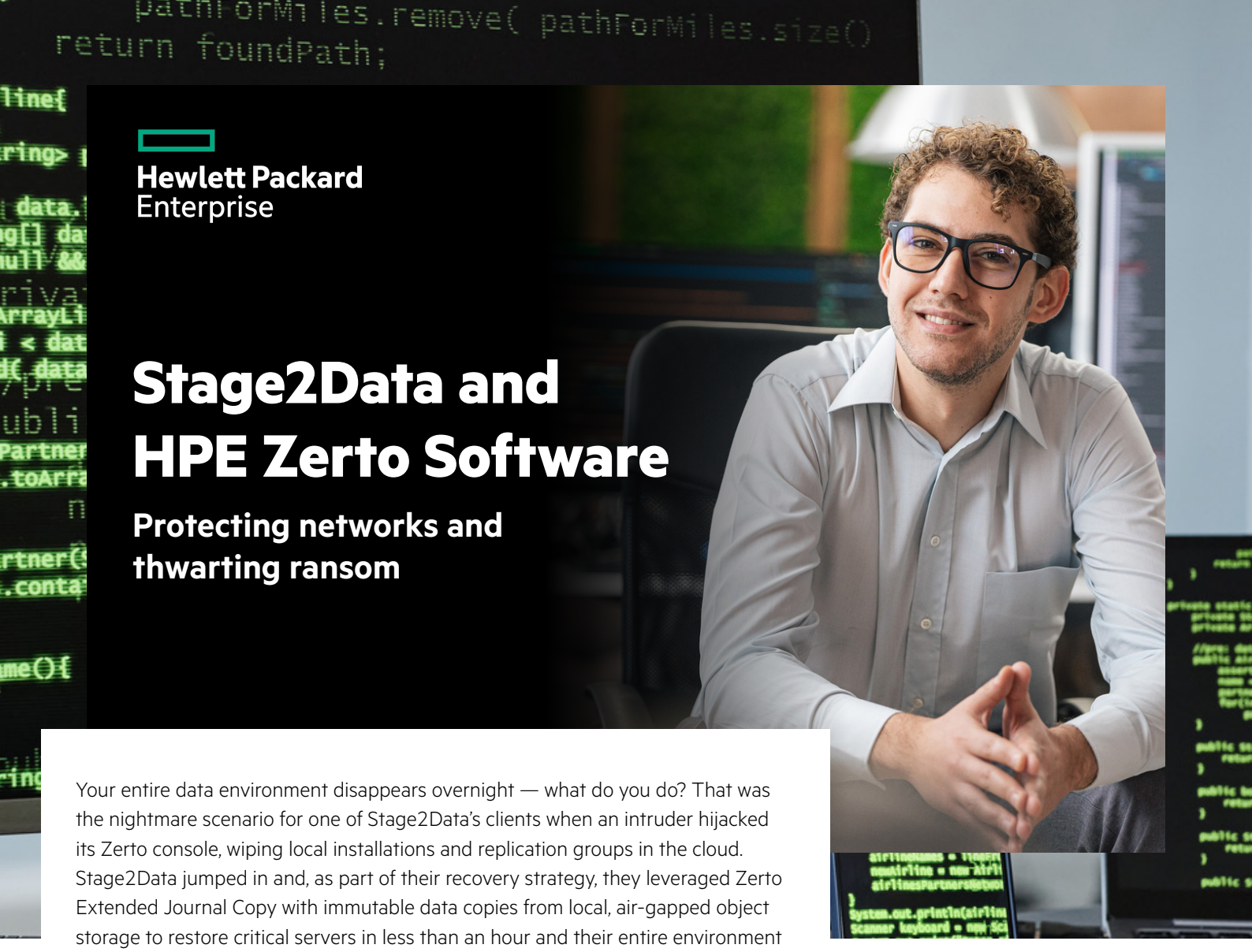

Hewlett Packard Enterprise

Stage2Data and HPE Zerto Software

Protecting networks and thwarting ransom

Your entire data environment disappears overnight — what do you do? That was the nightmare scenario for one of Stage2Data's clients when an intruder hijacked its Zerto console, wiping local installations and replication groups in the cloud. Stage2Data jumped in and, as part of their recovery strategy, they leveraged Zerto Extended Journal Copy with immutable data copies from local, air-gapped object storage to restore critical servers in less than an hour and their entire environment within a few hours. Freed from paying ransom or losing vital data, the client switched focus to future-proofing its IT setup. This project shows how rapid disaster recovery can save more than just data — it preserves customer confidence and business momentum. By deploying locked backups and a dependable hosting partnership, the client shifted to a more resilient model and emerged stronger. Their experience underscores one truth: fast, reliable protection can be the difference between a crisis and a comeback.

A catastrophe unfolding

A Stage2Data client in the United States fell victim to a cyberattack in which an intruder gained admin-level access to its infrastructure.

The Stage2Data team was alerted at 4:00 a.m. that something was amiss and immediately reached out to the client, confirming that an intruder was deleting not only the client's local production environment and severing the client's connection between their two sites but also the associated virtual protection groups (VPGs) stored in Stage2Data's S3 compatible cloud environment.

This action could have catastrophic consequences for the client. Losing local servers is bad enough, but losing your protection groups means your fallback plan is also gone. The intruder aimed to force a ransom payment by taking away every restoration option. Since the client's direct path to recovery vanished, the odds of retrieving data without paying the ransom looked grim. With the main environment sabotaged, the only remaining question was whether there was an extra layer of security that the intruder couldn't touch.

STAGE2DATA

Industry: Computer software/ services
Country: Canada

Vision

Recover data environment and remediate ransomware attack

Strategy

Restore virtual machines (VMs) from locally stored immutable data copies

Outcomes

- Brings servers back online within one hour
- Prevents downtime and data loss
- Shuts down cyberattacks without paying ransom

The Stage2Data client's head of information technology was alarmed. "Our entire business hinges on making sure data is at our fingertips. The idea of paying a ransom felt impossible. We knew that if we lost access to our data for even a few hours, our employees wouldn't be able to serve our customers, and we'd lose trust in the market."

Saving the day

Fortunately, as part of the client's disaster recovery solution, archival to Stage2Data's S3 object storage was added, creating an air-gapped long-term backup that the hackers couldn't touch. This layered approach — combining the HPE Zerto software-based replication and Zerto Extended Journal Copy features with Stage2Data's local object storage — addressed the challenge. This storage design includes object locking with immutable snapshots. Once written, these snapshots cannot be removed or changed for the duration that the retention policy specifies.

By storing these copies locally, the recovery process could begin without having to download huge files from a remote third-party provider. The technical team used the local, locked snapshots to restore critical servers, bypassing the standard replication path in the VMware® environment that had been wiped. Then, the team tapped into the Zerto Extended Journal Copy to recover completely.

Since the object storage was already in Stage2Data's cloud, there was no need to wait for data transfers from an internet-based, third-party object storage provider. A direct copy of the necessary VMs was instantly available, so the restore started right away. Testing to see if data was malware-free required some steps, but the first group of servers was up in about an hour.

"We were then able to, within the hour, have servers back up and running for our secondary recovery path. If we didn't have EJC and the object storage local, that wouldn't have been feasible. The attackers knew the customer infrastructure well enough to delete the primary path, so having a locked backup off that path saved the day," says the Stage2Data client's head of information technology.

The approach involved spinning up the client's systems on Stage2Data's own infrastructure, free from any taint left behind by the attacker. This move bypassed the compromised local network and let the client's workforce get back to work in a clean virtual environment.

Stage2Data used its proprietary Network Recovery-as-a-Service (NRaaS) solution to quickly pull from the client's selected recovery point objective (RPO) and recovery time objective (RTO) points. Then, using HPE Zerto Software, Stage2Data took the virtual machine disks (VMDKs) and system files and restored the VMs to the way they were at the time of the recovered snapshot. Typically, in the event of a cyberattack, NRaaS can failover a client's internal intrusion prevention system (IPS) and their internet-facing IP addresses within a few hours, so a client doesn't have to change its DNS.

Petrus Human, president & CEO, Stage2Data comments, "We've got many Zerto customers. The preference is always to go with Zerto because of their ability to failover and recover a client's environment as quickly as possible."

> The idea of paying a ransom felt impossible. We knew that if we lost access to our data for even a few hours, our employees wouldn't be able to serve our customers, and we'd lose trust in the market."
>
> – **Stage2Data** client's head of information technology

Shutting down the cyberattack

Combining HPE Zerto's software-based replication and LTR features with Stage2Data's local object storage successfully shut down the cyberattack. The client's standard backup system had been destroyed, and the snapshots that the attackers could not remove proved to be the last line of defense.

The outcome of the recovery effort stands as a strong example of thoughtful preparation and swift action. The collaboration between Stage2Data and HPE Zerto resulted in several significant benefits.

Firstly, the client did not have to pay any ransom. When the primary replication path was compromised, the client had a fallback path. By utilizing immutable data copies retained on Stage2Data's object storage, the team had a reliable way to restore vital systems. Consequently, there was no need for the client to risk paying criminals for a potentially ineffective decryption key. Additionally, the client's servers were brought back online in about one hour from the time the internal systems triggered an alert. Stage2Data's internal alert system detected the intruder early, allowing the team to address the issue before more damage occurred. The combination of Zerto Extended Journal Copy capability and Stage2Data's locked object storage proved crucial, keeping the data accessible for immediate action. This resulted in minimal disruption, which is critical, as every minute of downtime can be costly. This incident clearly demonstrated the importance of multilayered data protection in safeguarding an organization from irreversible losses. It underscored the value of advanced threat detection and alert systems.

Transitioning to infrastructure as a service post recovery

The incident forced the Stage2Data's client to rethink how it ran its core workloads. They recognized that local infrastructure left them vulnerable to human-driven intrusions. "We wanted an approach that would protect our data, give our employees confidence, and preserve our relationships with customers," says the Stage2Data client's CIO.

A move to infrastructure as a service (IaaS) looked appealing. Once the client had recovered and assessed the situation, they realized they had superior performance on Stage2Data's NVMe-powered DR site. They decided to remain as an IaaS customer and not fail back to their legacy infrastructure. The benefits that came from this decision include predictable costs, and a safe environment, removing the need to rebuild in-house from local hardware that was already compromised. By shifting to IaaS, the client now benefits from a fully managed platform that boosts performance and provides peace of mind.

> We've got many Zerto customers. The preference is always to go with Zerto because of their ability to failover and recover a client's environment as quickly as possible."
>
> – **Petrus Human**, President & CEO, Stage2Data

“We were then able to, within the hour, have servers back up and running from our secondary recovery path. If we didn’t have Stage2Data’s team recommend and configure Zerto EJC and the object storage local, that wouldn’t have been feasible.”

– **Stage2Data** client’s head of information technology

Looking ahead

This case reinforces the wisdom of a belt and suspenders model when it comes to data safety. When the primary replication path was destroyed, the client had a fallback path. A malicious actor tried to remove every route to recovery, but locked LTR snapshots in Stage2Data’s local object storage stayed intact.

For a stronger disaster recovery plan, they combined multiple data protection technologies such as Zerto Extended Journal Copy with local immutable object storage for added protection. Stage2Data uses HPE Zerto not just in emergencies but across its broader disaster recovery services. With the HPE Zerto continuous data protection capability, clients achieve near real-time recovery points and nondisruptive failover. This enhances Stage2Data’s Disaster Recovery as a Service (DRaaS) platform, protecting VMs, reducing downtime, and simplifying backup management.

Solution

- HPE Zerto Software
- Stage2Data’s DRaaS, NRaaS, and IaaS

Explore more

→ **Learn** how HPE Zerto can help you with ransomware resilience and disaster recovery

Visit **HPE.com**

Chat Email Call Updates

a00146504ENW, Rev. 1

Hewlett Packard Enterprise