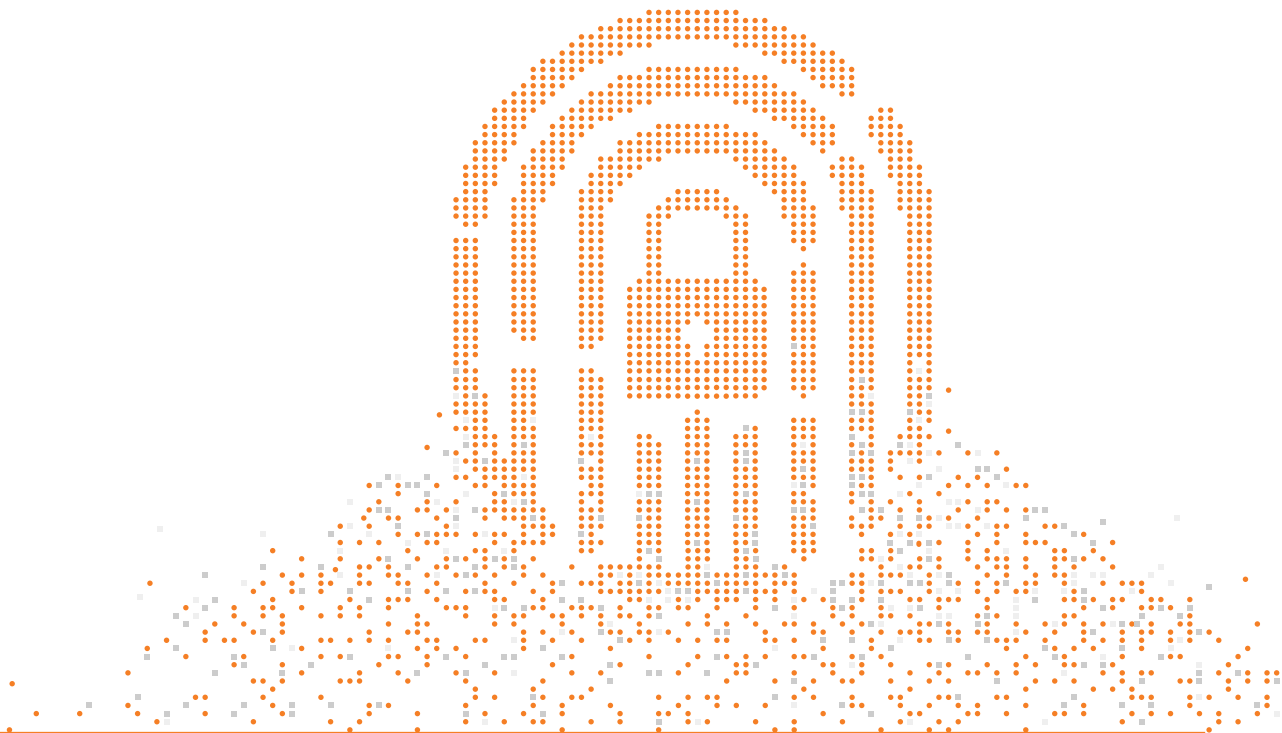


CASE STUDY

The Auto Club Group Modernizes and Strengthens Hybrid Identity Administration, Detection, and Recovery with Cayosoft

They have shifted left from reactive firefighting to identity resilience at enterprise scale.



Executive Summary

The Auto Club Group (ACG), one of the largest AAA clubs in North America, supports nearly 16 million members across 14 U.S. states, Quebec, and two U.S. territories. With vast volumes of PII and PCI data under management, identity security and operational continuity are mission-critical.

After a serious Active Directory incident exposed gaps in monitoring, change control, and recovery readiness, ACG's security leadership knew they needed a modern alternative to legacy and native Microsoft tools.

They selected the Cayosoft Enterprise Suite to:

- Continuously monitor hybrid Entra ID, Active Directory, and Microsoft 365
- Instantly roll back unwanted or malicious changes
- Reduce privilege exposure through secure delegation
- Implement instant recovery at the identity layer

The result is a purpose-built identity foundation that strengthens operational continuity, reduces risk exposure, and supports ACG's long-term modernization goals.

The Challenge:

Gaining Clear Visibility and Control Across Their Hybrid Identity Operations

ACG operates in a highly regulated environment with significant exposure to:

- Personally Identifiable Information (PII)
- Payment Card Industry (PCI) data
- Financial and insurance systems

The Breaking Point

An internal PowerShell script mistake severely disrupted the AD user base, disabling accounts and triggering days of downtime and recovery effort.

Native Microsoft tools provided logs, but:

- Too much noise
- Limited rollback capability
- No streamlined change intelligence
- No rapid, reliable remediation

The conclusion was clear:

They could not afford to be in that situation again.



Organization Profile

Industry: Insurance, Financial Services, Travel, Roadside Assistance

Members: ~14–16 million

IT Environment: Hybrid Active Directory, Microsoft Exchange, Microsoft 365

Scope: Hundreds of applications dependent on secure, resilient identity infrastructure

ACG's identity systems underpin financial services, member services, and internal operations. If AD is unstable, business stops.

Requirements

ACG defined clear, non-negotiable criteria:

- Real-time monitoring of hybrid AD changes
- Rapid, granular rollback
- Clear audit visibility (who, what, when, where)
- Secure delegation to minimize privilege risk
- Enterprise-grade reliability
- A technology partner, not just a vendor

They were not just buying software. They were investing in operational certainty.

The Solution

When an organization has almost 16 million users, protecting data is one of its highest priorities.

“We have a ton of PII and PCI data, and we have to make sure it's safeguarded. So, change management is critical, protecting identities is important - who did what, where, and how,” says Hussein Alalawi, Senior Security Information Engineer at ACG/AAA. Cayosoft Administrator + Guardian Instant Forest Recovery

ACG selected the Cayosoft Enterprise Suite to have full capability across its entire Microsoft identity environment.

Real-Time Hybrid Change Monitoring

Cayosoft provides continuous visibility across:

- Active Directory
- Microsoft 365
- Hybrid objects and permissions

ACG relies on Guardian Instant Forest Recovery for change intelligence and rollback.

“If you find something, click three buttons, reverse that change, and you're done. It's that easy.”

Instead of manually reconstructing object states or restoring from backup, the team reverses changes instantly, at the attribute level if necessary.

This shift from investigation to immediate correction dramatically reduces operational risk.

Instant Rollback Before A Change Becomes A Problem

Guardian Instant Forest Recovery captures every change and maintains a rollback catalog. If:

- An admin makes a mistake
- A script runs incorrectly
- A malicious change occurs

ACG can immediately reverse it.

No full domain restore.

No lengthy recovery window.

No guessing.

“You know how people ask what keeps you up at night? That doesn't keep me up at night anymore. It just works.”

Business Impact From Reactive Recovery to Identity Resilience

Before Cayosoft:

- Noise-heavy logs
- Script dependency
- Risky privilege models
- Manual recovery workflows

After Cayosoft:

- Real-time hybrid change visibility
- One-click rollback
- Controlled delegation
- “Set it and forget it” Confidence in recovery readiness

Strategic Benefits

- Reduced risk of extended outages
- Reduced reputational exposure
- Faster incident containment
- Improved compliance posture
- Greater executive confidence in IT resilience

As Alalawi summarizes:

“Time is money. The faster you recover, the less money you're losing. You don't want to be struggling and figuring things out. You want to see things are OK, click the button, and move on.”

Why ACG Chose Cayosoft

ACG didn't just choose features. They chose:

- Hybrid-native architecture
- Immediate rollback capability
- Secure delegation model
- Enterprise-grade monitoring
- Responsive partnership

“My interactions with the Cayosoft team were always so positive and focused on helping us, not just selling a product. We received such high levels of attention and the genuine desire for us to succeed with their solution. Cayosoft is a partner, not just a vendor.”

The Outcome

ACG now operates with:

- Continuous hybrid identity monitoring
- Instant rollback capability
- Reduced privilege risk
- Measurable operational efficiency
- Peace of mind at the identity layer

Cayosoft is Built for the Moments That Matter to The Auto Club Group

Hybrid Microsoft identity runs the business.

Cayosoft ensures it stays secure, governed, and recoverable, before a mistake, outage, or attack becomes a crisis.