# Why Zerto for Ransomware Resilience

Ransomware attacks have become increasingly common in recent years, targeting organizations of all sizes and industries. The consequences of a ransomware attack can be devastating, with organizations losing access to critical data and systems, even facing financial losses and reputational damage. To combat the ever-growing threat of ransomware, Zerto, a Hewlett Packard Enterprise company, uses a combination of advanced technologies and best practices.

## Continuous Data Protection and Journal-Based Replication

Zerto continuous data protection (CDP) and unique journaling technology enable organizations to continuously capture and store changes to virtualized data in near real time, allowing for near-instant recovery after data loss or corruption. Even if ransomware manages to encrypt data on a system, the journal can quickly restore the data from one of thousands of recovery checkpoints. Each of these checkpoints are only 5–15 seconds apart, enabling granular restores instead of reverting back to a nightly backup copy that is hours behind production.

Journal-based replication complements CDP by creating multiple, consistent copies of data across different storage systems, ensuring that even if one data copy is lost or corrupted, other copies can be used for recovery. This method also prevents ransomware from spreading, since multiple copies of data provide multiple points of entry where ransomware can be isolated and removed. In addition, one-to-many, journal-based replication enables organizations to protect and restore their data anywhere. This allows data to be easily copied from a production site to multiple target locations either on-premises, in the public cloud, or co-located. With journal-based replication, organizations can protect their data beyond the traditional 3-2-1 data protection rule.

Zerto can also create immutable copies from the journal on Azure Blobs, Amazon S3, or S3-compatible storage. This gives you a copy of your data that can't be modified or changed—allowing you to restore that copy to any available Zerto infrastructure for recovery.

## Granular Recovery and Seamless Integration

A major benefit of these technologies is granular recovery. Organizations can choose to recover specific files or folders rather than restore an entire system or data set. This targeted and efficient recovery reduces downtime and minimizes the impact on the organization.

Organizations also benefit from Zerto's seamless integration with other security and data management systems. Using Zerto APIs can provide an easy way to interface with existing infrastructure and technology investments—including security event and incident management and endpoint detection and response—to gain further value through automation. This can improve an organization's overall security posture and help it respond to and recover from security events rapidly.

## Real-Time Encryption

The Zerto Encryption Analyzer instantly detects and alerts about suspicious write activity on protected workloads. Get the earliest warning sign of malicious anomalies with the in-line encryption and alerting system. You don't need to wait for ransomware detection after backing up; you can now detect within seconds at the first moment of impact.

You can also minimize data loss by enabling IT or SecOps to act mid-attack rather than days or weeks later. The API-first approach allows security teams to integrate with existing security solutions for added value. These security enhancements are included at no additional cost, without any need for additional infrastructure, and with no effect to the production environment.

## Isolate and Lock with a Cyber Resilience Vault

The Zerto Cyber Resilience Vault provides recoverability after even the worst attacks. Its completely isolated, air-gapped recovery environment stores immutable copies on secure, high-performance hardware. The Zerto Cyber Resilience Vault uses zero trust architecture and a combination of best-in-class software and hardware to provide a highly secure clean room—all while enabling rapid recovery in minutes or hours, not days or weeks.

## Why Make the Switch to Zerto?

All the above Zerto features are critical to accomplishing ransomware resilience. Here are the top reasons for choosing Zerto to mitigate and eliminate the threat of ransomware.

**Recover everything from files to data centers.**

With Zerto, organizations can recover not only individual files and folders, but entire VMs, applications, and data centers as well.

**Match the pace of today's digital business environment.**

Zerto offers near real-time replication and data protection through CDP. This is critical in today's fast-paced business environment, where even the smallest amount of downtime can be costly and disruptive.

**Leverage—rather than replace—what you already own.**

Zerto integrates seamlessly with existing IT infrastructure through open APIs. Organizations can easily incorporate Zerto into their existing cybersecurity operations and workflows.

**Benefit from a resilience strategy tailored to your needs.**

Zerto offers flexible recovery options. Instead of modifying infrastructure to meet the demands of an inflexible solution, organizations can tailor Zerto to meet their unique needs—whether that's recovering data to the same location, a different location, or a cloud-based platform.

**Simplify your infrastructure and management overhead.**

Zerto is easy to use and provides intuitive and user-friendly features. Even organizations with limited IT expertise can use Zerto to successfully recover from ransomware attacks—no additional data centers or personnel required.

## Choose the Industry Best in Ransomware Resilience

Zerto for ransomware resilience provides comprehensive recovery capabilities, uses real-time replication and synchronization, integrates seamlessly with existing IT infrastructure, offers flexible recovery options, and is easy to use. With Zerto, organizations can detect and protect their data from ransomware attacks and recover from those attacks without incident when they do occur.

Learn more about rapid air-gapped recovery through the new Zerto Cyber Resilience Vault.

**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**



RITM0077112