Microsoft Commvault

Cyber Resilience That Helps Deliver Clinical Continuity

The cost of healthcare disruption

Healthcare organizations depend on resilient, highly available systems but increasingly face cyberattacks that disrupt patient care and expose sensitive data. Nearly three out of four organizations experience patient care disruption following a cyber incident, and 60% struggle to protect private data as attackers use automation, AI, and advanced social engineering to scale their impact.[1] As a result, rapid recovery of EHR and other critical platforms becomes essential to maintaining continuous care.

- 93% of healthcare organizations experienced a cyberattack in 2024[1]
- Healthcare breaches are expected to reach $12.6 million in 2026 – representing the most expensive cyber incidents[2]
- 4 in 10 healthcare organizations are expected to experience a ransomware attack in 2026[2]

Delivering uninterrupted patient-centered care

Healthcare organizations must meet requirements like HIPAA, HITRUST, and global regulatory frameworks such as GDPR and ISO 27001. As breaches increase, leaders must assess:

- Are we equipped to protect, collect, and preserve patient data to meet regulatory and legal requirements?
- Can we detect and respond to cyber threats targeting PHI and customer data?
- How do we define minimum viable, compliant operations for restoring EHR systems and resuming patient care after an incident?

Built on Microsoft Azure, Commvault® and Microsoft deliver enterprise-scale cyber resilience for healthcare, combining compliant hybrid cloud infrastructure with rapid recovery to help reduce downtime and maintain continuous access to EHRs and other critical systems.[3]

1 https://www.proofpoint.com/us/resources/threat-reports/ponemon-healthcare-cybersecurity-report
2 https://www.scnsoft.com/healthcare/cybersecurity-statistics
3 https://documentation.commvault.com/11.40/software/compliance_search_and_legal_hold_for_hipaa.html

Minimize clinical downtime. Maximize patient trust.

Commvault and Microsoft help healthcare organizations maintain:

- **Continuous patient-centered care:** Reduce downtime and maintain access to medical systems, records, and applications
- **Secure sensitive health data:** Help protect PHI and PII, maintain access, and restore essential operations during cyber incidents
- **Regulatory confidence:** Support forensics and repeatable recovery testing with evidence to help meet audit expectation
- **Adaptive security:** Extend Microsoft Sentinel and AI-enabled security insights to help SOC teams detect threats earlier and accelerate recovery of critical data while minimizing TCO

Air Gap Protect: Protect EHR backups with zero-trust framework and pre-emptive early warning deception technology in an isolated, immutable, indelible environment.

Cleanroom Recovery: Test, investigate, and recover in an isolated environment – without affecting production, while helping meet strict regulatory and compliance standards.

Identity Resilience: Govern resilience across hybrid clouds, SaaS, and AI-enabled workloads to support protected data modernization and healthcare innovation on a single pane of glass.

Cyber threats require a unified response

When ransomware attacks disrupt EHR access, organizations take an average of 24 days to recover.[4] Commvault, built on Microsoft Azure, helped one customer resume operations in nine days – protecting 300+ virtual machines and 60 TB of healthcare data.[5] Utilize isolated recovery environments that help healthcare organizations resume clinical operations while preserving forensic evidence for audits and investigators.

Schedule your demo

Buy on Marketplace

Better together: Commvault + Microsoft

Commvault and Microsoft have partnered for 29+ years to deliver trusted, enterprise-grade data environments with cyber resilience solutions. Our solutions, built on Azure, enable cloud resilience with NIST standards and zero-trust principles. Commvault and Microsoft provide cyber resilience and rapid recovery for continuous business.

Why Commvault

14th consecutive year: 2025 Gartner Magic Quadrant Leader for Backup and Data Protection Platforms

Highest product scores in five of six use cases: Gartner's 2025 Critical Capabilities for Backup and Data Protection Platforms

4 https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack-us/

5 https://www.commvault.com/resources/case-studies/case-study-bilthoven-biologicals

Learn more at:
microsoft.com/commvault

Contact us:
microsoft@commvault.com