Building a Cyber Resilience Vault with Zerto

How to Achieve Rapid Air-Gapped Recovery After a Ransomware Attack

Ransomware threats and cyber-attacks continue to grow in frequency, 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 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.

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 use composable data protection to build a fast, scalable solution to quickly detect, respond, and recover.

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, including data vaults. In the US specifically, the SEC is proposing even stricter requirements for public corporations, including identifying parties responsible for 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 tape 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 architect and customize an ironclad 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

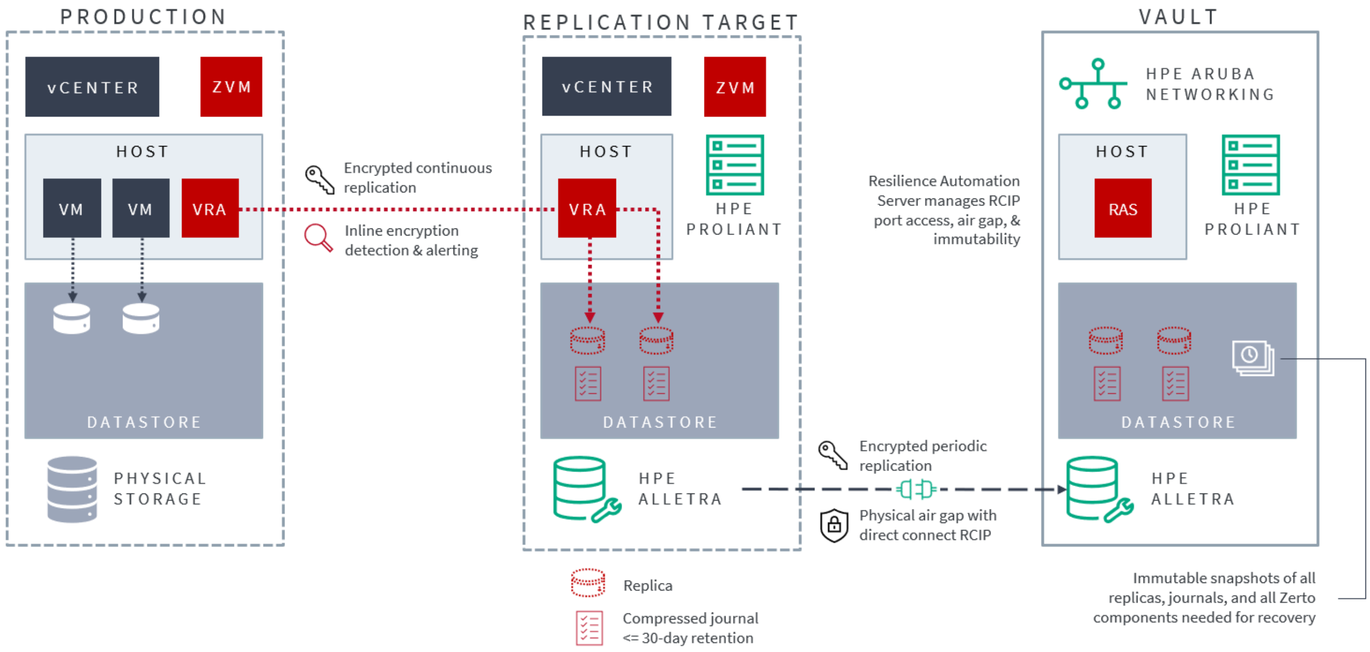
Streaming near-synchronous data replication protects every production write in real-time and immediately detects and alerts on any suspicious anomalies.

Isolate and Lock

Separated vault is physically air-gapped and stores immutable data copies on secure, high-performance, FIPS-validated hardware.

Test and Recover

Easily identify clean restore points and then quickly recover entire multi-VM apps onto high-performance storage—all while maintaining cross-VM consistency, even with 1000s of VMs.


PRODUCTION
vCENTER
ZVM
HOST
VM
VM
VRA
DATASTORE
PHYSICAL STORAGE
Encrypted continuous replication
Inline encryption detection & alerting
REPLICATION TARGET
vCENTER
ZVM
HOST
VRA
HPE PROLIANT
DATASTORE
HPE ALLETRA
Replica
Compressed journal <= 30-day retention
Resilience Automation Server manages RCIP port access, air gap, & immutability
Encrypted periodic replication
Physical air gap with direct connect RCIP
VAULT
HPE ARUBA NETWORKING
HOST
RAS
HPE PROLIANT
DATASTORE
HPE ALLETRA
Immutable snapshots of all replicas, journals, and all Zerto components needed for recovery

How it Works

The core of this cyber resilience solution is based on HPE Alletra, HPE ProLiant, HPE Aruba Networking, and Zerto, with three key infrastructure concepts aligned to the pillars above.

1 Replication Target

Securely paired with the production site, this vSphere-based landing zone can be local or remote and can also serve as a traditional DR target if located offsite. The 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 replication target, 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 Cyber Resilience Vault

The vault itself, co-located with the replication target, also includes HPE ProLiant and HPE Alletra. The isolated vault, or clean room, is physically 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 on the recovery site and the HPE Alletra inside the vault use direct connect remote copy over IP (RCIP) for point-to-point replication of all data from the recovery site, 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).

3 Vault Automation

The Resilience Automation Server (RAS) inside the vault is a lightweight VM that works with native services in HPE Aruba and HPE Alletra to control key cyber resilience measures, including:

- Enabling and disabling RCIP on the HPE Alletra to maintain a truly isolated vault bubble.
- Randomizing the replication ports to reduce traffic predictability.
- Creating snapshots and making them immutable with HPE Alletra's Virtual Lock technology (not even HPE Technical Support can override these tamper-proof retention locks).
- Recovering the Zerto Virtual Manager, journals, and replicas to rebuild a clean Zerto deployment inside the vault should everything else outside it be compromised.
- Logging all activity inside the vault to keep an audit record.

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 recovery site is still live and unaffected, a full failover can ensure operations are back up and running in minutes. Because HPE Alletra is top-tier, 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:

1. Rebuild the recovery site: Inside the isolated vault, use an immutable snapshot to redeploy the VMFS while preserving the UUID signatures.

2. 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.

3. 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, not hours, 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 physical air gap for an isolated, disconnected vault
- Zero trust architecture
- FIPS 140-2 Validated
- Hardened Linux virtual appliances
- Built-in principles of least privilege
- Immutable offsite/offline copies secured with unremovable Virtual Lock
- Tamper-proof NTP protection
- Inline, real-time encryption detection
- Scalable to 10,000 VMs per vCenter
- Encryption at-rest and in-flight
- Ciphertext-, time-, and encryption-based passwords
- 99.9999% Availability Guarantee on the recovery/DR site storage
- Production-grade arrays to run any demanding application
- AI-powered, self-healing storage
- Silicon Root of Trust for all hardware
- Decentralized management to eliminate single points of compromise

Unlocking True Cyber Resilience

With the Cyber Resilience Vault from Zerto, enterprises now have secure, highly customizable options to architect a solution tailor-made for their business. Zerto's unique, flexible architectures enable you to rapidly recover from ransomware.

- Dramatically reduce downtime after an attack and avoid direct or indirect loss of revenue.
- Meet compliance needs, such as HIPAA, 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 recovery chain.

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

CONTACT US

About Zerto

Zerto, a Hewlett Packard Enterprise company, empowers customers to run an always-on business by simplifying the protection, recovery, and mobility of on-premises and cloud applications. Zerto eliminates the risk and complexity of modernization and cloud adoption across private, public, and hybrid deployments. The simple, software-only solution uses continuous data protection at scale to solve for ransomware resilience, disaster recovery, and multi-cloud mobility. Zerto is trusted by over 9,500 customers globally and is powering offerings for Amazon, Google, IBM, Microsoft, and Oracle and more than 350 managed service providers. **www.zerto.com**