

# What's New in Zerto 10

## Real-Time Detection Meets Real-Time Protection

There is no larger threat to an organization today than a ransomware or malware attack. Last year, 61% of reported disaster recovery (DR) responses were triggered by ransomware<sup>1</sup>, and the average recovery time after an attack was an alarming one month<sup>2</sup>. Today's organizations can't afford these types of disruptions. Zerto 10 introduces new enhancements to unlock ransomware resilience and rapid recovery to address this evolving threat landscape.

### 1. Real-Time Encryption Detection

The new encryption analyzer in Zerto 10 instantly detects and alerts about suspicious write activity on protected workloads. Get the earliest warning sign of malicious anomalies with the new inline encryption and alerting system. You no longer must wait to detect ransomware after backing up—detect within seconds at the first moment of impact.

The new feature allows you to stay protected and minimize data loss by enabling IT or SecOps to take action 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 new security enhancements in Zerto 10 come at no additional cost, without any need for additional infrastructure, and without affecting your production environment.

### 2. Isolate and Lock with Cyber Resilience Vault

Ensure recoverability after even the worst attacks with Zerto's new Cyber Resilience Vault, a completely isolated, air-gapped recovery environment with immutable copies on secure, high-performance hardware.<sup>3</sup> The 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.

*Note: built on Zerto 10, the vault requires separate bundle purchase.*



Replicate and Detect



Isolate and Lock



Test and Recover

### Three Pillars of Ransomware Resilience with Zerto

#### KEY HIGHLIGHTS

##### Real-Time Encryption Detection

Earliest warning alarm so you can take action within seconds of a malicious encryption event.

##### Cyber Resilience Vault

Highly secure, air-gapped, and isolated recovery environment with immutable data copies using zero trust architecture.<sup>3</sup>

##### Secure Zerto Appliance

New Linux-based appliance for greater security and simplified management.

##### Zerto for Azure at Scale

Refactored cloud-native architecture with new support for multi-disk consistency for replication to, from, and across Azure regions.

### 3. Enhanced Cloud Protection for Azure

With all new replication architecture for Microsoft Azure, Zerto 10 enhances DR and mobility for more efficient scale-out protection of hundreds or thousands of cloud VMs to, from, and within Azure. In-cloud protection with Zerto protects VMs across regions with replication, failover, and recovery. Zerto for Azure also includes support for multi-disk consistency during replication using a new API co-developed with Microsoft. Plus, the new cloud-based Virtual Replication Appliances (VRAs) use cloud-native scale sets to easily adapt to replication loads and burst when needed.

### 4. Secure Management Appliance

Minimize the attack surface and experience seamless migration with the new Linux-based appliance. The Zerto Virtual Manager Appliance (ZVMA) is easy to deploy and is more secure, including support for multi-factor authentication (MFA) and role-based access control (RBAC). The ZVMA is pre-hardened and simplifies management, with an OVF that bypasses manual VM or OS setup and provides automatic updates to maintain the appliance. A new utility simplifies the migration from existing Windows ZVMs to the ZVMA, so transitioning to the new Zerto appliance can be done in minutes.

## Other Enhancements

Additional improvements in Zerto 10 include:

- **Immutable incrementals:** Scheduled copies from the Extended Journal can be made immutable on Azure Blobs, Amazon S3, or other S3-compatible storage. With Zerto 10, incremental retention sets, not only full copies, can be locked as well.
- **Support for UEFI for AWS:** VMs using UEFI can now be replicated to AWS to support a broader range of configurations and options for hybrid cloud deployments.
- **Self-service recovery reports:** Enterprises or MSPs using the Zerto Self-Service Portal (ZSSP) can now enable or disable access to recovery and compliance reports.

## Zerto 10 Offers Unparalleled Ransomware Resilience

Get unparalleled speed in protection and recovery from ransomware attacks, as well as early detection, with Zerto 10. Embrace the future of data protection and recovery in a hybrid, multi-cloud environment. Ready to start using Zerto? Try a hands-on lab or start a 14-day free trial today:

[Request a Demo](#)

<sup>1</sup> IDC, "State of Ransomware and Disaster Preparedness"

<sup>2</sup> Sophos, "State of Ransomware Report"

<sup>3</sup> Built on Zerto 10; requires separate vault purchase of all-in-one bundle combining the necessary software and hardware

## 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](http://www.zerto.com)