

CoreView Identity Resilience

Many tools tell you what changed on identities. CoreView Identity Resilience puts it back, in one click.

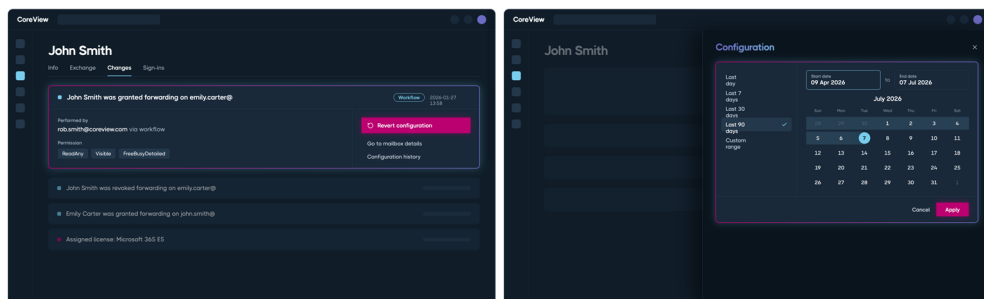
The Challenge: Putting identity state back after something breaks

Identity-impacting changes never stop in a Microsoft 365 tenant at scale. Delegated admins, scripts, lifecycle automations, and compromised accounts all move group memberships, licenses, and mailbox permissions away from where they should be. Logs tell you what changed, when, and by whom, but putting it back still falls to someone working by hand, leaving teams to deal with:

- Hours spent parsing audit logs
- Persistence changes that outlive the alert
- State rebuilt from memory and tickets
- No evidence the baseline was restored

The Solution: CoreView Identity Resilience

CoreView Identity Resilience enables IT and security teams to detect identity drifts in near-real time, restore to a known-good state, and prove the correct baseline was re-established.



What CoreView Identity Resilience does for you

See every identity change: Review 30 days of attribute, group, license, and mailbox changes from the user card, filtered to any window, with Microsoft and CoreView logs combined.

Restore prior state instead of rebuilding it: Return a changed attribute, membership, license, or mailbox permission to its previous value in a click, leaving the rest of the configuration intact.

Close the loop after a compromise: Mailbox forwarding and delegation are common persistence moves after a takeover. Both are tracked, and both can be reverted.

Track each change to its operator: Events name the admin or operator who performed them, and flag whether the change came through CoreView or from outside it.

Let the help desk fix its own mistakes: Grant operators read-only or revert rights, and require approval from an admin, the user's manager, or named approvers before a revert applies.

Detect, Restore, Prove

Identity Resilience turns detection into recovery. Three steps take a change from discovered to demonstrably fixed:

1. Detect

Find out what actually changed on an identity, without manually reconstructing it from raw audit logs.



2. Restore

Revert the most recent change of each type to its prior value, instead of rebuilding it from memory and tickets.



3. Prove

Hand an auditor a forensic record of what changed and how it was restored, instead of a screenshot and a ticket note.

What objects it covers

- User attributes
- Group membership and ownership
- Licenses and service plans
- Mailbox: permissions, delegation, forwarding, holds, and audit settings

Availability

Identity Resilience is available as an optional add-on to any CoreView plan.

Module	Tenant Resilience	Tenant Management
Platform Core Report on, manage and automate Entra ID and Exchange Online, with Corey Chat built in. 30+ playbook policies · 50+ management actions - Identity - Entra ID - Mail - Exchange Online - Playbooks & policy remediation - Corey Chat - CoreView action log	 Included	 Included
Configuration Resilience Back up tenant configuration, align it to industry baselines, detect drift, and restore the known-good state. - Tenant configuration, health & usage - Configuration backup - Baselines & drift detection - Restore the known-good state - Configuration change management - Multi-tenant configuration deployment	 Included	 Add-on
Operations Management Run every Microsoft 365 workload from one console: cross-workload reports, bulk actions, workflows and lifecycle templates. 100+ policies · 150+ actions, together with Platform Core - Cross-workload reports & governance dashboards - Collaboration workloads - Endpoint Manager / Intune reports, actions and playbooks - License optimization & chargeback - Workflows & third-party integrations - User lifecycle templates - Bulk actions & custom policies - Custom actions	 Add-on	 Included
Scoped Access Control Scope Microsoft 365 admin control with virtual tenants, delegated RBAC, license and number pools. - Virtual tenants - Delegated RBAC - License pools & number pools - Teams Voice delegation	 Add-on	 Included
Identity Resilience Track every change to users, groups, memberships and admin roles, and roll back accidental changes, misconfigurations or attacks.	 Add-on	 Add-on
Control for SharePoint Find and fix risky SharePoint file and folder permissions, sharing exposure, and storage sprawl.	 Add-on	 Add-on
Extended M365 Logs Retain Microsoft 365 unified audit log activity beyond the native window, then search, report and alert on it.	 Add-on	 Add-on
Hybrid Connector Manage cloud and on-premises AD/Exchange tasks from one CoreView interface.	 Add-on	 Add-on
Access Reviews Automate periodic reviews of user, guest, group, Teams, SharePoint and mailbox access, with an auditable record.	 Add-on	 Add-on
SIEM Connector Stream CoreView activity into Sentinel, Splunk or any SIEM for correlation and long-term analysis.	 Add-on	 Add-on