DATASHEET

Cayosoft Guardian Audit & Restore

Detect Threats. Reverse Risky Changes. Protect Hybrid Identity.

Real-Time Hybrid Identity Monitoring, Threat Detection, Rollback, and Compliance for Active Directory, Entra ID, and Microsoft 365

Identity is the control plane of your business.

Any change to users, groups, roles, policies, applications, or privileges can impact security, operations, and compliance. Yet most organizations still rely on fragmented native tools, scripts, SIEM alerts, and manual investigation to understand what changed and how to recover.

Cayosoft Guardian Audit & Restore continuously monitors Active Directory, Microsoft Entra ID, Exchange Online, Microsoft Teams, Intune, and Microsoft 365 to detect risky changes, identify identity threats, and instantly reverse unauthorized modifications before they become outages, breaches, or audit findings.

Purpose-built for hybrid Microsoft environments, Guardian delivers the visibility, control, and resilience required for modern Zero Trust security.

Why Organizations Choose Cayosoft Guardian Audit & Restore

Detect Identity Threats Before They Become Incidents

Gain real-time visibility into identity changes across hybrid Microsoft environments.

Monitor:

- Active Directory
- Microsoft Entra ID
- Exchange Online
- Microsoft Teams
- Microsoft Intune
- Microsoft 365

Detect:

- Privilege escalation attempts
- Unauthorized administrative changes
- Group membership abuse
- Suspicious account activity
- Configuration drift
- Policy changes
- Indicators of Exposure (IOEs)
- Indicators of Compromise (IOCs)

Benefits:

- Reduce identity attack surface
- Accelerate threat detection
- Improve SOC visibility
- Strengthen Zero Trust initiatives

Reverse Risky Changes in Seconds

Most tools can tell you something has changed.

Instantly roll back:

- User changes
- Group membership changes
- Object deletions
- Attribute modifications
- Administrative actions
- Policy changes

No:

- Backup restores
- PowerShell scripts
- Domain controller recovery
- Downtime

Benefits:

- Stop security incidents from spreading
- Recover from mistakes immediately
- Reduce operational disruption
- Eliminate manual recovery processes

Maintain Continuous Compliance

Compliance requires proof. Guardian provides complete visibility into who changed what, when, where, and why.

Built-in reporting supports:

- SOX
- HIPAA
- PCI-DSS
- CJIS
- GDPR
- Internal governance initiatives

Capabilities include:

- Immutable audit trails
- Scheduled reporting
- Audit-ready dashboards
- Separation of duties
- Role-based access controls
- SIEM integration

Benefits:

- Accelerate audit preparation
- Reduce compliance risk
- Improve governance
- Simplify reporting

Key Capabilities

Real-Time Hybrid Change Monitoring

- Continuous monitoring across AD, Entra ID, Exchange Online, Teams, Intune, and Microsoft 365
- Real-time alerting on privileged changes
- Complete change context and history
- Identity threat visibility across hybrid environments

Identity Threat Detection

- Privilege escalation detection
- Excessive permissions monitoring
- Administrative activity tracking
- Security policy monitoring
- Attack path visibility

One-Click Rollback

- Object-level recovery
- Attribute-level recovery
- Group membership recovery
- Bulk change reversal
- No backup dependency

Zero Trust Enforcement

- RBAC and ABAC support
- Separation of duties
- Delegated administration controls
- Audit accountability
- Identity governance support

SIEM and SOC Integration

- Microsoft Sentinel
- Splunk
- QRadar
- Syslog
- Existing security workflows

Enterprise Scalability

- Agentless deployment
- Multi-domain support
- Multi-forest support
- Multi-tenant support
- 100,000+ identities

How Guardian Audit & Restore Works

Guardian continuously captures identity activity across your Microsoft environment and creates a tamper-evident audit history of every change.

When risky or unauthorized activity occurs, administrators can:

1. Detect the change immediately
2. Understand who made it and its impact
3. Investigate related activity
4. Roll back the change instantly
5. Restore security and compliance

The result is a shift from reactive investigation and recovery to proactive identity protection.

Why Cayosoft

Capability	Cayosoft Guardian Audit & Restore	Native Tools & Legacy Solutions
Real-Time Hybrid Monitoring	✓	Limited
Active Directory Monitoring	✓	Partial
Entra ID Monitoring	✓	Partial
Exchange, Teams & Intune Monitoring	✓	Limited
One-Click Rollback	✓	No
Agentless Deployment	✓	Often Requires Agents
Immutable Audit Trail	✓	Add-On Required
Compliance Reporting	✓	Manual Effort
SIEM Integration	✓	Custom Development
Zero Trust Support	✓	Limited

Built for Microsoft Identity Resilience

Guardian Audit & Restore helps organizations:

- Detect identity threats faster
- Reduce attack surface exposure
- Enforce Zero Trust controls
- Recover from mistakes instantly
- Maintain continuous compliance
- Protect hybrid Microsoft environments

From Active Directory and Entra ID to Exchange Online, Teams, Intune, and Microsoft 365, Guardian delivers the visibility, rollback capabilities, and operational resilience modern enterprises require.

Customer Outcomes

State Government Agency

Reduced audit preparation from days to minutes through automated hybrid identity reporting.

Enterprise Security Team

Recovered from a privileged access misconfiguration in seconds with no user impact or downtime.

Hybrid Identity Operations Team

Continuously identifies and remediates unauthorized changes before they become security incidents.

Learn More

Schedule a personalized demo and see how Cayosoft Guardian Audit & Restore protects hybrid Microsoft environments with real-time monitoring, threat detection, rollback, and compliance visibility.