TECHNICAL BRIEF

Supported Recovery Scenarios in Guardian Instant Forest Recovery

Published:
2026

Sponsored by:
Cayosoft

+1 (614) 423-6718

One Platform for Every Identity Recovery Scenario

Active Directory, Entra ID, Intune and Microsoft 365 failures do not follow a single pattern. Identity incidents range from simple administrative mistakes to widespread corruption, ransomware, and complete forest level compromise. Most organizations address these risks with disconnected tools, manual processes, or recovery approaches that only work for a narrow set of scenarios.

Cayosoft Guardian Instant Forest Recovery (Guardian) is designed differently. It is a single, integrated solution that supports the full spectrum of identity recovery scenarios, from granular object and attribute rollback to complete forest recovery in a clean, isolated environment. Guardian combines recovery, change management, and threat detection into one coordinated platform, allowing organizations to detect risky changes, reverse damage immediately, and execute validated recovery workflows when larger incidents occur.

By unifying change monitoring, threat detection, and operational disaster recovery across Active Directory and Microsoft Entra ID, Guardian eliminates guesswork during incidents and ensures the right recovery method is applied every time, based on the scope and severity of the failure.

Leading with Innovation: Guardian's Patented Instant Standby

Leveraging patented methodology and technology, Guardian ensures rapid recovery in minutes of full scale disasters while adhering to AD best practices. Its unique approach encompasses not only data restoration but also crucial elements like metadata and DNS cleanup, guaranteeing a healthy and functional forest post-recovery.

With Guardian, each step of the process is recorded, providing detailed reports and triggering alerts in the event of errors during backup or recovery. In contrast to monitoring AD with native tools, Cayosoft helps you eliminate the complex task of manually parsing and correlating logs from multiple domain controllers and Entra ID for continuous monitoring.

Guardian can validate the Active Directory disaster recovery plan by restoring a forest to a recovery site. Deploying the recovery site in Azure or AWS can allow Guardian to configure virtual machines automatically with the appropriate network and operating system settings for the recovery site network. This feature is known as Instant AD Forest Recovery.

Integrated Change Management and Threat Detection with Recovery

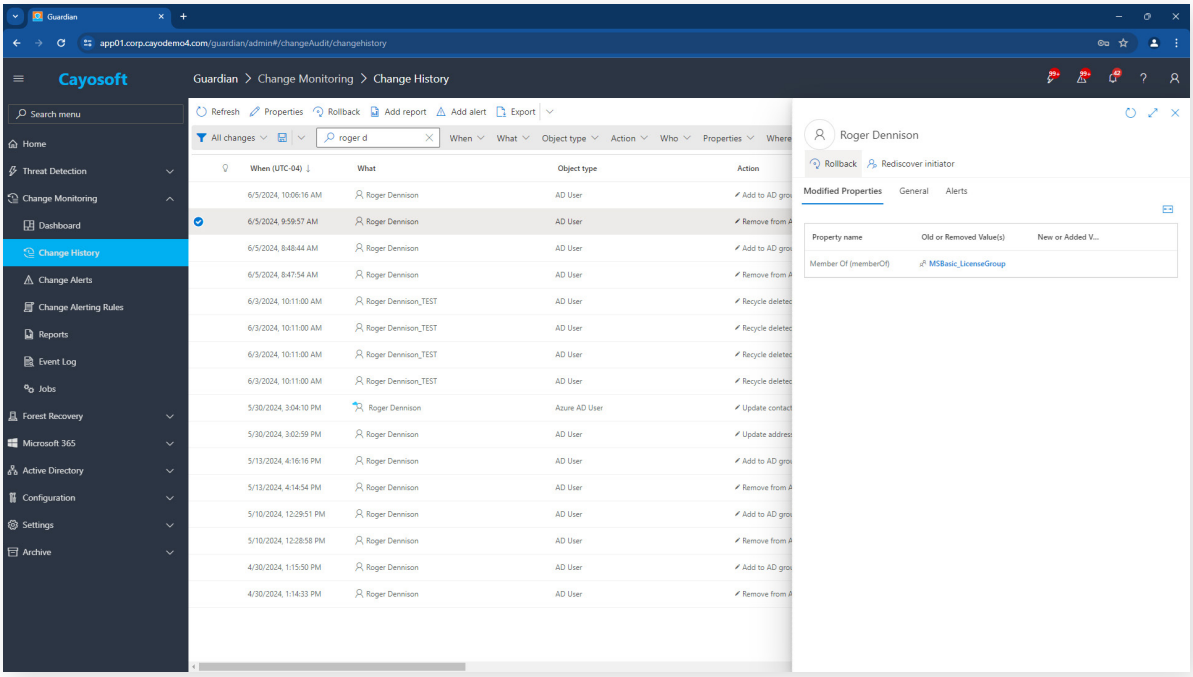
With Cayosoft Guardian, changes to objects are tracked and stored. Creating a job under the Change Monitoring configuration lets you define which objects are protected and excluded from the Change Monitoring feature. Additionally, change history records can be exported.

Cayosoft Guardian extends its comprehensive protection to Entra ID (Azure AD), safeguarding critical objects like users, groups, and application registrations. For some use-cases, this may be particularly important as many items in Azure can be permanently deleted, bypassing the recycle bin or extending past the 5-day window of Microsoft Entra Backup and Recovery.

Leveraging the Microsoft Graph API, Guardian provides unparalleled change tracking and restoration capabilities for Entra ID objects of user objects at both the object and attribute levels, even after they've been hard/permanently-deleted from AD.

Guardian's extensive restoration capabilities cover a wide range of Entra ID objects:

- **Users** (Includes guest users and users synced from AD)
- **Groups** (Includes assigned groups and dynamic groups)
- **Devices**
- **Roles**
- **Administrative Units**
- **Policies**
- **Enterprise Apps** (Security Principals)
- **App Registrations** (Application Objects)
- **And more...**



Cayosoft Guardian restoring a user object from the Change Records view

Microsoft Hybrid Identity Recovery Scenarios Supported

Below is a summary of the most frequent AD recovery scenarios and the recommended recovery options using Cayosoft Guardian.

Scenario	Recommended Recovery Method with Cayosoft Guardian	Recovery Scope	Why This Matters
Accidental Deletion of Active Directory Objects	Guardian Change History Object-level rollback	Users, groups, computers, GPOs	Restores deleted identities with original attributes and access without affecting healthy objects
Attribute-level Corruption or Overwrite	Guardian Change History Attribute rollback	Specific attributes	Reverses unwanted attribute changes without rolling back entire objects
Entra ID, M365, and Intune Recovery	Guardian Change History Rollback	Object and Attribute level rollback	Rollbacks and restores objects, attributes and restores objects that bypass Microsoft Recycle Bin
Accidental Organizational Unit (OU) Deletion	Guardian AD DC recovery Plan Authoritative container restore (Single DC)	Entire OU structure	Rebuilds deleted OUs and nested objects consistently
Domain Controller Failure	Guardian AD DC recovery Plan Non-authoritative domain controller restore.	Single DC	Safely rebuilds a failed DC and synchronizes with healthy DCs
Domain Corruption	Guardian AD DC recovery Plan Authoritative domain restore.	Entire domain	Restores the domain from clean backup data in a consistent state
Forest-wide Disaster (On-Premises)	Guardian AD Forest Recovery Plan	Entire forest	Automatically restores the entire forest to pre-existing servers using standardized Microsoft aligned steps
Forest-wide Disaster: Standby Forest Recovery	Guardian Standby Forest Recovery Plan (Azure or AWS)	Entire forest	Provides rapid restoration using a clean cloud-based recovery forest
Ransomware Attack: Forest-wide Impact	Guardian Standby Forest Recovery Plan (Azure or AWS)	Entire forest	Best option when on-premises infrastructure is compromised and unsafe

Accidental Deletion of Active Directory Objects

Accidental deletion frequently affects users, groups, computers, and GPOs during cleanup or administrative tasks.

Why it matters:

Access breaks immediately; licensing fails, and applications dependent on group membership or attributes stop working.

Why this method:

Object-level restore is the most efficient way to recover deleted data without impacting healthy AD components.

How Recovery Works:

- Use Guardian one-click rollback
- Changes are reversed directly in the existing production environment

Key Point: This is rollback, not disaster recovery. No servers, no rebuilds, no downtime

Attribute-level Corruption or Overwritet

Scripts, sync tools, or misconfiguration can unintentionally overwrite attributes across hundreds of objects.

Why it matters:

Incorrect attributes break access, misconfigure licenses, or disrupt cloud identity synchronization.

Why this method:

Attribute rollback restores only what changed, reducing business impact and avoiding overcorrection.

How Recovery Works:

- Use Guardian one-click rollback
- Changes are reversed directly in the existing production environment

Key Point: This is rollback, not disaster recovery. No servers, no rebuilds, no downtime

Accidental Deletion or Attribute Level Entra ID, M365, and Intune

Accidental deletion frequently affects users, groups, devices, policy, and Entra applications during cleanup or administrative tasks.

Why it matters:

Access breaks immediately; licensing fails, and applications dependent on group membership or attributes stop working or conditional access poicy changes weaken security.

Why this method:

Object-level restore is the most efficient way to recover deleted or changed data without impacting the rest of tenant.

How Recovery Works:

- Use Guardian one-click rollback
- Changes are reversed directly in the existing production tenant

Key Point: This is rollback, not disaster recovery.

Accidental Organizational Unit (OU) Deletion

Entire OUs can be deleted accidentally, along with all nested objects.

Why it matters:

Departments or locations may lose access completely; GPO links vanish, and automation fails.

Why this method:

Authoritative container restore accurately rebuilds the OU and child objects.

How Recovery Works:

- Uses Guardian recovery to existing production
- Authoritative restore of the affected partition or container

Key Point: Production remains in place. Only the affected scope is recovered. No servers, no rebuilds, no downtime

Domain Controller Failure

Hardware issues, OS corruption, or configuration problems can make a DC unusable.

Why it matters:

Authentication may slow or fail, and replication topology suffers.

Why this method:

A non-authoritative DC restore quickly returns the DC to service and updates it using healthy DCs.

How Recovery Works:

- Guardian supports to recover a DC to pre-deployed hardware or VM
- Rarely used in practice

Why It Is Rare:

- Most organizations do not back up every DC
- It is often faster and simpler to build a new DC by installing Directory Services and promoting it

Key Point: Supported, but not the common path.

Domain Corruption

A domain may become unstable due to replication issues, schema changes, or misconfiguration.

Why it matters:

Authentication outages and replication failures spread quickly.

Why this method:

Authoritative domain restore ensures the domain is rebuilt using clean data.

How Recovery Works:

- Restore to pre-deployed hardware or VMs with OS
- Infrastructure may be virtual or physical
- Recovery uses validated backups

Key Point: This is not standby. Infrastructure must already exist before the incident.

Forest-wide Disaster (On-Premises)

Forest-level corruption can occur due to misconfiguration, schema issues, or catastrophic operational mistakes or ransomware event.

Why it matters:

Identity becomes unavailable across the enterprise.

Why this method:

An AD Forest Recovery Plan coordinates the rebuild of all domains and DCs.

How Recovery Works:

- Restore to pre-deployed hardware or VMs with OS
- Infrastructure may be virtual or physical
- Recovery uses validated backups

Key Point: This is not standby. Infrastructure must already exist before the incident.

Forest-wide Disaster: Standby Forest Recovery

Organizations sometimes require recovery into a safe, isolated environment such as Azure or AWS.

Why it matters:

Clean recovery avoids issues linked to compromised on-prem systems.

Why this method:

Standby Forest Recovery uses a preconfigured cloud environment for rapid, clean restoration.

How Recovery Works:

- Cloud Instant Standby Forest Recovery
- Immediate cutover to a clean, isolated standby forest

Key Point: No rebuilding. No dependency on compromised infrastructure. Fastest recovery option.

Ransomware Attack: Forest-wide Impact

Ransomware increasingly targets identity infrastructure. This is the best option for Ransomware recovery if your organization supports cloud recovery. If you can't support cloud recovery, use forest wide disaster on premises.

Why it matters:

Compromised DCs and corrupted replication make on-premises recovery risky. Reinfection is likely if compromised systems are reused.

Why this method:

Standby Forest Recovery provides the safest option by rebuilding AD in a clean, isolated cloud forest.

How Recovery Works:

- Cloud Instant Standby Forest Recovery
- Immediate cutover to a clean, isolated standby forest

Key Point: No rebuilding. No dependency on compromised infrastructure. Fastest recovery option.

Conclusion

Active Directory and Entra ID recovery is not a single problem with a single solution. As this document demonstrates, different failure scenarios demand different recovery strategies, from granular object rollback to full forest recovery in a clean, isolated environment. Applying the wrong approach can increase downtime, amplify risk, and extend business disruption.

Cayosoft Guardian Instant Forest Recovery provides a complete, identity first recovery framework that spans prevention, rollback, and disaster recovery across on-premises Active Directory and Microsoft Entra ID. With patented instant standby forest technology, integrated change monitoring, and proven recovery workflows aligned to Microsoft best practices, Guardian enables organizations to recover quickly, safely, and with confidence, even in the face of ransomware or catastrophic identity failure.

By matching the right recovery method to the right incident, organizations can eliminate guesswork, reduce recovery time, prevent reinfection, and ensure identity services are restored as a foundation for business continuity.