Cayosoft

CASE STUDY: Healthcare Under Attack

The Cayosoft Case Study That Should Have Happened

National Health Service Cyberattack: How Cayosoft Could Have Prevented & Mitigated the Synnovis Ransomware Breach

Published:
2025

Sponsored by:
Cayosoft

+1 (614) 423-6718

Incident Overview: The Synnovis NHS Ransomware Attack

What Happened?

On June 3, 2024, a major ransomware attack targeted Synnovis, a pathology service provider for the UK's National Health Service (NHS). The cyberattack brought pathology services to a standstill at some of London's largest healthcare organizations, including Guy's and St Thomas' NHS Foundation Trust and King's College Hospital NHS Foundation Trust.

The aftermath was severe: Cancer treatments, blood transfusions, and organ transplants were delayed or canceled. Hundreds of appointments had to be rescheduled, and thousands of patients were affected by an outage that highlighted the fragility of identity infrastructure in healthcare.

How Did Attackers Gain Access?

- **Compromised Active Directory Credentials:** Attackers may have accessed privileged credentials via phishing, credential stuffing, or brute-force techniques.
- **Privilege Escalation Techniques:** Methods like Kerberoasting or Pass-the-Hash likely enabled attackers to elevate their privileges to Domain Admin levels.
- **Lateral Movement Across Hybrid Identity Systems:** Once inside, attackers moved across the hybrid Microsoft environment—including on-prem AD and cloud-based Entra ID—deploying ransomware payloads.
- **Gaps in MFA Enforcement:** Unprotected endpoints, VPN, or RDP interfaces may have been exploited to bypass inadequate multifactor authentication policies.
- **Backup Tampering:** Attackers may have targeted or deleted backup systems to prevent rapid restoration.

The attack demonstrated a critical weakness in identity governance and disaster recovery. And this is exactly where Cayosoft could have made the difference.

How Cayosoft Could Have Identified & Mitigated the Attack

1 Real-Time Identity Threat Detection & Prevention

How It Helps:

Cayosoft Guardian continuously monitors every change across on-prem Active Directory, Entra ID, and Microsoft 365. It provides real-time visibility into unauthorized access attempts, suspicious changes, and privilege escalation tactics.

How It Could Have Stopped the Attack:

- Detects unauthorized group membership changes, admin account elevation, or suspicious authentication patterns.
- Alerts security teams when lateral movement or credential abuse is detected.
- Flags impersonation attempts or service account misuse before ransomware is deployed.

In the case of Synnovis, Cayosoft would have flagged the initial compromise and elevated access before attackers gained Domain Admin control.

2 Automated Rollback of Unauthorized Changes

How It Helps:

Cayosoft Guardian features one-click rollback for directory changes, including users, groups, GPOs, and attributes. It captures each change and maintains a real-time rollback catalog, allowing IT to reverse damage instantly.

How It Could Have Stopped the Attack:

- Immediately revokes unauthorized admin access, restoring previous privilege levels.
- Recovers deleted security groups, conditional access policies, and GPOs disabled by attackers.
- Undoes configuration drift introduced by malicious actors—without needing to initiate a full recovery. Cayosoft could

have reversed attacker actions in minutes, isolating the threat and preserving operational continuity.

3 Ransomware Kill-Switch for Active Directory

How It Helps:

Cayosoft includes logic to detect ransomware indicators of attack (IOAs) and stop them before encryption spreads. It can intercept malicious Group Policy changes and automatically disable compromised accounts.

How It Could Have Stopped the Attack:

- Identifies suspicious GPOs designed to deploy ransomware or disable security tools.
- Automatically reverts harmful policies and resets permissions.
- Locks down targeted admin accounts before malware spreads laterally.

By treating AD as a Tier 0 asset, Cayosoft acts as a firewall between identity compromise and enterprise-wide failure.

4 Immutable AD Backups & Rapid Recovery

How It Helps:

Cayosoft Guardian Forest Recovery offers tamper-proof backups of Active Directory with full validation and ransomware scanning. It enables recovery of an entire forest—including DNS, SYSVOL, and FSMO roles—in under an hour.

How It Could Have Stopped the Attack:

- Ensures that backup data is isolated and immune from encryption or deletion.
- Enables full recovery to clean environments—on-prem, in Azure, or AWS.
- Supports granular recovery of users, groups, and policies without restoring the full forest.

In the event the attackers succeeded in disrupting operations, Cayosoft could have restored core identity services in under 30 minutes—dramatically reducing patient impact.

5 Proactive Business Continuity and Disaster Recovery for Healthcare IT

How It Helps:

Cayosoft enables automated DR validation and aligns recovery operations with Tier 0 identity resilience planning. It supports:

- **RTO (Recovery Time Objective)** of less than 30 minutes for AD and Entra ID
- **RPO (Recovery Point Objective)** near-zero via frequent, immutable snapshots
- **Automated Recovery Testing** to validate readiness and compliance

Why It Matters:

Healthcare IT systems must remain operational 24/7. DR plans that rely on outdated scripts, legacy backups, or manual intervention put patient safety at risk. Cayosoft enforces readiness through automation, clean separation of standby forests, and instant failover procedures.

Key Takeaways: Why Cayosoft Is Essential for NHS and Healthcare IT

The Synnovis incident underscores a truth that healthcare leaders already know: identity is the attack surface. Without resilient hybrid identity management, even the best endpoint protections can be bypassed.

Cayosoft offers:

Proactive detection of privilege escalation and impersonation

Rollback of malicious changes within seconds

Real-time monitoring across AD, Entra ID, and Microsoft 365

Ransomware kill-switch and secure delegation controls

Immutable, tested backups with one-click forest recovery

Healthcare organizations can't afford days—or even hours—of downtime. Cayosoft guarantees business continuity for the systems that enable clinical care.

The Solution That Could Have Prevented Disaster

Had Cayosoft been deployed at Synnovis, the outcome could have been entirely different:

- The initial identity compromise would have triggered alerts before attackers escalated.
- Any unauthorized changes to GPOs or admin roles would have been rolled back instantly.
- AD forests could have been restored from clean, validated backups within 30 minutes.
- Patient services could have resumed the same day.

Instead, the NHS services involved were left paralyzed—reliant on paper-based workflows and manual testing.

Conclusion: Strengthening Cyber Resilience in Healthcare

In healthcare, time is everything. When patient care depends on digital systems, identity outages aren't just IT problems—they're life-threatening failures.

Cayosoft empowers healthcare IT teams with the tools they need to defend the frontline of care. From automated user provisioning and real-time rollback to ransomware-proof recovery, Cayosoft transforms reactive identity security into a resilient, proactive defense system.

We Wish We Had Been There

If Cayosoft Guardian and Forest Recovery had been in place at Synnovis, the breach could have been contained—and the chaos avoided.

Want to learn more?

Request a Demo