Hewlett Packard Enterprise

Cyber vault competitive landscape

What is a cyber vault?

A cyber vault is a secure system where sensitive data, cryptographic keys, or other valuable digital assets are stored and managed. It is designed to provide the highest level of security, access to controls, and auditing capabilities to protect critical information from unauthorized access, ransomware, and data loss. Common terminology when discussing cyber vaults:

- **Immutable data vault (IDV)**
  - A secure storage location for storing copies of critical data to protect against cyberattacks, data loss, or corruption. It acts as a central repository for multiple versions of data from various sources, applications, and systems.
- **Isolated recovery environment (IRE)**
  - Isolated, secure infrastructure dedicated to data recovery in the event of a cyberattack or system compromise. It ensures business continuity to swiftly restore critical systems.

There are several types of vault solutions, each with their strengths and weaknesses.

Table 1. Vault technology categories

	Cloud vaults	On-premises vaults
Example solutions	• Rubrik Cloud Vault • VMWare Live Cyber Recovery	• Dell PowerProtect Cyber Recovery • IBM FlashSystem Cyber Vault
Category strengths	• Lowest up-front cost • Flexible management • Simple • Object lock	• Lower total cost of ownership • Data efficiency (compression and deduplication) • Customer owned • Highest level of immutability • High performance if using production-grade, not backup-grade, storage
Category weaknesses	• Lack of isolation—Needs persistent internet connectivity to support data movement and management • Hidden costs • Less flexibility	• Lack of isolation—Needs persistent internet connectivity to support data movement and management • Often uses backup-grade storage leading to slow recovery

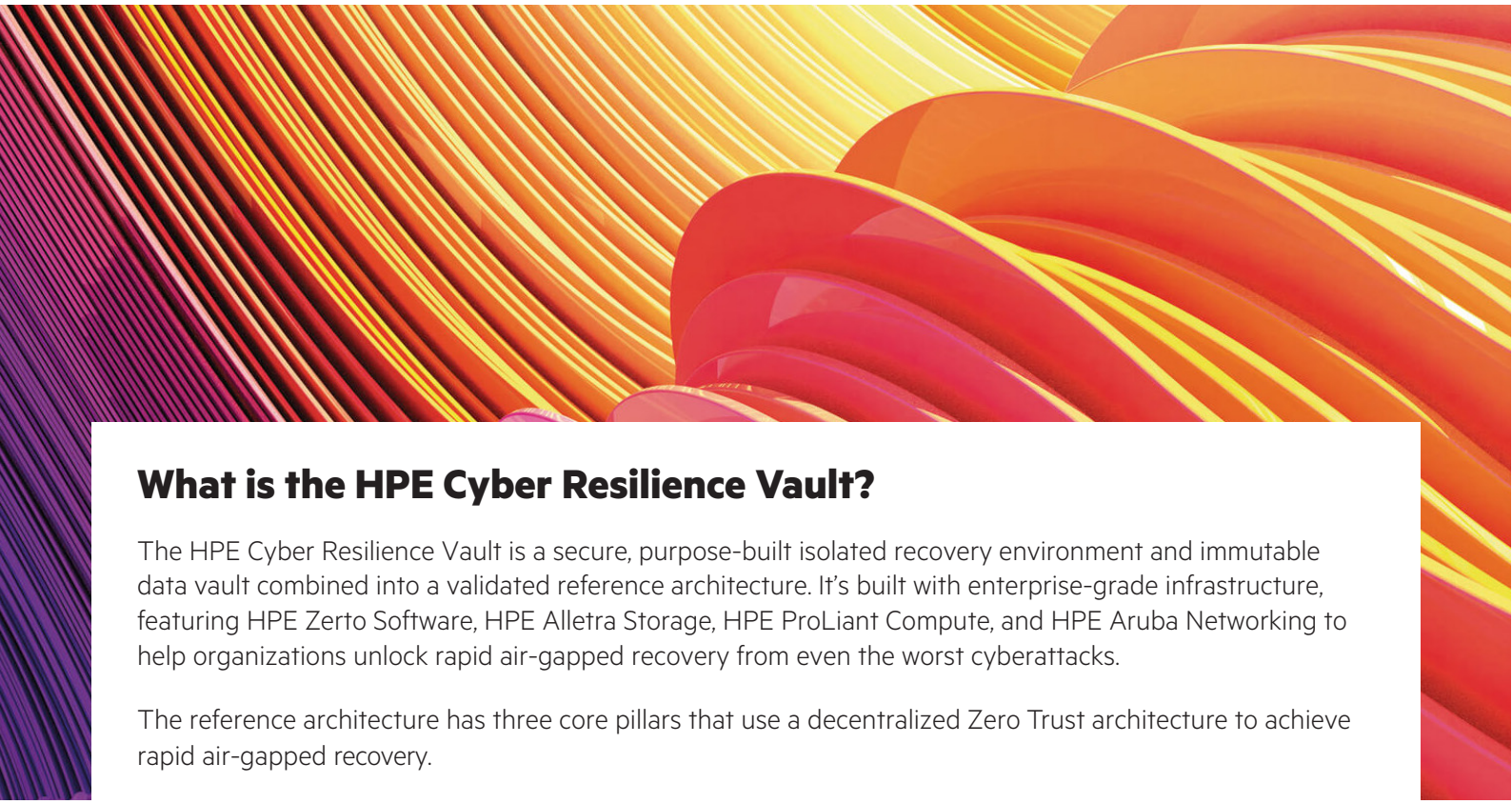
General challenges with traditional vault solutions

Implementing a robust vault solution poses several challenges in modern security infrastructure.

- **Prolonged recovery time.** Common vault technologies often have slow recovery times. Backup processes, such as rehydrating from lower-tier storage or scanning for clean copies, can extend recovery by days or weeks.
- **Post-recovery operation limitations.** Traditional backup appliances or cold cloud storage solutions are not equipped to support extended operation of workloads after a recovery event. This limitation can be critical if ongoing forensic analysis or other activities are required on the production infrastructure.
- **Inadequacy for quick business resumption.** Legacy backup and archive solutions typically do not align with the needs of businesses that require a quick return to operations post recovery. They are often not designed for rapid business resumption, which is crucial in minimizing the impact of downtime on business continuity.

Table 2. Vault competitive analysis

	HPE Cyber Resilience Vault	Dell PowerProtect Cyber Recovery	IBM FlashSystem Cyber Vault	VMWare Live Cyber Recovery	Rubrik Cloud Vault
Real-time, inline encryption detection	✓				
Includes both IRE + IDV	✓			✓	
Rapid, app-centric, journal-based recovery	✓				
Ability to vault cloud data and apps	✓	* Limited	* Limited	✓	✓
Decentralized offline management	✓				
Customer-owned vault	✓	✓	✓		
Production-grade storage	✓		✓		
No slow post-processing data security scans	✓				
No lengthy replication window	✓				



What is the HPE Cyber Resilience Vault?

The HPE Cyber Resilience Vault is a secure, purpose-built isolated recovery environment and immutable data vault combined into a validated reference architecture. It's built with enterprise-grade infrastructure, featuring HPE Zerto Software, HPE Alletra Storage, HPE ProLiant Compute, and HPE Aruba Networking to help organizations unlock rapid air-gapped recovery from even the worst cyberattacks.

The reference architecture has three core pillars that use a decentralized Zero Trust architecture to achieve rapid air-gapped recovery.

1. Replicate and detect

Streaming, near-synchronous data replication protects every production write in real time and immediately detects and alerts any suspicious anomalies. HPE Zerto Software's continuous data protection (CDP) is agentless, so there is nothing inside a protected VM that can be disabled or hijacked by malware.

2. Isolate and lock

The vault itself also includes HPE ProLiant and HPE Alletra Storage. This physically separated, offline vault is air gapped with no access to the internet or production network. It stores immutable data copies on secure, high-performance, FIPS-validated hardware.

3. Test and recover

Easily identify clean restore points, then quickly recover entire multi-VM apps onto high-performance storage—all hile maintaining cross-VM consistency, even with thousands of VMs. Use HPE Zerto's unique, battle-tested journal to unlock RTOs of minutes or hours, not days or weeks.

The HPE Cyber Resilience Vault is a unique combination of hardware and software that dramatically reduces data loss and downtime after an attack—and without having to pay any ransoms.

Learn more at
HPE Cyber Resilience Vault

Chat now (sales)

Hewlett Packard Enterprise

a50010606ENW