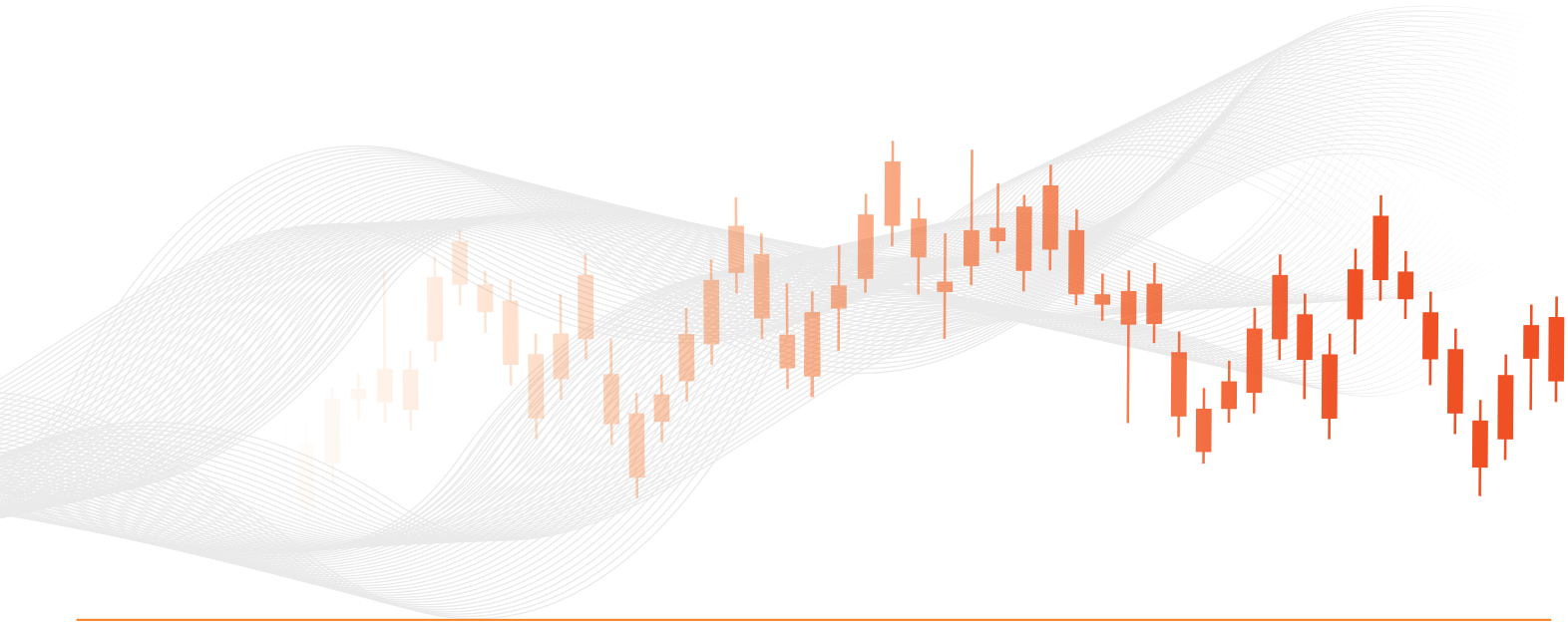
Cayosoft

CASE STUDY

Financial Services Organization Achieves Instant Active Directory Recovery

Cayosoft's breakthrough high availability and recovery capabilities for hybrid Active Directory win over legacy AD recovery tools



Published:
2025

Sponsored by:
Cayosoft

+1 (614) 423-6718

Summary

As ransomware attacks continue to increase, a prominent east coast fi financial services organization recognized the potentially devastating consequences an attack would pose to both business operations and to their clients. Cyberattacks directed against Active Directory (AD) and Azure Active Directory (Azure AD) pose a serious threat to business continuity for all Microsoft customers. Additional business crippling effects became growing concerns, like lost revenue, damage to reputation with their clients, and loss of industry credibility. With cyberattacks and breaches against high-value organizations, like theirs, they needed to become both resistant to and resilient from attacks. As such, hybrid AD recovery became an immediate priority for leadership.

The Challenge

To ensure business continuity and to protect their clients, the organization decided they must find a way to make their Microsoft platforms resilient. This included being prepared for the worst: planning for when an attack happens, not if an attack would happen.

Like 77% of all enterprises worldwide, the organization's on-premises Active Directory was configured in hybrid mode, meaning the on-premises AD identities are synchronized with cloud-based Entra ID. In hybrid mode, the on-premises AD is the authoritative directory and the source for user identities and access control across the organization. In other words, all employees rely on the Active Directory to sign in and perform their jobs.

If hybrid AD is down – business stops. During a business outage, every second is expensive, especially when considering the total cost of lost productivity, reputation, and sales. In order to be successful and meet recovery requirements, the solution had to provide resistance to outages and, when an outage occurs, drive the recovery time as close to zero as possible. The solution had to also be reliable, easy to test, easy to configure and maintain, and it had to eliminate the possibility of a failed forest recovery.

Finding a Partner

Initial research produced two vendors: Quest and Semperis, who provide legacy Active Directory forest recovery tools. Both vendors use a traditional approach for backup and recovery, that includes prestaged physical servers or virtual machines. Their research excluded traditional backup vendors, like Veeam, Metallic, and others. These vendors rely on server-based backups, which include the Windows operating system (OS) and, when used for recovery, reintroduces the malware.

East Coast Financial Group

Customer Profile

- Financial Industry
- 90+ years in business
- Over 20 branches with 700+ employees
- 250,000+ clients

Challenge

- Reduce outages & recover as quickly as possible
- Ensure hybrid AD is resilient from cyberattacks
- Solution must be easy to implement & maintain
- Eliminate forest recovery failures

Results

- Maintained business continuity with instant forest recovery
- Achieved resilience with instant change rollback & threat detection
- Implemented an all-in-one solution that is easy to deploy & maintain

Initially, Semperis appeared to offer the better tool of the two vendors selected. They began a proof of concept (POC) and procurement activities were initiated. During both activities dissatisfaction arose and the need for additional outside advice was determined. The evaluators then reached out to Gartner, a well-known industry source for research and consulting, and a meeting was set to discuss their recommendations.

During the Gartner consultation, the organization's requirements and progress choosing a solution were discussed. Gartner suggested that prior to moving forward with a purchase, the reviewers should consider Cayosoft's solutions. Shortly after the consultation, an initial call and demonstration was scheduled with Cayosoft and then a POC was initiated. At the completion of the POC, citing the unique features provided by Cayosoft, the decision was made to purchase the Cayosoft solution over the alternative.

The Chosen Path Forward

After review, the organization determined Cayosoft Guardian Forest Recovery was the best match for their hybrid AD resilience and recovery requirements.

Designed to protect businesses from costly AD outages caused by ransomware cyberattacks, wiper cyberattacks, unwanted changes, and directory data corruption, Cayosoft Guardian Forest Recovery is an all-in-one, instant recovery solution for all Microsoft directories, on-premises AD, hybrid AD, and Azure AD, and all major directory recovery scenarios, including AD object and attribute, partition, domain controller (DC), and forest recovery. Cayosoft Guardian Forest Recovery also includes continuous change monitoring to allow for quick detection and rollback of mistakes or malicious changes, preventing outages or attacks before they happen.

Key Features & Benefits

- The only instant forest recovery solution
- All-in-one architecture for all key recovery scenarios
- Easy to test, configure, & maintain
- Eliminate potential failed AD forest recoveries
- Instantly rollback unwanted directory data changes
- Minimize the complexity & ongoing costs of forest recovery
- Quickly detect risks & indicators of attack with continuous threat protection

> *"After evaluating traditional AD recovery tools, we contacted Gartner and they recommended we look at Cayosoft. The all-in-one interface, which included instant forest recovery, hybrid change monitoring, and hybrid AD object recovery, made Cayosoft an easy decision."*
>
> **Solution Evaluator**
> East Coast Financial Organization

About Cayosoft

Cayosoft delivers the only unified solution enabling organizations to securely manage, continuously monitor for threats or suspect changes, and instantly recover their Microsoft platforms, including on-premises Active Directory, Entra ID, Microsoft 365, Intune and more.

To learn more, visit cayosoft.com

Request a Demo