Zerto

Overview

Zerto, a Hewlett Packard Enterprise (HPE) company, provides data protection software for virtualized infrastructure and containerized and cloud environments. Its main product, Zerto Virtual Replication (ZVR), was released in August 2011. ZVR is the foundation of the Zerto Platform, which was announced in May 2018. Zerto provides continuous data protection (CDP), including disaster recovery (DR) and data mobility by mirroring I/O traces through a filter driver and writing them to a local or remote log.

Zerto is sold standalone and through managed service providers (MSPs). Effective June 2023, Zerto will also be delivered as HPE GreenLake for Disaster Recovery, alongside the HPE GreenLake for Backup and Recovery offering that is based on HPE StoreOnce code. The HPE GreenLake for Data Protection offerings are covered in The Futurum Group's Backup-as-a-Service research, and HPE StoreOnce appliances are covered in The Futurum Group's Data Protection Systems coverage.

Highlights

- Input/output (I/O) logging for continuous data protection
- Agentless, changed block tracking (CBT)-based replication that is both hypervisor-based and hypervisor-native.
- Supports Microsoft and VMware virtualized environments (on-premises and cloud).
- Zerto for Kubernetes launched April 2021.
- Focus on continuous data protection is broadening to include multi-cloud workload mobility and analytics-driven insights and testing.

Usage and Deployment

Zerto provides ransomware resilience, disaster recovery, and workload mobility for virtualized and containerized on-premises and public cloud-based environments. Journaling and replication of data provides the foundation of Zerto's ability to deliver these functionalities.

- Characteristics
  - Performance – Depends on source infrastructure including network connections. No performance impact on production systems or VMs.
  - Availability – Journal-based CDP approach provides application-consistent recovery to granular restore points.
  - Replication – Journal-based with heterogeneous support (can replicate to another Kubernetes cluster, etc.).

- Use Cases/Implementations
  - Disaster recovery
  - Ransomware resilience
  - Continuous data protection (CDP)
  - Operational recovery
  - DR testing, documentation, automation
  - Monitoring and analytics
  - Hybrid, multi-cloud data mobility & migrations
- System Environments
  - Supported sources
    - On- and off-premises VMware ESXi environments
      - Maintains write-order fidelity and consistency across multiple VMs using consistency grouping.
      - Additionally, provides application consistency for Microsoft VSS applications, a number of databases (incl. Oracle), and VMware vCloud Director vApps.
    - Kubernetes environments are supported via Zerto for Kubernetes.
- Deployment and Administration
  - Virtual Replication Appliances (VRAs) are installed on host infrastructure as the data movers.
  - Management is through a Zerto Virtual Manager (ZVM), an appliance based on Linux
  - Simple-to-use interface and native integration with hypervisor management capabilities (e.g. VMware vMotion).
  - On-premises or cloud-based deployment
    - Requires knowledge for configuring underlying infrastructure.

Key Capabilities

Architecture and Deployment

Zerto initially focused on protecting virtualized environments, with Microsoft Hyper-V and VMware ESXi environments as well as VMware vSphere Virtual Volumes, vVols. The solution has since been expanded to support Kubernetes environments, including Amazon Elastic Kubernetes Service (Amazon EKS), Azure Kubernetes Service (AKS), Google Kubernetes Engine (GKE), Red Hat OpenShift, VMware Tanzu, HPE Ezmeral, and IBM Cloud Kubernetes Service (IKS). Through an OEM partnership with Keepit, Zerto Backup for SaaS can also protect cloud-based software-as-a-service (SaaS) applications.

Zerto can be deployed on-premises or in the cloud. On-premises, the Zerto configuration consists of:

- Zerto Virtual Manager (ZVM), which oversees the data replication between the protected and recovery sites.
    - In virtualized environments, this includes interacting with the hypervisor management interface (e.g., VMware vCenter) to monitor changes in the hypervisor environment and respond accordingly (e.g., executing a VMware vMotion).
    - In Kubernetes environments, this includes interacting with the Zerto Kubernetes Manager Proxy, which orchestrates replication between a Kubernetes cluster and virtual replication appliances (VRAs).
    - Deploys from an OVF and runs as a virtual appliance
- Virtual Replication Appliance (VRA), which manages the replication of data from the protected source to the target where data is stored in the journal or a long-term retention repository.
    - In virtualized environments, this is a purpose-built appliance installed on each hypervisor host where VMs are to be protected from or to.
    - In Kubernetes environments, this is automatically installed on a DaemonSet on each cluster node.

When deployed in the cloud, Zerto consists of:

- Zerto Cloud Appliance (ZCA), a dedicated cloud VM comprised of the Zerto Virtual Manager (ZVM), a service that hosts the UI and integrates with the native APIs of Azure/AWS for management and orchestration, and a VRA that integrates natively with the platform it is deployed on, and that utilizes Azure Blob storage or Amazon S3 buckets for journal storage.

Whether deployed on- or off-premises, data protection and mobility operations are configured through the creation of Virtual Protection Groups, or VPGs. VPGs allow for application-consistent protection and mobility, spanning the multiple VMs, microservices, and storage volumes that modern applications are composed of.

Every write to a protected source is mirrored by Zerto and replicated to the Zerto journal, for storage for a user-defined period of up to 30 days. Additionally, point-in-time data copies can be offloaded to a secondary storage repository, such as Amazon S3 or Azure Blob Storage.

Zerto has two licensing options for its VM and Kubernetes protection: Zerto Data Protection (ZDP), which addresses local replication and operational recovery use cases, and Zerto Enterprise Cloud Edition (ECE), which includes ZDP as well as multi-cloud DR functionality.

Administration and Management

Protection and recovery sites can be managed by a single vCenter Server. Additionally, Zerto offers a web-based console that allows all of the assets under its protection to be centrally managed and monitored. This includes configuration of protection policies, including replication policies, monitoring of performance and success of protection jobs, and the ability to initiate recovery options.

Data Cataloging, Search and Analytics

Zerto's Analytics Resource Planner and centralized dashboard provide analytics within the context of, and centralized visibility and alerting for, the protected Zerto environment, spanning on-and off-premises data stores. Use cases include resource planning, monitoring, and troubleshooting. Customers can use the dashboard to improve efficiencies as well as their data protection strategies, for example conducting "what-if" scenario modeling and obtaining visibility into average recovery point objectives (RPOs). Zerto also has the ability to identify unprotected virtual machines and to forecast what infrastructure would be required to protect them.

Recovery and Replication

As opposed to more traditional backup and operational recovery solutions, Zerto offers replication and journal-based disaster recovery and migration capabilities for applications, files, VMs and entire datacenters. On the Kubernetes side, all associated persistent data, metadata, and Kubernetes objects are protected.

Zerto uses agentless I/O captures from the hypervisor in a VM environment, or through I/O capture facilities when deployed on a public cloud. Data can be replicated to and from VMs and clusters operating on different platforms, including different hypervisors, storage infrastructures, and storage protocols.

The VRA continuously replicates data between the source and target hosts. Only changed data is replicated, for what Zerto calls "near synchronous" replication in that it blends the lower cost and reduced performance impact of asynchronous replication with the more limited data loss and downtime of synchronous replication. Both VMs and virtual disks (VMDKs) are supported, and multiple VMs or VMDKs with dependencies can be protected consistently via a VPG.

Replicated data is stored in the Zerto journal and full replicas. Users can recover to any data point stored within the journal.

Zerto has steadily been enhancing its ability to deliver CDP, notably by complementing its short-term retention capabilities with the addition of immutable data copies. In an effort to leverage CDP to displace traditional backup products, Zerto has added compression and audit trail logging,

as was the ability to protect to Azure, AWS and GCP. A workflow-based instant (per Zerto) file and folder restore capability was also added.

Automation and orchestration capabilities for workload mobility, alongside richer analytics and testing capabilities for analysis, compliance, and reporting purposes, have also been introduced to Zerto.

One of Zerto's key differentiators compared to earlier-to-market CDP providers is its ability to provide data and workload migration and recovery across on-premises and cloud environments. Today, Zerto supports Amazon Web Services (AWS), Microsoft Azure, Microsoft Azure VMware Solution, Google Cloud VMware Engine, IBM Cloud for VMware Solutions, and Oracle Cloud VMware Solution. Additionally, it has automated operating system and failback configuration for streamlined failover to the public cloud. Failovers can be tested, and virtual protection appliances re-populated for load balancing purposes either specifically by the administrator, or automatically by Zerto. Zerto In-Cloud (ZIC) for Amazon Web Services (AWS), introduced in late 2021, brought DR cross-region and availability zone disaster recovery orchestration to Amazon EC2 instances. Cross-region DR is also available inside Microsoft Azure.

Data Efficiency

Data is compressed at the source and transferred to the target over a wide-area network (Zerto itself does not support native deduplication, but deduplication is available through partner solutions).

Encryption and Immutability

Zerto supports Immutable Retention sets for Azure Blobs, Amazon S3, and S3-compatible repositories via S3 Object Lock. The solution supports in-flight encryption using industry-standard secure communication protocols including SSL/TLS. It also supports encryption of data at rest. The AWS Key Management Service (KMS) is supported.

Access Control

Zerto includes role-based access control and multi-factor authentication.

Data Vaulting

The Zerto Cyber Resilience Vault was introduced in May 2023. Please see the Significant Announcements section of this report or The Futurum Group's blog for additional details.

Significant Announcements

- 2023
  - May: Zerto 10 launch (GA June)
    - Real-time Detection
      - Analysis of journal recovery points for anomalous and potentially suspicious activity.
        - Each change that is replicated and logged as a recovery checkpoint is assessed as clean or not.
      - No additional cost; rolled in to Zerto 10.
      - Extensibility via Swagger-based APIs for integration with third-party security tools.
        - E.g., observability via Grafana, Datadog, etc.
    - Cyber Resilience Vault
      - Serves as an isolated data vault and cleanroom environment.
      - Co-located on-premises with the replication target.
        - Not connected to the Internet
          - Encrypted data is periodically replicated over a direct RCIP connection
        - Closed management interface
        - Immutable snapshots
          - Replicas
          - Journals
          - All Zerto components required for recovery
        - Based on HPE Alletra, Aruba and ProLiant hardware
      - A Resilience Automation Server deployed in the vault environment, coordinates network port access, immutability, and the replication processes (e.g., replication/vaulting window and rotating ports for replication windows).
      - Includes nondisruptive testing, the ability to validate clean restore points, orchestrated and automated failover, and compliance reporting.
      - Meets HIPAA, GDPR, SOX, Sheltered Harbor, or FISMA and NIST standards.
      - Can be a GreenLake contract, but is not a part of the GreenLake cloud platform.
      - Includes professional services.
    - Secure Appliance
      - Added migration utility to accelerate migration from ZVM to the secure, Linux-based Zerto Virtual Manager Appliance (ZVMA).
    - Enhanced Azure Protection
      - Refactored architecture.

        - Supports multi-disk consistency via APIs co-developed with Azure.
    - Forthcoming availability on the Azure Marketplace.
- August
    - Zerto In-Cloud added to AWS Marketplace
    - Zerto joins the AWS Independent Software Vendor (ISV) Accelerate Program

Futurum Group EvaluScale – Data Protection Software

The Futurum Group product review methodology "EvaluScale" assesses each product within a specific technology area. The evaluation of each product is based on its capabilities, with capabilities for each technology segment grouped into distinct categories. For the Data Protection Software EvaluScale products are evaluated based on the following 4 criteria categories:

- Protection Environment
- Advanced Capabilities
- Cyber Resiliency
- Ability to Execute

The full Data Protection EvaluScale can be found here.

The Futurum Group Opinion and Outlook for Zerto

Zerto has gained market traction on the back of its ability to serve two pressing requirements: the need to protect virtualized environments, and the need to greatly simplify, accelerate and increase the granularity of recoveries as compared to traditional backup solutions.

Zerto changes the model for data protection away from an application that pulls data from storage devices and writes to another storage device. It also changes disaster recovery from restores of backups or having replica copies made by the storage system, to storage system functions. Its approach (using a filter driver to capture I/Os for CDP, and journal-based recovery) is valuable for virtualized and cloud-based environments. At the same time, it requires a major revision of (often longstanding) operations, which is a major hurdle to adoption for customers to overcome (especially for the larger enterprises that Zerto targets). Zerto's integration into HPE will help to alleviate this hurdle, in particular through the integration into HPE's GreenLake service delivery.

Zerto for Kubernetes became generally available in April 2021, helping to round out the sources it can protect. Customers will still have need for some physical server protection, so Zerto will continue to coexist with other backup software.

Zerto's roots are decidedly DR, but it has been building a broader focus on CDP and on data and workload mobility across multi-cloud environments. For example, it has added the ability to leverage years-worth of journals to recover files and VMs and recovery from ransomware. It also continues to build out analytics, dashboarding and resource planning capabilities.

Zerto's focus on using its journal-based approach presents a unique differentiator in potentially allowing customers to detect ransomware attacks earlier when compared to traditional backup solutions. Additionally, its addition of a cyber vaulting capability provides an important check box for cyber resiliency in the form of data and clean room isolation.