DELL Technologies | CyberSecurity & GRC Services by HCL Technologies

HCL

HCL Cyber Resiliency with Dell Technologies

www.hcltech.com

Protect your critical data and rebound from threats quickly with an end-to-end solution

Your business-critical data is essential for maintaining business continuity, yet that data is at risk from myriad threats — ranging from a natural disaster to malware to a full-scale cyberattack. A disaster recovery plan can help you eventually get your business up and running in the case of an outage or an accidental delete. But it falls well short of what you need to defend against increasingly sophisticated and frequent cyberattacks and the damage they can do.

Challenges in protecting and recovering business-critical data

Traditional business continuity and disaster recovery approaches focus on recovering applications and systems but not the critical data they might hold.

Organizational complexities can prevent you from identifying all of your critical data and executing a coordinated response.

Cyberattacks are unplanned and unpredictable, they can have far-reaching repercussions. Your response must be agile, robust and coordinated to address all organizational stakeholders and department.

Businesses operate diversely across different industries. This diversification at times poses challenges to developing or adopting unified business resilience strategies across technologies, platforms, tools, people and regulatory compliance requirements.

Businesses do not have a complete view of their sensitive data across systems and infrastructure. All critical data may not necessarily be part of their recovery strategy.

Cyberattacks go well beyond disrupting operations but attack the critical data. Cyber resiliency allows organization to protect and quickly recover from breaches while at the same time protecting that data.

Cyber Resiliency from HCL Technologies and Dell Technologies

Cyber resiliency requires thoughtful planning and the right tools. It is an iterative process that provides guidance on recovery while maintaining constant vigilance across the organization. As the need for this service is felt across industries, HCL has enhanced its Business Resiliency and Disaster Recovery portfolio by adding cyber recovery solutions from our strategic partnership with Dell Technologies.

Leveraging the combination of HCL Service Expertise and Dell Infrastructure, the uniqueness of HCL Cyber Resiliency service, is in the protocol followed to identify the business critical application, Infrastructure and the interdependencies, to formulate a standard operating procedures to maximize business continuity by offering lowest RTO, while maintaining the highest security standards in protecting your organizations critical data.

The HCL phased approach to develop and deploy a mature cyber recovery program and solution includes:

- Identification of critical workloads/data that are set to be included in the cyber recovery strategy and solution.
- Review and enhancement of the existing business continuity planning/disaster recovery strategy by including data recovery as a key element of the resiliency process.
- Development of the architecture for the cyber recovery strategy.
- Development and deployment of the cyber recovery strategy
- Configuration of AI and ML enabled algorithms for proactive detection of patterns, data/ signature changes, risks and threats that can impact business continuity.

55% of executives identified investment in cybersecurity protection as essential to their 5-year business goals

40% of businesses are not protected by any cybersecurity program

44% of organizations had the data of 500,000+ customers exposed in 2019

Prepare

- Project plan and kickoff
- Governance
- Business environment
- Risk management strategy
- Collateral on potential application

Detect & analyze

- Technical assessment
- Data visualization
- Infrastructure design workshop
- Information asset
- Critical workloads
- Cyber security architecture design
- Implementation planning

Secure & protect

- Information protection process and procedures
- Implement/ configure cyber recovery vault
- Data domain hardening
- Air gap workflow automation deployment
- Immutable copy

Recover & report

- Recovery planning
- Historical changes analysis
- Recovery evaluation
- Cyber reporting/ compliance
- Improvements and knowledge transfer of vault operation
- Communication and signoff

Unique features of Dell Technologies' cyber recovery solution

Stronger data protection and greater flexibility through the cyber vault:
A cornerstone of the solution is an operationally air gapped cyber vault for storing and recovering critical data. The vault is separate from the network for stronger protection. Rather than recovering data directly into production, data can be tested outside the system during the recovery process.

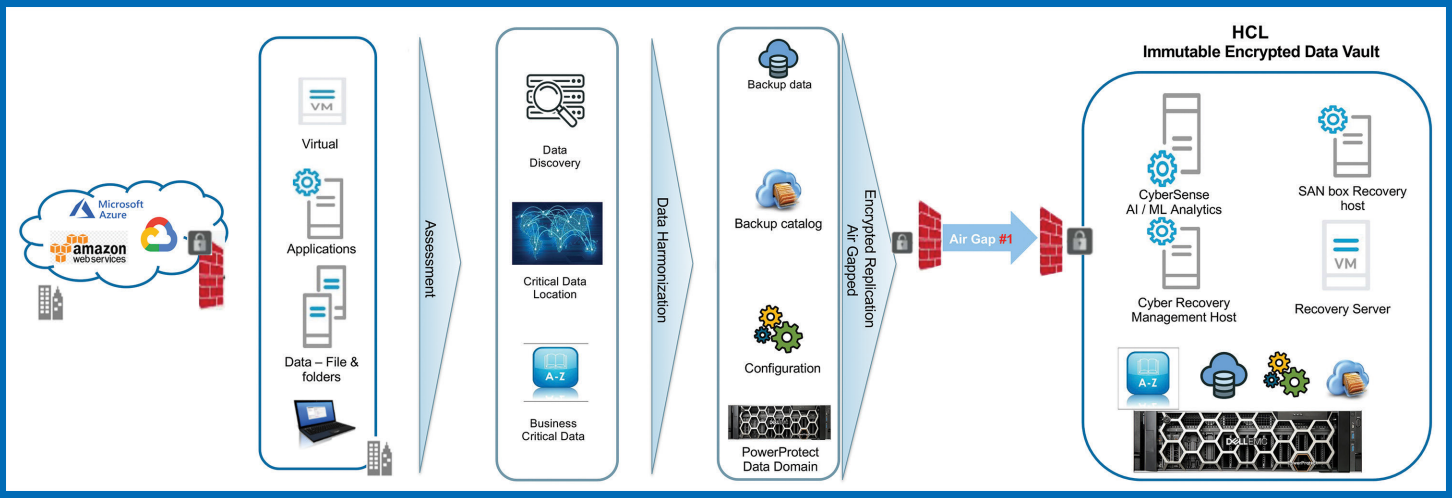
[1] Matt Eastwood, Is Hybrid Multi-Cloud a New Reality for Enterprises?, IDC, July 19, 2020.
[2] Kelly Bissell, "Lessons from leaders to master cybersecurity execution," Accenture, January 28, 2020.
[3] Ibid.

Additional security with CyberSense analytics:
Inside the vault is a unique analytical layer that continues to analyze incoming data as well as data that's already in the vault. The automated recovery process adds even more security by eliminating human error and insider threats.

Controlled access and ongoing monitoring through data encryption:
All data in the vault requires encryption access and cannot be overwritten. The analytical layer continually monitors activity. If an attack is detected, it shuts off access to the vault and isolates it from the network.

Endorsed and proven solution:
Dell Technologies' solution documentation is ISO 9000 compliant, complies with all relevant standards and regulations, and can be customized to enterprise specific requirements. Dell Technologies' solutions are used by the Federal Bureau of Investigation and endorsed by the Sheltered Harbor solution advisory provider program.

End-to-end cyber resiliency for managing any threat, endorsed by Sheltered Harbor
Dell Technologies' end-to-end solution gives an enterprise the resiliency to maintain business continuity in the face of any threat to critical data. We leverage your existing disaster recovery processes and procedures, and then go one step further to identify and protect your critical data so that you can quickly bring up applications without risk to that data.



HCL Technologies (HCL) empowers global enterprises with technology for the next decade today. HCL's Mode 1-2-3 strategy, through its deep-domain industry expertise, customer-centricity and entrepreneurial culture of ideapreneurship™ enables businesses to transform into next-gen enterprises.

HCL offers its services and products through three lines of business - IT and Business Services (ITBS), Engineering and R&D Services (ERS), and Products & Platforms (P&P). ITBS enables global enterprises to transform their businesses through offerings in areas of Applications, Infrastructure, Digital Process Operations, and next generation digital transformation solutions. ERS offers engineering services and solutions in all aspects of product development and platform engineering while under P&P. HCL provides modernized software products to global clients for their technology and industry specific requirements. Through its cutting-edge co-innovation labs, global delivery capabilities, and broad global network, HCL delivers holistic services in various industry verticals, categorized under Financial Services, Manufacturing, Technology & Services, Telecom & Media, Retail & CPG, Life Sciences, and Healthcare and Public Services.

As a leading global technology company, HCL takes pride in its diversity, social responsibility, sustainability, and education initiatives. As of 12 months ending on March 31, 2021, HCL has a consolidated revenue of US$ 10.17 billion and its 168,977 ideapreneurs operate out of 50 countries. For more information, visit www.hcltech.com

www.hcltech.com