What's New in Cayosoft Guardian v1

Major New Features in Cayosoft Guardian v1

Security alerts for Microsoft 365 Global Admin privilege escalation to Azure Resources administrator and other Azure Resources roles assignments at root scope

By default any Microsoft 365 Global Administrator can elevate his/her access to full control over Azure including delegation of roles in Azure and other critical security and compliance sensitive settings. Cayosoft Guardian now tracks such role assignments at root scope, raises alert, and allows to quickly rollback malicious changes.

Change Monitoring and Immediate Rollback for Exchange Mailbox Permissions and Settings

Backup and manage Exchange online mailbox delegate permissions and settings with Cayosoft Guardian. Quickly isolate and rollback malicious or mistaken changes to Exchange licenses that can impact mailbox metadata including delegation, forwarding and more.

Continuous Protection for Hybrid Identities

Cayosoft Guardian now provides protection for Hybrid Active Directory Identities as well as on-premises Active Directory identities and provides immediate change roll-back should those changes be made in error or as the result of a malicious attack.

Continuous Protection for Cloud Identities

Cayosoft Guardian provides protection for Cloud Only Identities and provides immediate change roll-back should those changes be made in error or as the result of a malicious attack.

Continuous Protection for Microsoft Teams Settings

Microsoft Teams has become mission-critical as organizations ramp-up work at home efforts. Cayosoft Guardian continuously monitors Microsoft Teams and provides immediate change roll-back should those changes be made in error or as the result of a malicious attack.

Continuous Protection for Azure Active Directory and Hybrid Active Directory

Cayosoft Guardian continuously monitors Azure AD for changes, records those changes and provides immediate change roll-back should those changes be made in error or as the result of a malicious attack.

Continuous Protection for Legacy Active Directory

Cayosoft Guardian continuously monitors On-premises AD for changes, records those changes and provides immediate change roll-back should those changes be made in error or as the result of a malicious attack.

Change Monitoring and Rollback for Native Azure AD Administrative Units

Backup and restore changes in Administrative units with Cayosoft Guardian. Quickly isolate and rollback malicious or mistaken changes to Administrative unit membership and scoped roles membership that can impact boundaries of security or administrative segment defined in your organization.

Improved Performance and Support for External Microsoft SQL Server

Cayosoft Guardian has been updated to provide better performance in larger enterprise environments including support for the use of a separate Microsoft SQL Server. After installation Cayosoft Guardian is pre-configured for using lightweight Microsoft SQL Server Express LocalDB database. To achieve better performance and scalability Cayosoft Guardian can now be configured to connect to a Microsoft SQL.

Enhanced Filtering

Filter change history based on time frame, types of event, priority of events and more.

Enhanced filtering helps administrators to zero-in on specific changes based on who did it, when it happened or other criteria to more quickly identify, isolate and rollback suspect changes.

Enhanced storage management and Azure SQL support

Cayosoft Guardian now supports Azure SQL database. Storage settings in Guardian Web Portal allow to manage database connection settings and provide an option to migrate the existing configuration to a new database.

Version	ID	Item	Product
1.4.0	6022, 7090	Protection and change audit for Azure AD Native Administrative Units has been added. Cayosoft Guardian now tracks changes and allows administrators to restore unwanted modifications to Native Administrative Unit membership and scoped roles membership.	Azure AD / 365 Backup
1.4.0	6865	Escalation of Privilege Detection and Remediation: A Microsoft 365 Global Administrator can elevate his privileges to access all subscriptions and management groups across all Azure Resources. Cayosoft Guardian now detects this dangerous escalation of privilege, raises a critical alert and allows Guardian Administrators to revoke these unwanted changes. Learn more about Azure User Access Administrator role assignments at root scope: https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin	Azure / Sec

1.4.0	5282	To better support various topology configurations for legacy AD Domain Controllers, Cayosoft Guardian now allows specification of a preferred Domain Controller and a separate Domain Controller holding the Global Catalog role. Cayosoft Guardian uses the preferred Domain Controllers for collection and restore operations and automatically fails-over to the next nearest Domain Controller if the connection to a preferred Domain Controller fails.	Active Dire
1.4.0	6274	Guardian can now be added to User's Application menu through added support for Azure AD Application Proxy. Now MFA, conditional-based access, and other advanced sign-in scenarios can be configured for Guardian Web Portal with integration with Azure AD Application Proxy.	Service
1.4.0	6962	The Guardian Service has been updated so that if AD Audit Jobs complete with a warning if a Domain Controller is not available. Cayosoft Guardian can also be configured to skip the collection of security log events from specific Domain Controllers.	Service
1.4.0	7081, 7085	Cayosoft Guardian has passed OWASP ZAP security scanner vulnerability tests for the web application.	Security
1.4.0	4714	Cayosoft Guardian now supports Azure SQL database. Storage settings in Guardian Web Portal allow you to manage database connection settings and provide an option to migrate the existing configuration to a new database.	Service
1.4.0	6675	To reduce built-in database size and improve performance scheduled Storage Maintenance Job has been added. During the maintenance, all scheduled jobs paused and Guardian Web Portal displays a global alert.	Service
1.4.0	6719	Service log settings now can be managed from Guardian Web Portal.	Service
1.4.0	7160	New classification rules have been added for account lockout and unlock account records.	Security, U

1.4.0	7208	An event is now reported to the event log when Guardian Service failed to start.	Service
1.4.0	6912	An issue has been resolved in the *Default Audit job* when excessive events for read-only operations were collected.	Service
1.4.0	6862	Cayosoft Guardian might not show membership updates for cloud groups in case such changes contain devices or security principals. Now reconciliation period setting has been added for groups membership collection and such group membership updates will be collected within a defined period.	Service
1.4.0	7029	In Cayosoft version 1.3.1 or older restore was available for all change records. If a change can't be restored warning or an error is reported. Now restore option is no longer available for change history records that can't be restored.	Usability

1.4.0	7072	Cayosoft Guardian now shows timescale on the Recent changes dashboard within the time zone of the client where Guardian Web Portal is opened.	Usability

1.4.0	5128, 5386, 5832, 5842, 6443, 6581, 6598, 6886, 6919, 7088, 7171, 7173, 7177, 7183	Cayosoft Guardian's user experience was improved in several different areas.	Usability

Version	ID	Item	Product Area
1.3.1.3	6915	Performance of Active Directory event log data collection was improved by excluding events about changes in private information data set.	Service

Version	ID	Item	Product Area
1.3.1.2	6773, 6852	Multiple usability and performance enhancements related to Active Directory event log data collection.	Service, Usability
1.3.1.2	6850	Initiator discovery for hybrid group membership change was improved.	Service
1.3.1.2	6853	Default Active Directory connection timeout was increased.	Service
1.3.1.2	6854	Azure AD backup performance was improved by introducing batch operations for collecting of missing information about linked objects.	Service
1.3.1.2	6832	An issue has been resolved when Guardian couldn't identify a Domain Controller with a Global Catalog role.	Service
1.3.1.2	6600	Default Exchange Online Backup Job was improved with additional retry attempts on error.	Service

Version	ID	Item	Product
1.3.1.1	6729	Windows 2008 introduced a new property set called Private information that includes msPKI* properties. By design, these properties are secured in such a manner that only the SELF object can access them. This design might lead to excessive 4662 events on the domain controller. To reduce Guardian database size is possible to exclude events with specific properties or properties sets from collecting. By default, msPKI* properties are excluded.	Service
1.3.1.1	6747	Default change history retention job settings were adjusted to keep more change records in the database.	Service
1.3.1.1	6748	To reduce Guardian service starting time database maintenance procedures are disabled by default.	Service
1.3.1.1	6756, 6757,	Minor enhancements related to backup and restore of msPKI* properties have been added.	Usability

Version	ID	Item	Product
1.3.1	5781	To address limitations of the Microsoft SQL Server Express LocalDB Cayosoft Guardian now supports external SQL database (Microsoft SQL Server 2016 and later).	Scalability
1.3.1	6669, 6673, 6674	To optimize database size and performance multiple improvements were made including adjustments of the audit log retention job parameters and SQL database request timeout parameter, reorganization of database maintenance procedures and enhancements of change record deletion process in the retention job.	Service
1.3.1	6687	To support specific initial deployment scenarios certificate checks can be disabled in Cayosoft Guardian settings.	Service
1.3.1	6584, 6661,	Guardian's user interface was improved in several different areas.	Usability

Version	ID	Item	Product
1.3.0	4240, 6089	Protection and change audit for Exchange Online mailbox settings and permissions has been added. Cayosoft Guardian now tracks changes and allows administrators to quickly restore unwanted modifications to user mailboxes, shared mailboxes and resource mailboxes. Event data collection now includes new Exchange Online related events from Microsoft Office 365 Audit Logs required to identify initiator for mailbox permissions and settings, and event date/time.	Azure AD Office 365 Backup

1.3.0	4246	Change History Saved Queries have been added to the Change History view. Cayosoft Guardian now allows administrators quickly filter Change History records by many new conditions and save these conditions as a filters for future use. Built-in Saved Queries can also be copied and modified making more complex queries simpler to create.	Change Isc
1.3.0	5788	Change History Quick filter have been added to provide in-place editing of filtering conditions to narrow search scope with a few clicks.	Usability
1.3.0	6424	When a hard-deleted cloud-only azure user account is restored, Guardian will attempt to find the user's original inactive mailbox. If mailbox is found, the new re-created cloud-only azure user would will be granted access to that mailbox content.	Azure AD Office 365 Restore
1.3.0	5283	When a Hybrid user account deletion restore is performed Guardian will now trigger Active Directory cross-site replication, so that the changes in Active Directory are picked up by the next Azure AD Connect synchronization cycle.	Hybrid Re
1.3.0	5678	On the Change History record Properties screen, the initiator's name is now displayed as a hyperlink for quick access to the initiator's account details.	Usability
1.3.0	6052	User notification of critical issues has been improved to show multiple alerts simultaneously.	Usability
1.3.0	6054	The issue was resolved when a change in Conditional Access Policy (CAP) might not be restored successfully when the CAP contains links to deleted objects.	Azure AD Office 365 Restore
1.3.0	6084	The issue was resolved when the Initiator for Teams creation record was not the same as for the associated group creation record.	Change Au
1.3.0	6106	Initiator discovery from the Microsoft Office 365 Audit Logs was improved to cover longer delays between the change and a corresponding event(s) appear in Microsoft's logs.	Change Au
1.3.0	6129	New predefined alerts were added: • "New Guest user created" rule triggered on a guest invitation • "Guest user added to group" rule triggered on guest user added to any group	Alerting
1.3.0	6328	A new event category was added: "Password reset or force sign-out". This event category includes password resets and forced sign-outs of user accounts in Azure AD.	Change Au
1.3.0	6194	A link to the list of the related third-party components and their respective licensing terms has been added to About screen.	Document
1.3.0	6446, 5589, 6168,	Guardian's user interface was improved in several different areas.	Usability

Version	ID	Item	Product
1.2.2	6072, 6088	User experience has been improved for users signing in with their Office 365/Azure Active Directory accounts. 1. Hybrid user, whose AD account was added to the Guardian Global Administrators role, can use her cloud account to sign in to Web Portal. 2. User from the managed tenants can sign-in to Guardian Web Portal without a prompt for additional permissions. 3. Hybrid user can use her cloud account for automatic sign in to Guardian Web Portal in case of indirect membership in the group being added to the Guardian Global Administrators role.	Usability
1.2.2	6095	User experience with product upgrade has been improved, when Azure Consent needs to be re-granted after the upgrade.	Usability
1.2.2	6114	An issue was fixed with added member names missing in the group and role membership changes alerts	Alerting
1.2.2	6128	An issue was fixed with duplicate Display Specifiers in Active Directory Schema.	Service
1.2.2	5632	Several minor user interface issues were resolved.	Usability

Version	ID	Item	Product
1.2.1	4219	Guardian Web Portal sign-in experience is now integrated with Azure AD/Microsoft Office 365. You can use your on-premises AD account or your Microsoft Azure AD/Office 365 account to sign in to Guardian Web Portal. All Azure AD security features, like Multi-factor Authentication and Conditional Access Policies, are enforced when you authenticate.	Security
1.2.1	5777	Protection for Microsoft Teams has been added. Cayosoft Guardian now tracks changes in Microsoft Teams and channel settings, membership, ownership, and allows to quickly restore unwanted changes.	Azure AD Office 365 Backup
1.2.1	6030	A role named Global Administrators has been added allowing you to delegate access to Cayosoft Guardian. You can now add additional administrators to Cayosoft Guardian with Configuration > Global Administrators role. Membership in the role can be users and groups from Active Directory or Azure AD. These users will be granted full product access to be able to track changes in connected systems, restore unwanted changes, and update product configuration. Additional roles are being planned.	Service

1.2.1	4265	An Alert for Guardian Web Portal Connection Health has been added. Cayosoft Guardian now checks connection credentials and permissions in connected systems and sends an alert when issues are detected. For example, as Cayosoft Guardian is extended with new capabilities, a set of new permissions may be required to collect data your Office 365 / Azure AD tenant. The requirement to update your Azure AD consent would be reported through such a global alert after an upgrade.	Service
1.2.1	4788	Event data collection now includes Microsoft Office 365 Audit Logs in addition to Azure AD Logs for activity initiator and event date/time. Now Cayosoft Guardian collects Office 365 Unified Audit Log to track and discover initiator for changes made outside Azure AD. For example, the initiator for changes in Microsoft Teams policies is discovered through Office 365 Unified Audit Log.	Change Au
1.2.1	5337	"Load more" function has been added to Change History and other lists that exceed 100 records. By default, 100 records are displayed, and when you scroll to the bottom of the list a the Load More link appears. Clicking the Load More link displays an additional 100 records.	Usability
1.2.1	5563	Object properties for linked objects can now be opened in the Web Portal. For example, you can now open changed object properties from the Change History record for this object.	Usability
1.2.1	5710	A "break glass" access feature now provides members of the local Administrators group on the machine running the Cayosoft Guardian Service Global Administrator level access.	Security
1.2.1	5837	Additional reliability for tenant access has been added. Cayosoft Guardian requires administrative consent. Now you can grant consent manually if Cayosoft sign-in redirection cloud service is experience service issues.	Service
1.2.1	5931	Now you can use these filters for live browsing of groups in Office 365 / Azure AD tenant: • All Groups • Groups With Teams • Groups Synced With On-Premises • Groups With Dynamic Membership • Office 365 • Security	Usability
1.2.1	5950	Following Microsoft requirements, Cayosoft Guardian now supports LDAP channel signing and LDAP binding when connecting to the Active Directory Domain Controllers.	Active Dir Backup
1.2.1	5958	Cayosoft Job Execution alerting has been tuned to remove Success Alerts for scheduled jobs as they are unnecessary. Failures and the results of manual executions will continue to provide both Success and Failure alerts.	Alerting

1.2.1	6011	Messaging related to Hybrid Restore Jobs has been improved. Target system information was added to messaging reported by the restore job, for attributes that were ignored. Target system information is helpful when reading details for hybrid restore job, that combines restore actions in various systems.	Hybrid Re
1.2.1	4182	Dozen of minor user interface bugs were fixed in different areas of the product.	Usability