COHESITY

Executive summary

Products:
DataProtect,
FortKnox, SmartFiles

Region:
Americas

Use Case:
Backup and Recovery,
Disaster Recovery

Industry:
Healthcare

Environments:
Azure VMs, Azure NetApp files, Microsoft SQL Server, Oracle SQL, VMware

Benefits

Stronger
cyber resilience

1 Management interface for all backup sites

3 Backup copies for resilience:
2 on-premises and 1 in FortKnox

50% Lower costs

45% Faster backups

Leading health system inoculates itself against data loss from attack or system failure

Challenge

This academic health system consistently ranks as a leader in inpatient and outpatient care. Care quality, patient safety, and accurate billing require the ability to quickly recover data after cyberattacks or system failures. After losing data backed up with the previous backup and recovery system, the health system decided to replace it with a modern data platform with simpler management, faster backup and recovery, scalability to meet unpredictable growth, and stronger security protections for personal health information (PHI) and other sensitive information.

Why Cohesity

Comparing leading solutions, the health system selected the Cohesity Data Cloud. Management burden is lower because staff can manage backups and restores in every location—on-prem and in the cloud—from a single dashboard. **Compared to the previous solution, Cohesity backs up data 45% faster and recovers virtual machines (VMs), databases, and individual files in seconds, down from hours**. Total cost of ownership for data protection dropped by 50%. Today the organization maintains immutable copies of all data in two data centers —and a third copy in Cohesity FortKnox, a Cohesity-managed cyber vault.

Business value

Healthcare continuity

With immutable Cohesity backups in three locations, the health system has confidence it can restore from a clean snapshot, minimizing disruption to patient care.

Agility to meet changing needs

When the health system took over responsibility for the medical school's backups, the Cohesity solution scaled to support 20% more data. Later, when the health system consolidated from many data centers to two, it cut costs by installing high-density Cohesity nodes, which require less rack space and fewer switch ports.

Stronger security posture

Adhering to Zero Trust principles, the health system integrated the Cohesity Data Cloud with its single-sign on system and uses multifactor authentication and role-based access controls. Backup snapshots are immutable; they can't be altered by anyone before the retention period expires.

Early awareness of cyber events

Cohesity Professional Services worked with the health system's IT and security teams on an automated workflow to respond to cyber events. If the Cohesity Data Cloud detects an anomaly consistent with ransomware, the security team receives an email alert giving them direct access to the Cohesity backups to contain and investigate the threat. Plans under consideration include AI-based threat detection with Cohesity DataHawk, and conducting investigations with a Cohesity Clean Room solution.

Learn more at www.cohesity.com

COHESITY.com | 1-855-926-4374 | 300 Park Ave., Suite 1700, San Jose, CA 95110

5000152-001-EN 1-2025