

VaultNXT: Cyber resiliency redefined

Secure your data from cyberattacks

In today's landscape of increasing cyber threats, organizations must safeguard their crown jewel applications and data to avoid financial and reputational losses. Organizations need a robust cyber resiliency solution. This ensures their business remains secure and resilient, even in the face of sophisticated cyber-attacks.

Worldwide cybercrime costs are estimated to hit \$10.5 trillion annually by 2025. This highlights the need for enhanced cyber recovery measures to be taken by organizations.

[Source](#)

Key challenges

- 1 Cyber attacks are becoming more advanced and harder to detect. As a result, safeguarding against them is becoming more challenging
- 2 Post-attack data recovery is often incomplete, causing operational disruptions
- 3 Balancing data integrity and regulatory compliance is becoming increasingly difficult



VaultNXT: Ensuring uninterrupted business continuity with robust cyber resiliency

As cyber threats continue to evolve, maintaining operational continuity has never been more critical. HCLTech VaultNXT offers a comprehensive, end-to-end solution. It is designed to enhance organization's ability to withstand, recover from, and adapt to cyber disruptions across on-premises, cloud, and endpoints.

By leveraging a multi-layered approach, VaultNXT strengthens your ability to minimize downtime, ensure rapid recovery, and maintain data integrity. This ensures that your critical operations stay resilient in the face of evolving challenges.

VaultNXT overview

The VaultNXT framework encompasses



Assess

Discovery

- Define CR objective and goals
- Identify critical data (Crown Jewels)
- Map critical application and infrastructure
- Breach likelihood and Readiness review
- IR plan review and threat briefing

Analyse

- Crown jewel protection
- Security controls and protection policy
- Risk detection and compliance review
- Ransomware readiness assessment

Objective mapping | Assessments | Readiness review | Current CR maturity



Build

Formulation

- Define Solution approach and deployment model
- Finalize OEM / vendor selection
- Allocate resources for Cyber-vault setup
- Design secure Vault connectivity and infrastructure
- Prepare for Incident handling process

Build

- Implement resiliency and firewall builds
- Integrate Cyber-vault with existing infra.
- Set up vault landing zones and recovery pathways
- Update security policies as per CERT processes

Solution locking | R&R with timelines | infra build



Operate

Monitor

- VaultNXT monitoring/reporting
- Regular testing and monitoring of incident response plans (cyberattacks, outages, disruptions)
- Cyber incident event/change management
- Run and manage recovery operation tasks with one console
- Automated threat scanning/anomaly detection/IOCs within backups

React

- Post breach validation of recovery points which contain clean copies of data.
- Documentation, updation, maintenance and Execution of cyber recovery plan
- Regular testing

Steady state | Monitoring | Recovery and restoration

Key features



Hybrid deployment model



Sensitive data discovery



Proactive real-time threat monitoring



One-click recovery



Neutral vendor-neutral approach for identifying the best-fit tool



Crown jewel data identification



Air gap isolation



CR incidence response strategy



Scalable security controls



AI/ML-based risk detection



Proactive golden copy validation



Flexible pricing model

Benefits



Proactive identification, actionable recommendations and threat detection using AI/ML



Stringent recovery process even in situations where cyber ransomware compromises backup data



Secured and validated data ensuring recoverability



Identifying and mitigating the risk of evolving cyberattacks



Develop and deploy a mature cyber recovery strategy



Revised content: Establish a robust cyber recovery strategy to ensure business continuity

Case studies



Leading Insurance provider company

Implemented a secure, scalable solution. This enhanced data security, ransomware protection, cost efficiency, and disaster recovery.



One of Europe's leading telecommunication company

Implemented a modern backup solution. This reduced failures, enhanced security, streamlined backups with lower TCO and improved SLAs.

Why HCLTech

- Leader in all analyst reports for cloud
- Vast experience in infrastructure security, governance, risk and compliance
- Robust partnership ecosystem consisting of leading industry-leading OEMs
- Dynamic security framework offering end-to-end solutions with managed service
- A large number of certified resources to cater to every need of customers with customized SLAs

Partners



To know more, you may reach out to us at HCBU-PMG@hcltech.com