What's new in Cayosoft Guardian V5

Contents:

AD Connector

With AD Connector, you can easily monitor Active Directory environments on segregated networks with minimal network changes. This setup provides secure, efficient AD monitoring in complex environments without compromising network structure.

GMSA Support

Now, a Group Managed Service Account (gMSA) can be used as a connection account for monitoring your Active Directory domains. With read-only gMSA, the rollback feature in the Change History is protected with just-in-time elevation.

Modifying DNS Records for Recovery Sites

The ability to modify the DNS record for the recovery sites has been enhanced with the option to clean up DNS and create records only for domain controllers to be recovered, in addition to updating existing DNS records for domain controllers to be recovered option for Forest recovery plan and Recovery plan for standby forest.

This option allows administrators to clean up old or irrelevant DNS records and generate new records specifically for the domain controllers that need to be recovered.

Filter Changes by Type

The Change History now has a new filter by change type. Administrators can pinpoint specific changes to create reports or alerting rules, such as creations, modifications, and deletions.

Change History and Rollback for Microsoft Intune

Cayosoft Guardian now monitors changes in Microsoft Intune objects, including managed devices, configuration profiles, Group Policy configurations, settings catalog, device compliance policies, device configurations, and PowerShell script assignments. Change History provides administrators with important details for each change in Intune and changes in Entra ID related to Intune and allows them to roll back unwanted modifications. Each release adds more coverage. Learn more about specific object types supported in Cayosoft Guardian today.

Near Real-Time Threat Alerts

Alerts to critical threats can now be sent immediately when the attack is detected and not have to

wait until the next scheduled report.

Note: Some features mentioned below may not be available to all users yet. By default, Cayosoft Guardian utilizes the Mainstream channel to provide updates, which is the recommended option for most production environments. However, if you wish to try out new features before they become generally available, you can select the Early Adopter channel. Note that changing this setting will only impact future updates. Learn more.

New in version 5.4.4

ID	Item	Produc
20280	This update modifies the default settings of Intune Change Collection jobs. We have reduced the frequency of data collection and disabled tracking of device-related changes, following Microsoft's guidance for vendors to alleviate the load on Intune API cloud services. **Important Considerations** • Reduced data collection frequency: With the schedule change, Cayosoft Guardian will collect updates less frequently. If you have Intune-related alerting rules in place, notifications may be delayed. • Limited Intune Device tracking: Disabling device collection means changes related to the device lifecycle in Microsoft Intune will no longer be visible. However, you can still track device changes coming from Microsoft Entra ID.	Microsoft Intu
19967	Device users can now be excluded from Intune Change Collection, allowing for improved performance and reduced database load.	Microsoft Intu
20051, 20052	General improvements and bug fixes have been implemented.	Threat Detecti History
17798	Improvements and bug fixes have been implemented for Linux scripts.	Microsoft Intu
20093	Resolved: an issue where running a standby forest recovery plan with default recovery site settings failed with the 'No Availability Zone found' error.	Forest Recove
19957	Resolved: an issue when deploying a PowerShell script for macOS in Intune with the execution frequency set: the Intune Change Collection job could fail with the 'SqlDbType.Time overflow' error:	Microsoft Intu
19892	Resolved: an issue when creating an iOS/iPadOS configuration policy using the *iosDeviceFeaturesConfiguration* property with *null* values, subsequent modifications to the policy could fail.	Microsoft Intu

19971	Resolved: an issue where rollback could be disabled for AD object deletion records under specific permission configurations: if an AD object was deleted by an account that lacked the *Allow* action for the *Delete* permission on the object but had *Delete child objects* permission at the parent OU level, the deletion record incorrectly attributed the action to the domain controller account instead of the actual initiator.	Change Histor
19932	Resolved: an issue where Change Monitoring jobs could stop running if the configuration database, hosted on an external SQL server, became temporarily unavailable.	Change Monit

New in version 5.4

ID	Item	Produc
15047	A new AD connector feature has been implemented. With this feature, you can easily monitor Active Directory environments on segregated networks with minimal network changes. This setup provides secure, efficient AD monitoring in complex environments without compromising network structure.	Change Monitori
17940	Now, a Group Managed Service Account (gMSA) can be used as a connection account for monitoring your Active Directory domains. With read-only gMSA, the rollback feature in the Change History is protected with just-in-time elevation.	Service, Security,
5597	The ability to run queries for data from the previous or last quarter or month has been implemented, providing more flexibility in generating time-based reports.	Change History
16196	Cayosoft Guardian now monitors, backs up, and recovers PowerShell scripts in Microsoft Intune. For the full list of Intune objects supported by Guardian, see Objects supported by Cayosoft Guardian in Entra ID, Exchange Online, Microsoft Teams, Intune, and other Microsoft 365 Services.	Intune
9578	A new option in the Backup Plan has been implemented to automatically select and back up two domain controllers (DCs) from each domain. The selection process considers FSMO roles, ensuring that DCs with recent changes (e.g., DNS) are prioritized for backup.	Forest Recovery
18263	The end-user license agreement (EULA) has been updated.	Service

17001	The .NET library has been upgraded to 8.0 version.	Service
17114	The *Export execution history* action has been implemented which allows for collecting information about jobs\rules\plans with one export action.	Service
17069	The *Hybrid search* action has been added to show all related changes for a selected object in the Change History.	Change History
16871	New event categories have been introduced for several object types such as Exchange Online mailboxes, teams and channels in Teams, Entra groups, Entra devices, and AD printers to improve visibility and auditing capabilities.	Change History
15051	Authentication settings have been enhanced.	Service
18216	Cayosoft Guardian now enforces the User Principal Name (UPN) format for all gMSA login attempts to ensure that Kerberos authentication is used. This requires all gMSA account names entered in the *Add domains and partitions* wizard to be saved and used in UPN format when accessing AD resources.	Service
16681	The *Preview* action has been implemented for the saved queries.	Change History
13741	Azure AD has been renamed to Entra ID.	Service
18738	Resolved: an issue with sporadic failures during EC2 instance deployment that affect the site deployment process.	Service
18812	Resolved: an issue with the *Collect Diagnostics* action where records were not exported in the expected order.	Change Monitori
18108	Resolved: an issue in Change History to ensure that all records included in the export match the applied filters throughout the entire dataset, without arbitrarily stopping.	Change History

New in version 5.3.0

ID	Item	Prod

17532	The ability to modify the DNS record for the recovery sites has been enhanced with the option to clean up DNS and create records only for domain controllers to be recovered, in addition to updating existing DNS records for domain controllers to be recovered option for Forest recovery plan and Recovery plan for standby forest. This option allows administrators to clean up old or irrelevant DNS records and generate new records specifically for the domain controllers that need to be recovered.	Forest Recove
17525	Recovery plans now include configuring SYSVOL replication as authoritative or non-authoritative, giving administrators greater control over the replication process. This enhancement ensures that SYSVOL contents are managed precisely during recovery to prevent conflicts and maintain consistency.	Forest Recove
17526	General enhancements have been implemented for the Forest Recovery.	Forest Recove
17800	Resolved: an issue where saved queries and alerting rules do not function as expected in case saved queries with conditions and Advanced filters were applied simultaneously when upgraded to Guardian version 5.2.2.	Change Histor
17815	Resolved: an issue where the nested items were not excluded when the *Where* filter was applied.	Change Histor
17915	Resolved: an issue where the 'Value cannot be null' error was thrown when entering a quick filter value that was missing from a dictionary.	Change Histor

New in version 5.2.2

ID	Item	Product Area
5444, 5284	Cayosoft Guardian now monitors, backs up, and recovers Exchange Online mail contacts. The Change History provides administrators with essential details about the lifecycle of mail contacts and enables them to roll back unwanted modifications. **Link:** • Manage mail contacts in Exchange Online | Microsoft Learn	Change Monitoring, Exchange Online

15602 14211, 14366	Cayosoft Guardian now monitors, backs up, and recovers Device Configuration, Compliance Policies, and PowerShell scripts in Microsoft Intune. For the full list of Intune objects supported by Guardian, see Objects supported by Cayosoft Guardian in Entra ID, Exchange Online, Microsoft Teams, Intune, and other Microsoft 365 Services.	Change Monitoring, Intune
14075, 16281	The option to exclude values from the search in the Change History has been added to the following filters: • What • Action • Who • Where	Change History
7428, 16294	Change History can now be filtered by the value of a modified property. Administrators can specify a condition to search for specific new and old values using a point-and-click interface. Cayosoft Guardian automatically suggests operators and possible values that match the property syntax, ensuring the resulting query is correct.	Change History
12808	The Change History now has a new filter by change type. Administrators can pinpoint specific changes to create reports or alerting rules, such as creations, modifications, and deletions.	Change History
15869	Related change history records can now be included in alert notifications sent to Teams or email to provide administrators with additional context.	Notifications
14717	During the forest recovery process, Cayosoft Guardian now identifies and removes all lingering objects in the Active Directory forest to prevent issues with the replication process in the recovered forest.	Forest Recovery
16530	The end-user license agreement has been updated.	Licensing
15066	During the initial configuration, an administrator can specify whether the Cayosoft Guardian deployment is intended for production or test purposes. This enables Cayosoft to track subscription usage accurately.	Licensing
14848, 16034, 14869	Multiple enhancements have been implemented to improve usability. Cayosoft is continuously seeking ways to enhance the user experience.	UX/UI
16548	The database performance has been improved by optimizing the audit log data indexes.	Service
15868	Resolved: An issue in Reports where the downloaded file name was incorrect.	Service

17526	General enhancements have been implemented for the Forest Recovery.	Forest Recovery
17800	Resolved: an issue where saved queries and alerting rules do not function as expected in case saved queries with conditions and Advanced filters were applied simultaneously when upgraded to Guardian version 5.2.2.	Change History
17815	Resolved: an issue where the nested items were not excluded when the *Where* filter was applied.	Change History

New in version 5.2.1

ID	Item	Product Area
16396	An issue has been addressed when some antivirus software products identified the components of Cayosoft Guardian as potentially dangerous.	Service

New in version 5.2.0

ID	Item	Pro
15871	Cayosoft Guardian now gives BitLocker enablement options within the backup plan. By default, BitLocker enablement is turned off, i.e., administrators must manually configure it on each domain controller. However, you can opt for automatic BitLocker deployment by Guardian during the backup process.	Forest Recov
15950	Forest recovery plans can now automatically set up the Active Directory-integrated DNS service necessary for successful recovery if the DNS service was not configured in the original Active Directory forest.	Forest Recov
16093	Forest recovery plans now include checks and temporary disablement of NetLogon policies that interfere with DNS records' automatic registration, ensuring success in relevant recovery scenarios.	Forest Recov
16272	The issue has been resolved in cases where a recovery plan, configured with default settings, encountered an error. This issue occurred specifically in environments where the DIT file size exceeded 10 GB.	Forest Recov

New in version 5.1.2

ID	Item	Prod
16017	An issue has been resolved where the database settings in the initial configuration wizard could not be modified.	Initial configu
16005	An issue has been resolved when an automatic threat definition update could alter notification settings specified in the threat definitions.	Alerting

New in version 5.1.1

Cayosoft Guardian can now send immediate notifications about critical threats detected in your environment via Teams or email.

The message includes all important details and a link to step-by-step instructions on how to find additional evidence and resolve the issue.

ID	Item	
15018	Cayosoft Guardian now collects additional events related to failed logon attempts and uses these events to detect specific Password Spray attacks.	Se
14208, 14210, 15147	Cayosoft Guardian now monitors, backs up, and recovers Device Configuration Policies and Compliance Policies in Microsoft Intune.	Int
6999	To avoid sending excessive alert notifications, alerting rules now allow limiting the number of raised alerts in a specific time interval. When the threshold is reached, this alerting rule will be paused for a designated period before being resumed.	Al
15775	Cayosoft Guardian now constantly monitors the duration of job execution and sends an alert if job execution takes too long to complete. This feature is useful in identifying problems in the target systems that might be hindering the extraction of events or changes during the collection jobs.	He
15143	The login form has been updated to provide a more simplified and secure sign-in experience. Now, we no longer support authentication method that bypasses multifactor authentication in Entra ID.	UX Se
15328	The threat definitions widget has been updated to show only definitions with active alerts.	UX
14905	An issue has been resolved when a blank page was shown after a click on a link with a security descriptor.	UX
15054	An issue has been resolved when Cayosoft Guardian failed to replicate backups to Azure blob storage.	Fo
15177, 14929	An issue has been resolved when a search query in Change History was executed every time after opening an item in the table.	Ch Pe
15898	An issue has been resolved when downloading the Forest Recovery agent from Cayosoft Guardian Web Portal failed.	Fo