netwrix

All Netwrix Auditor Predefined Reports

Complete list of the predefined reports with short descriptions

Table of Contents

All Netwrix Auditor Predefined Reports

Organizational Level Reports

- **Enterprise Overview**

Shows consolidated statistics on changes across all data sources. Review this diagram to get a general understanding of changes to your IT infrastructure. Drill down for more details on any data source.

- **All Activity with Review Status**

Shows all activity across the entire IT infrastructure and the review status of each change, read access, or logon. Use this report to analyze changes in your IT infrastructure and track team workflows by making notes on the review status or reasons for the change.

- **All Changes by Data Source**

Shows all changes across the entire IT infrastructure, grouped by data source. Review this report to visualize the whole picture and identify systems that need your attention.

- **All Changes by Server**

Shows all changes across the entire IT infrastructure, grouped by the server where the change was made. Review this report to visualize the whole picture and identify servers that need your attention.

- **All Changes by User**

Shows all changes across the entire IT infrastructure, grouped by user who made the changes. Review this report to paint the whole picture, identify users that need your special attention, and investigate suspicious activities.

- **All Integration API Activity**

Shows all activity records imported with Netwrix Auditor Integration API.

User Behavior and Blind Spot Analysis

Data Access

- **Access to Archive Data**

Shows users who accessed files in your archive storage. A high number of reads may indicate malicious activity. Use this report to detect suspicious activity and exercise security control over your data.

- **Data Access Surges**

Shows users who have accessed sensitive data they almost never accessed before (by default, the inactivity threshold is set to 2 actions). The report highlights previously inactive users who performed more actions within a short period of time (by default, 7 days) than during a considerably longer preceding period (by default, 30 days). Use this report to analyze data usage patterns and detect suspicious activity surges.

- **Data Access Trend**

Shows consolidated statistics on data usage patterns across file servers and SharePoint. Be sure to inspect activity spikes closely, as these may indicate potential threats or malicious activity.

- **Excessive Access Permissions**

Shows accounts with permissions to infrequently accessed files and folders (either directly or via group membership). Use this report to spot unnecessary permissions and thereby prevent data leaks. Clicking the group link opens the "Group Membership by User" report, which shows the groups in Active Directory that the user is a member of. Local file server users and groups are not included.

- **All Exchange Online Non-Owner Mailbox Access Events**

Shows all mailbox access performed by someone other than the mailbox owner. Use this report to protect your Exchange Online organization by identifying unauthorized activity.

- **All Exchange Online Non-Owner Mailbox Access Events by User**

Shows users who accessed other users' mailboxes. Use this report to identify unauthorized activity and exercise security control over your Exchange Online organization.

- **All Exchange Server Non-Owner Mailbox Access Events**

Shows all mailbox access performed by someone other than the mailbox owner. Use this report to protect your Exchange organization by identifying unauthorized activity.

- **All Exchange Server Non-Owner Mailbox Access Events by User**

Shows users who accessed other users' mailboxes. Use this report to identify unauthorized activity and exercise security control over your Exchange organization.

Information Disclosure

- **Creation of Files with Sensitive Data**

Shows users who created files with names that suggest they contain sensitive data (e.g., MyPasswords.docx). Run this report regularly to promptly identify users with files that disclose confidential data. The following words are disallowed by default: password, social security number, credit card, cardholder, payment, payroll, ssn, pwd.

- **File Names Containing Sensitive Data**

Shows files with names that suggest they contain sensitive data (e.g., MyPasswords.txt). Names should not disclose confidential data, such as credit card number or Social Security number. Use this report to prevent data breaches and exercise security control over your data. The following words are disallowed by default: password, social security number, credit card, cardholder, payment, payroll, ssn, pwd.

Privilege Elevation

- **Temporary Users in Privileged Groups**

Shows user accounts deleted soon after they were created and added to privileged groups, such as Domain Admins, Enterprise Admins, Schema Admins, Account Operators, and other groups you specified. For each user account, the following is reported: creation and deletion dates and the user who made each change. Use this report to detect intruders attempting to hide malicious activity.

Suspicious Activity

- **Activity Outside Business Hours**

Shows users who performed any actions outside their business hours. Use this report to detect suspicious user activity.

- **Failed Activity Trend**

Shows consolidated statistics on failed actions, including failed read attempts, failed modification attempts, failed logons, etc. The report also lists the users with most failed attempts. A certain number of failed attempts are almost inevitable during normal business operations, but a sudden spike or a gradual growth may indicate malicious activity. Review this report to determine the normal level of failed actions for your organization and spotlight suspicious trends.

Suspicious Files

- **Potentially Harmful Files – Activity**

Shows changes and access to potentially harmful files, such as executables, installers, scripts, and registry keys, on your file shares and SharePoint sites. These files may be malware, viruses, or inappropriate distributives, and should not be stored on shared resources. Use this report to track incidents and prevent security threats.

- **Potentially Harmful Files on File Shares**

Lists files on your file shares that may be harmful or malicious, such as executables, installers, scripts, and registry keys. These files may be malware, viruses, or inappropriate distributives and should not be stored on shared resources. Use this report to detect potentially harmful files and prevent security threats.

User Identity Theft

- **Logons by Multiple Users from Single Endpoint**

Shows endpoints from which several users logged on in a short period of time. While this activity pattern is typical for public computers, an increased number of logons from a personal device may indicate a malicious user or bot trying to access your environment. Use this report to detect suspicious user activity and prevent data breaches.

- **Logons by Single User from Multiple Endpoints**

Shows users who logged on from several endpoints within a short period of time. Such occurrences may indicate that the accounts password was stolen or compromised. Use this report to detect suspicious user activity and prevent data breaches.

- **Recently Enabled Accounts**

Shows user accounts that were recently enabled. Accounts should never be enabled or disabled without proper justification. Review this report on a regular basis for security and compliance purposes.

- **Temporary User Accounts**

Shows user accounts that were deleted soon after they were created. For each user account, the following is reported: creation and deletion dates, the user who made each change, and total number of actions on the account. Use this report to detect intruders attempting to hide malicious activity.

Active Directory

Active Directory Changes

- **Active Directory Overview**

Shows consolidated statistics on changes in Active Directory. Review this diagram to analyze the overall landscape of Active Directory changes.

- **All Active Directory Changes**

Shows changes to all Active Directory objects, including changes to permissions, configuration, etc. This is the most comprehensive report on Active Directory changes. Use it when you need to review every single change to any Active Directory object. Apply flexible filters to narrow the results.

- **All Active Directory Changes by Domain Controller**

Shows all changes to Active Directory, grouped by the domain controller where the change was made. Review this report to detect domain controllers that need your attention or use it to limit the scope of an analysis to specific domain controllers.

- **All Active Directory Changes by Group**

Shows changes to Active Directory, organized by group.

- **All Active Directory Changes by Object Type**

Shows all Active Directory changes, grouped by the type of object modified.

- **All Active Directory Changes by User**

Shows all Active Directory changes, grouped by the user who made the changes.

- **All Active Directory Changes with Review Status**

Shows changes to all Active Directory objects with their review status. Use this report to analyze changes in Active Directory and track team workflow by making notes on the review status or reasons for the change.

- **Active Directory Configuration Container Changes**

Shows changes to objects in the Active Directory Configuration container (sites, services, Exchange organizations, etc.). Because these changes are critical for the entire IT infrastructure, be sure to subscribe to this report or review it on a regular basis to detect security issues and ensure that all configuration changes comply with your organization’s security policies.

- **Active Directory Schema Container Changes**

Shows changes to objects (classes and attributes) in the Active Directory Schema container. These changes are critical for the entire IT infrastructure, since inappropriate schema changes can result in data loss and corruption. It is advisable to update schema only rarely. Subscribe to this report or review it on a regular basis to be aware of these critical changes and ensure that they are in compliance with your organization's security policies.

- **Active Directory Site Changes**

Shows changes to objects in the Active Directory Sites container.

- **Administrative Groups Membership Changes**

Shows changes to membership of the Domain Admins, Enterprise Admins, Schema Admins, Account Operators, and other administrative groups. Members of these groups are entitled to perform critical activities in your IT infrastructure. Subscribe to this report or review it on a regular basis to detect security issues and ensure that administrative group membership is granted or revoked in compliance with your organization's security policies.

- **Computer Account Changes**

Shows changes to computer accounts (renaming, changes to delegation settings, etc.).

- **Contact Object Changes**

Shows changes to contact objects (email address, organization, address, phone number, etc.).

- **Distribution Group Changes**

Shows changes to distribution groups (membership, permissions, description, etc.).

- **Domain Controller Changes**

Shows changes to domain controllers, including demoting and promoting.

- **Domain Trust Changes**

Shows changes to domain trusts.

- **Objects Security Changes**

Shows changes to the security settings of Active Directory objects (permissions, auditing settings, etc.).

- **Operations Master Role Changes**

Shows transfers of operations master roles on both the domain level (relative identifier [RID] master, primary domain controller [PDC] emulator master, infrastructure master) and the forest level (schema master, domain naming master).

- **Organizational Unit Changes**

Shows changes to the configuration of organizational units (name, description, delegation settings, etc.).

- **Password Resets by Administrator**

Shows accounts whose passwords were reset by administrator through the Users and Computers snap-in.

- **Security Group Changes**

Shows changes to security groups (permissions, membership, descriptions, etc.

- **Security Group Membership Changes**

Shows changes to the membership of security groups.

- **Service Pack Installations**

Shows installations of operating system service packs on domain controllers, member servers, and workstations.

- **User Account Changes**

Shows changes to user accounts (creation, modification, and deletion).

- **User Account Status Changes**

Shows changes to the status (enabled or disabled, locked or unlocked) of user accounts.

- **User Password Changes**

Shows users whose passwords were changed.

Active Directory - State-in-Time

- **Groups**

Shows Active Directory groups, with the path and type (Security, Local, Global, Builtin, etc.) for each group.

- **Group Members**

Shows members of the specified groups, with the type (user, group, computer, etc.) and status (enabled or disabled) for each member.

- **Effective Group Membership**

Lists user and computer accounts that belong to a specified group, the status (enabled, disabled) for each account, and whether the account was explicitly named as a member of the group or was included implicitly through group membership.

- **Administrative Group Members**

Lists all members of the Domain Admins and Enterprise Admins groups, with the type (user, group, etc.) and status (enabled or disabled) for each member.

- **Computer Accounts**

Shows computer accounts, with the path and status (enabled or disabled) for each account.

- **Service Principal Names of Computer Accounts**

Shows computer accounts, their paths, the operating systems running on them, and the service principal names used to invoke services on them.

- **Users Not in Any Distribution Group**

Shows accounts that do not belong to any distribution group.

- **Domain Controllers**

Lists domain controllers, with the path and status (enabled or disabled) for each DC.

- **Service Principal Names of Domain Controllers**

Shows domain controllers, their paths, the operating systems running on them, and the service principal names used to invoke services on them.

- **Organizational Units**

Shows organizational units and their paths.

- **Organizational Unit Accounts**

Shows accounts belonging to the specified organizational units or the Users or Builtin containers, with the types (user, computer, inetOrgPerson) and status (enabled or disabled) for each account.

- **User Accounts**

Shows user accounts, with the path, logon name, status (enabled or disabled), and last logon time for each account. Note that a user's last logon time is updated only once every 9-14 days, so some data may be outdated. Use the Days Inactive filter to identify users who have been inactive for the specified number of days or longer.

- **User Accounts – Expired**

Shows expired user accounts, with the paths, logon name, and expiration date for each account.

- **User Accounts – Locked**

Shows locked user accounts, with the path and logon name for each account.

- **User Accounts – Passwords Never Expire**

Shows user accounts whose passwords never expire, with the path and status (enabled or disabled) for each account.

- **User Accounts - Group Membership**

Shows user accounts, with the group membership, group path, and type (Security, Local, Global, Builtin, etc.) for each account.

- **User Accounts - Last Logon Time**

Shows user accounts, with the path, status (enabled, disabled), and last logon time for each account. Note that a user's last logon time is updated only once every 9-14 days, so some data may be outdated.

Group Policy Changes

- **All Group Policy Changes**

Shows all changes to Group Policy objects, settings, links, and permissions, with the name of the originating workstation.

- **All Group Policy Changes by Group**

Shows all changes to Group Policy objects, settings, links, and permissions, organized by group, along with the name of the originating workstation.

- **All Groups Policy Changes with Review Status**

Shows all changes to Group Policy objects and the review status of each change. Use this report to analyze changes to Group Policy and track team workflows by making notes on the review status or reasons for the change.

- **Account Policy Changes**

Shows changes to account policies and their settings.

- **Renaming of Administrator and Guest Accounts**

Shows changes to the settings of the "Accounts: Rename administrator account" and "Accounts: Rename guest account" policies.

- **Administrative Template Changes**

Shows changes to the administrative templates, including pre-defined and custom policy definitions.

- **Audit Policy Changes**

Shows changes to audit policies and their settings.

- **GPO Link Changes**

Shows changes to links between Group Policy objects and domains or OUs.

- **Interactive Logon Setting Changes**

Shows changes to the interactive logon settings of Group Policy objects.

- **Password Policy Changes**

Shows changes to password policy settings, such as maximum password age and minimum password length.

- **Public Key Policy Changes**

Shows changes to public key policies and their settings.

- **Registry Policy Changes**

Shows registry keys that have been added or deleted, or had their permissions changed.

- **Restricted Groups Policy Changes**

Shows changes to restricted groups.

- **Security Settings Changes**

Shows changes to policy settings grouped under the Security Settings node, such as Account Policies, Local Policies, and Event Log.

- **Software Restriction Policy Changes**

Shows changes to the settings of software restriction policies.

- **Software Settings Changes**

Shows software installations and uninstallations through Group Policy.

- **System Services Policy Changes**

Shows changes to the settings of the Windows services startup policy.

- **User Configuration Changes**

Shows changes to policies and preferences located under the User Configuration node.

- **User Rights Assignment Policy Changes**

Shows changes to the settings of user rights assignment policies and their settings.

- **Windows Settings Changes**

Shows changes to Windows Settings, under both the Computer Configuration node and the User Configuration node.

- **Wireless Network Policy Changes**

Shows changes to the settings and permissions for wireless network connections.

Group Policy – State-in-Time

- **Group Policy Objects by Policy Name**

Shows Group Policy objects, organized by policy name, with each object's settings and their values.

- **Group Policy Objects by Setting Name**

Shows Group Policy settings, with a list of the Group Policy objects for which these settings are defined and their values.

- **Group Policy Object Status**

Shows Group Policy objects, with the status (enabled, disabled, etc.) for each object.

- **Group Policy Object Link Status**

Shows Group Policy objects and their delegation settings.

- **Group Policy Object Delegation**

Shows existing Group Policy Objects with their delegation settings.

- **Account Policies**

Shows account policies with their paths and policy settings.

- **Empty Group Policy Objects**

Shows empty Group Policy objects with their links.

- **Identical Settings in Different GPOs**

Shows identical settings defined in different Group Policy objects (these settings can have different values in different GPOs). By clicking the link on the GPO name, you will be redirected to the “Group Policy Object Link Status” report showing where that GPO is applied.

Logon Activity

- **Accounts with Most Logon Activity**

Shows accounts with the most logon attempts, including failed logon attempts. Use this report to validate compliance and analyze user activity.

- **All Logon Activity**

Shows interactive and non-interactive logons, including failed logon attempts. Use this report to analyze user activity and validate compliance.

- **Failed Logons**

Shows failed logon attempts. Use this report to analyze user activity and validate compliance.

- **Interactive Logons**

Shows interactive logon attempts. Use this report to analyze user activity and validate compliance.

- **Successful Logons**

Shows successful interactive and non-interactive logons. Use this report to analyze user activity and validate compliance.

- **User Logons and Logoffs on Domain Controllers**

Shows interactive logon and logoff activity, including failed logon attempts. Use this report to analyze user activity and validate compliance.

Azure AD

- **Azure AD Overview**

Gives at-a-glance statistics for changes and failed logon attempts in Azure AD. Use this report to monitor AD's pulse and review important metrics.

- **All Azure AD Activity by Object Type**

Shows all changes made to Azure AD objects (creation, modification, and deletion), as well as successful and failed logon attempts, grouped by object type. This report can be used in compliance audits to show that logon activity and changes are traceable and auditable.

- **All Azure AD Activity by User**

Shows all changes made to Azure AD objects (creation, modification, and deletion), as well as successful and failed logon attempts, grouped by user. This report can be used in compliance audits to show that logon activity and changes are traceable and auditable.

- **Azure AD Logon Activity**

Shows successful and failed logon attempts in Azure AD. Use this report to analyze user activity and validate compliance.

- **Group Membership Changes in Azure AD**

Shows changes to group membership in Azure AD. Use this report to exercise security control over your data.

- **User Account Management in Azure AD**

Shows changes to Azure AD user accounts, including their creation, modification, and deletion.

- **User Accounts Created and Deleted Directly in Azure AD**

Shows user accounts that were created or deleted directly in Azure AD without provisioning from on-premises Active Directory. Changes made directly in Azure AD may represent a potential security threat. Use this report to detect intruders attempting to hide malicious activity.

- **User-Initiated Password Changes in Azure AD**

Shows Azure AD users who changed or restored their passwords directly in Azure AD without provisioning from on-premises Active Directory. Changes to passwords made directly in Azure AD may represent a potential security threat. Use this report to detect intruders attempting to hide malicious activity.

Exchange

- **Exchange Server Overview**

Shows consolidated statistics on changes across all audited Exchange servers.

- **All Exchange Server Changes**

Shows all changes to Exchange Server objects, configuration, and permissions.

- **All Exchange Server Changes by Server**

Shows all Exchange Server changes, grouped by the server where the change was made.

- **All Exchange Server Changes by Group**

Shows all changes to Exchange Server objects, configurations, and permissions, organized by the group that the user who made the change belongs to. The report also lists the originating workstation from which the change was made.

- **All Exchange Server Changes by Object Type**

Shows all Exchange Server changes, grouped by the modified object type.

- **All Exchange Server Changes by User**

Shows all Exchange Server changes, grouped by the user who made the change.

- **All Exchange Server Changes with Review Status**

Shows changes to all Exchange Server objects with their review status. Use this report to analyze changes in your Exchange organization and track team workflows by making notes on the review status or reasons for the change.

- **All Exchange Server Non-Owner Mailbox Access Events**

Shows all mailbox access performed by someone other than the mailbox owner. Use this report to protect your Exchange organization by identifying unauthorized activity.

- **All Exchange Server Non-Owner Mailbox Access Events by User**

Shows users who accessed other users' mailboxes. Use this report to identify unauthorized activity and exercise security control over your Exchange organization.

- **Address List Changes**

Shows changes to address lists, including their creation, modification, and deletion.

- **Mailbox Changes**

Shows changes to user and inetOrgPerson mailboxes, including their creation, modification, and deletion.

- **Mailbox Delegation and Permissions Changes**

Shows changes to mailbox permissions and delegation. Use this report to detect unapproved changes and enhance security in your Exchange organization.

- **Mailbox Storage Quota Changes**

Shows changes to user mailbox storage quotas settings ("Issue warning at", "Prohibit send at", etc.), and how each change was made.

- **Email Address Policy Changes**

Shows changes to email address policies, including their creation, modification, and deletion.

- **Exchange Database Changes**

Shows changes to the settings and permissions of the mailbox database and the public folder database, as well as database mount and dismount events.

- **New Exchange Servers**

Shows servers that have recently been added to the Exchange organization.

Exchange Online

- **Office 365 Overview**

Gives at-a-glance statistics for changes in Exchange Online and SharePoint Online, including OneDrive for Business.

- **All Exchange Online Changes**

Shows all changes to Exchange Online objects, configurations, and permissions.

- **All Exchange Online Non-Owner Mailbox Access Events**

Shows all mailbox access performed by someone other than the mailbox owner. Use this report to protect your Exchange Online organization by identifying unauthorized activity.

- **All Exchange Online Non-Owner Mailbox Access Events by User**

Shows users who accessed other users' mailboxes. Use this report to identify unauthorized activity and exercise security control over your Exchange Online organization.

- **Exchange Online Groups Changes**

Shows changes to Exchange Online groups. Use this report to monitor the structure of your Exchange Online groups for changes that could lead to data leaks.

- **Exchange Online Mail User Changes**

Shows changes to the properties of mail users, including delivery restrictions. Use this report to detect suspicious activity in your Exchange Online organization.

- **Exchange Online Mailbox Permissions Changes**

Shows changes to mailbox permissions. Use this report to detect unapproved changes and enhance your security in the cloud.

- **Exchange Online Mailbox Policy Changes**

Shows changes to mailbox policies. Use this report to monitor security in your Exchange Online organization and spot changes to business-critical policies.

- **Exchange Online Management Role Changes**

Shows changes to management roles. Use this report to detect unwarranted management role assignments and ensure Exchange Online security.

- **Exchange Online Public Folder Changes**

Shows changes to folders with shared access. Use this report to detect suspicious activity and control information flow.

File Servers (Windows File Servers, EMC, NetApp)

File Servers Activity

- **File Servers Overview**

Shows consolidated statistics on all activity across all audited file servers.

- **All File Server Activity**

Shows activity (changes, failed modifications, reads, and failed read attempts) on all audited file servers.

- **All File Server Activity by Action Type**

Shows activity (changes, failed modifications, reads, and failed read attempts) on all audited file servers, grouped by action type.

- **All File Server Activity by Server**

Shows activity (changes, failed modifications, reads and failed read attempts) on all audited file servers, grouped by the server.

- **All File Server Activity by User**

Shows activity (changes, failed modifications, reads and failed read attempts) on all audited file servers, grouped by users.

- **Failed Change Attempts**

Shows attempts to modify files and folders that failed due to lack of access rights. This report must be reviewed on a regular basis to track unauthorized access attempts.

- **Failed Delete Attempts**

Shows attempts to delete files and folders that failed due to lack of access rights.

- **Failed Read Attempts**

Shows attempts to read files that failed due to lack of access rights. This report can be used during compliance audits to show that all unauthorized data access activities are traceable and easily auditable.

- **File Server Changes**

Shows files, folders, shares and permissions that were created, deleted, or modified.

- **File Server Changes by Action**

Shows files, folders, shares, and permissions that were created, deleted, or modified, grouped by type of action.

- **File Server Changes by Server**

Shows files, folders, shares, and permissions that were created, deleted, or modified, grouped by file server name.

- **File Server Changes by User**

Shows files, folders, shares and permissions that were created, deleted, or modified, grouped by the username of the person who made the change.

- **Files and Folders Created**

Shows newly created files and folders. This report can be used to analyze increased disk space usage.

- **Files and Folders Deleted**

Shows deleted files and folders, with their attributes of each.

- **Files and Folders Moved**

Lists files and folders that were moved to a new location. For each file or folder, the following is reported: the name and location of the original object (or likely candidates), who moved the object, and when it was moved. Use this report to exercise security control over your data.

- **Files and Folders Renamed**

Lists files and folders that were likely renamed. For each file or folder, the following is reported: the old and new names, who renamed the object, and when the change was made. Use this report to track your data flow and prevent data loss.

- **Files Copied**

Lists copied files. For each copy, the following is reported: the name and location of the original file (or likely candidates), who copied the file, and when it was copied. Use this report to ensure that files containing sensitive data are not copied without proper justification.

- **Folder Changes**

Shows folders that were added, removed, or modified.

- **Most Used File Types**

Shows the most frequently accessed file types. Use this report for analyzing usage patterns.

- **Permissions Changes**

Shows changes to file, folder, and share permissions. View this report on a regular basis to detect unauthorized access and verify that only the proper groups of people have access to sensitive data.

- **Share Changes**

Shows shares that have been created, deleted, or modified.

- **Successful File Reads**

Shows file read attempts that were successful. This report can be used during compliance audits to show that access to all sensitive information is traceable and auditable.

- **User Activity Summary**

Shows the most active users. Use this report to detect suspicious user activity such as high numbers of failed access attempts or file reads.

File Server – State-in-Time

- **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. Clicking the group link opens the "Group Membership by User" report, which shows the groups in Active Directory that the user is a member of. Local file server users and groups are not included.

- **Duplicate Files**

Shows files with the same name and size. Use this report to identify potentially duplicate files that might be safely removed.

- **Empty Folders**

Shows folders that can be safely removed. Use this report to spot obsolete data structures.

- **Excessive Access Permissions**

Shows accounts with permissions for infrequently accessed files and folders. Use this report to spot unnecessary permissions and thereby prevent data leaks.

- **Files and Folders by Owner**

Shows files and folders inside the share, grouped by owner.

- **Folder Summary Report**

Shows the total number of files and folders, the file owners, and the total file size.

- **Largest Files**

Lists 25 largest files across the audited file servers, with the owner, location, creation date, last modification date, and last access date for each file.

- **Object Permissions by Object**

Shows file and folder permissions granted to accounts (either directly or via group membership), grouped by object path. Use this report to see who has access to files and folders, and determine whether the set of permissions on an object is the same or different from its parent. Clicking the group link opens the "Group Membership by User" report, which shows the groups in Active Directory that the user is a member of. Local file server users and groups are not included.

- **Potential Data Owners by Folder**

Shows users who frequently access files in a given folder. Use this report to identify factual data owners and analyze usage patterns.

- **Stale Data by Folder**

Shows folders containing files with no recent changes (180 days by default). Use this report to identify files and folders that can be safely deleted or archived.

- **Top Owners by Total File Size**

Lists the users who own files that comprise the largest total file size.

Oracle Database

- **Oracle Database Overview**

Shows consolidated statistics on activity across all audited Oracle Database instances.

- **Account Management**

Shows successful and failed attempts to create, modify, delete, enable, or disable Oracle Database accounts. Use this report to detect suspicious activity and exercise security control over your data.

- **All Oracle Database Activity by Object**

Shows all changes made to Oracle Database, including changes to configuration and privileges, as well as successful and failed logon attempts, grouped by object name.

- **All Oracle Database Activity by Session ID**

Shows all changes made to Oracle Database, including changes to configuration and privileges, as well as successful and failed logon attempts, grouped by session ID. Use this report during security incident investigations to provide individual accountability, since it enables review of user activity within a connection session.

- **All Oracle Database Activity by User**

Shows all changes made to Oracle Database, including changes to configuration and privileges, as well as successful and failed logon attempts, grouped by the user who made the change or logged on.

- **All Oracle Database Administrative Activity**

Shows all changes made to Oracle Database, including changes to configuration and privileges, as well as successful and failed logon attempts, made by users connected as DBA. Administrative privileges empower users to perform critical activities in your Oracle Database. Use this report to detect security issues and ensure that administrative privileges are used in compliance with your organization's security policies.

- **All Oracle Database Logons**

Shows successful and failed attempts to connect to Oracle Database. For each attempt, both the account used to log on to the host OS and the Oracle Database account are reported. Use this report to analyze user activity on production databases and validate compliance.

- **Audit Policy and Setting Changes**

Shows successful and failed attempts to make changes to Oracle Database native audit, including creating, modifying, or deleting audit policies and their settings.

- **Data Access**

Shows users who accessed sensitive data in your Oracle Database. A high number of reads may indicate malicious activity.

- **Data Deletions**

Lists dropped tables and tables where data was removed. Use this report to promptly react to data deletion and prevent its loss.

- **Failed Activity**

Shows failed actions, including failed read attempts, failed modification attempts, failed logons, etc., grouped by user.

- **Privilege Management**

Shows changes to roles and privileges. Use this report to detect unwarranted role assignments or modifications and ensure Oracle Database security.

- **Trigger Management**

Shows successful and failed attempts to create, modify, or delete triggers. Run this report regularly to promptly identify changes to your workflows and exercise security control over your data.

SharePoint

- **SharePoint Overview**

Shows consolidated statistics on changes across all audited SharePoint farms.

- **All SharePoint Activity**

Shows changes and reads on all audited SharePoint farms. Use this report to detect suspicious activity and monitor farm capacity.

- **All SharePoint Changes**

Shows changes to farms, site collections, web applications, policies, permissions, lists, documents, etc.

- **All SharePoint Changes by Site Collection**

Shows all SharePoint changes, grouped by the site collection where the change was made.

- **All SharePoint Changes by Object Type**

Shows all SharePoint changes, grouped by the modified object type.

- **All SharePoint Changes by User**

Shows all SharePoint changes, grouped by the users who made the change.

- **Most Active Users and Entities in SharePoint**

Shows the most active SharePoint users. Use this report to detect suspicious user activity, such as the modification of a large number of files.

- **SharePoint Changes with Review Status**

Shows SharePoint changes with their review status. Use this report to analyze changes in your SharePoint farm and track team workflows by making notes on the review status or reasons for the change.

- **SharePoint Configuration Changes**

Shows changes to the audited SharePoint farm configuration made through the Central Administration website.

- **SharePoint Content Changes by User**

Shows content changes to sites, lists, list items, and documents, grouped by the user who made the change.

- **SharePoint Permissions Changes by User**

Shows permissions changes to sites, lists, list items, and documents, grouped by the user who made the change.

- **SharePoint Read Access**

Shows which users viewed documents and lists on your SharePoint site.

SharePoint Online

- **Office 365 Overview**

Gives at-a-glance statistics for changes in Exchange Online and SharePoint Online, including OneDrive for Business.

- **All SharePoint Online Activity by User**

Shows changes and reads across all audited SharePoint Online sites and OneDrive for Business. Use this report to supervise overall activity and spot suspicious actions.

- **Content Management**

Shows content changes (uploads, downloads, modifications, etc.) to sites, lists, list items, and documents. Use this report to detect suspicious activity and prevent the loss of important data.

- **Data Access**

Shows which users accessed or downloaded documents from your SharePoint Online sites, or synchronized files in OneDrive for Business.

- **Sharing and Security Changes**

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

SQL Server

- **SQL Server Overview**

Shows consolidated statistics on activity across all audited SQL Servers.

- **All SQL Server Activity**

Shows all changes made to SQL Server objects and permissions, including created, modified, and deleted server instances, roles, tables, columns, stored procedures, etc., as well as successful and failed logon attempts. This report can be used in compliance audits to show that logon activity and changes are traceable and auditable.

- **All SQL Server Activity by Server**

Shows all changes made to SQL Server objects and permissions, as well as successful and failed logon attempts, grouped by the server where the action was made.

- **All SQL Server Activity by Object Type**

Shows all changes made to SQL Server objects and permissions, as well as successful and failed logon attempts, grouped by object type.

- **All SQL Server Activity by User**

Shows all changes made to SQL Server objects and permissions, as well as successful and failed logon attempts, grouped by the user who made the change or logged on.

- **All SQL Server Data Changes**

Shows all data manipulations that occurred on a specified SQL Server.

- **All SQL Server Logons**

Shows successful and failed attempts to connect to a SQL Server instance through Windows or SQL Server authentication. Use this report to analyze user activity on production databases and validate compliance.

VMware

- **VMware Overview**

Shows consolidated statistics on changes across the audited VMware infrastructure.

- **All VMware Changes**

Shows all changes to VMware infrastructure objects and settings, including hosts, containers, resource pools, virtual machines.

- **All VMware Changes by Server**

Shows all VMware infrastructure changes, grouped by the server where the change was made.

- **All VMware Changes by Object Type**

Shows all VMware infrastructure changes, grouped by the modified object type.

- **All VM ware Changes by User**

Shows all VMware infrastructure changes, grouped by the user who made the change.

- **VMware Cluster Changes**

Shows changes to clusters. Such changes must be carefully reviewed because they usually affect the entire virtual infrastructure.

- **VMware Datacenter Changes**

Shows changes to datacenters. Such changes must be carefully reviewed because they usually affect the entire virtual infrastructure.

- **VMware Datastore Changes**

Shows changes to datastores, including the creation of new datastores.

- **VMware Host System Changes**

Shows changes to host systems (ESX and ESXi servers). Such changes must be carefully reviewed because they usually affect the entire virtual infrastructure.

- **VMware Resource Pool Changes**

Shows changes to resource pools. Because resource pools control resource allocation, changes to them usually affect the entire virtual infrastructure.

- **VMware Virtual Machine Permissions Changes**

Shows changes made to virtual machine permissions. Since permissions affect who can access virtual machines these changes must be reviewed on a regular basis.

- **VMware Virtual Machine Changes**

Shows changes to configuration of virtual machines, such as virtual hardware, settings, and permissions.

- **VMware Power State Changes**

Shows actions performed on virtual machines (power on, pause, resume, and power off). This report can be used when planning maintenance of virtual machines.

- **VMware Snapshot Changes**

Shows creation, modification, and deletion of virtual machine snapshots. This report can be used to control changes to snapshots and prevent loss of important data and settings.

Windows Server

Windows Server Changes

- **Windows Server Overview**

Shows consolidated statistics on changes across all Windows servers.

- **All Windows Server Changes**

Shows changes to all Windows Server objects and settings, including services, DNS, scheduled tasks, firewall settings, etc.

- **All Windows Server Changes by Server**

Shows all Windows Server changes, grouped by the server where the change was made.

- **All Windows Server Changes by Object Type**

Shows all Windows Server changes, grouped by the modified object type.

- **All Windows Server Changes by User**

Shows all Windows Server changes, grouped by the user who made the change.

- **All Windows Server Changes with Review Status**

Shows all Windows Server changes with their review status. Use this report to analyze changes in your IT infrastructure and track team workflows by making notes on the review status or reasons for the change.

- **Audit Log Clearing**

Shows audit trail cleanup operations. Since such operations should never be performed without proper justification, this report must be carefully reviewed on a regular basis for security and compliance purposes.

- **DNS Configuration Changes**

Shows DNS configuration changes, including zones, properties, etc.

- **DNS Resource Record Changes**

Shows changes to DNS resource records, including their creation and deletion.

- **File Share Changes**

Shows file shares that have been added, modified, deleted, or had their share permissions or properties changed.

- **General Computer Settings Changes**

Shows changes to system properties, such as computer name, environment variables, general, startup and recovery, and system time, log clearing, and system restore.

- **Hardware Changes**

Shows changes to the hardware configuration of a specified Windows Server.

- **Local Audit Policy Changes**

Shows changes to local audit policies. Audit policies must be clearly defined in every organization and changed only after explicit approval by management.

- **Local Users and Groups Changes**

Shows changes made through the Local Users and Groups console. This report is crucial since changes to local Windows user accounts and groups can have a critical impact on the security of a server, including the applications and data it is hosting.

- **Printer Changes**

Shows changes to printer properties.

- **Programs Added and Removed**

Shows programs that were installed or uninstalled on a specified Windows Server.

- **Scheduled Task Changes**

Shows changes to the properties of scheduled tasks. Use this report to spot potential misuse of Windows task automation and issues that can lead to application or process failures.

- **Services Changes**

Shows changes to services that may significantly impact functions of the operating system or applications running on a server.

- **System Shutdowns and Reboots**

Shows computers that were restarted or shut down. This report can be used during audits to show that server downtime is traceable and easily auditable.

- **System Time Changes**

Shows changes to the system time and time zones.

- **Windows Registry Changes**

Shows changes to Windows registry keys. These changes can alter application or system configuration or lead to application and even system failures. Note that some applications make constant registry changes. Make sure you configure auditing for only the specific registry keys you need.

User Activity

- **All User Activity**

Shows video recordings of user activity.

- **All User Activity by Server**

Shows video recordings of user activity, grouped by server.

- **All User Activity by User**

Shows video recordings of user activity, grouped by user.

Event Log

- **Netwrix Auditor System Health**

Shows events from the Netwrix Auditor System Health event log. Use this report for product performance monitoring.

- **All Events by Computer**

Shows all events, grouped by computer.

- **All Events by Source**

Shows all events, grouped by source (e.g. Security or Application Management).

- **All Events by User**

Shows all events, grouped by user.

- **All Security Events by User**

Shows all security events, grouped by user.

- **All System Events by User**

Shows all system events, grouped by user.

- **All Generic Syslog Events**

Shows all syslog events of the Generic platform.

- **Failed Logon Attempts**

Shows failed authentication attempts in Active Directory. This report is crucial to every organization's security and compliance.

- **IIS Application Pools Changes**

Shows changes to application pools, grouped by user.

- **IIS Websites Changes**

Shows changes to websites, grouped by user.

- **Logoffs by User**

Shows logoffs, grouped by the username of the person who made the change. Examine user logoffs to expose unauthorized access. Knowing the exact time someone logged off can also alleviate suspicions during investigations of security incidents.

- **Remote Desktop Sessions**

Shows remote desktop sessions (initiated, terminated, and reconnected).

- **Service Events**

Shows events from the Applications and Services logs.

- **Service Starts and Stops**

Shows started and stopped services.

- **Successful Logons by User**

Shows logons, grouped by username. This report is one of the most important security reports. It can be used to track user activity during security and compliance reviews.

- **User Account Locks and Unlocks**

Shows user account lock and unlock events. This report can be used during security investigations related to unauthorized access.