

Zerto

a Hewlett Packard
Enterprise company

Zerto Architecture Guide

Disaster Recovery, Ransomware
Resilience, and Multi-Cloud Mobility



Table of Contents

Abstract	2
Zerto Overview and Use Cases	2
Zerto for Disaster Recovery.....	2
Zerto for Ransomware Resilience.....	3
Zerto for Multi-Cloud Mobility	3
Analytics	4
Core Components of Zerto	4
Zerto Virtual Manager	4
Virtual Replication Appliance	4
Zerto Cloud Appliance for Microsoft Azure	5
Zerto Cloud Appliance for AWS.....	5
Virtual Protection Groups	5
Journal.....	6
Immutable Repositories	6
Reference Architectures	6
Use Cases.....	7
Architecture 1: Disaster Recovery.....	7
Architecture 2: Local Replication and Detection with On-Premises Disaster Recovery.....	8
Additional Use Cases.....	9
Architecture 3: Local Continuous Replication and Detection with Public Cloud Disaster Recovery	9
Additional Use Cases.....	10
Conclusion	10
Additional Resources	11

Abstract

This document provides an architecture guide for anyone designing or implementing a data protection solution with Zerto—particularly anyone using an on-premises production environment paired with either an on-premises or public cloud disaster recovery (DR) target.

This document includes a full overview of all design principles, architecture considerations, and sizing, as well as an installation overview for anyone considering or already using Zerto. We also look at common challenges and use cases that are solved using Zerto.

The architectures in this guide show only a glimpse of what Zerto can support. Having a true software-only, scale-out architecture with a technology-agnostic approach allows you to protect, move, and recover your applications in a mix-and-match nature.

Zerto Overview and Use Cases

Zerto delivers disaster recovery (DR), ransomware resilience, and multi-cloud mobility across on-premises and cloud environments. The solution is built on a foundation of continuous data protection (CDP), with built-in orchestration and automation to provide IT teams with simplicity, enterprise scale, and agile data protection that saves time, resources, and costs. Intelligent analytics—including dashboards, live reports, and predictive resource planning capabilities—provide complete visibility across multi-site and multi-cloud environments, giving organizations confidence that business service levels and compliance needs are met now and in the future.

Zerto for Disaster Recovery

Organizations of all sizes with virtualized environments use replication for DR because the impact of unsuccessful or slow recovery can be catastrophic, creating systemic risk to the business. Different enterprise-class DR technologies have been available since the mass adoption of virtualization, but they were typically designed to protect physical servers using storage-based replication, not virtual machines (VMs).

Storage-based replication adds significant complexity because it's configured on a disk/LUN basis, requiring matching storage and LUN configurations. There is no VM-level granularity or integration into the virtualization platform. In addition, storage-based replication requires separate complex software for VM orchestration and automation, which involves multiple skill sets and resources and does not fully align with the benefits of virtualization.

Another common replication method is snapshot-based. Products using snapshot-based replication have typically been designed with backup as their primary use case and DR as an afterthought. Most of these products lack scalability, orchestration, and automation at the level required for enterprise architecture. Snapshots also impact production workloads, so they cannot be utilized as often as organizations need. Because snapshots are usually only taken once a day, they leave large amounts of data loss in between backup windows.

Zerto is built from the ground up to be the simplest, most powerful DR solution for virtualized infrastructures. By including all the replication, recovery orchestration, and automation in one simple software solution, Zerto enables users to recover one, all, or a subset of virtualized applications from anywhere to anywhere, maximizing the benefits of virtualization and the cloud.

Through native integration into all supported platforms, Zerto not only allows replication and recovery between any storage, but also protects across and between multiple hypervisors and public cloud platforms. This market-leading technology delivers a best-of-breed business continuity (BC) and DR solution, regardless of underlying hypervisor, public cloud, or storage.

Zerto uses CDP instead of storage- or snapshot-based protection. This allows Zerto to achieve best-in-class recovery point objectives (RPOs) and recovery time objectives (RTOs) without impact to production workloads. Zerto's typical RPOs of seconds and RTOs of minutes allow organizations to drastically limit data loss and downtime, no matter the type of disaster or disruption.

Zerto for Ransomware Resilience

Cybercrime, including ransomware, is one of the biggest challenges IT leaders face today. Cybersecurity focuses preventative efforts on network security or endpoint protection, such as antivirus solutions. While incredibly important by themselves, these pieces belong to a much larger puzzle.

Ransomware prevention is not enough on its own. Attackers only need to be correct once to inflict damage to an organization. The solution is shifting focus from prevention to resilience—incorporating a plethora of technologies and methodologies to truly achieve ransomware resilience. Broadly speaking, we can split these technologies and methodologies up into four key pieces:

1. Education
2. Prevention
3. Detection
4. Recovery

Investment is required in all areas to give organizations the best chance of achieving ransomware resilience.

Zerto focuses on ransomware resilience by providing best-in-class ransomware recovery. As soon as ransomware starts to encrypt data in your environment, Zerto gives the earliest warning that an attack is underway. Detection occurs in real time as data is streaming in and being protected by Zerto, not as a post-processing scan after data has been written to a replica. Real-time encryption detection with immediate alerts gives organizations the ability to respond faster than ever before.

Organizations can then use Zerto to pinpoint which applications were impacted and recover any data that may have been encrypted back to only seconds before the impact occurred. Recovery is incredibly granular, with thousands of restore points that are each separated by only 5–15 seconds. Recovery also extends to individual files or folders, single VMs, entire multi-VM applications, and even whole virtualized sites. And with automation and orchestration, the RTOs stay as low as possible.

Zerto for Multi-Cloud Mobility

Data mobility is a crucial capability in today's computing environment. It allows organizations to move applications and data across multiple platforms with minimal business impact and no infrastructure constraints. With the growing popularity of cloud computing, there are now numerous cloud platforms available, each with unique attributes that suit them to certain workloads. However, not all workloads may be appropriate for the cloud, and some organizations may still rely on traditional on-premises deployments. As a result, multi-cloud and hybrid cloud strategies are becoming increasingly popular as organizations seek to avoid lock-in to any one platform or vendor and retain the flexibility to move their applications and data where they fit best.

True data mobility enables organizations to move applications and data across platforms seamlessly, whether on-premises or in the cloud, without any impact on production. This allows organizations to validate migrations before the live event and ensure that their applications and data are not locked into any one platform or vendor.

Once data is in the cloud, Zerto enables freedom to move back out as needed or to protect and migrate across regions and zones within the cloud. This flexibility is key to keeping up with an ever-changing cloud landscape and an

evolving cloud strategy. With the freedom to move applications and data across multiple platforms, organizations can capitalize on the unique attributes of each platform and optimize their computing environment to achieve their goals.



Analytics

Zerto Analytics provides added visibility over protected IT environments across private, public, and hybrid clouds, making it a valuable tool for IT leaders. With Zerto Analytics, users gain a comprehensive overview of their entire multisite, multi-cloud environment via metrics like average RPO, network performance, and storage consumption. This enables real-time and historical analysis of the health and protection status of applications and data.

Another feature of Zerto Analytics is the capacity planning tool, which helps users plan and predict resource requirements for future data protection needs based on their real data. This ensures that users have the exact requirements needed to expand their data protection capabilities and protect more workloads.

Additionally, Zerto Analytics provides intelligent dashboards that allow users to spot trends, identify anomalies, and troubleshoot issues, all from a single view across their entire IT environment. This includes both on-premises and cloud data, which allows users to confidently monitor the real-time health and protection status of their applications and data.

Overall, Zerto Analytics can help IT leaders make better decisions and achieve a more efficient, resilient mode of operation by providing them with the insights they need to manage their complex, diverse, and disparate data center and cloud workloads.

Core Components of Zerto

Zerto Virtual Manager

The Zerto Virtual Manager (ZVM) plays a critical role in managing the replication process between the protected and recovery sites. It acts as a centralized control plane, communicating with the hypervisor management interface and other components of the Zerto infrastructure to orchestrate replication and ensure that protected data is consistent and accurate.

Additionally, the ZVM provides a user-friendly interface for managing replication, configuring recovery workflows, and monitoring the health of the replication environment. Deployed as a security-hardened virtual appliance, it is designed to protect against unauthorized access or tampering, ensuring the integrity and confidentiality of your critical data. With the ZVM in place, you can have confidence that your replication environment is running smoothly and that your data is protected from loss or corruption.

Virtual Replication Appliance

The Virtual Replication Appliance (VRA) is a lightweight virtual appliance installed on each hypervisor host to manage the replication of data between protected VMs and their local or remote targets. It provides a true scale-out architecture that can grow and shrink with your environment, making it easy to manage and scale your replication

needs. The VRA also manages real-time, inline encryption detection to help organizations detect ransomware impact as it is occurring. It requires a minimum of only 3 GB RAM and 1 vCPU, making it a highly efficient and lightweight solution.

Zerto Cloud Appliance for Microsoft Azure

When used within Microsoft Azure, the Zerto Cloud Appliance (ZCA) provides a fully scalable management layer for all replication in, out, and between Microsoft Azure regions. It is similar to the ZVM for on-premises environments. The single appliance runs inside of Azure IaaS and utilizes block and page blob storage to cost-effectively store data. The replication is then performed with dedicated in-cloud VRA instances that offer a true scale-out architecture using cloud-native technologies like Azure scale set workers and Azure queues. The VRAs will automatically and dynamically adjust to replicate the current data set.

Zerto Cloud Appliance for AWS

Unlike on-premises and Azure managers, the AWS ZCA combines the management and replication components into a single cloud appliance. The AWS ZCA is a dedicated VM comprised of the following services:

- **ZVM:** This is a Windows service that hosts the UI and integrates with the native APIs of Azure/AWS for management and orchestration.
- **VRA:** This is a Windows service that performs the replication of data itself from or to Azure/AWS.

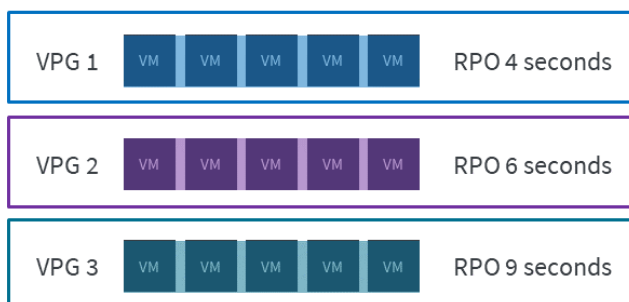
The ZCA integrates natively with the AWS platform, allowing you to use Amazon S3 buckets for journal storage in AWS. This ensures the most cost-efficient deployment.

Virtual Protection Groups

Virtual Protection Groups (VPGs) are at the heart of Zerto’s protection and recovery capabilities. They provide a consistent and cohesive approach to protecting multiple VMs that comprise an application. Instead of protecting each VM individually, VPGs allow you to protect one or more VMs together in a consistent fashion, ensuring every point in time inserted into the Zerto journal is the same for all VMs within the VPG, even if those VMs reside on different hosts or data stores. This means that when a recovery is required, all VMs within the VPG can be recovered to the same point in time, providing cohesive and consistent recovery of the entire application.

VPGs promote ransomware resilience through Zerto’s detection of, and automatic recovery from, ransomware attacks. By monitoring the journal for any unexpected changes, Zerto can detect malicious or anomalous encryption as it is occurring, enabling recovery to a point in time just before the attack started. VPGs also enable multi-cloud mobility by allowing applications to be moved to, from, and between multiple platforms/clouds with minimal business impact and no traditional infrastructure constraints.

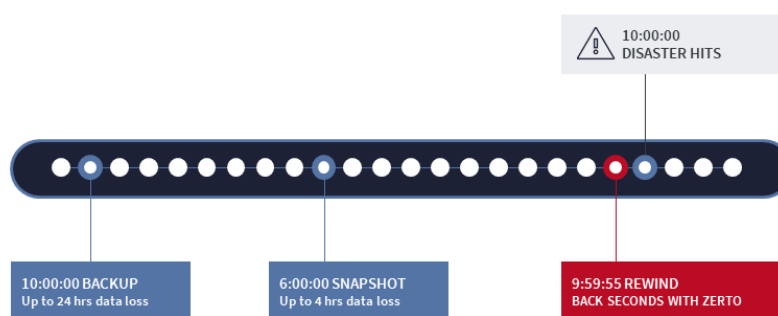
Journal



In addition to VPGs, Zerto CDP stores all replicated data in the journal. The journal stores all changes for a user-defined period, from 1 hour up to 30 days, and allows you to recover to any point in time within the journal, ensuring your RPO is always as low as possible, typically in seconds. Every write to a protected VM is copied by Zerto. These writes are replicated locally and/or remotely using Zerto's one-to-many features and written to a journal managed by a VRA. Each protected VM has its own journal. In addition to the writes, all journals within the VPG are updated with a checkpoint timestamp every few seconds. Checkpoints are used to ensure write-order fidelity and crash consistency across the VPG.

With Zerto, recovery can be performed to the last checkpoint or a user-selected checkpoint. This enables recovery of files, folders, VMs, applications, or entire sites. The recovery point can either be set to the previous crash-consistent point in time or to a point in time before the attack (in the case of the VM being attacked by a virus or ransomware, for example). Combined with Zerto's detection capabilities, this recovery enables users to tag anomalous checkpoints and thereby easily identify a checkpoint moments before suspicious activity occurred. After that, Zerto makes it simple to test and recover data to seconds before the disruption occurred.

Immutable Repositories



In addition to flexible options for short-term ransomware recovery scenarios using the journal, most organizations that have compliance requirements need an immutable copy as an integral part of their data protection strategy. Traditional methods of providing immutable protection have always been performed on the production environment itself, impacting performance and often disrupting user experiences.

Zerto extended journal copy (EJC) uses your existing journal to store data from any point in time for days, weeks, months, or even a year. It uses the data already protected by CDP, combining and storing it in a journal on the target side. This allows you to offload point-in-time copies to secondary storage targets and mark these copies as immutable without impacting production workloads. When using public cloud storage targets (such as AWS and Azure), Zerto offers native data tiering features to ensure data is stored on the most cost-efficient offering.







Zerto supports the use of disk, object, and cloud storage; for a full list of supported repositories and their versions, please see our [Interoperability Matrix](#).

Reference Architectures

In this section, three example configurations highlight Zerto's different capabilities in an easy-to-understand format. These are intended only as guides to help visualize the benefits that Zerto can provide your organization while also demonstrating the simplicity of the solution.

Use Cases

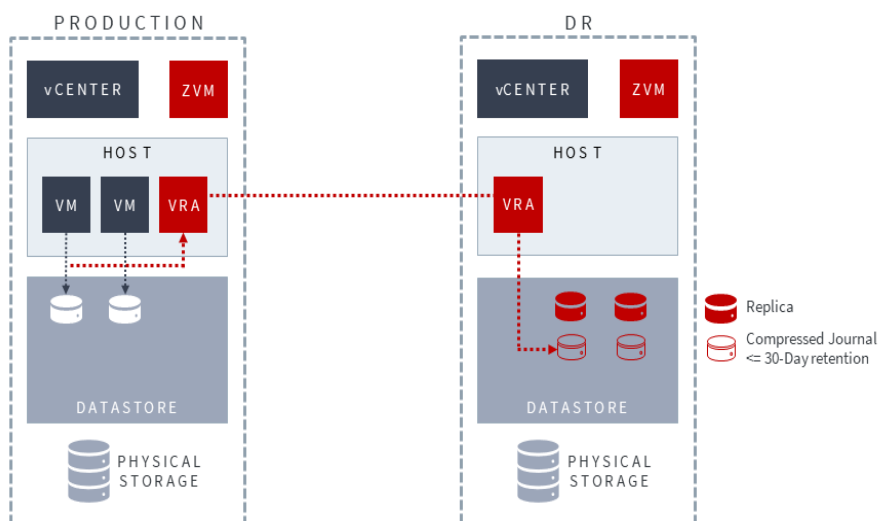
All three example configurations support the following use cases. Where there are unique differences, they will be highlighted under the relevant architecture.

 Outages & Disruptions	<p>Any disruption on the production site, whether it's power, network, or otherwise, is protected with recovery of your files and folders, VMs, applications, or entire site within just a few minutes to a point in time just seconds before the issue occurred. <i>Example: Recovery of your entire site within minutes after a power outage.</i></p>
 Ransomware Attacks	<p>Recovery from ransomware attacks can be from just seconds before encryption occurred, minimizing data loss and business impact. You can recover your files and folders, VMs, applications, or entire sites. <i>Example: Recover encrypted files from seconds before they were encrypted.</i></p>
 Infrastructure Modernization	<p>This same architecture can be used to move your workloads from an end-of-life platform to your new infrastructure in just minutes, significantly speeding up infrastructure modernization projects. These migrations can also be tested ahead of time to minimize migration times and risk. <i>Example: Move your workloads to a new platform in just minutes with no data loss.</i></p>
 Consolidations & Migrations	<p>Where multiple sites are to be consolidated or migrated to the same target, this architecture can be used to streamline the process. This enables pre-migration testing and live migration times of just minutes. <i>Example: Consolidate workloads from diverse hardware, hypervisors, and cloud platforms to meet business standards in minutes.</i></p>
 Testing & DevOps	<p>Allows the creation of replicas, at the remote site, of your production environment from any point in time in just minutes. This provides greater flexibility for your development teams and reduces overhead on DevOps teams, as well as enabling DR testing and validation. <i>Example: Create exact replicas of production applications from seconds ago in just minutes for UAT purposes.</i></p>
 Analytics Across Clouds	<p>A single SaaS-based analytics platform providing complete data analysis across all your sites, both on-premises and in the cloud. This provides a single view that simplifies management and monitoring without added cost. <i>Example: Identify bandwidth bottlenecks across your entire IT infrastructure through a single portal.</i></p>

Architecture 1: Disaster Recovery

Figure 1 depicts a DR architecture where a single remote target is used as the recovery site.

Figure 1

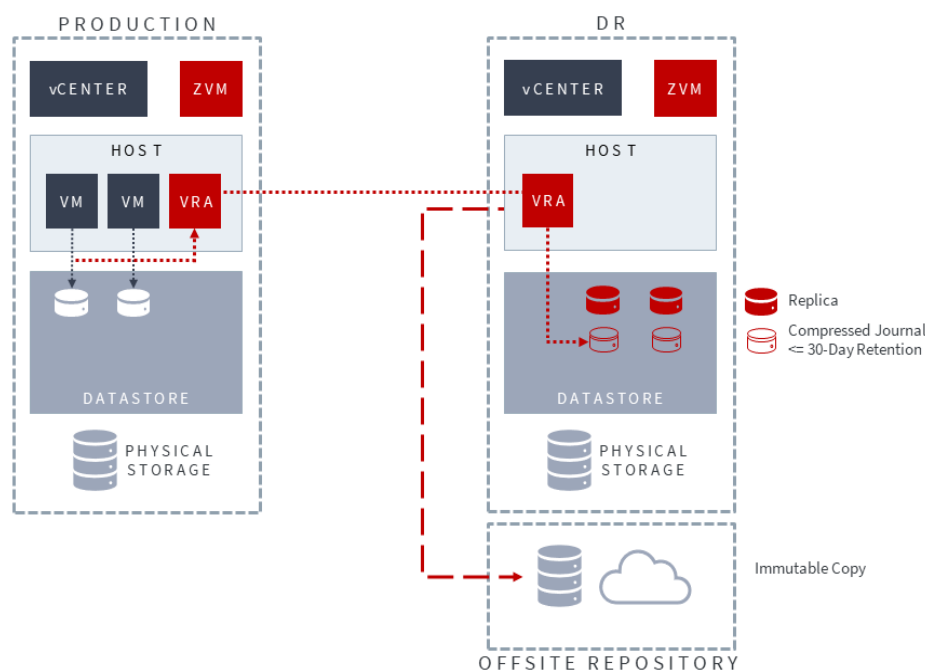


Protected VMs are grouped in VPGs with consistency across all the VMs in each VPG. A remote journal is configured on the remote target side and used for short-term recovery scenarios where a recovery granularity of just seconds can be achieved. The recommended journal history period for this journal is eight days, since this will cover most recovery scenarios. All changes on the protected VMs are then kept for eight days before being promoted to the remote replica disk(s).

Architecture 2: Local Replication and Detection with On-Premises Disaster Recovery

Figure 2 depicts a reference architecture similar to the previous DR reference architecture, but with the addition of a local journal as well as an immutable offsite copy from the journal. This local journal provides continuous replication and detection capabilities, allowing users to benefit from real-time, inline encryption detection. It also allows users to recover files, VMs, or applications locally with a granularity of seconds, ensuring minimal data loss in the event of an issue, as well as rapid recovery back to production-grade storage and compute.

Figure 2






In this configuration, the same VMs exist in two VPGs. The first VPG is for the creation of the journal on the source, and the second VPG is created to provide journal capability on the remote target. The local journal is configured on the source site and used for local replication and encryption detection where a logical failure occurs, providing recovery granularity of just seconds. The recommended journal history period for this journal is 14 days, since this will cover most logical recovery scenarios. With the deduplication capabilities of modern storage arrays, it will consume minimal storage space. A daily process will send points in time from the local journal to the EJC repository for compliance and immutability needs.

In addition to the previous reference architecture, this architecture provides you with the ability to recover data directly onto the source site, rather than just the remote site. With this architecture, the minimum recommended remote journal history is three days; this will cover most recovery scenarios where a physical failure has occurred. All changes on the protected VMs are then kept for three days before being promoted to the remote replica disk(s).

Additional Use Cases

In addition to the standard platform use cases, the use cases below are unique to this architecture.

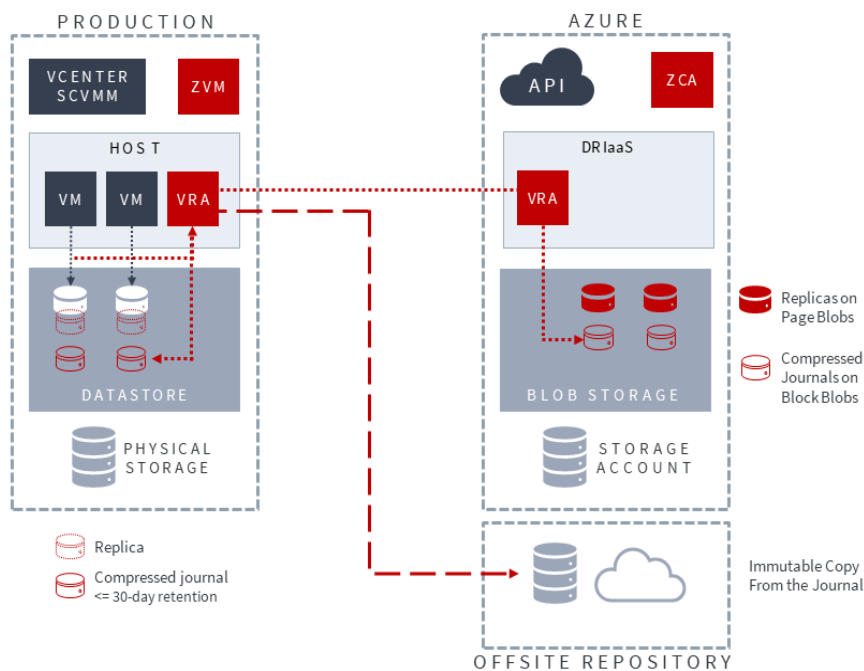
 Outages & Disruptions	<p>The ability to recover files and folders, VMs, applications, or sites locally in the event of a logical failure is included in this configuration. Example: If just one application has an issue, recover just this application locally, rather than remotely, to seconds before the issue.</p>
 Ransomware Attacks	<p>The ability to recover files and folders, VMs, applications, or sites locally in the event of a ransomware attack is included in this configuration. Example: Recover only impacted files, VMs, or applications locally, rather than remotely, to seconds before the issue.</p>
 Testing & DevOps	<p>The ability to test recovery or create replicas for DevOps purposes locally is included in this configuration. Example: Create a replica of a production workload locally, for development purposes.</p>

Schedule a demo today or use [hands-on labs](#) to see how Zerto can protect your business and manage any disruption (both planned and unplanned). Zerto gives you more time to focus on IT innovation and drive business value while mitigating risks and accelerating transformation and innovation.

Architecture 3: Local Continuous Backup and Public Cloud Disaster Recovery

Figure 3 depicts a reference architecture with local replication and a remote DR target in the public cloud.

Figure 3





In this configuration, the same VMs exist in two VPGs. The first VPG is for the creation of the journal on the source, and the second VPG is created to provide a journal capability on the remote public cloud target. This cloud journal is placed on blob storage in Azure or on an S3 bucket in AWS and is configured on the cloud side. This reduces the cost footprint, since only storage costs are incurred and the compute requirements spun up in a recovery scenario.

The local journal is configured on the source site and used for local replication and encryption detection, where a logical failure or ransomware occurs, providing recovery granularity of just seconds. The recommended journal history period for this journal is 14 days, since this will cover most logical recovery scenarios, and with the deduplication capabilities of modern storage arrays, it will consume minimal storage space. A daily retention process will archive points in time from the local journal to the offsite repository to leverage immutability for additional security.

With this architecture, it is recommended that the remote journal history period is at a minimum of three days, since this will cover most recovery scenarios where a physical failure has occurred. All changes on the protected VMs are then kept for three days before being promoted to the remote replica, which resides in cloud storage.

Additional Use Cases

In addition to the standard platform use cases, the below use cases are unique to this architecture or have unique capabilities added to the specific use case.

 <p>Cloud Integration & Migration</p>	<p>Cloud adoption, and the challenges associated with it, can be simplified with this architecture to move workloads to your chosen cloud platform in just minutes with zero data loss. In this use case, long-term retention is likely not needed during the migration. Example: Move complex applications to the cloud in just three steps.</p>
 <p>Multi-Cloud Hybrid Cloud</p>	<p>With the increasing adoption of hybrid and multi-cloud strategies, this architecture provides freedom to move workloads around on demand as requirements change. Example: Move workloads to, from, and across cloud platforms to gain maximum efficiency.</p>

Conclusion

Zerto provides ransomware resilience, multi-cloud mobility, and DR with multiple distinct benefits, from vendor and cloud freedom to the rapid detection and recovery. Its multiple potential architectures demonstrate simplicity and agility, with use cases that span the entire range of IT infrastructures and team needs. To see how Zerto can fit into your IT environment, get a demo today.

[GET A DEMO](#)

Additional Resources

The resources below provide more detailed prerequisites, guidelines, and sizing information.

[Zerto Prerequisites and Requirements](#)

[Zerto Scale, Sizing, and Benchmarking Guidelines](#)

[Zerto Interoperability Matrix](#)

[Zerto Analytics](#)

Please visit <https://help.zerto.com> for all Zerto's technical documentation.

About Zerto

Zerto helps customers accelerate IT transformation through a single, scalable platform for cloud data management and protection. Built for enterprise scale, Zerto's simple, software-only platform uses continuous data protection to converge disaster recovery, backup, and data mobility and eliminate the risks and complexity of modernization and cloud adoption. Zerto enables an always-on customer experience by simplifying the protection, recovery, and mobility of applications and data across private, public, and hybrid clouds. Zerto is trusted by over 9,000 customers globally www.zerto.com.

Copyright 2023 Zerto. All information may be subject to change.