HCLTech | Supercharging Progress™

VaultNXT: Cyber resiliency redefined

Secure your data from sophisticated cyber attacks

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 an intelligent cyber resiliency solution to stay ahead of emerging risks.. This ensures their business remains secure and resilient, even in the face of highly coordinated cyber-attacks.

Global cybercrime is estimated to see growth plateau at 2.5 percent annually through 2031, at which point it will cost the world $12.2 trillion annually. This highlights the need for enhanced cyber recovery measures to be taken by the 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 AI-driven cyber resiliency strategy

As cyber threats continue to evolve, maintaining operational continuity has become more critical than ever. HCLTech VaultNXT offers a comprehensive, end-to-end, AI-powered cyber resiliency solution for advanced threat protection. It is designed to enhance an organization's ability to withstand, recover from, and adapt to cyber disruptions across on-premises environments, cloud platforms, and endpoints. By leveraging an advanced, multi-layered approach, VaultNXT strengthens the ability to minimize downtime, enable rapid clean recovery, and maintain data integrity. This ensures that critical operations remain resilient amid an evolving threat landscape.

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 orchestrated recovery with AI validated clean recovery point.
- 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 and policy automation for criticality
- Proactive real-time threat monitoring
- AI- driven guided clean recovery orchestartor
- Neutral vendor-neutral approach for identifying the best-fit tool
- Crown jewel data identification
- Responsible AI governance
- Air gap isolation with posture scoring and drift detection
- CR incidence response strategy
- Scalable security controls
- AI/ML-based ramsomeware and risk detection
- Proactive golden copy validation
- Flexible pricing model
- Agentic recovery

Benefits

- Proactive identification, actionable recommendations and threat detection using AI/ML
- Stringent recovery process even when cyber ransomware compromises backup data
- Secured and validated data ensuring recoverability
- Identification and mitigation of risks from evolving cyber attacks
- Development and deployment of a robust cyber recovery strategy to ensure cyber immunity and business continuity

Case studies

Leading Insurance provider company

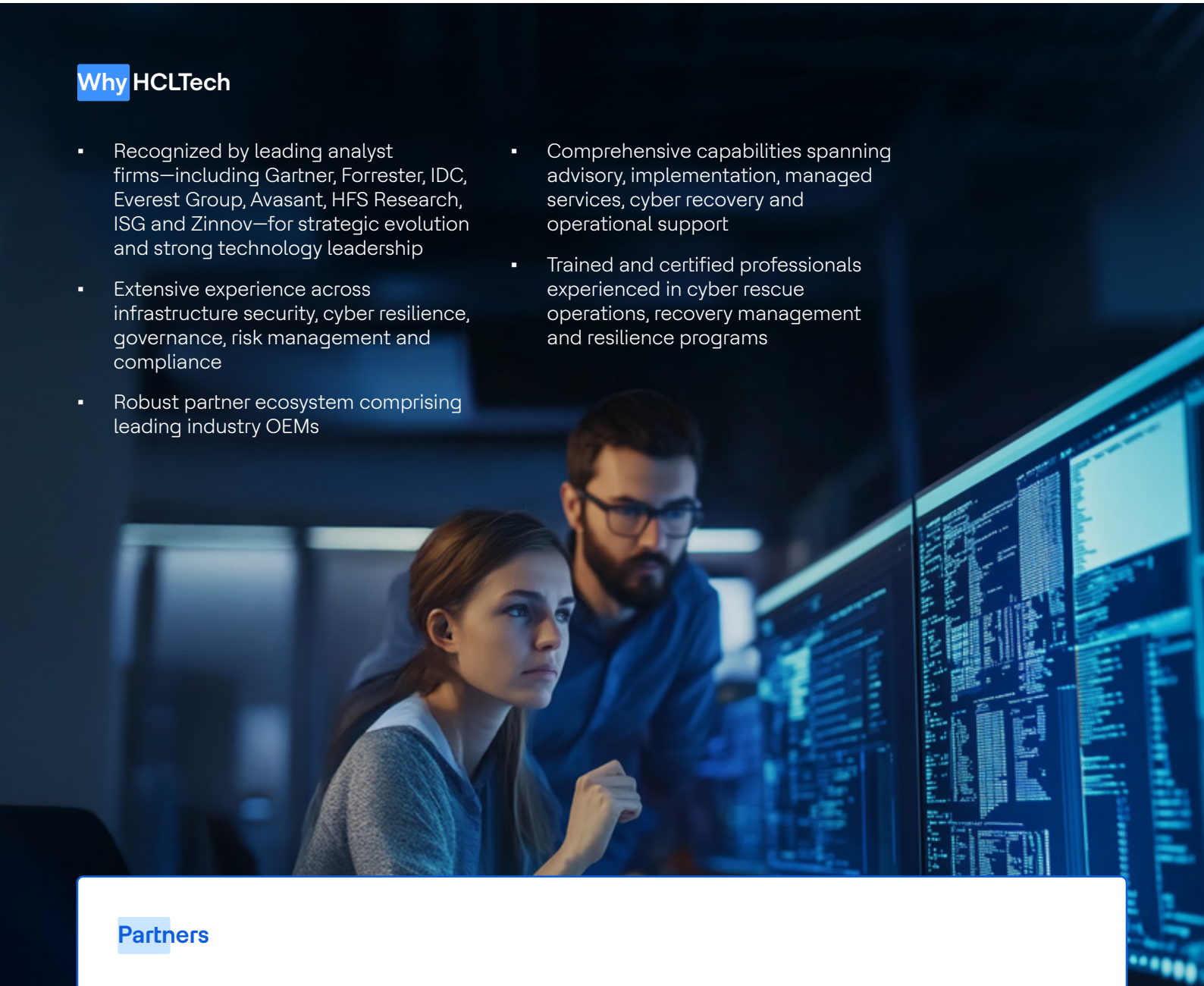
Implemented a secure, scalable solution. This enhanced data security, ransomware protection, cost efficiency, and disaster recovery.

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

- Recognized by leading analyst firms—including Gartner, Forrester, IDC, Everest Group, Avasant, HFS Research, ISG and Zinnov—for strategic evolution and strong technology leadership
- Extensive experience across infrastructure security, cyber resilience, governance, risk management and compliance
- Robust partner ecosystem comprising leading industry OEMs
- Comprehensive capabilities spanning advisory, implementation, managed services, cyber recovery and operational support
- Trained and certified professionals experienced in cyber rescue operations, recovery management and resilience programs



Partners

DELL Technologies | COMMVAULT | COHESITY | rubrik | Zerto

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