Zerto
a Hewlett Packard Enterprise company

# Zerto Cyber Resilience Vault vs. Dell PowerProtect Cyber Recovery

## 5 Reasons to Switch from Dell to Zerto

Ransomware threats and cyberattacks continue to grow in frequency, severity, and sophistication. A recent study by IDC found most disaster recovery incidents in the last 12 months were triggered by ransomware and malware. The cost of executing an attack continues to fall thanks to the rise of ransomware as a service, and successful ransom payments are fueling the development of next-gen malware.

Common methods for building cyber resilience against ransomware attacks rely on legacy technologies and architectures, such as Dell PowerProtect Cyber Recovery. Using a mix of hardware and software, Dell Cyber Recovery delivers a data vault that protects critical data, mitigates the impact of ransomware, and complies with regulatory requirements for data security. However, there are many drawbacks to Dell's vault solution, including slow recovery, network exposure, expensive administration, and more.

For each of these drawbacks, there is a better solution. The Cyber Resilience Vault from Zerto, a Hewlett Packard Enterprise company, provides ironclad protection and rapid air-gapped recovery. Its near-synchronous replication, full physical isolation, decentralized zero trust architecture, and real-time encryption scanning give you the best in cyber resilience—all at a lower total cost of ownership (TCO). Here are five reasons why you should choose the Zerto Cyber Resilience Vault over Dell PowerProtect Cyber Recovery.

---

## 1 Rapid Recovery

Data vault solutions typically prioritize data integrity and security for ransomware resilience. However, vault-based recovery from ransomware using Dell Cyber Recovery can be cumbersome and time consuming. Dell uses legacy recovery methods, including lower tier backup-grade storage, rehydration processes, and file-based security scanning. These processes are inherently slow and dramatically increase recovery time objectives (RTOs) once you account for lengthy backup windows, aging backup replicas, and prolonged scans using the 3rd party software Dell has licensed.

In addition, the Dell Cyber Recovery solution lacks mature orchestration and automation capabilities. Inherently slow recovery methods and manual processes increase RTOs, exacerbating ransomware's impact by further delaying the ability to resume normal operations.

The Zerto Cyber Resilience Vault, on the other hand, delivers several unique capabilities that shorten recovery times and minimize downtime for organizations. Zerto leverages a combination of robust integrated orchestration and automation, near-synchronous replication, and streaming encryption detection to deliver unmatched rapid recovery.

Additionally, the Cyber Resilience Vault leverages production-grade storage from HPE Alletra to temporarily run any workload in the vault without compromising on performance. The result is the ability radically reduce data loss and downtime by recovering within minutes or hours, not days or weeks like with Dell.

## 2 Secure Air-Gapping

Many vault solutions claim complete isolation, or air gap, from outside networks. But the Dell Cyber Recovery vault has numerous connections to outside networks for replication and management, providing only partial isolation. This includes a 24x7 management layer that is always connected. If the firewall facilitating the access gets compromised or bypassed during attack, then the vault infrastructure is jeopardized.

The Zerto Cyber Resilience Vault is a true separated vault that leverages physical and logical air-gaps to guarantee full isolation from other networks. It stores immutable data copies on secure, FIPS-validated hardware with tamper-proof NTP protection. This ensures that if attackers compromise your production and initial recovery environments, they cannot penetrate the isolated walls of the vault and thus cannot attack your vaulted data. There are no firewalls involved and no physical outside connections to manage, letting you rest assured that your data is always safe and secure from outside threats.

---

## 3 Decentralized Zero Trust Architectures

Securely and effectively managing vault solutions can be a struggle. Dell Cyber Recovery sacrifices security by using a centralized control plane, which requires network ports to be left persistently open and leaves companies open to another attack vector. The architectures possible with Dell are also rigid, forcing IT into specific configurations rather than supporting business-driven customizations.

The Zerto Cyber Resilience Vault leverages decentralized, zero trust architectures that can be flexibly defined and redefined to meet diverse business and technical requirements. For example, the vault can be physical located at either production or secondary sites; it supports replication from cloud sites (e.g. Microsoft Azure or Amazon Web Services) in addition to on-premises sites; and the Cyber Resilience Vault can be combined with backup solutions to maximize the power of the vault. Lastly, the decentralized nature of the Zerto vault means there is no one single point of compromise or failure—this includes not having external network communications for management in order to minimize risk.

---

## 4 Real-Time, Inline Security Scanning

Most vault solutions offer ransomware scanning or detection to ensure that data written to the vault is in a secure, usable state when needed for recovery. The Dell solution offers periodic security scanning with the data living on a dedicated backup appliance, which throttles scanning speed. The scans happen before and during recovery processes, which can significantly increase RTOs. Dell also requires use of specific OEM scanning software to read their proprietary backup formats rather than enabling the use of multiple security tools.

The Zerto Cyber Resilience Vault use real-time scanning, leveraging the power of continuous data protection (CDP) to validate the security and integrity of your data. Because this is done inline as the data streams in, there is no delayed validation of your data. Zerto's unique position in the data path also avoids performance impact and doesn't hamper normal application or storage operations while the encryption detection is occurring.

Zerto also exposes its encryption analyses via API to enable a defense-in-depth strategy—what's known as composable security. Since the scanning data is not locked into a closed black box, like with Dell, enterprises can easily integrate Zerto with their existing security stack and leverage the combined power of our detection right alongside their SIEMs, SOARs, or other solutions.

## 5 Cost-Effective

Vault technologies typically leverage expensive, dedicated backup storage appliances, security software, and professional services to administer the vault. The solution does not include everything needed for cyber resilience either, requiring paid add-ons to round out the picture. There are high indirect costs as well, such as the cost of downtime when accounting for the extended RTOs and the need to move restored data from the vault back to a production-grade storage after an attack.

The Zerto Cyber Resilience Vault implements a cost-effective, production-grade solution that has a significantly lower TCO. Not only is this vault a secure repository for your most critical data, but when a recovery event transpires, you can quickly restore and run your applications on the same infrastructure for extended periods of time. The Cyber Resilience Vault is also available as an all-in-one bundle that includes everything needed for the complete solution.

---

It's clear that cyberthreats and ransomware attacks pose a significant risk to organizations worldwide. While many vault solutions, such as Dell's, may initially seem like a viable option to protect data, they have slow recovery times, limited security, and high costs all while running on non-production grade storage.

The Zerto Cyber Resilience Vault offers a superior solution to safeguard against cyberthreats. Its advanced features—including rapid recovery, secure air gapping, decentralized zero trust management, and real-time, inline security scanning—equip organizations with the necessary tools to protect their data effectively even after the worst ransomware attacks.

For more information on the Zerto Cyber Resilience Vault, check out the solution brief.

**Learn More**



RITM0094369