COHESITY

HEALTHCARE:

When identity fails, patient care stops.

84% of organizations experienced an identity-related breach last years. In healthcare, the average cost: $7.42M per breach—the highest of any industry for the 14th year running.

How identity-based attacks put healthcare in the crosshairs

Healthcare has held the highest average breach cost of any industry for over a decade, and attackers increasingly treat identity systems as the fastest path to disrupt care. In 2025, 84% of healthcare organizations detected a cyberattack on their network and among those hit in the cloud, account compromise topped the list of incident types at 74%. Your identity attack surface continues to expand daily due to:

- **Legacy AD infrastructure:** Active Directory (AD) is a highly prevalent and decades-old identity system where vulnerabilities and misconfigurations have built up over the years. Coupled with aging infrastructure, many healthcare organizations cite inadequate protection and lack of visibility over security gaps affecting their most critical identity and access management systems.
- **Hybrid environment complexity:** Cloud identity systems expand the attack surface, and attackers are now pivoting between on-prem AD and cloud identity systems in hybrid environments. That introduces more blind spots and thus more vulnerabilities that can be exploited.
- **High concentration of attacks:** Attackers see identity as the front door to an organization's network and data. Cohesity's CERT team finds that 95% of security incidents involve AD. This is largely because attackers know that identity underpins enterprise access. Compromising AD doesn't just halt business operations—it can halt patient care.

Healthcare case study

Change Healthcare: Stolen Credentials Trigger the Largest Healthcare Breach in U.S. History (February 2024)

Target: Change Healthcare, a UnitedHealth Group subsidiary that processes roughly 15 billion healthcare transactions and $1.5 trillion in claims annually, connecting more than 900,000 physicians, 33,000 pharmacies, and 5,500 hospitals nationwide.

Attack vector: Compromised credentials on a Citrix remote access portal that lacked multi-factor authentication. Attackers used the stolen login to move laterally through the network undetected for nine days before deploying ransomware.

Business impact:

- Largest healthcare data breach in U.S. history – 192.7 million individuals' data exposed
- $22M ransom paid; UnitedHealth reported $872M in Q1 2024 costs alone, with full-year impact projected up to $1.6B
- Nationwide claims and payment disruption—some large health systems reported losing over $100M per day
- 80% of physician practices lost revenue from unpaid claims; pharmacies nationwide couldn't process prescriptions

Cohesity Identity Resilience:

Detect, withstand, and recover from identity-based attacks

Detect	Continuously monitor and harden AD, Entra ID, and Okta against identity threats and vulnerabilities with threat intelligence from leading identity security experts. Reduce attack likelihood by 25% while spending 40% less time monitoring.
Withstand	Automate rollback of malicious and suspicious identity changes to prevent compromise. Protect AD, Entra ID, and Okta data with immutable, hardened backups. Simplify identity recovery testing to meet RTO objectives and enhance readiness.
Recover	Fast, automated, malware-free AD forest recovery and Entra ID and Okta with a few clicks for 90% faster recovery. Advanced post-breach forensics that speed remediation and prevent follow-on attacks and validate trust in your identity systems.

How identity compromise affects healthcare

Everything patients and staff depend on is at risk of stopping immediately:

- Electronic health records (EHR) and clinical documentation
- Patient scheduling, registration, and admissions
- E-prescribing and pharmacy dispensing systems
- Claims processing, prior authorization, and billing
- Medical devices and systems that authenticate through AD, Entra ID, or Okta
- Telehealth platforms and patient portals
- Internal operations (email, file access, business applications)

Cost of downtime: $7,500 per minute in lost revenue and recovery costs for the average hospital—and up to $25,000 per minute for large health systems. Without identity resilience, recovery can take weeks or longer, as it did following the Change Healthcare attack.

Is your identity infrastructure resilient?

- ✓ Have you tested and proven that you can meet your identity recovery RTOs after a cyber-incident in the last 90 days?
- ✓ Do you have immutable backups of AD and Entra ID?
- ✓ Can you detect identity-based attacks (Golden Ticket, DCSync) and automatically remediate them in real-time?
- ✓ Can you validate that your identity recovery is malware-free?
- ✓ Can you perform recoveries without internet access?

If you answered "no" to any of these, your business—and your patients—are at risk.

Get a free identity security assessment today.

Contact your Cohesity rep to schedule a no-obligation assessment of your identity security posture.

© 2026 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity Logo, and other Cohesity Marks are trademarks of Cohesity, Inc. or its affiliates in the US and/or internationally. Other names may be trademarks of their respective owners. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

9100112-001-EN 9-2026