

Redefining cyber resilience for healthcare and life sciences

VaultNXT powered by Commvault



The HCLTech point of view

In today's digital landscape, the question is no longer if a cyberattack will occur, but rather when—and how swiftly and effectively an organization can recover.

HCLTech recognizes the escalating threat of ransomware attacks targeting Life Sciences and Healthcare (LSH) organizations. This surge is fueled by the sector's accelerated digital transformation and the high value of sensitive patient and research data. The widespread adoption of IoT-enabled medical devices, cloud technologies and decentralized data ecosystems has significantly broadened the attack surface, making robust cybersecurity measures and the ability to quickly restore minimum viable operations more critical than ever.

To address these challenges, HCLTech champions a holistic cybersecurity strategy anchored with Zero Trust architecture, real-time threat detection and secure recovery frameworks. By integrating AI-driven automation, advanced identity and access management and strategic industry partnerships, HCLTech delivers resilient and adaptive security solutions.

With a steadfast commitment to societal well-being and a proven track record in cybersecurity, HCLTech offers comprehensive, end-to-end data resiliency services. These solutions serve as a digital fortress, safeguarding LSH organizations against data loss and enabling operational continuity in an increasingly volatile threat environment.

This whitepaper explores the pressing challenges facing the LSH sector and presents actionable solutions designed to fortify digital infrastructure and enhance resilience.

Executive summary

As life sciences and healthcare organizations digitally transform their businesses, modernize infrastructure and embrace innovative technologies, they face a new breed of sophisticated and pervasive cyber threats like ransomware that jeopardize sensitive data and critical operations. Being able to identify a cyberthreat early and ready to respond quickly is crucial to continuous business operations. HCLTech VaultNXT, powered by Commvault provides a robust cyber resilience platform that allows healthcare organizations to move faster in their digital programs confident their sensitive patient and business data is always secure and always available.



Fact check: per market surveys in 2024, healthcare was the 2nd most targeted industry for cyber exploits.

<https://news.sophos.com/en-us/2024/04/30/the-state-of-ransomware-2024/>

Introduction

Importance of data security and cyber resilience in life sciences and healthcare

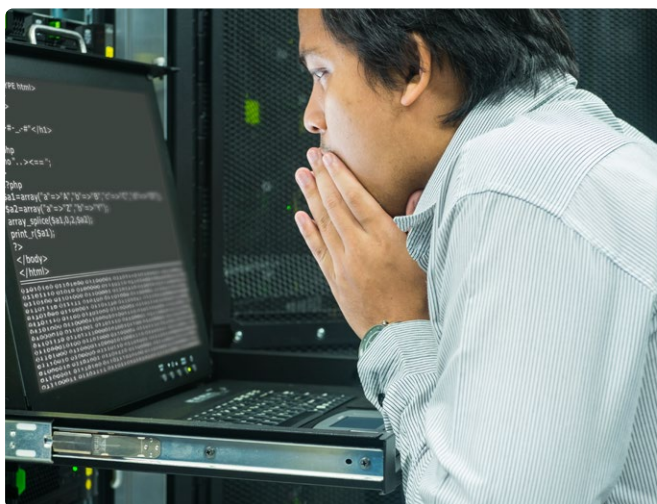
Healthcare organizations handle vast amounts of sensitive data, including patient records, research data and proprietary information. Often, these groups work together, maintaining trust between patients, doctors, hospitals, researchers and life

science companies. This helps them share important data that helps patients get better results. Protecting this data is crucial for maintaining patient trust, complying with regulations and ensuring uninterrupted operations. The integrity and

availability of this data are paramount. Any data breach or loss can have severe consequences, including legal repercussions, financial losses and damage to reputation.

Addressing a range of challenges

Healthcare organizations face unique challenges in protecting and recovering data and ensuring cybersecurity across their complex, distributed environments:



- **Cyberattacks are becoming more sophisticated and AI-driven.** They target healthcare data as a profitable target, putting operations and lives at risk by stopping access to diagnostic equipment and important systems with patient records. These attacks target organizations' backup copies, impacting rapid, effective recoveries.
- **Stringent regulatory compliance:** Failure to adhere to regulations such as GDPR, HIPAA and HITECH can result in hefty fines, legal actions and even the ability to provide services. Given the rise in cyberattacks, these regulations are expected to evolve and become even more demanding.

- **Burden of legacy systems and technical debt:** Whether healthcare organizations have grown organically or through acquisitions, all have added new applications and edge devices to technology stacks. Patched end-of-life operating systems and software with known vulnerabilities are also challenging IT and security teams to maintain secure environments while keeping up with the demands of an expanding group of users. These factors lead to siloed data, multiple data protection and

recovery tools and increasing technical debt for stretched IT and security teams to maintain.

- **Doing more with less:** Protecting distributed data is complex and costly for teams focused on data security and recovery mechanics. At the same time, organizations face even greater pressure to reduce costs. It doesn't help that healthcare organizations also face a very competitive market for professionals with this type of expertise.



Fact check: 96% of hospitals admit they are running end-of-life operating systems or software with known vulnerabilities.

<https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf>

Fact check: 99% of ransomware tamper with security and backup infrastructure

<https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWZb5v?culture=en-ca&country=ca>

A comprehensive approach to data security and cyber resilience

HCLTech VaultNXT, powered by Commvault, provides a data resilience platform designed to safeguard critical healthcare data across on-premises, cloud and edge environments. The platform unifies data protection, readiness and recovery processes with advanced automation and intelligence. A single pane of glass provides full visibility into how data is secured, defended and recovered with granular control.

Key features



Secure patient data

EHR data, PACS imaging files, backend databases and more seamlessly secured across cloud and on-premises environments. Commvault is certified by all major electronic health record providers to provide detailed reporting and efficient long-term retention of EHR records, including Epic, InterSystems and Meditech.



Bolster patient privacy

Reduces exposure by identifying exposed sensitive patient information (PII, PHI, PCI) and automatically remediating.



Compliance made easy

Helps meet requirements for HIPAA, GDPR, HITECH and other regulations to support organizational compliance.



Rapid recovery

Identifies breaches early and recovers clean data quickly to ensure patient care and operations continue without interruption.



Cyber insurance prerequisites

Provides proven recoverability to assure auditors and executive stakeholders that patient data is secure.



Reduce costs

Consolidate multiple point solutions to a single platform, automate routine data protection processes and simplify management across complex, hybrid and multi-cloud environments.

HCLTech VaultNXT powered by Commvault

For over a decade, HCLTech and Commvault have partnered to strengthen cybersecurity and data resilience for some of the world's largest organizations. Our joint offerings are founded on

zero-trust principles to secure, defend and recover data against rising ransomware threats and provide AI-enabled intelligence and automation to reduce risk across hybrid and multi-cloud

environments. The HCLTech VaultNXT solution is integrated into HCLTech's Infonomics framework for smart cloud data management services.

Key features



Cloud Rewind

Cloud native solution to rapidly recover cloud application data and automate rebuild with configurations and infrastructure following a cyberattack, misconfiguration or outage. Continuously identifies and catalogues cloud resource to create map of dependencies and enable precise and coordinated recovery of cloud services.



Cleanroom Recovery

An on-demand recovery environment to validate and restore clean data speeds recovery by preventing reinfection in production environments. It may also test recovery plans and validate resilience under multiple scenarios.



Compliance

Automatic Identification and classification of sensitive data to reduce the risk of data exfiltration and reduce eDiscovery time and costs. Built-in customizable reports to support audits and documentation of resilience operations.



Comprehensive, immutable data protection

Industry's broadest coverage of cloud workloads, SaaS applications and business-critical systems with immutable, indelible backups. Full portability across hybrid cloud environments.



Early threat warning

Continuously scan data environment for anomalies and leverage cyber deception tools to identify threats earlier and respond faster.



Founded on Zero Trust Architecture with Security integrations

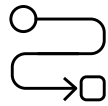
Integrates with SIEM and SOAR platforms for improved threat intelligence and incident response.

Implementation strategy



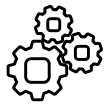
Assessment and planning

Evaluate current data protection and cybersecurity measures to identify gaps and areas for improvement.



Integration

Seamlessly integrate VaultNXT, powered by Commvault, to create a unified data resilience and cybersecurity framework that can be used across an organization's information systems.



Configuration

Set up encryption, backup and recovery protocols to ensure that data is protected and can be quickly restored during a cyber incident.



Testing and validation

Conduct regular tests to ensure the system's effectiveness and identify any areas for improvement.

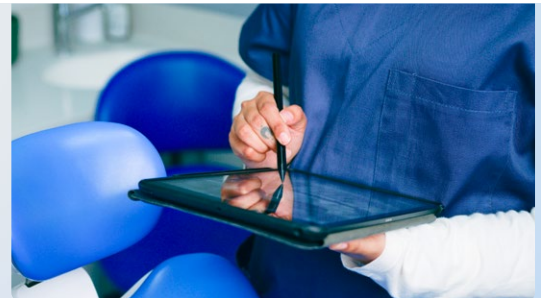


Monitoring and maintenance

Continuously monitor for threats and maintain the system to ensure ongoing protection and compliance.

Case study

Enhancing cyber resilience in a healthcare organization



Global healthcare insurer boosts Cyber resilience, cuts backup costs by more than 20%

A leading multinational healthcare insurer partnered with HCLTech Infonomics to revolutionize its data protection strategy. Facing the complex challenge of safeguarding multi petabytes of critical data across a diverse hybrid environment—including OpenShift, DB2, NAS, VMs, Oracle, SQL and Active Directory—they sought a solution that would enhance security while optimizing costs.

By leveraging Commvault Cloud and the VaultNXT framework, this insurer achieved a remarkable reduction in backup system costs over three years. More importantly, they significantly strengthened their cybersecurity posture. The new solution ensures a lightning-fast 10-minute Recovery Point Objective (RPO) for mission-critical systems. This means they can recover rapidly during any downtime, ensuring that essential patient services remain uninterrupted and enhance confidence in their ability to maintain seamless operations.

Key capabilities delivered by this transformation include

- Air-gapped, immutable copies that provide last line of defense for cyber recovery.
- Comprehensive workload coverage, protecting vital data across a sprawling IT landscape.
- Tailored reports offering clear insights into their backup infrastructure, enabling effective and proactive management.
- Efficient and scalable cyber resilience for all mission-critical applications and data, ensuring robust protection that grows with their needs.

This success story highlights how strategic data management can deliver both significant cost savings and unparalleled peace of mind in an increasingly complex digital world.

Conclusion

HCLTech VaultNXT powered by Commvault provides a comprehensive approach to data security, readiness and resilience in life sciences and medical sectors. By leveraging advanced technologies and best practices, organizations can safeguard sensitive data, support regulatory compliance and maintain operational continuity. This robust framework protects against cyber threats, delivers comprehensive recovery capabilities and improves overall data management and operational efficiency.

Connect with us for more information
HCBU-pmg@hcltech.com

References

- [HCLTech VaultNXT powered by Commvault](#)
- [Commvault Healthcare Use Cases](#)



Kunal Sharma

Group Manager
Hybrid Cloud Business Unit
HCLTech

About the Author

Extensive experience in leading cross-functional teams and driving strategic initiatives. He brings a strong focus on innovation, operational excellence, resiliency concepts and stakeholder collaboration to every project.



Saurabh Narula

Senior Global Alliance Architect
Commvault

About the Author

Saurabh Narula is specializing in delivering cyber resilience and data protection solutions that enable enterprise growth while minimizing business risk. With over 18 years of experience, he has architected data security and business continuity solutions for global clients across critical industries including financial services, healthcare and government sectors. His deep expertise spans cyber resilience initiatives, including cloud security architecture, AI/ML-driven threat detection, disaster recovery planning and regulatory compliance frameworks. Focused on helping executives navigate complex data protection challenges, Saurabh leads global partnership engagements to integrate Commvault's cyber resilience platform into enterprise architectures that supports innovation and scalable growth.

HCLTech | Supercharging Progress™

HCLTech is a global technology company, home to more than 223,000 people across 60 countries, delivering industry-leading capabilities centered around digital, engineering, cloud and AI, powered by a broad portfolio of technology services and products. We work with clients across all major verticals, providing industry solutions for Financial Services, Manufacturing, Life Sciences and Healthcare, High Tech, Semiconductor, Telecom and Media, Retail and CPG, and Public Services. Consolidated revenues as of 12 months ending June 2025 totaled \$14 billion. To learn how we can supercharge progress for you, visit hcltech.com.

hcltech.com

