplifier la mise œuvre et la gestion, tous ces processus sont en fait profondément liés et sont souvent intrinsèques à de nombreuses prescriptions et aux structures de pratiques exemplaires.

Contrôle d'Accès
Gestion de compte
Gestion des identifiants
Gestion des privilèges des utilisateurs
Surveillance de l'Intégrité
Gestion de la Configuration
Gouvernance des données
Trace d'Audit

Catégories de rapports de Netwrix Auditor

Pour une meilleure efficacité et une approche plus ciblée du traitement de données de vérification, les rapports de Netwrix Auditor sont classés dans les catégories suivantes :

Modification de Compte
Condition de Compte
Toutes les modifications
Toutes les conditions
Modification des Configurations
Conditions des Configurations
Accès aux Données
Modification des données
Intégrité des données
Modification d'appartenances
Conditions d'Appartenance
Modification des Mots de Passe
Politique de Modification des Mots de Passe
Modification d'Autorisations
Politique d'Autorisation des Conditions
Politique de Modification des Conditions
Sécurité des Modification du Système
Intégrité des accès au Système
Activité Utilisateur

Les tableaux ci-dessous détaillent les rapports prédéfinis dans chaque catégorie.

Contrôle d'accès

Mécanisme de fixation des restrictions sélectives de l'accès aux systèmes d'information et aux données.

Report Category	Netwrix Auditor Report	Audited System	Priority
Account Changes	Recently Enabled Accounts	Active Directory	Primary
Account Changes	User Account Status Changes	Active Directory	Secondary
Account States	Accounts with Most Logon Activity	Active Directory	Primary
Account States	Temporary User Accounts	Active Directory	Primary
Account States	User Accounts - Passwords Never Expire	Active Directory	Primary
Account States	User Accounts	Active Directory	Secondary
Account States	User Accounts - Expired	Active Directory	Secondary
Account States	User Accounts - Locked	Active Directory	Secondary
All Changes	All Active Directory Changes by Group	Active Directory	Secondary
All Changes	All Events by Source	Event Log	Primary
All Changes	Local Users and Groups Changes	Windows Server	Primary
Configuration Changes	Organizational Unit Changes	Active Directory	Secondary
Configuration Changes	User Account Locks and Unlocks	Event Log	Primary
Configuration Changes	Address List Changes	Exchange	Secondary
Configuration Changes	Interactive Logon Setting Changes	Group Policy	Primary
Configuration States	Organizational Units	Active Directory	Secondary
Data Access	All Exchange Server Non-Owner Mailbox Access Events	Exchange	Primary
Data Access	All Exchange Server Non-Owner Mailbox Access Events by User	Exchange	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events	Exchange Online	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events by User	Exchange Online	Primary
Data Access	Access to Archive Data	File Servers	Primary
Data Access	Data Access Surges	File Servers	Primary
Data Access	Excessive Access Permissions	File Servers	Primary
Data Access	Successful File Reads	File Servers	Secondary
Data Access	Data Access	Oracle Database	Primary
Data Access	SharePoint Read Access	SharePoint	Primary
Data Access	Data Access	SharePoint Online	Primary
Data Changes	SharePoint Content Changes by User	SharePoint	Secondary
Data Changes	All SQL Server Data Changes	SQL Server	Secondary
Data Integrity	Exchange Online Public Folder Changes	Exchange Online	Primary
Data Integrity	Failed Change Attempts	File Servers	Primary
Data Integrity	Failed Read Attempts	File Servers	Primary
Data Integrity	Share Changes	File Servers	Secondary

Data Integrity	Files and Folders Moved	File Servers	Secondary
Data Integrity	Files and Folders Renamed	File Servers	Secondary
Data Integrity	Files Copied	File Servers	Secondary
Group Membership Changes	Distribution Group Changes	Active Directory	Primary
Group Membership Changes	Security Group Membership Changes	Active Directory	Primary
Group Membership Changes	Administrative Group Membership Changes	Active Directory	Secondary
Group Membership Changes	Exchange Online Group Changes	Exchange Online	Primary
Group Membership Changes	Group Membership by User	File Servers	Primary
Group Membership States	Effective Group Membership	Active Directory	Primary
Group Membership States	Group Members	Active Directory	Primary
Group Membership States	Administrative Group Members	Active Directory	Secondary
Group Membership States	User Accounts - Group Membership	Active Directory	Secondary
Password Changes	Password Resets by Administrator	Active Directory	Secondary
Password Changes	User Password Changes	Active Directory	Secondary
Password Policy Changes	Password Policy Changes	Group Policy	Secondary
Permission Changes	Exchange Online Mail User Changes	Exchange Online	Primary
Permission Changes	Exchange Online Mailbox Permissions Changes	Exchange Online	Primary
Permission Changes	Permissions Changes	File Servers	Primary
Permission Changes	SharePoint Permissions Changes by User	SharePoint	Primary
Permission States	Account Permissions	File Servers	Primary
Permission States	Object Permissions by Object	File Servers	Primary
Policy Changes	Exchange Online Mailbox Policy Changes	Exchange Online	Primary
Policy Changes	User Rights Assignment Policy Changes	Group Policy	Primary
Policy Changes	Account Policy Changes	Group Policy	Secondary
Policy Changes	User Configuration Changes	Group Policy	Secondary
Policy States	Account Policies	Group Policy	Secondary
Security Changes	All Security Events by User	Event Log	Secondary
Security Changes	Renaming of Administrator and Guest Accounts Through Group Policy	Group Policy	Secondary
System Access	Activity Outside Business Hours	Active Directory	Primary
System Access	All Logon Activity	Active Directory	Primary
System Access	Failed Logons	Active Directory	Primary
System Access	Interactive Logons	Active Directory	Primary
System Access	Logons by Multiple Users from Single Endpoint	Active Directory	Primary
System Access	Logons by Single User from Multiple Endpoints	Active Directory	Primary
System Access	Successful Logons	Active Directory	Primary
System Access	User Accounts - Last Logon Time	Active Directory	Primary
System Access	User Logons and Logoffs on Domain Controllers	Active Directory	Primary
System Access	Azure AD Logon Activity	Azure AD	Primary
System Access	Failed Logon Attempts	Event Log	Primary

System Access	Logoffs by User	Event Log	Primary
System Access	Remote Desktop Sessions	Event Log	Primary
System Access	Successful Logons by User	Event Log	Primary
System Access	Wireless Network Policy Changes	Group Policy	Primary
System Access	All Oracle Database Logons	Oracle Database	Primary
System Access	All SQL Server Logons	SQL Server	Primary
User Activity	All Exchange Server Changes by User	Exchange	Secondary
User Activity	File Server Changes by User	File Servers	Primary
User Activity	All File Server Activity by User	File Servers	Secondary
User Activity	All SQL Server Activity by User	SQL Server	Primary
User Activity	All User Activity by User	User Activity	Primary
User Activity	All Windows Server Changes by User	Windows Server	Secondary

Gestion des comptes

Processus d'émission, retrait, entretien et configuration des comptes des systèmes d'information et des privilèges associés.

Report Category	Netwrix Auditor Report	Audited System	Priority
Account Changes	Computer Account Changes	Active Directory	Primary
Account Changes	Contact Object Changes	Active Directory	Primary
Account Changes	Recently Enabled Accounts	Active Directory	Primary
Account Changes	User Account Changes	Active Directory	Primary
Account Changes	User Account Status Changes	Active Directory	Primary
Account Changes	User Account Management in Azure AD	Azure AD	Primary
Account Changes	User Accounts Created and Deleted Directly in Azure AD	Azure AD	Primary
Account Changes	User-Initiated Password Changes in Azure AD	Azure AD	Primary
Account Changes	Account Management	Oracle Database	Primary
Account States	Accounts with Most Logon Activity	Active Directory	Primary
Account States	Organizational Unit Accounts	Active Directory	Primary
Account States	Service Principal Names of Computer Accounts	Active Directory	Primary
Account States	User Accounts	Active Directory	Primary
Account States	User Accounts - Expired	Active Directory	Primary
Account States	User Accounts - Locked	Active Directory	Primary
Account States	User Accounts - Passwords Never Expire	Active Directory	Primary
Configuration Changes	User Account Locks and Unlocks	Event Log	Secondary
Configuration States	Computer Accounts	Active Directory	Primary
Data Access	All Exchange Server Non-Owner Mailbox Access Events	Exchange	Primary
Data Access	All Exchange Server Non-Owner Mailbox Access Events by User	Exchange	Primary

Data Access	All Exchange Online Non-Owner Mailbox Access Events	Exchange Online	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events by User	Exchange Online	Primary
Data Access	Excessive Access Permissions	File Servers	Primary
Data States	Potential Data Owners by Folder	File Servers	Primary
Data States	Top Owners by Total File Size	File Servers	Secondary
Group Membership Changes	Group Membership Changes in Azure AD	Azure AD	Primary
Group Membership Changes	Exchange Online Group Changes	Exchange Online	Primary
Group Membership Changes	Group Membership by User	File Servers	Primary
Group Membership States	Temporary Users in Privileged Groups	Active Directory	Primary
Group Membership States	User Accounts - Group Membership	Active Directory	Primary
Group Membership States	Users Not in Any Distribution Group	Active Directory	Primary
Group Membership States	Effective Group Membership	Active Directory	Secondary
Group Membership States	Group Members	Active Directory	Secondary
Permission Changes	Privilege Management	Oracle Database	Primary
Permission States	Account Permissions	File Servers	Primary
Policy Changes	Account Policy Changes	Group Policy	Primary
Policy Changes	User Configuration Changes	Group Policy	Primary
Policy States	Account Policies	Group Policy	Primary
System Access	Failed Logons	Active Directory	Primary
System Access	Successful Logons	Active Directory	Primary
System Access	User Logons and Logoffs on Domain Controllers	Active Directory	Primary
User Activity	User Activity Summary	File Servers	Primary

Gestion des Identifiants

Processus de gestion des informations d'identification telles que les noms d'utilisateur et les mots de passe.

Report Category	Netwrix Auditor Report	Audited System	Priority
Account Changes	User-Initiated Password Changes in Azure AD	Azure AD	Primary
Account States	User Accounts - Passwords Never Expire	Active Directory	Primary
Password Changes	Password Resets by Administrator	Active Directory	Primary
Password Changes	User Password Changes	Active Directory	Primary
Password Policy Changes	Password Policy Changes	Group Policy	Primary

Gestion des privilèges des utilisateurs

Processus de gestion des comptes avec privilèges, y compris la gestion de l'approvisionnement et du cycle de vie, les authentifications, les autorisations, la gestion des informations d'identification, l'audit et le contrôle d'accès.

Report Category	Netwrix Auditor Report	Audited System	Priority
Account Changes	User Account Changes	Active Directory	Secondary
Account States	User Accounts - Passwords Never Expire	Active Directory	Primary
All Changes	All System Events by User	Event Log	Secondary
All Changes	Exchange Database Changes	Exchange	Secondary
All Changes	New Exchange Servers	Exchange	Secondary
All Changes	All Exchange Server Changes by Date	Exchange Online	Primary
All Changes	All Oracle Database Administrative Activity	Oracle Database	Primary
All Changes	All User Activity	User Activity	Secondary
All Changes	All VMware Changes by User	VMware	Secondary
All Changes	Local Users and Groups Changes	Windows Server	Secondary
Configuration Changes	Active Directory Schema Container Changes	Active Directory	Secondary
Configuration Changes	Mailbox Changes	Exchange	Secondary
Configuration Changes	Exchange Online Management Role Changes	Exchange Online	Primary
Configuration Changes	Interactive Logon Setting Changes	Group Policy	Secondary
Configuration Changes	DNS Configuration Changes	Windows Server	Secondary
Configuration Changes	DNS Resource Record Changes	Windows Server	Secondary
Configuration Changes	General Computer Settings Changes	Windows Server	Secondary
Configuration Changes	Programs Added and Removed	Windows Server	Secondary
Configuration Changes	Windows Registry Changes	Windows Server	Secondary
Data Integrity	Files and Folders Deleted	File Servers	Secondary
Data Integrity	Files and Folders Moved	File Servers	Secondary
Data Integrity	Files and Folders Renamed	File Servers	Secondary
Data Integrity	Files Copied	File Servers	Secondary
Group Membership Changes	Administrative Group Membership Changes	Active Directory	Primary
Group Membership Changes	Security Group Membership Changes	Active Directory	Secondary
Group Membership Changes	Exchange Online Group Changes	Exchange Online	Primary
Group Membership States	Administrative Group Members	Active Directory	Primary
Group Membership States	Temporary Users in Privileged Groups	Active Directory	Primary
Permission Changes	Mailbox Delegation and Permissions Changes	Exchange	Secondary
Permission Changes	Exchange Online Mailbox Permissions Changes	Exchange Online	Primary
Permission Changes	Privilege Management	Oracle Database	Primary
Permission Changes	VMware Virtual Machine Permissions Changes	VMware	Secondary

Permission States	Group Policy Object Delegation	Group Policy	Secondary
Policy Changes	Email Address Policy Changes	Exchange	Secondary
Policy Changes	Exchange Online Mailbox Policy Changes	Exchange Online	Primary
Policy Changes	Administrative Template Changes	Group Policy	Primary
Policy Changes	Restricted Groups Policy Changes	Group Policy	Primary
Policy Changes	Public Key Policy Changes	Group Policy	Secondary
Policy Changes	User Rights Assignment Policy Changes	Group Policy	Secondary
Security Changes	Security Group Changes	Active Directory	Secondary
Security Changes	Renaming of Administrator and Guest Accounts Through Group Policy	Group Policy	Primary
Security Changes	Security Settings Changes	Group Policy	Secondary
System Access	User Logons and Logoffs on Domain Controllers	Active Directory	Primary
System Access	Failed Logon Attempts	Event Log	Secondary
System Access	Logoffs by User	Event Log	Secondary
System Access	Remote Desktop Sessions	Event Log	Secondary
System Access	Successful Logons by User	Event Log	Secondary
User Activity	All Active Directory Changes by User	Active Directory	Secondary
User Activity	All Changes by User	All Audited Systems	Secondary
User Activity	All Events by User	Event Log	Secondary
User Activity	All Exchange Server Changes by Group	Exchange	Secondary
User Activity	File Server Changes by User	File Servers	Secondary
User Activity	All Group Policy Changes by Group	Group Policy	Secondary
User Activity	All SharePoint Changes by User	SharePoint	Secondary
User Activity	All SQL Server Activity by User	SQL Server	Secondary
User Activity	All User Activity by User	User Activity	Secondary

Surveillance de l'intégrité

Processus d'exécution de la validation de l'intégrité de données et des configurations par comparaison entre la situation actuelle et la ligne de base connue et correcte.

Report Category	Netwrix Auditor Report	Audited System	Priority
Account States	Accounts with Most Logon Activity	Active Directory	Primary
Account States	User Accounts - Passwords Never Expire	Active Directory	Primary
All Changes	All Active Directory Changes by Date	Active Directory	Primary
All Changes	All Active Directory Changes by Object Type	Active Directory	Secondary
All Changes	All Changes by Server	All Audited Systems	Secondary
All Changes	All Exchange Server Changes by Server	Exchange	Secondary
All Changes	All Exchange Server Changes by Date	Exchange Online	Primary
All Changes	All SharePoint Changes by Site Collection	SharePoint	Secondary
All Changes	All SQL Server Activity by Server	SQL Server	Secondary

All Changes	All VMware Changes by Server	VMware	Secondary
All Changes	All Windows Server Changes by Date	Windows Server	Primary
All Changes	All Windows Server Changes by Server	Windows Server	Secondary
Configuration Changes	Active Directory Schema Container Changes	Active Directory	Primary
Configuration Changes	All Exchange Server Changes by Object Type	Exchange	Secondary
Configuration Changes	VMware Cluster Changes	VMware	Secondary
Configuration Changes	VMware Snapshot Changes	VMware	Secondary
Configuration Changes	Programs Added and Removed	Windows Server	Primary
Configuration Changes	Service Changes	Windows Server	Primary
Configuration Changes	Windows Registry Changes	Windows Server	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events	Exchange Online	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events by User	Exchange Online	Primary
Data Access	Excessive Access Permissions	File Servers	Primary
Data Access	SharePoint Read Access	SharePoint	Primary
Data Changes	File Server Changes by Action	File Servers	Secondary
Data Changes	Folder Changes	File Servers	Secondary
Data Integrity	Potentially Harmful Files - Activity	File Servers	Primary
Data Integrity	Potentially Harmful Files on File Shares	File Servers	Primary
Data Integrity	All File Server Activity by Action Type	File Servers	Secondary
Data Integrity	All File Server Activity by Server	File Servers	Secondary
Data Integrity	Failed Change Attempts	File Servers	Secondary
Data Integrity	Failed Delete Attempts	File Servers	Secondary
Data Integrity	File Server Changes by Server	File Servers	Secondary
Data Integrity	Files and Folders Moved	File Servers	Secondary
Data Integrity	Files and Folders Renamed	File Servers	Secondary
Data Integrity	Files Copied	File Servers	Secondary
Data Integrity	Creation of Files with Sensitive Data	File Servers, SharePoint	Primary
Data Integrity	File Names Containing Sensitive Data	File Servers, SharePoint	Primary
Data States	Potential Data Owners by Folder	File Servers	Primary
Data States	Files and Folders by Owner	File Servers	Secondary
Data States	Largest Files	File Servers	Secondary
Policy Changes	Registry Policy Changes	Group Policy	Primary
Policy Changes	Software Restriction Policy Changes	Group Policy	Primary
Security Changes	Object Security Changes	Active Directory	Secondary
Security Changes	Operations Master Role Changes	Active Directory	Secondary
System Access	All Logon Activity	Active Directory	Primary
System Access	Failed Logons	Active Directory	Primary
System Access	Interactive Logons	Active Directory	Primary
System Access	Successful Logons	Active Directory	Primary

System Access	User Logons and Logoffs on Domain Controllers	Active Directory	Primary
System Access	Wireless Network Policy Changes	Group Policy	Secondary
System Integrity	Service Pack Installations	Active Directory	Primary
System Integrity	Event Details	Event Log	Primary
System Integrity	Message Details	Event Log	Primary
System Integrity	Service Events	Event Log	Secondary
System Integrity	Service Starts and Stops	Event Log	Secondary
System Integrity	Software Settings Changes	Group Policy	Primary
System Integrity	System Services Policy Changes	Group Policy	Primary
System Integrity	Windows Settings Changes	Group Policy	Primary
System Integrity	Failed Activity	Oracle Database	Primary
System Integrity	Trigger Management	Oracle Database	Primary
System Integrity	VMware Power State Changes	VMware	Secondary
System Integrity	All Activity with Review Status	Windows Server	Primary
System Integrity	Audit Log Clearing	Windows Server	Primary
System Integrity	Hardware Changes	Windows Server	Primary
System Integrity	System Shutdowns and Reboots	Windows Server	Primary
User Activity	All File Server Activity by Date	File Servers	Primary
User Activity	User Activity Summary	File Servers	Primary
User Activity	SharePoint Activity Summary	SharePoint	Primary
User Activity	All SQL Server Activity by Date	SQL Server	Primary
User Activity	All User Activity by Server	User Activity	Secondary

Gouvernance des données

Processus de gestion de la disponibilité, de la facilité d'utilisation, de l'intégrité et de la sécurité des données employées dans un organisme.

Report Category	Netwrix Auditor Report	Audited System	Priority
All Changes	File Server Changes	File Servers	Primary
All Changes	All File Server Activity	File Servers	Secondary
All Changes	All SharePoint Changes by Date	SharePoint	Primary
Configuration Changes	Mailbox Storage Quota Changes	Exchange	Secondary
Configuration Changes	SharePoint Configuration Changes	SharePoint	Secondary
Data Access	All Exchange Server Non-Owner Mailbox Access Events	Exchange	Primary
Data Access	All Exchange Server Non-Owner Mailbox Access Events by User	Exchange	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events	Exchange Online	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events by User	Exchange Online	Primary

Data Access	Access to Archive Data	File Servers	Primary
Data Access	Data Access Surges	File Servers	Primary
Data Access	Excessive Access Permissions	File Servers	Primary
Data Access	Successful File Reads	File Servers	Primary
Data Access	Data Access	Oracle Database	Primary
Data Access	SharePoint Read Access	SharePoint	Primary
Data Access	Data Access	SharePoint Online	Primary
Data Changes	All Data Activity	All Audited Systems	Primary
Data Changes	File Server Changes by Action	File Servers	Primary
Data Changes	Files and Folders Created	File Servers	Primary
Data Changes	Folder Changes	File Servers	Primary
Data Changes	Data Deletions	Oracle Database	Primary
Data Changes	SharePoint Content Changes by User	SharePoint	Primary
Data Changes	Content Management	SharePoint Online	Primary
Data Changes	All SQL Server Data Changes	SQL Server	Primary
Data Integrity	Exchange Online Public Folder Changes	Exchange Online	Primary
Data Integrity	All File Server Activity by Action Type	File Servers	Primary
Data Integrity	All File Server Activity by Server	File Servers	Primary
Data Integrity	Failed Delete Attempts	File Servers	Primary
Data Integrity	File Server Changes by Server	File Servers	Primary
Data Integrity	Files and Folders Deleted	File Servers	Primary
Data Integrity	Potentially Harmful Files - Activity	File Servers	Primary
Data Integrity	Potentially Harmful Files on File Shares	File Servers	Primary
Data Integrity	Share Changes	File Servers	Primary
Data Integrity	Failed Read Attempts	File Servers	Secondary
Data Integrity	Files and Folders Moved	File Servers	Secondary
Data Integrity	Files and Folders Renamed	File Servers	Secondary
Data Integrity	Files Copied	File Servers	Secondary
Data Integrity	Creation of Files with Sensitive Data	File Servers, SharePoint	Primary
Data Integrity	File Names Containing Sensitive Data	File Servers, SharePoint	Primary
Data States	Duplicate Files	File Servers	Primary
Data States	Empty Folders	File Servers	Primary
Data States	Files and Folders by Owner	File Servers	Primary
Data States	Folder Summary Report	File Servers	Primary
Data States	Largest Files	File Servers	Primary
Data States	Most Used File Types	File Servers	Primary
Data States	Potential Data Owners by Folder	File Servers	Primary
Data States	Stale Data by Folder	File Servers	Primary
Data States	Stale Files	File Servers	Primary
Data States	Top Owners by Total File Size	File Servers	Primary

Permission Changes	Exchange Online Mail User Changes	Exchange Online	Primary
Permission Changes	Exchange Online Mailbox Permissions Changes	Exchange Online	Primary
Permission Changes	Permissions Changes	File Servers	Secondary
Permission Changes	SharePoint Permissions Changes by User	SharePoint	Secondary
Permission States	Account Permissions	File Servers	Primary
Permission States	Object Permissions by Object	File Servers	Secondary
Policy Changes	Exchange Online Mailbox Policy Changes	Exchange Online	Primary
User Activity	All File Server Activity by User	File Servers	Primary
User Activity	User Activity Summary	File Servers	Primary
User Activity	All SharePoint Activity	SharePoint	Primary
User Activity	SharePoint Activity Summary	SharePoint	Primary
User Activity	All SQL Server Activity by Date	SQL Server	Primary

Gestion de la configuration

Processus pour les évolutions interdépendantes et les techniques de gestion afin d'évaluer, coordonner et contrôler les modifications et les configurations de l'état des systèmes d'information.

Report Category	Netwrix Auditor Report	Audited System	Priority
Account States	Organizational Unit Accounts	Active Directory	Secondary
Account States	Service Principal Names of Computer Accounts	Active Directory	Secondary
All Changes	All Active Directory Changes with Review Status	Active Directory	Secondary
All Changes	Exchange Database Changes	Exchange	Primary
All Changes	New Exchange Servers	Exchange	Primary
All Changes	All Exchange Server Changes	Exchange	Secondary
All Changes	All Exchange Server Changes with Review Status	Exchange	Secondary
All Changes	GPO Link Changes	Group Policy	Primary
All Changes	All Group Policy Changes with Review Status	Group Policy	Secondary
All Changes	All SharePoint Changes by Site Collection	SharePoint	Primary
All Changes	SharePoint Changes with Review Status	SharePoint	Primary
All Changes	All SQL Server Activity by Object Type	SQL Server	Secondary
All Changes	All VMware Changes by Object Type	VMware	Secondary
All Changes	All Windows Server Changes with Review Status	Windows Server	Secondary
All States	Groups	Active Directory	Secondary
All States	Group Policy Objects by Policy Name	Group Policy	Primary
Configuration Changes	Active Directory Configuration Container Changes	Active Directory	Primary
Configuration Changes	IIS Application Pool Changes	Event Log	Primary
Configuration Changes	IIS Application Pool Changes	Event Log	Primary
Configuration Changes	IIS Website Changes	Event Log	Primary
Configuration Changes	IIS Website Changes	Event Log	Primary
Configuration Changes	Address List Changes	Exchange	Primary

Configuration Changes	Mailbox Changes	Exchange	Primary
Configuration Changes	Mailbox Storage Quota Changes	Exchange	Primary
Configuration Changes	Exchange Online Management Role Changes	Exchange Online	Primary
Configuration Changes	SharePoint Configuration Changes	SharePoint	Primary
Configuration Changes	VMware Cluster Changes	VMware	Primary
Configuration Changes	VMware Datacenter Changes	VMware	Primary
Configuration Changes	VMware Datastore Changes	VMware	Primary
Configuration Changes	VMware Host System Changes	VMware	Primary
Configuration Changes	VMware Resource Pool Changes	VMware	Primary
Configuration Changes	VMware Snapshot Changes	VMware	Primary
Configuration Changes	VMware Virtual Machine Changes	VMware	Primary
Configuration Changes	DNS Configuration Changes	Windows Server	Primary
Configuration Changes	DNS Resource Record Changes	Windows Server	Primary
Configuration Changes	File Share Changes	Windows Server	Primary
Configuration Changes	General Computer Settings Changes	Windows Server	Primary
Configuration Changes	Printer Changes	Windows Server	Primary
Configuration Changes	Scheduled Task Changes	Windows Server	Primary
Configuration Changes	System Time Changes	Windows Server	Primary
Configuration States	Domain Controllers	Active Directory	Primary
Configuration States	Organizational Units	Active Directory	Primary
Configuration States	Service Principal Names of Domain Controllers	Active Directory	Primary
Configuration States	Computer Accounts	Active Directory	Secondary
Configuration States	Empty Group Policy Objects	Group Policy	Primary
Configuration States	Group Policy Object Link Status	Group Policy	Primary
Configuration States	Group Policy Objects by Setting Name	Group Policy	Primary
Configuration States	Identical Settings in Different GPOs	Group Policy	Primary
Group Membership States	Users Not in Any Distribution Group	Active Directory	Secondary
Permission Changes	Mailbox Delegation and Permissions Changes	Exchange	Primary
Permission Changes	Exchange Online Mailbox Permissions Changes	Exchange Online	Primary
Permission Changes	VMware Virtual Machine Permissions Changes	VMware	Primary
Permission States	Account Permissions	File Servers	Primary
Permission States	Group Policy Object Delegation	Group Policy	Primary
Policy Changes	Email Address Policy Changes	Exchange	Primary
Policy Changes	Exchange Online Mailbox Policy Changes	Exchange Online	Primary
Policy Changes	Public Key Policy Changes	Group Policy	Primary
Policy Changes	Registry Policy Changes	Group Policy	Secondary
Policy Changes	Restricted Groups Policy Changes	Group Policy	Secondary
Policy Changes	Software Restriction Policy Changes	Group Policy	Secondary
Policy Changes	Audit Policy and Setting Changes	Oracle Database	Primary
Policy Changes	Local Audit Policy Changes	Windows Server	Primary

Policy States	Group Policy Object Status	Group Policy	Primary
Security Changes	Security Settings Changes	Group Policy	Primary
System Integrity	Service Events	Event Log	Primary
System Integrity	Service Starts and Stops	Event Log	Primary
System Integrity	All Events by Computer	Event Log	Secondary
System Integrity	Software Settings Changes	Group Policy	Secondary
System Integrity	System Services Policy Changes	Group Policy	Secondary
System Integrity	VMware Power State Changes	VMware	Primary

Trace d'audit

Processus de collecte, de consolidation, de rétention et de traitement des données d'audit.

Report Category	Netwrix Auditor Report	Audited System	Priority
Account Changes	User Account Management in Azure AD	Azure AD	Primary
Account Changes	User Accounts Created and Deleted Directly in Azure AD	Azure AD	Primary
Account Changes	User-Initiated Password Changes in Azure AD	Azure AD	Primary
Account Changes	Account Management	Oracle Database	Primary
All Changes	All Active Directory Changes	Active Directory	Primary
All Changes	All Active Directory Changes by Date	Active Directory	Primary
All Changes	All Active Directory Changes by Domain Controller	Active Directory	Primary
All Changes	All Active Directory Changes by Group	Active Directory	Primary
All Changes	All Active Directory Changes by Object Type	Active Directory	Primary
All Changes	All Active Directory Changes with Review Status	Active Directory	Primary
All Changes	Activity by Audited System	All Audited Systems	Primary
All Changes	All Changes by Audited System	All Audited Systems	Primary
All Changes	All Changes by Date	All Audited Systems	Primary
All Changes	All Changes by Server	All Audited Systems	Primary
All Changes	All Azure AD Activity by Date	Azure AD	Primary
All Changes	All Azure AD Activity by Object Type	Azure AD	Primary
All Changes	All Azure AD Activity by User	Azure AD	Primary
All Changes	All Generic Syslog Events	Event Log	Primary
All Changes	All System Events by User	Event Log	Primary
All Changes	All Events by Source	Event Log	Secondary
All Changes	All Exchange Server Changes	Exchange	Primary
All Changes	All Exchange Server Changes by Server	Exchange	Primary
All Changes	All Exchange Server Changes with Review Status	Exchange	Primary
All Changes	All Exchange Online Changes	Exchange Online	Primary

All Changes	All Exchange Server Changes by Date	Exchange Online	Primary
All Changes	All File Server Activity	File Servers	Primary
All Changes	File Server Changes	File Servers	Secondary
All Changes	All Group Policy Changes with Review Status	Group Policy	Primary
All Changes	All Oracle Database Activity by Object	Oracle Database	Primary
All Changes	All Oracle Database Activity by Session ID	Oracle Database	Primary
All Changes	All Oracle Database Activity by User	Oracle Database	Primary
All Changes	All Oracle Database Administrative Activity	Oracle Database	Primary
All Changes	All SharePoint Changes	SharePoint	Primary
All Changes	All SharePoint Changes by Date	SharePoint	Primary
All Changes	All SharePoint Changes by Object Type	SharePoint	Primary
All Changes	SharePoint Changes with Review Status	SharePoint	Secondary
All Changes	All SharePoint Online Activity by User	SharePoint Online	Primary
All Changes	All SQL Server Activity	SQL Server	Primary
All Changes	All SQL Server Activity by Object Type	SQL Server	Primary
All Changes	All SQL Server Activity by Server	SQL Server	Primary
All Changes	All User Activity	User Activity	Primary
All Changes	All VMware Changes	VMware	Primary
All Changes	All VMware Changes by Date	VMware	Primary
All Changes	All VMware Changes by Object Type	VMware	Primary
All Changes	All VMware Changes by Server	VMware	Primary
All Changes	All VMware Changes by User	VMware	Primary
All Changes	All Windows Server Changes	Windows Server	Primary
All Changes	All Windows Server Changes by Date	Windows Server	Primary
All Changes	All Windows Server Changes by Object Type	Windows Server	Primary
All Changes	All Windows Server Changes by Server	Windows Server	Primary
All Changes	All Windows Server Changes with Review Status	Windows Server	Primary
All States	Groups	Active Directory	Primary
All States	Group Policy Objects by Policy Name	Group Policy	Secondary
Configuration Changes	Active Directory Site Changes	Active Directory	Primary
Configuration Changes	Domain Controller Changes	Active Directory	Primary
Configuration Changes	Organizational Unit Changes	Active Directory	Primary
Configuration Changes	IIS Application Pool Changes	Event Log	Primary
Configuration Changes	IIS Website Changes	Event Log	Primary
Configuration Changes	All Exchange Server Changes by Object Type	Exchange	Primary
Configuration Changes	Exchange Online Management Role Changes	Exchange Online	Primary
Configuration Changes	File Share Changes	Windows Server	Primary
Configuration Changes	System Time Changes	Windows Server	Primary
Configuration States	Empty Group Policy Objects	Group Policy	Secondary
Configuration States	Group Policy Objects by Setting Name	Group Policy	Secondary

Configuration States	Identical Settings in Different GPOs	Group Policy	Secondary
Data Access	All Exchange Server Non-Owner Mailbox Access Events	Exchange	Primary
Data Access	All Exchange Server Non-Owner Mailbox Access Events by User	Exchange	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events	Exchange Online	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events by User	Exchange Online	Primary
Data Access	Access to Archive Data	File Servers	Primary
Data Access	Data Access Surges	File Servers	Primary
Data Access	Data Access	Oracle Database	Primary
Data Access	Data Access	SharePoint Online	Primary
Data Changes	All Data Activity	All Audited Systems	Primary
Data Changes	Files and Folders Created	File Servers	Secondary
Data Changes	Data Deletions	Oracle Database	Primary
Data Integrity	Exchange Online Public Folder Changes	Exchange Online	Primary
Data Integrity	Potentially Harmful Files - Activity	File Servers	Primary
Data Integrity	Files and Folders Moved	File Servers	Secondary
Data Integrity	Files and Folders Renamed	File Servers	Secondary
Data Integrity	Files Copied	File Servers	Secondary
Data Integrity	Creation of Files with Sensitive Data	File Servers, SharePoint	Primary
Data Integrity	File Names Containing Sensitive Data	File Servers, SharePoint	Primary
Data States	Folder Summary Report	File Servers	Secondary
Group Membership Changes	Group Membership Changes in Azure AD	Azure AD	Primary
Group Membership Changes	Exchange Online Group Changes	Exchange Online	Primary
Permission Changes	Exchange Online Mail User Changes	Exchange Online	Primary
Permission Changes	Exchange Online Mailbox Permissions Changes	Exchange Online	Primary
Permission Changes	Privilege Management	Oracle Database	Primary
Permission States	Object Permissions by Object	File Servers	Secondary
Policy Changes	Exchange Online Mailbox Policy Changes	Exchange Online	Primary
Policy Changes	All Group Policy Changes	Group Policy	Primary
Policy Changes	Audit Policy Changes	Group Policy	Primary
Policy Changes	Audit Policy and Setting Changes	Oracle Database	Primary
Policy Changes	Local Audit Policy Changes	Windows Server	Primary
Policy States	Group Policy Object Status	Group Policy	Secondary
Security Changes	Domain Trust Changes	Active Directory	Primary
Security Changes	Object Security Changes	Active Directory	Primary
Security Changes	Operations Master Role Changes	Active Directory	Primary
Security Changes	Security Group Changes	Active Directory	Primary

Security Changes	All Security Events by User	Event Log	Primary
Security Changes	Netwrix Auditor System Health	Event Log	Primary
Security Changes	Sharing and Security Changes	SharePoint Online	Primary
System Access	Activity Outside Business Hours	Active Directory	Primary
System Access	All Logon Activity	Active Directory	Primary
System Access	Failed Logons	Active Directory	Primary
System Access	Interactive Logons	Active Directory	Primary
System Access	Logons by Multiple Users from Single Endpoint	Active Directory	Primary
System Access	Logons by Single User from Multiple Endpoints	Active Directory	Primary
System Access	Successful Logons	Active Directory	Primary
System Access	User Logons and Logoffs on Domain Controllers	Active Directory	Primary
System Access	Azure AD Logon Activity	Azure AD	Primary
System Access	All Oracle Database Logons	Oracle Database	Primary
System Access	All SQL Server Logons	SQL Server	Primary
System Integrity	All Events by Computer	Event Log	Primary
System Integrity	Failed Activity	Oracle Database	Primary
System Integrity	All Activity with Review Status	Windows Server	Primary
System Integrity	Audit Log Clearing	Windows Server	Primary
System Integrity	System Shutdowns and Reboots	Windows Server	Primary
System Integrity	Hardware Changes	Windows Server	Secondary
User Activity	All Active Directory Changes by User	Active Directory	Primary
User Activity	All Changes by User	All Audited Systems	Primary
User Activity	All Events by User	Event Log	Primary
User Activity	All Exchange Server Changes by Group	Exchange	Primary
User Activity	All Exchange Server Changes by User	Exchange	Primary
User Activity	All File Server Activity by Date	File Servers	Primary
User Activity	All SharePoint Activity	SharePoint	Primary
User Activity	All SharePoint Changes by User	SharePoint	Primary
User Activity	All SQL Server Activity by Date	SQL Server	Primary
User Activity	All User Activity by Server	User Activity	Primary
User Activity	All Windows Server Changes by User	Windows Server	Primary