JANUS ASSOCIATES

A JANUS ASSOCIATES CASE STUDY

HOW IMMUTABLE BACKUPS STRENGTHENED A HEALTHCARE PROVIDER'S CYBER RESILIENCE

MAY 2026

TEL: +1 203.251.0200

FAX: +1 203.251.0222

INFO@JANUSASSOCIATES.COM

1200 HIGH RIDGE ROAD STAMFORD, CT 06907

Client

A mid-sized regional healthcare provider with multiple clinics and a central data center relied on traditional backup infrastructure to protect electronic health records, clinical systems, and core business applications.

As ransomware attacks targeting backups increased across the healthcare sector, the organization's leadership engaged JANUS Associates to evaluate whether their backup and recovery capabilities were sufficient to support HIPAA, business continuity, and cyber resilience objectives.

Challenge

During an IT risk assessment and cybersecurity consulting engagement, JANUS identified that the client's backup environment was highly centralized and fully manageable with standard administrative credentials.

This meant a successful attacker could potentially gain privileged access, lockout those with legitimate credentials, locate the backup infrastructure, delete or corrupt backup repositories, disable backup agents, and then launch a successful ransomware attack, leaving the organization with no recovery options and significant operational and regulatory exposure.

The client needed a resilient backup strategy that:

- Reduced the risk of ransomware destroying recovery data.
- Aligned with NIST CSF and HIPAA Security Rule expectations for availability and recoverability.
- Strengthened incident response (IR) and disaster recovery (DR) without disrupting clinical operations.

As the CIO noted, *"We knew that if our backups were compromised, our ability to deliver patient care and meet our regulatory obligations would be at risk."*

JANUS Approach

JANUS Associates applied a structured cyber risk strategy grounded in NIST CSF and industry backup resilience guidance to assess the client's current-state environment. Our team conducted:

- A focused IT risk assessment of backup and recovery processes, including identity and access controls, network segmentation, and monitoring.
- A review of backup configurations, retention policies, and offsite storage practices mapped against the 3-2-1-1-0 model (three copies of data, two media types, one offsite, one immutable or air-gapped copy, zero backup errors through testing).
- Workshops with IT operations, security, and compliance stakeholders to clarify recovery point objectives (RPOs), recovery time objectives (RTOs), and regulatory commitments.

Based on this analysis, JANUS recommended implementing immutable backups as a critical control to prevent attackers or administrative errors from modifying or deleting backup data for defined retention periods.

What Are Immutable Backups

Immutable backups are backup copies of data that cannot be altered, encrypted, overwritten, or deleted for a specified retention period. Once a backup is written and marked as immutable, it becomes a "write-once, read-many" (WORM) storage medium.

Immutable backups rely on storage-level enforcement rather than relying solely on software permissions. This distinction is critical because attackers who gain administrative privileges may still be unable to bypass storage-enforced retention controls. The process typically includes:

1. Backup Creation

Data is backed up from production systems to a backup repository.

2. Retention Lock Applied

The backup is written with an immutable retention policy specifying how long the data must remain unchanged.

3. Storage-Level Enforcement

The underlying storage platform prevents modification or deletion until the retention timer expires.

4. Read-Only Access

Authorized users may restore the backup data, but the stored objects themselves cannot be altered.

Solution and Implementation

Working closely with the client's infrastructure and security teams, JANUS designed and guided the deployment of an immutable backup architecture integrated with their existing backup platform and cloud storage.

Key elements included:

- Implementing storage-level immutability (write-once, read-many) so backup copies could not be altered, encrypted, or deleted during the immutability window, even by privileged administrators.
- Establishing off-site immutable backup repositories to protect critical systems, including electronic health records, key clinical applications, and domain services.
- Aligning retention-lock policies with business RPOs and regulatory requirements, ensuring that at least one known-good backup remained available across the defined retention period.
- Introducing logical air-gapping via segmented backup networks and restricted administrative paths to reduce the likelihood that an attacker who compromised the production network could reach the backup environment.
- Strengthening identity and access management for backup systems, including multi-factor authentication for backup administrators and enhanced logging and monitoring of backup configuration changes.

JANUS also helped the client update disaster recovery and incident response plans to incorporate immutable backup workflows, including:

- Procedures for identifying the last known-good immutable restore point during an incident.
- Step-by-step runbooks for isolating compromised systems and restoring from immutable backups.
- Regular test restorations and tabletop exercises to validate that immutable backups could support real-world recovery scenarios.

According to the client's IT director, *"JANUS translated immutable backup concepts into a practical architecture and playbook our team could operate day-to-day."*

Results and Impact

Following implementation, the client materially improved its ability to withstand ransomware and destructive cyber incidents without paying a ransom or experiencing prolonged downtime.

The organization benefited by:

- **Significantly reducing the risk** that attackers or administrative errors could delete or corrupt recovery data before it was needed.
- **Greater confidence** that at least one clean, tested backup copy would be available within defined RPOs, even during a sophisticated or prolonged attack.
- **Stronger alignment with NIST CSF and HIPAA** expectations for backup, recovery, and business continuity, improving readiness for compliance audits and regulatory reviews.
- **More predictable incident response**, with clearly defined steps to identify immutable restore points, restore systems, and return to normal operations.

By integrating immutable backups into their broader disaster recovery and incident response programs, the client enhanced operational resilience, reduced potential financial impact, and strengthened stakeholder confidence in their cybersecurity posture.

Why JANUS Associates

JANUS Associates leveraged decades long deep expertise in cybersecurity, IT risk, disaster recovery, and incident response to deliver a practical and cost-effective solution. We acted as independent advisors, prioritizing real risk reduction instead of product promotion. Our team helped the client make immutable backups a core part of a broader cyber risk management strategy that also included vulnerability management, audit preparedness, and ongoing monitoring.

For this client, immutable backups were a key part of a multi-layered resilience plan, not just a standalone tool.

If you want to ensure your backups can withstand ransomware or insider threats, JANUS Associates can help assess and improve your recovery capabilities. We offer targeted risk assessments, backup reviews, and incident response planning that incorporate immutable backups and practical cyber strategies.

To review your backup posture or explore options like immutable backups, penetration testing, or incident response planning, **contact JANUS Associates for a cybersecurity and disaster recovery consultation.**