

DATASHEET

Cayosoftware Guardian
Real-Time Monitoring, Rollback &
Compliance for Microsoft
Environments

Built For Hybrid AD

Overview

Cayosoft Guardian Base delivers real-time hybrid AD change monitoring, instant rollback, and audit-ready visibility to secure identities and enforce compliance across Microsoft environments. Purpose-built for hybrid environments, it helps IT and security teams detect unauthorized changes, prevent privilege escalation, and maintain audit-ready compliance—without agents, scripts, or manual recovery processes.

Whether you're securing identities, stopping privilege escalation, or preparing for audits, Guardian delivers the control and clarity hybrid environments demand.

Top 3 Benefits



Hybrid Identity Visibility in Real Time

Track identity changes across on-prem AD and Entra ID—user attributes, group memberships, policy shifts, and more.

- Surface indicators of exposure, compromise, or attack
- Get real-time alerts and full context on who changed what, when, and where



One-Click Rollback Without Backups

Undo risky or mistaken changes instantly—with no restore points, scripts, or domain controller reboot.

- Roll back attribute-level, object-level, or group membership changes
- Recover from misconfigurations or malicious edits in seconds



Built for Hybrid Security and Compliance

Achieve Zero Trust-aligned identity governance with audit-ready logs, immutable change tracking, and SIEM integration.

- Prebuilt compliance reporting (SOX, HIPAA, GDPR, etc.)
- Role-based access controls (RBAC) and separation of duties built-in

Who It's For

Primary Buyers

- IT Security / IAM Leads
- SOC Analysts & DR Planners

Secondary Buyers

- IT Managers & AD Engineers
- Compliance / GRC Officers

Key Capabilities

Continuous Hybrid Monitoring

- Track changes across AD, Entra ID, Exchange Online, Intune, and Teams
- Detect privilege escalations, dormant account activity, and GPO edits
- Log all changes with full context (who, what, when, where)

Rollback Engine

- Reverse changes at the attribute, object, or group level
- No backup files, scripts, or downtime required
- Roll back misconfigurations, malicious changes, or bulk updates

Zero Trust-Ready

- Role-based access control with virtual OUs for delegated scopes
- Tamper-evident audit trail with secure change logging
- Aligns with Zero Trust, least privilege, and compliance frameworks

Audit & Reporting

- Immutable audit logs exportable to CSV, JSON, and PDF
- Scheduled reports for identity drift, admin changes, and access anomalies
- Prebuilt templates for SOX, HIPAA, PCI, GDPR, and more

Deployment Simplicity

- Agentless install—no changes to domain controllers or Entra ID
- Deploy in hours on Windows Server VM or physical server
- Scales to 100K+ identities and supports multi-domain, multi-tenant environments

Differentiators That Matter

| Feature | Cayosoft Guardian | Legacy Tools |
|------------------------|--------------------------|-----------------------|
| Real-Time Monitoring | Yes – Hybrid native | Partial or siloed |
| One-Click Rollback | Yes – No backup required | Manual/scripted |
| Agentless Deployment | Yes | Often required |
| Immutable Audit Trail | Built-in | Add-on or third-party |
| SIEM/Alert Integration | Syslog/Sentinel native | Manual setup |
| Compliance Reporting | Prebuilt + Custom | Manual effort |

Technical Highlights

Real-Time Change Engine

- Tracks identity changes across AD and Entra ID
- Captures object/attribute changes, deletions, group activity, GPO edits

Rollback & Recovery

- Instantly reverse unauthorized changes
- Object-level and attribute-level rollback without downtime

Zero-Trust Architecture

- RBAC/ABAC with audit trails and access zone scoping
- Clean separation of duties for secure operations

SIEM-Integrated Alerts

- Custom thresholds for privilege changes, deletions, bulk updates
- Integrates with Splunk, Sentinel, QRadar, and other tools

Proof Points

State Agency reduced audit prep from days to minutes with Guardian's built-in hybrid change reporting.

The Enterprise Security Team instantly recovered from privilege escalation—there was no downtime or impact on users.

The hybrid Identity Admin Team tracks and resolves all unauthorized changes before they become security incidents.

Summary

Cayosoft Guardian provides hybrid identity protection with real-time monitoring, secure rollback, and compliance readiness—without complexity. It gives IT and security teams the visibility and control they need to manage risk, stop privilege misuse, and respond to identity-layer threats before they become incidents.

Learn More or Request a Demo

www.cayosoft.com/demo