What's new in Cayosoft Guardian V3

Go to What's New v2

Downloads

Instant Active Directory Forests Recovery (Patent Pending)

Cayosoft Guardian Forest Recovery now includes **Instant Active Directory Full-Forest Recovery** that allows Recovery Plans to create and update multiple isolated stand-by Recovery Forests in Azure AD. Cayosoft Guardian already provides the fastest recovery time of any product on the market today, and this forth coming feature will reduce the age of related AD data latency so there is less missing data in Active Directory. With Instant Recovery, there is always an up to date stand-by directory at the ready should the Forest fall victim to a ransomware or wiper cyberattack.

New: Threat Detection for Hybrid Azure AD (No purchase needed)

Cayosoft Guardian now includes a Threat Detection to identify security issues in Azure AD and on-premises Active Directory before they are exploited by a bad actor. Like Anti-Virus for your Microsoft Directories, Threat definitions are automatically downloaded and automatically begin detection of security issues in real-time and with scheduled checks in Azure AD, Exchange Online, Azure resources, and Active Directory. Threat alerts are created for each issue to track and trace overall security posture and remediation progress. Cayosoft Guardian also collects evidence from the connected systems and provides detailed remediation advice for each threat alert. After completing a full trial of Guardian, threat protection along with a limited amount of Change History data will continue to be provided under the Cayosoft Freeware license.

New: Group Policy Change Monitoring & Rollback

Cayosoft Guardian now allows monitoring changes, creating backups, and performing recovery of Group Policy Objects down to individual GPO settings. Cayosoft Guardian tracks changes in all types of GPO settings. Change History view was improved to present changes in GPO settings and other complex data structures in a human-readable form.

New: Improved Support for SIEM Tools

Cayosoft Guardian can be configured to write events to Windows Event Log for specific threat and change alerts. These events might be used to provide SIEM solutions with valuable information about security issues detected in real-time or by schedule.

Cayosoft Guardian vs. Guardian Forest Recovery

Cayosoft Guardian now has two distinct licensing modes, **Guardian** and **Guardian Forest Recovery**. Guardian Forest Recovery is an affordable premium upgrade to Guardian adding Immediate Active Directory Full-Forest Recovery. Go here if you have questions about

Guardian Forest Recovery.

Change History Archiving

Cayosoft Guardian now supports archiving of older records to a separate database. Archiving allows controlling active database size, keeping performance at the expected level, and at the same time preserving records for a long-term period.

Multiple Collection Points

Cayosoft Guardian now supports configuration where multiple services to collect data, and data collected by one service can be easily accessed via the web portal of another service.

Advanced to Azure AD Support for Conditional Access Policies

Cayosoft Guardian provides enhanced support for granular auditing, backup, and rollback of Azure AD Conditional Access Policies.

Change History Entry Classification

Change History now supports event classifications. Classifications can be used to create more precise searches and reports while providing administrators with higher visibility and insight into changes in and across Active Directory, Azure AD, and Office 365.

Secure Cloud Storage Location

Cayosoft Guardian Forest Recovery provides the ability to configure a dedicated secure cloud backup storage location in Azure or Amazon AWS. When you use a Secure Cloud Storage Location in your environment it helps prevent unauthorized modification or malware attacks on backup data and makes the backup data highly available while supporting your key data security and compliance initiatives.

Version	ID	Item	Product Area

3.4.0	6437	Cayosoft Guardian now includes a Threat Detection component to identify security issues in Azure AD and on-premises Active Directory. Threat definitions allow the detection of security issues in real-time and with scheduled checks in Azure AD, Exchange Online, Azure resources, and Active Directory. Threat alerts are created for each issue to track and trace overall security posture and remediation progress. Cayosoft Guardian also collects evidence from the connected systems and provides detailed remediation advice for each threat alert.	Active Directory, Forest Recovery, Threat Detection
3.4.0	6415, 10009, 11045, 11078	Cayosoft Guardian now allows monitoring changes, creating backups, and performing recovery of Group Policy Objects down to individual GPO settings. Cayosoft Guardian tracks changes in all types of GPO settings. Change History view was improved to present changes in GPO settings and other complex data structures in a human-readable form.	Active Directory, Group Policy
3.4.0	11323, 10572	Cayosoft Guardian now offers two new subscription tiers. With the Freeware subscription, which includes most threat detection features, you can scan your environment to detect security issues and use remediation advice to resolve these issues, improving the security of your Azure AD and on-premises Active Directory. With a Forest Recovery Only subscription, you can use Cayosoft Guardian to automate Active Directory backup and forest recovery scenarios.	Licensing

3.4.0	6619, 11095	Cayosoft Guardian allows updating its components from the cloud. Cayosoft team is constantly working on delivering updates for threat definitions and related components to ensure better protection of your environment. The update process is fully automated and performed in the background. Once the update process is initiated manually or by schedule, downloadable extensions are securely delivered in encrypted packages to ensure protection in transit and at rest.	Service
3.4.0	9861	Cayosoft Guardian can be configured to write events to Windows Event Log for specific threat and change alerts. These events might be used to provide SIEM solutions with valuable information about security issues detected in real-time or by schedule.	Service, Security
3.4.0	4678	Now, changes in assigned Microsoft 365 licenses and plans are presented in a user-friendly format in the Change History.	Azure AD
3.4.0	5073	Cayosoft Guardian now allows customizing columns in grids to adjust the view.	UX
3.4.0	8315, 10483	Multiple dashboards with new widgets were added to Cayosoft Guardian to visualize various stats related to new threat detection features and to provide a better user experience, simplifying access to frequently performed tasks.	UX
3.4.0	10097	Cayosoft Guardian now uses a newer version of a built-in local SQL database.	Service
3.4.0	10517	Cayosoft Guardian now provides additional network settings such as proxy configuration and certificate management.	Service
3.4.0	10645	Cayosoft Guardian now offers audit, backup, and recovery for domains configuration settings in the Azure AD. Domain configuration includes federation settings that must be closely monitored to ensure protection against various cyberattacks.	Azure AD, Threat detection

3.4.0	10659	Cayosoft Guardian no longer uses WinRM to perform calls to Exchange Online when restoring distribution groups, unified groups, and mailboxes. The REST API for Exchange Online is used for integration with Exchange Online.	Service
3.4.0	11288	Cayosoft Guardian now uses customer usage attribution identification in virtual machines created within Forest Recovery plans. Customer usage attribution associates usage from Azure resources in your Azure subscription with Cayosoft Inc as a Microsoft partner. Microsoft recommends that ISVs establish these associations and get product usage visibility within Microsoft systems to provide better support and enhanced compatibility with partners' products. When you deploy Azure resources from Cayosoft templates within Forest Recovery plans, Microsoft can identify the installation of our software with the Azure resources deployed. Microsoft can correlate the Azure resources that are used to support the software. Microsoft collects this information to provide the best experiences with its products and to operate its business. The data is collected and governed by Microsoft's privacy policies, which can be found at https://www.microsoft.com/trustcenter. Learn more about customer usage attribution.	Service
3.4.1	11373, 11099, 11376	Cayosoft Guardian now offers numerous enhancements for management of threat alerts. New threat definitions were added, see full list of the threat definitions here.	Threat detection
3.4.1	11392	An issue has been resolved when forest recovery plan failed with error due to unexpected reboot of the target domain controller. Additional retries and timeouts were added to enhance resilience of the forest recovery process.	Forest Recovery
3.4.1	11386	An issue has been resolved when a forest recovery plan reported a lot of errors in case of incorrect DNS configuration.	Forest Recovery

3.4.1	11385	An issue has been resolved when a backup plan, using local storage, failed with error due to excessively strict requirements for local storage size on a domain controller.	Forest Recovery
3.4.1	11330	An issue has been resolved when a backup plan might fail if there are too many DNS delegations in the environment.	Forest Recovery
3.4.1	11350	An issue has been resolved when Cayosoft Guardian collected excess data in SYSVOL resulting in prolonged duration of the backup process.	Forest Recovery
3.4.1	11371	An issue has been resolved when an Azure AD user with a disabled account in Cayosoft Guardian was able to log in into Cayosoft Guardian Web Portal.	Service, Security

Version	ID	Item	Product Area
3.2.2	10925	An issue has been resolved when an error that appeared on the General tab of the AD user or AD group object if specific attribute values were set.	Active Directory
3.2.2	10960	An issue has been resolved where initial data collection in the Azure AD environment, with an extremely large number of groups, was canceled automatically due to exceeding the built-in timeout.	Azure Active Directory
3.2.2	10992	An issue has been resolved where collection job execution might fail with an error in the Active Directory environment where passwords are synchronized to read-only domain controllers (RODC).	Azure Active Directory
3.2.2	10993, 10999	An issue has been resolved where Cayosoft Guardian was unable to detect the initiator of DNS zone or domain root object modification.	Azure Active Directory
3.2.2	11046	An issue has been resolved where Cayosoft Guardian might not detect some changes in Azure AD Administrative units.	Azure Active Directory

Version	ID	Item	Produ

3.2	10081	A recovery plan for the standby Active Directory forest is added to Cayosoft Guardian. The new recovery plan automatically creates a copy of your production Active Directory forest in the Azure cloud, isolates it from your production Active Directory, and maintains it up-to-date on a scheduled basis. The standby forests in the Azure cloud can be used immediately in case of emergency without the need to go through a time-consuming forest recovery process.	Active Direct Forest
3.2	4937	Now the **Where** property of a Change History record contains a more precise location of a changed object. A related Where query filter in the Change History allows searching for a changed object within a specific location such as a Managed system, an Active Directory container, an Azure AD Administrative Unit, and/or a Microsoft 365 Team.	Active Direct Azure Chang
3.2	5360, 5892	Cayosoft Guardian now offers audit and protection for Azure AD roles assigned with Azure AD Privileged Identity Management. All changes in temporary or permanent, eligible or active role assignments are now tracked and categorized.	Servic
3.2	6105	The discovery status is now displayed in Change History as a new column. Cayosoft Guardian collects events from Windows Security Event Log on each domain controller and correlates these events with previously collected change history records. Once a corresponding event is found for a change history record, Cayosoft Guardian updates the values of the **Discovery status**, **Initiator**, and **When** in this change history record. **When** is updated with an event time registered by a managed system. If the corresponding event is not found, Cayosoft Guardian stops the search after a predefined timeout and updates the value of the **Discovery status**. In this case, the **Initiator** field remains empty and the **When** value indicates when Cayosoft Guardian collected the change from a connected managed system.	Chang
3.2	9203	Additional verification checks were added to an Active Directory forest recovery plan to ensure that the recovered forest is fully functional.	Forest
3.2	9643	Cayosoft Guardian now offers audit and protection for Active Directory-integrated DNS zones and records.	Active Direct

3.2	9756	Cayosoft Guardian now provides better protection for the integrity of the backup files by calculating the CRC32 hash of backup files. This data is used to verify the backup file's integrity before recovery.	Forest
3.2	9769, 10244, 10109, 10128, 10129, 10108	Multiple enhancements were introduced for backup plans such as support for synchronization of the backup files to the Azure cloud storage using REST API, automatic selection of domain controllers to be backed up, built-in notifications via email or Teams, additional plan settings related to local backups created on domain controllers, and the option to execute retention rules with a backup plan.	Forest
3.2	9889	With the new version of the Cayosoft Guardian, the database maintenance job is no longer performed on a scheduled basis. Execute database maintenance job manually if necessary.	Servic
3.2	9991	Now multiple archive databases from different SQL servers can be added simultaneously and the search can be executed across all connected archives.	Chang Histor Archiv
3.2	10132	Jobs now have notification rules that allow sending notifications on job start and completion results. Fine-tuned notification rules are added for various execution results. Communication channels must be configured in order to receive notifications.	Servic
3.2	10080	An option to export data from any grid is added to Cayosoft Guardian.	Servic
3.2	10088, 10089	A number of potential security issues were fixed based on the results of the penetration tests.	Securi
3.2	10103	An alert is now raised if archiving and retention configuration allows Change History data to be deleted.	Servic
3.2	10603	Now Cayousoft Guardian shows SID (Security Identifiers) in the SIDHistory attribute in a user-friendly format.	Chang
3.2	10303	An issue has been resolved when changing the recovery method resets the value of the target IP address in the domain controller settings of the recovery plan.	UX

3.2	10312	An issue has been resolved when a backup job fails with an error if group policy settings do not allow storage of passwords and credentials for network authentication.	Servic
3.2	10130, 9994, 10084, 10603	Cayosoft Guardian's user experience was improved.	UX

Version	ID	Item	Product Area
3.1.3	10413	Environments with HTTP proxy requiring Windows integrated authentication are now supported in Cayosoft Guardian.	Azure AD
3.1.3	10514	An issue has been resolved where a retention rule in Cayosoft Guardian didn't delete backup files located on a network share.	Service
3.1.3	10516	An issue has been resolved when the forest recovery plan execution fails with an error if BOOTKEY sequence contains an unexpected value.	Forest Recovery
3.1.3	10518	An option to skip the check for backup file integrity was added to the recovery plan. While the backup file validity check (CRC) ensures backup integrity, disabling the option might result in a significant reduction in the verification and recovery duration.	Forest Recovery
3.1.3	105520	An issue has been resolved when the recovery plan failed with error due to the inability of the NETLOGON service to be restarted within a specified time. An increased timeout and additional retries were added for this scenario.	Forest Recovery

Version	ID	Item	Product Area

3.1.2	10279	An issue has been resolved where a rollback of a change or a deletion of Azure AD named location fails with a warning.	Azure AD
3.1.2	10294	An issue has been resolved where Cayosoft Guardian service crushes with an error if an Active Directory object in a connected managed system contains a reference to itself as a value in specific Exchange-related attributes such as authOrig, unauthOrig, dLMemSubmitPerms, dLMemRejectPerms attributes. .	Service

Version	ID	Item	Product Area
3.1.1	10156	Cayosoft Guardian can be configured with read-only access to Azure AD and Microsoft 365 services. A script is provided to add a tenant to Cayosoft Guardian in read-only mode. The script creates an Azure AD enterprise application with read-only permissions and configures Cayosoft Guardian to use a service account with a Global Reader role. In read-only mode, rollback action is disabled in the Change History for all Azure-related changes.	Service, Azure AD, Security
3.1.1	10147	An issue related to event collection from Azure AD has been resolved for environments with the Azure AD cloud sync agent deployed. An issue is reproduced as the Azure AD event collection job failing with errors in environments with a large number of events in the Azure AD log. Now the job action has an option to configure specific events to be collected. Events generated by Azure Cloud Sync are excluded by default as these events are not used by Cayosoft Guardian. An option to configure Azure AD graph client timeouts was added.	Azure AD, Change Auditing

3.1.1	10040	An issue has been resolved where rollback of AD Group Policy Container creation failed with errors.	Usability
3.1.1	10110	An event category Update permission(s) name was changed to Update EXO mailbox permission(s).	Usability
3.1.1	10186	An issue has been resolved when a backup plan failed when SysVol did not contain a temporary folder.	Service
3.1.1	10241	An issue has been resolved when alerting rule for Conditional access policies generated excessive alerts on Azure AD system changes.	Service
3.1.1	10246	An issue has been resolved when a PowerShell remote connection failed during agent deployment or logs collection.	Service

Version	ID	Item	Product Area
3.1.0	7927	Cayosoft Guardian now supports archiving of older records to a separate database. Archiving allows to control active database size, to keep performance at the expected level, and at the same time to preserve records for a long-term period. Also, Cayosoft Guardian now supports configuration where multiple services to collect data, and data collected by one service can be easily accessed via the web portal of another service. For example, Cayosoft Guardian can be installed in multiple locations and provide a consolidated view of all changes in a central location.	Service
3.1.0	5545	Cayosoft Guardian provides enhanced support for granular auditing, backup, and rollback of Azure AD Conditional Access Policies. Now, Cayosoft Guardian has a built-in alerting rule to notify an administrator about critical changes in Azure AD Conditional Access Policies, such as modifications or deletions.	Azure AD, Change Auditing, Alerting, Security

3.1.0	7333, 9940, 9575, 9939, 9901, 9932, 9791	New classification categories and filters in Change history deliver better capabilities for creating more precise searches and reports, provide administrators with better visibility and insight into changes in Active Directory and Azure AD. Now, Cayosoft Guardian automatically converts specific attributes changes and values of some frequently changing attributes to a human-readable event category or a virtual attribute. Also, change records now contain object location for Active Directory objects and administrators can search change records of objects located within specific containers.	Usability, Security, Azure AD, Active Directory
3.1.0	9890, 9888, 9872	The performance of alerting rules and reports improved in some scenarios. Also, the performance of collection jobs targeted at Active Directory was optimized for highly-loaded environments.	Service
3.1.0	9797	Performance statistics provide better visibility into computing resources consumed by every job, action, or alerting rule. This data might be critical for planning performance optimizations in larger environments.	Service
3.1.0	9608, 9789, 9790, 9792	Cayosoft Guardian provides enhanced automation and error handling for the DNS configuration processes in various Active Directory forest recovery scenarios.	Forest Recovery
3.1.0	9810	All collected change records now can be forwarded to the Windows event log and collected by a third-party SIEM solution such as Microsoft Sentinel or Splunk.	Integration
3.1.0	9348	Alerting rules for Exchange Online permissions no longer raise alerts on changes initiated by Exchange Online internal processes.	Exchange Online, Alerting

3.1.0	9987, 9864,9956, 10004, 9952, 9949, 9985	Cayosoft Guardian's user experience was improved.	Usability