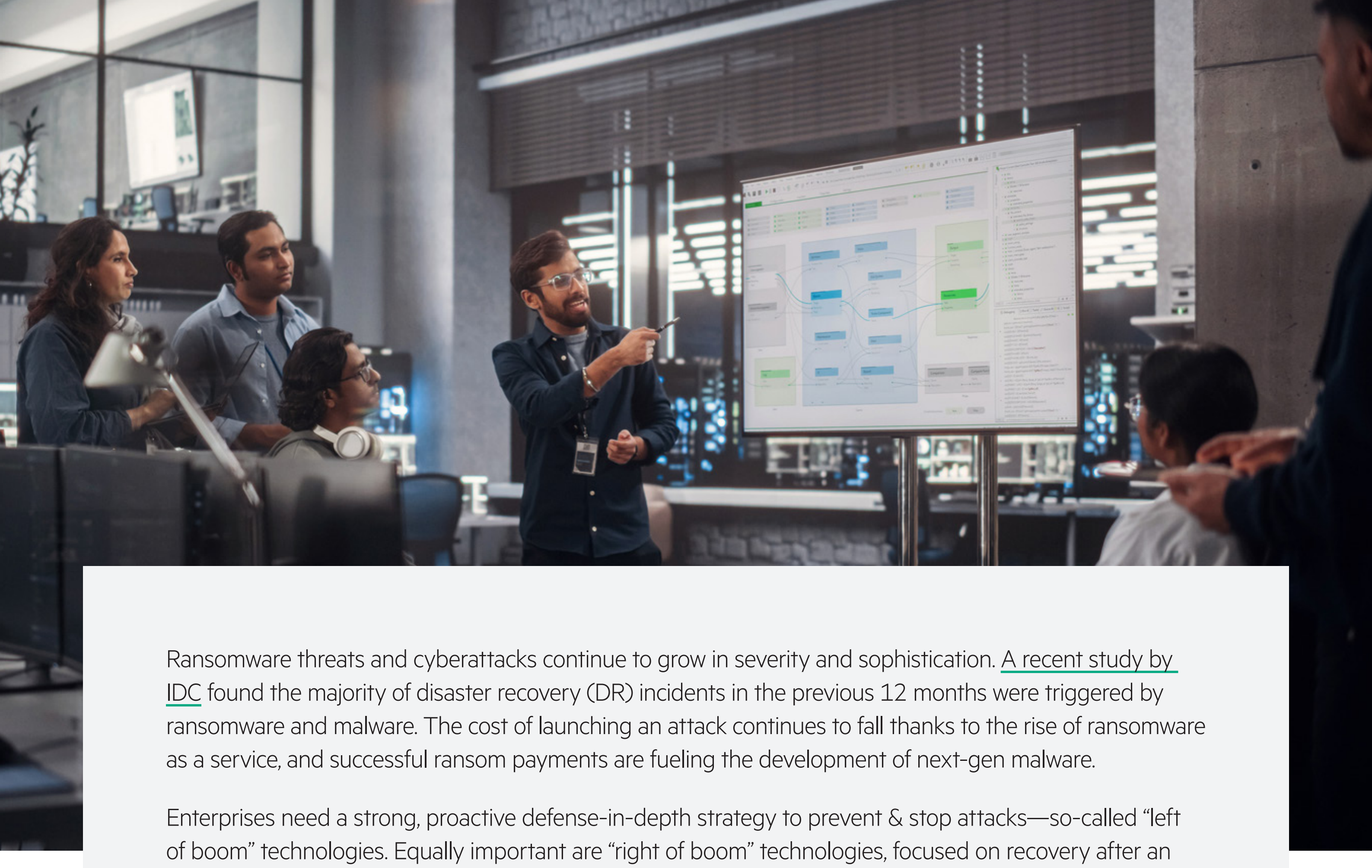
HPE Storage

Brochure

Zerto Cyber Resilience Vault

Unlocking rapid air-gapped recovery

HPE GreenLake



Ransomware threats and cyberattacks continue to grow in severity and sophistication. A recent study by IDC found the majority of disaster recovery (DR) incidents in the previous 12 months were triggered by ransomware and malware. The cost of launching 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.

Enterprises need a strong, proactive defense-in-depth strategy to prevent & stop attacks—so-called "left of boom" technologies. Equally important are "right of boom" technologies, focused on recovery after an attack. Organizations must prioritize both in order to quickly detect, respond, and recover from ransomware.

Why Now?

Although preventive left of boom solutions are more effective than ever, there are increasingly stringent demands placed on enterprise IT. Cyber insurance companies are demanding that companies have better security in place, potentially including data vaults. In the EU, the Digital Operational Resilience Act (DORA) is refocusing attention on security and business continuity. In the US, the SEC has rolled out strict requirements for public corporations, including identifying parties responsible for their cyber resilience strategy. The need for a comprehensive, rigorous approach has never been higher.

Traditional Vaults Leave You at Risk

The common methods for addressing cyber resilience rely on risky vault technologies & architectures. Chief among the drawbacks is the speed of recovery—i.e., recovery time objective (RTO). Pulling from old copies or rehydrating from lower tier storage can extend recovery by days or weeks. Scanning for clean copies prolongs the process even further, as does recovery onto anything other than production-grade arrays. If law enforcement or security teams are performing forensic analysis on production infrastructure, you may need to run workloads elsewhere for some time after recovery—something no purpose-built backup appliance (PBBA) or cold cloud storage can support. It's imperative to quickly resume business operations, which legacy backup and archive solutions are not designed to do.

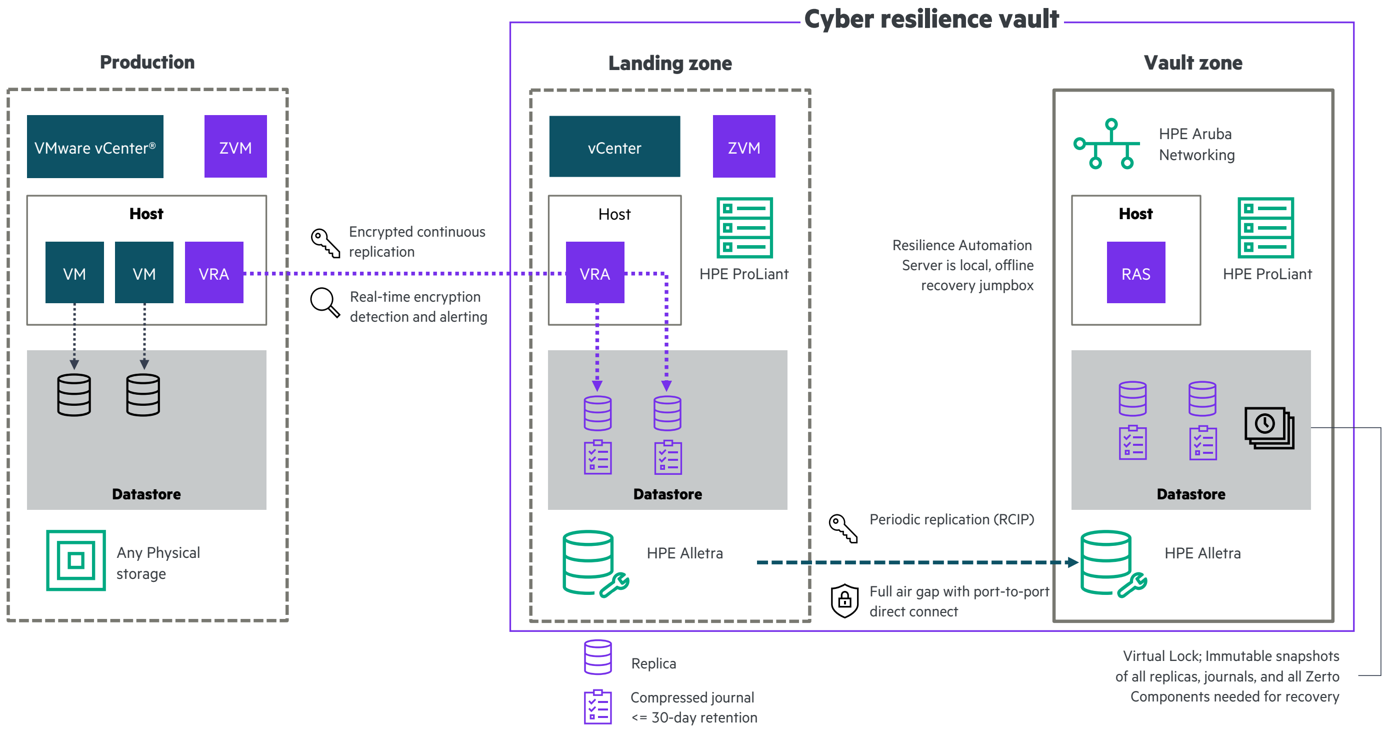
Rapid Recovery with Zerto

Zerto, a Hewlett Packard Enterprise company, enables enterprises to rely on an all-in-one cyber recovery vault designed for mitigating even the most devastating ransomware scenarios.

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

Replicate and detect	Isolate and lock	Test and recover
Streaming near-synchronous data replication protects every production write in real-time and immediately detects and alerts on any suspicious anomalies.	Separated vault is offline, air-gapped, and stores immutable data copies on secure, high-performance hardware from HPE.	Easily identify clean restore points and then quickly recover entire multi-VM apps—all while maintaining cross-VM consistency, even with 1000s of VMs.

How it Works



Cyber resilience vault
Production
VMware vCenter®
ZVM
Host
VM
VM
VRA
Datastore
Any Physical storage
Encrypted continuous replication
Real-time encryption detection and alerting
Landing zone
vCenter
ZVM
Host
VRA
HPE ProLiant
Datastore
HPE Alletra
Periodic replication (RCIP)
Full air gap with port-to-port direct connect
Resilience Automation Server is local, offline recovery jumpbox
Vault zone
HPE Aruba Networking
Host
RAS
HPE ProLiant
Datastore
HPE Alletra
Replica
Compressed journal <= 30-day retention
Virtual Lock; Immutable snapshots of all replicas, journals, and all Zerto Components needed for recovery

Figure 1. Zerto Cyber Resilience Vault architecture overview

The core of the solution is HPE Alletra Storage, HPE ProLiant Compute, HPE Aruba Networking, and Zerto, with two key infrastructure zones aligned to the pillars above.

1

Landing zone

Securely paired with the production site, the VMware vSphere®-based landing zone can be local or remote and can also serve as a traditional DR target if located off-site. The landing zone serves as a replication target for continuous data protection (CDP) with Zerto. Zerto's CDP replication is agentless, so there is nothing inside a protected VM that can be disabled or hijacked by malware. Every write on protected VMs is encrypted, compressed, and sent to the landing zone, where it is stored in a dynamic CDP journal—a streaming log of thousands of restore points with cross-VM consistency and write-order fidelity. The journal has a user-defined history of one hour up to 30 days and is the first and best option for ransomware recovery.

The journals and all associated replicas are attached to virtual appliances running on HPE ProLiant, with their datastores on HPE Alletra vLUNs. As writes are mirrored for the journal, they are also inspected using real-time encryption detection from Zerto for the earliest warning of possible infections. The encryption analysis is also available via API to enable further assessment and visualization with your existing security solutions stack.

2

Vault zone

The vault itself, physically co-located with the landing zone, also includes HPE ProLiant and HPE Alletra. The isolated vault zone, or clean room, is fully air-gapped and has no access to the internet or production network. Since there is no centralized control plane, the vault does not have an exposed management port and does not have any single point of compromise. The HPE Alletra in the landing zone and the HPE Alletra in the vault zone use direct connect remote copy over IP (RCIP) for point-to-point replication of all data from the landing zone, including the Zerto journals and replicas. This approach combines the best of synchronous replication (e.g., hyper-low RPOs and high performance) and traditional asynchronous approaches (e.g., higher latency tolerances and reduced storage consumption). Lastly, the Resilience Automation Server (RAS) inside the vault zone is a lightweight server that runs critical services and works with the native services in HPE Aruba Networking and HPE Alletra to control key cyber resilience measures.

Recovery process

This Zerto architecture covers a variety of infection scenarios, including:

File/Folder/VM Infection: If the ransomware blast radius is limited to files and folders on a VM, these can be near-instantly restored back to their source location from a Zerto journal timestamp that is only 5–15 seconds before the infection. If one or more VMs are encrypted with ransomware, Zerto can near-instantly restore back to production with no intermediate steps (e.g., storage vMotion). This recovery can also apply to all VMs that comprise a multi-VM application stack, including using the exact same clean point-in-time checkpoint, separated by seconds with write-order fidelity, for the restore instead of timestamps staggered across a nightly backup window.

Full Workload Contamination: If all VMs in the production/source site have been infected, but the landing zone is still live and unaffected, a full failover can ensure operations are back up and running in minutes. Because HPE Alletra is all-flash, production-grade storage designed for mission-critical workloads, applications can be run from this secondary site with no performance degradation and no need for additional migration to extra standby storage that's capable of running enterprise workloads.

Multi-Site Infection: If both production and recovery sites are down—e.g., encrypted hosts and rapid lateral movement despite network segmentation—then the Zerto Cyber Resilience Vault becomes the safest clean room in which to recover. A high-level summary of the recovery process is as follows:

- Rebuild the recovery site: Inside the isolated vault, use an immutable snapshot to redeploy the VMFS while preserving the UUID signatures.
- Restore Zerto: Because of Zerto's resilience, the virtual managers and data movers will come online and resume operations without any manual re-configuration or setup.
- Recover data: Using the Zerto journal, select one of the thousands of available restore points to bring up all VMs in the boot order of your choice. Zerto's orchestration engine, combined with the top-tier performance of HPE Alletra, means an RTO of minutes or hours, not days or weeks. Multi-VM app stacks quickly come online together from the exact same point in time to minimize manual configuration after recovery.

Security-By-Design Meets Performance-By-Design

The Zerto Cyber Resilience Vault combines security and performance to meet today's regulatory and compliance requirements with:

- Full air gap for an isolated, disconnected vault
- Zero Trust architecture
- Hardened Linux® virtual appliances
- Built-in principles of least privilege
- Immutable off-site and offline data copies
- Tamper-proof NTP protection
- Inline, real-time encryption detection
- Scalable to 10,000+ VMs per vCenter
- Ciphertext-, time-, and encryption-based passwords
- 100% Availability Guarantee on the landing zone storage
- Next-gen all-flash arrays to temporarily run any demanding application post-recovery
- AI-powered, self-healing storage
- Silicon root of trust from HPE for all hardware
- Decentralized management to eliminate single points of compromise

Unlocking True Cyber Resilience

With the Zerto Cyber Resilience Vault, enterprises now have a secure, high-performance solution to meet the threat of ransomware. Zerto's unique, decentralized architecture enables rapid air-gapped recovery after even the worst attack.

- Dramatically reduce downtime after an attack and avoid direct or indirect loss of revenue.
- Help meet compliance needs, such as HIPAA, DORA, GDPR, SOX, or FISMA/NIST SP 800-34.
- Lower complexity with one vendor delivering a single solution comprised of best-of-breed products at every step in the cyber recovery chain.

Contact us **to see a demo, get bundle pricing, and hear what ransomware resilience can mean for your business.**

Learn more at

Zerto.com/solutions/use-cases/cyber-recovery/cyber-resilience-vault/

Visit **HPE GreenLake**

Chat now (sales)

Hewlett Packard Enterprise