



What's New in Zerto: Latest Product Features and Enhancements

Ransomware is the most prevalent disaster threat to organizations in every industry, disrupting business, causing reputational damage, and resulting in lost revenue. With attacks growing in both volume and severity, malicious actors are finding sophisticated methods of targeting any vulnerability, in every cloud and every platform. PaaS, SaaS, and IaaS are not immune, so full spectrum protection across VMs, containers, and cloud-native environments is now an IT imperative.

Staying in lock step with advancing data protection methods for ransomware recovery, disaster recovery, and multi-cloud mobility, Zerto, a Hewlett Packard Enterprise company, released new product features in Zerto 9.5, Zerto In-Cloud for AWS, and Zerto Backup for SaaS, powered by Keepit. These new capabilities make it easier to adopt multi-cloud and multi-platform architectures that offer increased recovery options and greater security for ransomware readiness. With this latest release, Zerto bolsters protection for any app, any cloud, and any threat.

New Immutability Options for Ransomware Recovery

- Microsoft Azure Blob Storage is now supported as a destination for Zerto users to create and manage immutable data copies for ransomware recovery.
- Zerto expanded support and management of immutability for third-party S3-compatible storage so that recovery data managed by Zerto can be stored in an immutable state for ransomware recovery on a variety of storage systems.
- Azure Active Directory may now be backed up with immutability offsite through Zerto Backup for SaaS.

New Virtual Zerto Appliance and Security Enhancements

- Hardened security is more important than ever with ransomware attacks on the rise. Zerto now offers a Linux-based appliance for Zerto management that is pre-hardened for enhanced security, deploys quickly, enables multi-factor authentication (MFA), and offers easy management via hands-off upgrades and troubleshooting.
- Zerto's new role-based access controls (RBAC) and multi-factor authentication (MFA) for the customer web portal, MyZerto, and Zerto Analytics allows customers greater control over access to their Zerto solution.
- Additional security enhancements including replication appliance updates, more granular control over SSH communication between components, and optional pre- and post-login banners improve security awareness.

Instant File Restore for Linux

- Zerto expands operational recovery by supporting instant file restore for Linux servers, complementing existing support for instant VM for Linux as well as full Windows support.

Zerto In-Cloud for AWS Updates

- Zerto In-Cloud, for region-to-region protection across EC2 instances, now has new CloudWatch integration that increases monitoring capabilities to support automating recovery based on specific events, more integration options with third-party management tools, and monitoring Zerto alongside other cloud applications and tools.
- Zerto In-Cloud is now fully integrated into Zerto Analytics so deployments can be fully viewed alongside other Zerto solutions across multi-site, multi-cloud deployments.

Google Cloud Storage Support for Additional Data Copies

- Google Cloud Storage is now a destination for long-term retention of replica copies providing extra data resilience on an additional platform.

Managed DRaaS Enhancements

- Providers can now assign one or more service profiles to a tenant and mask any unassigned profiles.
- Users can configure long-term retention settings inside their service profiles. This feature allows service providers to have continued control over these critical SLA/SLO settings for their customers.

Additional Product Enhancements

- The Zerto Virtual Manager is now supported on Windows Server 2022.
- For more granular control of what data is replicated per Virtual Machine, individual disk volumes may now be excluded from replication with Zerto continuous data protection.
- Disaster recovery testing may now be carried out in a storage area separate from the recovery data to allow you more time to test and validate recovery.
- Enhancements to selected Zerto alerts, errors, and messages simplify management with more detailed information and context.
- Zerto disaster recovery to Microsoft Azure is now optimized for API integration efficiency and require fewer Zerto Cloud Appliances for protection.

As our digital world expands, there are more platforms, more data in the hands of more users, and more applications to protect. New and growing threats to your organization mean that your data protection strategy must evolve to keep your SLAs intact to deliver always-on business. Zerto's leading solution for disaster and ransomware recovery underpinned by always-on, continuous data protection defeats threats head-on with modernized data protection for any app, any cloud, and any threat.



TRY ZERTO NOW



GET OUT OF RANSOMWARE JAIL WITH ZERTO FREE EDITION

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. Built for enterprise scale, Zerto's simple, software-only platform uses continuous data protection to eliminate the risks and complexity of modernization and cloud adoption. www.zerto.com

Copyright 2022 Zerto. All information may be subject to change.