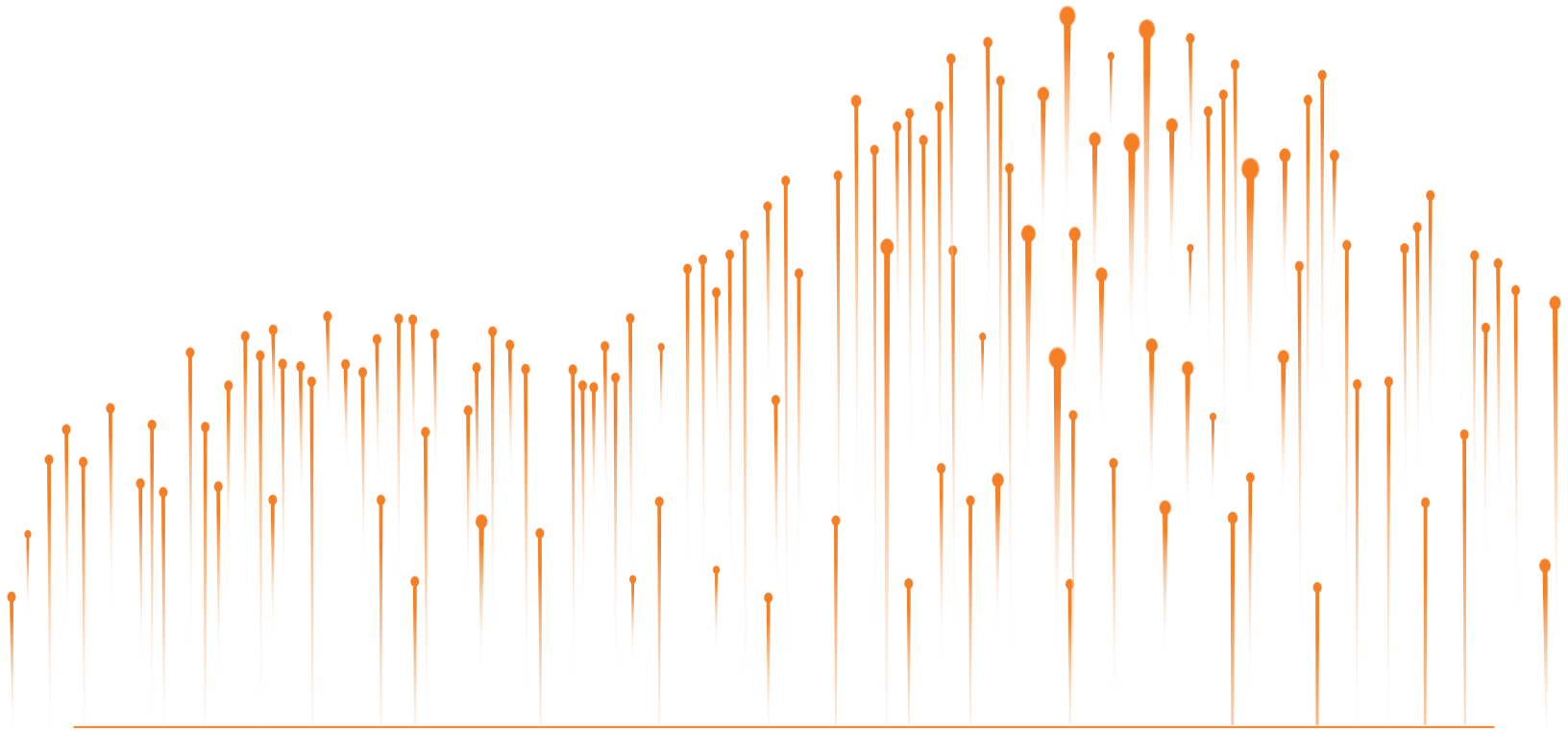
TECHNICAL BRIEF

Controlled Cutover for Active Directory Forest Outage and Ransomware Scenarios

Cayosoft Guardian Instant Forest Recovery

Cutover for Forest Outage (Non-Ransomware) and Full Ransomware



Published:
2026

Sponsored by:
Cayosoft

+1 (614) 423-6718

OVERVIEW

Cayosoft Guardian Instant Forest Recovery supports controlled cutover to a validated standby Active Directory forest hosted in an isolated Azure or AWS recovery site.

This brief defines two operationally distinct cutover scenarios that require different assumptions and decision logic:

- **Scenario 1: Forest Outage (Non Ransomware)**

  Active Directory is down due to corruption or operational failure, but the organization is not operating under an active ransomware or breach assumption.

- **Scenario 2: Full Ransomware**

  The production environment is untrusted or unavailable, and threat analysis plus change history analysis are required to determine which standby forest can be safely activated.

CORE PRINCIPLE: CUTOVER IS CONTROLLED ACTIVATION

Guardian's standby model shifts identity recovery work ahead of the incident by maintaining a clean, validated standby forest in an isolated cloud recovery site.

Cutover is not a rebuild. It is a controlled activation of a pre validated identity control plane.

Across both scenarios, cutover focuses on three consistent outcomes:

- Select the correct standby forest instance for the incident
- Activate the standby forest and apply required network and DNS configuration changes
- Pass validation gates that confirm forest health and administrative access before declaring cutover complete

ARCHITECTURE SUMMARY

PRODUCTION IDENTITY ENVIRONMENT

Guardian provides continuous visibility through threat detection and change monitoring. This visibility supports both early detection of risky changes and post-incident root cause analysis when Active Directory becomes unstable or unavailable.

ISOLATED RECOVERY SITE (AZURE OR AWS)

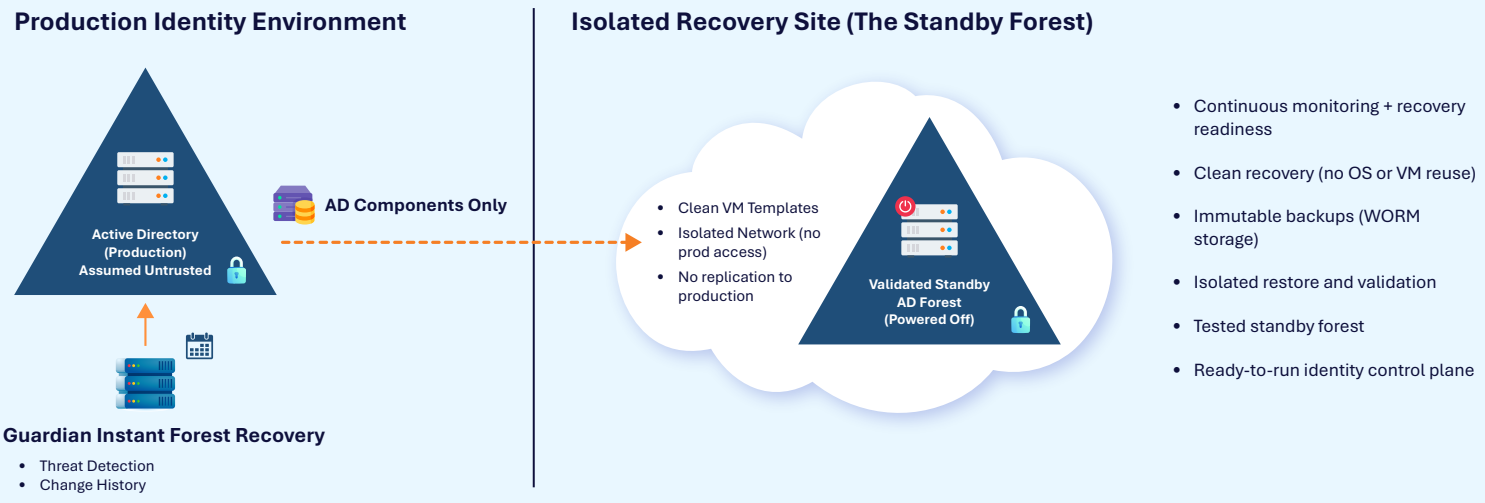
Guardian maintains a clean, isolated standby forest hosted in Azure or AWS. The recovery site is independent of production domain controllers, operating systems, and infrastructure dependencies.

STANDBY FOREST OUTCOME

The standby forest exists as a ready to run recovery target. When activated, it becomes the authoritative identity control plane through controlled network and DNS actions, rather than through emergency rebuild steps.

Cayosoft Guardian Instant Forest Recovery

Clean, Validated, Tested Standy AD Forest (AZURE/AWS)



Guardian continuously monitors identity, builds clean recovery points, and maintains a validated standby forest so recovery is a controlled activation, not a rebuild under pressure.

SCENARIO 1:
FOREST OUTAGE CUTOVER (NON RANSOMWARE)

SCENARIO DEFINITION

A non-ransomware forest outage occurs when Active Directory becomes unavailable due to corruption or operational failure, without assuming an active adversary has compromised the environment.

Common triggers include:

- Schema corruption or failed schema updates
- Bad patches or failed upgrades
- Replication failures or DC cascades
- Directory database or SYSVOL corruption

This scenario does not assume attacker persistence.

OBJECTIVE

Restore authentication and directory services quickly by cutting over to a validated standby forest, then use change monitoring to identify the root cause and prevent recurrence.

ASSUMPTIONS

- Active Directory is down or unstable, causing authentication and application outages
- Core infrastructure required to execute cutover may still be available (cloud console, networking, admin workstations)
- The environment is treated as operationally failed, not adversarially compromised

STANDBY FOREST SELECTION

Standby selection in a non-ransomware outage is driven by service restoration and change window alignment, not breach containment.

- Use change monitoring to identify the outage trigger window such as schema changes, patches, or configuration updates
- Select the most recent standby forest instance that predates that window
- Threat detection data may be reviewed for context, but selection does not require an assume breach posture

CUTOVER EXECUTION (AZURE STANDBY FOREST EXAMPLE)

Activation of an Azure standby forest follows a controlled sequence:

- Power on all standby forest recovery site virtual machines and sign in using the break glass account
- Configure Azure network peering so the recovered AD environment is routable to the production network
- Configure DHCP to point clients to the standby recovered domain controllers for DNS and update any static DNS configurations
- Promote and deploy additional domain controllers from the standby recovered forest as required

VALIDATION GATES BEFORE DECLARING CUTOVER

Before declaring the standby forest authoritative, validate forest health and functionality:

- Replication health validation using repadmin
- Directory diagnostics using dcdiag
- DNS zone presence and name resolution validation
- Basic directory function testing (create, modify, delete object)
- Administrative access validation, including break glass sign in

STABILIZATION

After service restoration, use change monitoring to determine the root cause of the forest outage and confirm that corrective actions align to the identified failure window.

SCENARIO 2:
FULL RANSOMWARE CUTOVER (EVERYTHING DOWN)

SCENARIO DEFINITION

A full ransomware event is treated as a catastrophic identity outage where the production environment is untrusted or unavailable.

In this scenario, identity recovery must first establish a trusted control plane before broader restoration can occur.

OBJECTIVE

Select the correct standby forest using threat analysis and change history analysis, bring the chosen standby forest online in the isolated recovery site, and enforce strict post-breach change control while the environment is stabilized and hardened

STANDBY FOREST SELECTION (THREAT ANALYSIS + CHANGE HISTORY ANALYSIS)

The mechanical steps required to activate the standby forest including network connectivity, DNS configuration, and domain controller expansion are the same as those used in a non ransomware forest outage.

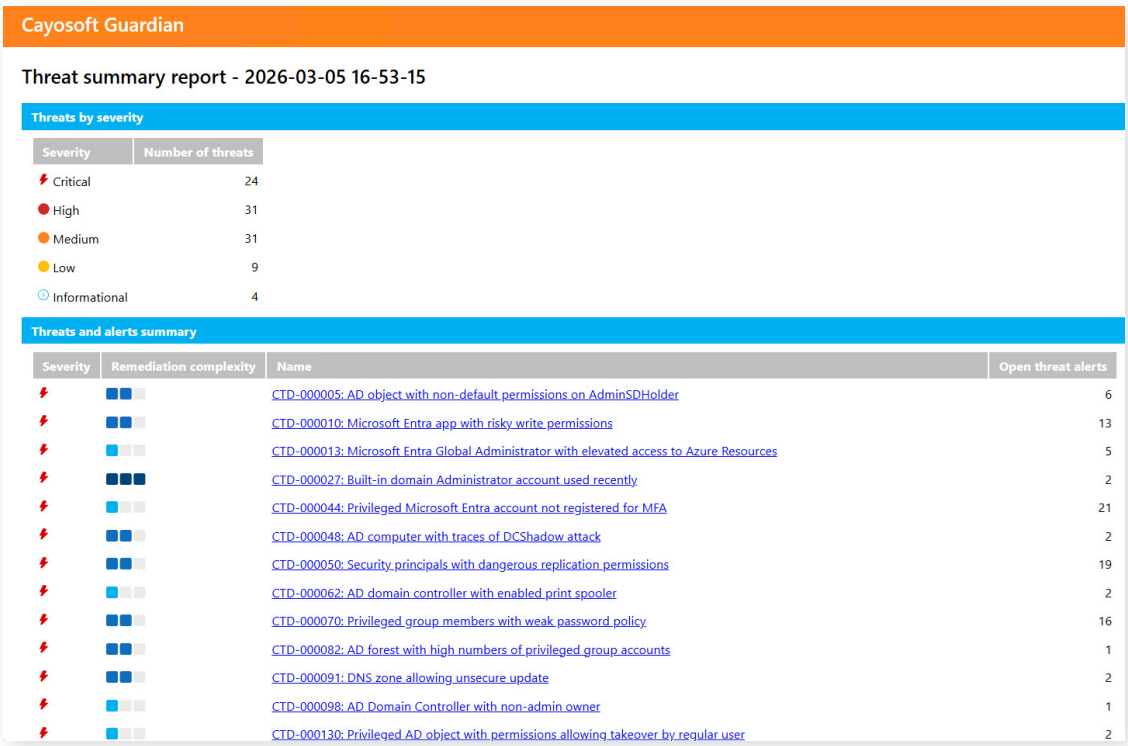
In a ransomware scenario, these steps are executed after standby forest selection and trust establishment, and under restricted change enforcement, to prevent reintroduction of compromised identity state.

Standby selection is the critical decision point in ransomware recovery because the compromise window is often uncertain.

Selection is based on three gates:

- **Threat analysis**

  Identify indicators of attack, privilege abuse, or configuration compromise



Cayosoft Guardian

Threat summary report - 2026-03-05 16-53-15

Threats by severity

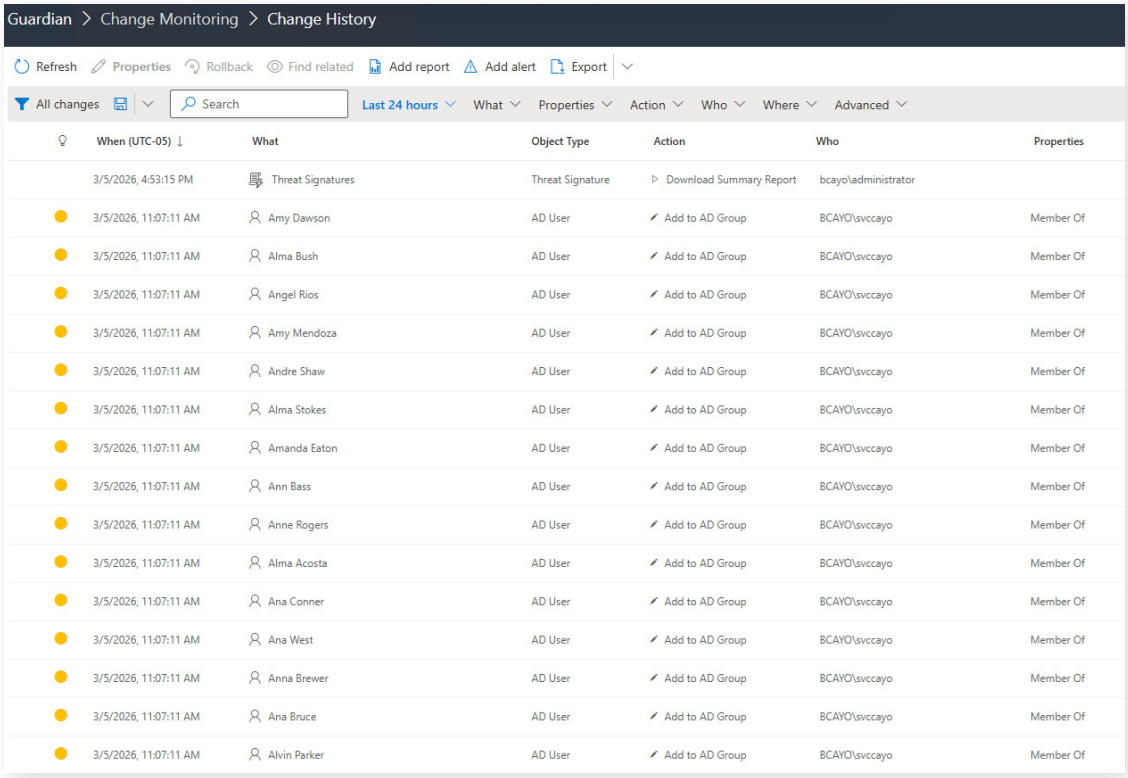
Severity	Number of threats
Critical	24
High	31
Medium	31
Low	9
Informational	4

Threats and alerts summary

Severity	Remediation complexity	Name	Open threat alerts
		CTD-000005: AD object with non-default permissions on AdminSDHolder	6
		CTD-000010: Microsoft Entra app with risky write permissions	13
		CTD-000013: Microsoft Entra Global Administrator with elevated access to Azure Resources	5
		CTD-000027: Built-in domain Administrator account used recently	2
		CTD-000044: Privileged Microsoft Entra account not registered for MFA	21
		CTD-000048: AD computer with traces of DCShadow attack	2
		CTD-000050: Security principals with dangerous replication permissions	19
		CTD-000062: AD domain controller with enabled print spooler	2
		CTD-000070: Privileged group members with weak password policy	16
		CTD-000082: AD forest with high numbers of privileged group accounts	1
		CTD-000091: DNS zone allowing unsecure update	2
		CTD-000098: AD Domain Controller with non-admin owner	1
		CTD-000130: Privileged AD object with permissions allowing takeover by regular user	2

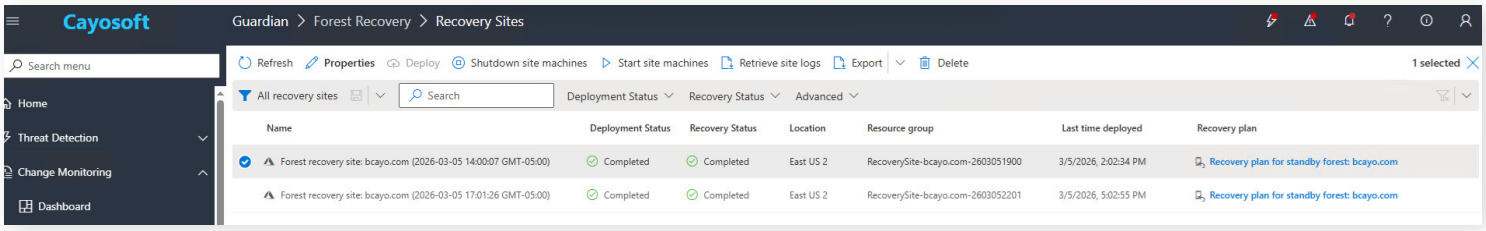
- **Change history analysis**

Establish the high-risk change window and understand what changed leading up to the incident



- **Standby selection**

Choose the standby forest instance that predates the compromise window using retained recovery points



CUTOVER EXECUTION: ESTABLISH TRUSTED CONTROL PLANE FIRST

Ransomware cutover prioritizes trust establishment:

- Bring the approved standby forest online in the isolated recovery site
- Maintain isolation from production until validation is completed
- Validate break glass access by interactive sign in to recovered domain controllers

Once the forest is online:

- Deploy a secondary Guardian server into the recovery environment
- Register the recovered forest in Guardian
- Create custom change alert rules to alert on or roll back changes not initiated by the break glass account
- Disable or restrict privileged accounts until Tier 0 hygiene is complete

During ransomware recovery, Guardian supports enforcement of break-glass-only change control. Configuration details are provided in Appendix A.

VALIDATION GATES BEFORE DECLARING CUTOVER

Before declaring cutover complete:

- Validate replication and directory health
- Confirm DNS functionality and name resolution
- Validate administrative access via break glass account
- Confirm custom change alerting is active

TRANSITION OUT OF RESTRICTED CHANGE ENFORCEMENT

Once the recovered standby forest has been validated as trusted and initial remediation activities are complete, restricted change enforcement can be intentionally relaxed.

This transition occurs only after:

- Forest health and replication validation succeeds
- DNS and authentication are stable
- Tier 0 hygiene activities are completed or actively governed
- No unexpected changes are observed during the restricted recovery window

At this point, organizations may:

- Gradually re enable administrative access beyond the break glass account
- Adjust or disable the temporary change enforcement rule
- Return to standard Guardian monitoring and alerting policies

This ensures the recovery environment remains protected during the highest risk period, while allowing a controlled return to normal operational governance.

SUMMARY: CLEAN SCENARIO SEPARATION

FOREST OUTAGE (NON RANSOMWARE)

Cutover is driven by rapid restoration of Active Directory service and alignment to the failure window identified through change monitoring.

FULL RANSOMWARE

Cutover is driven by trust establishment, threat analysis, and selection of a standby forest that predates attacker activity.

WHY THIS MATTERS

Guardian supports both scenarios without forcing a one size fits all recovery model. Organizations can restore service quickly when AD fails operationally and recover safely when identity itself has been compromised.

APPENDIX A: POST BREACH CHANGE CONTROL CONFIGURATION (RANSOMWARE SCENARIO)

PURPOSE

During a full ransomware recovery, the recovered standby forest must remain protected from unauthorized or residual identity changes while remediation and hardening activities are performed.

Guardian supports this requirement by enforcing break glass only change control, ensuring that only explicitly trusted recovery identities can modify the directory during the recovery window.

WHEN THIS CONTROL IS USED

This control is applied only during full ransomware recovery scenarios where:

- The production environment is untrusted
- Privileged credentials may be compromised
- Identity persistence must be actively prevented

It is not required for non ransomware forest outages.

CONTROL MODEL

Once the standby forest is activated:

- A break glass account is validated as the sole trusted administrative identity
- All other privileged identities are disabled or restricted
- Guardian monitors all directory changes in real time
- Any change not initiated by the break glass account is either:
  - Alerted on, or
  - Automatically rolled back, depending on policy

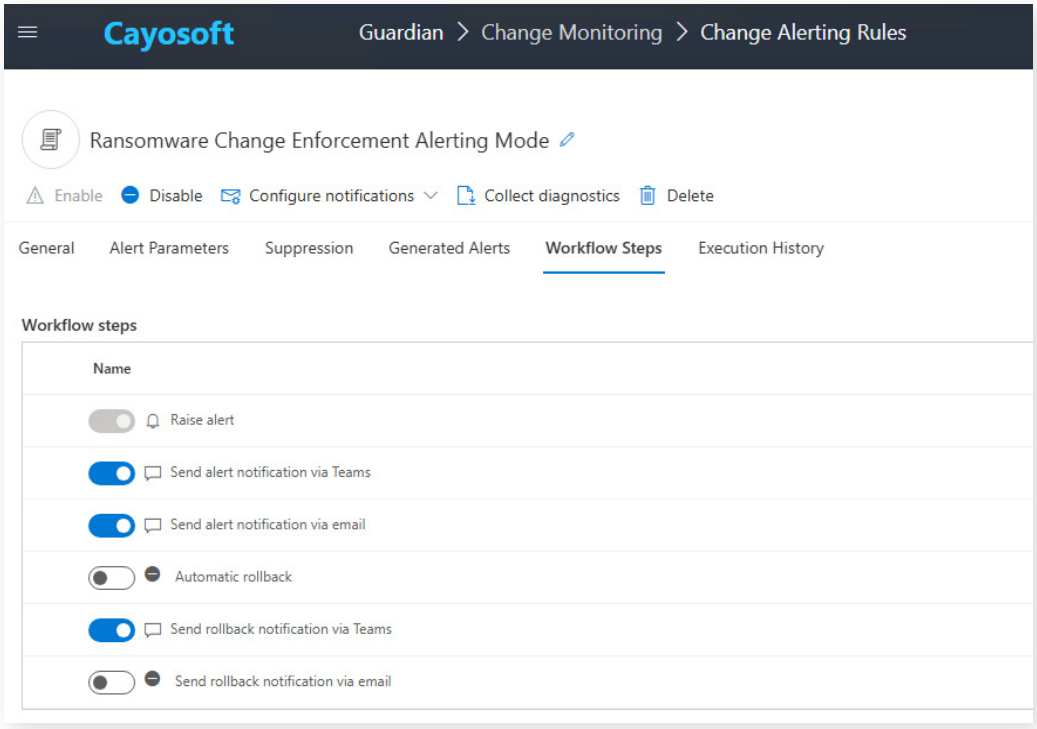
This creates a controlled identity reconstruction window where all changes are intentional, attributable, and auditable.

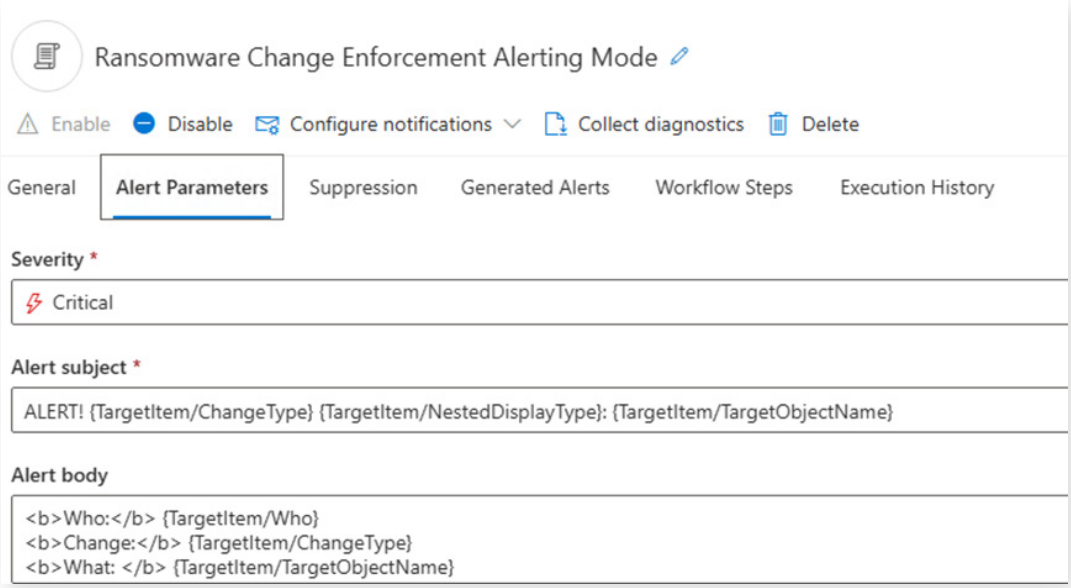
CUSTOM CHANGE ALERT RULE DEFINITION

The custom change alert rule enforces the following logic:

- **Scope:** Active Directory objects and attributes within the recovered forest
- **Allowed initiator:** Who (exclude) breakglass
- **Disallowed initiators:** All other users, service accounts, and automation
- **Action:**
  - Alert only, or
  - Alert and automatic rollback

All events are recorded for forensic and audit purposes.





OPERATIONAL OUTCOME

This control ensures that:

- No attacker controlled persistence can be reintroduced during recovery
- Recovery activities are fully attributable
- The standby forest remains a trusted identity control plane until normal operations resume