

Zerto


a Hewlett Packard
Enterprise company

Hypervisor-Based Replication

A Better Approach to Disaster Recovery and
Ransomware Detection

Version 3.0

September 2023



Contents

Background.....	3
Array-Based Replication: Insufficient Granularity	3
Agent-Based Replication: Impossible to Scale.....	4
The Best Approach: Hypervisor-Based Replication.....	5
Zerto Architecture: Simple, Effective, and Scalable.....	5
Journal-Based Recovery	6
Application-Centric Protection: Another Important Differentiator.....	7
Granularity	7
Scalability	8
Ease of Management.....	8
Server and Storage Motion.....	8
Hardware Agnostic	9
RPOs and RTOs	9
Ransomware Detection	9
Conclusion	10

Virtualized data centers have transformed the IT landscape, giving IT departments more flexibility for and control over production workloads. Virtualization also streamlines implementation and operational support, spurring organizations continue to expand virtualization initiatives to private, public and hybrid cloud environments.

But to realize the benefits of virtualization and maximize their investments, organizations need to fully optimize all IT processes and activities for their virtual environment. These processes include security, compliance, and disaster recovery (DR). Of the three, DR is perhaps the most difficult to optimize. Until now, there were no simple, agnostic, virtual-ready remote replication methods available on the market.

Zerto, a Hewlett Packard Enterprise company, is here to change that. Zerto has revolutionized the industry with a software-only solution for enterprise-class replication that's purpose-built for virtual environments.

Background

Traditionally, most common replication technologies and methods essential to DR have been tied to the physical environment. Although they do work in the virtual environment, they aren't optimized for it. Physical hardware dependency undermines the benefits of virtualization and creates significant operational and organizational challenges, like those below.

- If a replication solution isn't virtual-ready, management overhead could be more than doubled. Many of the benefits achieved through virtualization, therefore, could be lost in the DR sphere.
- Virtualization is scalable, but traditional DR methods are not. Customer data is always growing, so a company may find that its replication solution can't keep pace with the exponentially expanding information inventory.
- In an increasingly heterogeneous IT environment, some replication methods remain firmly tied to a single vendor and hardware platform, limiting the organization's ability to obtain newer, best-of-breed solutions—and service—at the best price.

These array-based and agent-based replication technologies, developed specifically for use with physical IT assets, have issues that inhibit the efficiency and effectiveness organizations require in their data centers. With competitive and regulatory pressures at an all-time high, organizations need every advantage to guarantee excellent DR capability. They need DR capabilities that support the promise of virtualization.

To answer this call, Zerto introduced hypervisor-based replication, elevating DR up the infrastructure stack to where it belongs: the virtualization layer. As we review the structures and limitations of traditional replication methods, we can better amplify the advantages and benefits of Zerto's virtual-ready, hypervisor-based replication solution.

Array-Based Replication: Insufficient Granularity

Array-based replication products are provided by storage vendors and deployed as modules inside the storage array. These single-vendor solutions are compatible only with the specific storage solution already in use and lack the granularity required in a virtual environment. With array-based replication products:

- The relationship between the VM and storage is fixed, eliminating the flexibility of the virtual environment.
- The entire LUN is replicated regardless of its actual utilization—whether it's 40% or 90% utilized, the power, cooling, and storage costs will increase.

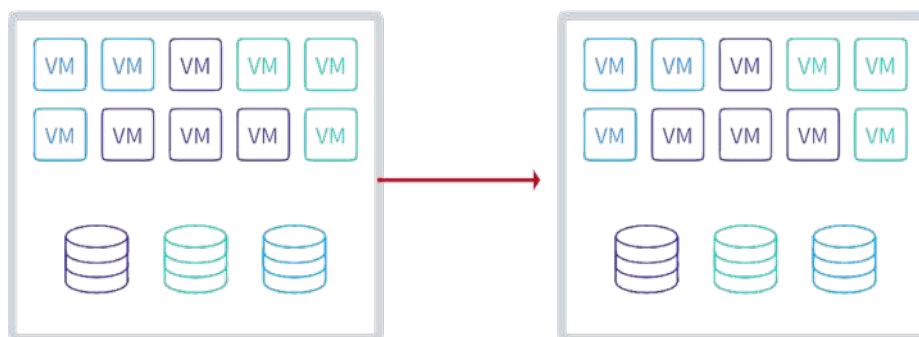


Figure 1: Array-based replication requires strict relationships between the virtual and storage environment, undermining the investment in virtualization.

Array-based replication has other important disadvantages as well. Consider:

- Array-based replication is designed to replicate physical entities, not virtual ones. It doesn't "see" virtual machines or configuration changes. But virtual environments are dynamic, with a high rate of change. As a result, a DR strategy using array-based replication will be out of sync with the current production environment.
- Array-based replication requires multiple points of control. In addition to the physical storage array's management console, IT will also have to manage virtual assets from a virtualization management console, such as VMware's vCenter.
- Though optimized to work with an organization's existing storage array, array-based replication locks the organization into a single vendor, eliminating the flexibility to try new storage arrays and innovate alongside.

"When we purchased Zerto, we knew it would improve our BC/DR process, but we got so much more. We reduced our storage footprint by more than 40%. We never expected that. Now, we do not have to purchase storage for the foreseeable future, which is a huge savings for us."

— Bill Rausch, Software Engineering Manager HAPO Community Credit Union

Agent-Based Replication: Impossible to Scale

Guest/OS-based replication solutions comprise software components that must be installed on each individual physical and virtual server. Although more portable than array-based solutions, agent-based replication isn't fit for enterprises for the following reasons:

- Installing an agent on every single guest OS server limits scalability, making the solution impossible to implement and manage in high-scale enterprise environments.
- Shadow VMs are often part of the implementation, increasing management complexity and burden on the IT team.
- There are no consistency groups; each VM is protected individually. This is counterintuitive to applications that typically span multiple VMs.

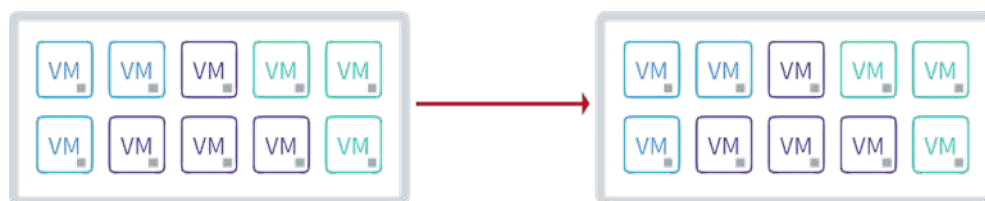


Figure 2. Host-based replication requires an agent on each VM, greatly increasing complexity.

“We really like the simplicity of having full automation and orchestration, combined with robust replication, in just one product. I had two separate products—VMware SRM and RecoverPoint—which was challenging to manage. For example, when a new version of vSphere was released, it had a feature I wanted to leverage. In order to use it and ensure BC/DR would not be affected, I had to upgrade not only vSphere but also SRM, RecoverPoint, and the array; it was just too much. Zerto is not only easier to manage, but it handles VSS checkpoints seamlessly, and the ability to easily rollback a failover streamlines our BC/DR processes.” — Zach Dickins, Senior Network Administrator Rapidparts, Inc

The Best Approach: Hypervisor-Based Replication

Before virtualization, replication was managed at the storage layer. This made sense for a physical environment, because physical storage is where the information was. If there is a physical box you want to monitor, you would track it with physical sensors. But in a virtual environment, the boxes aren't (all) physical—so putting a physical sensor on a virtual box won't help you monitor its contents.

Now, there is a gap between the traditional ways of replicating and today's virtualized environments. This is a common historical problem, where one technology often advances at a faster rate than others, creating a capability gap. Virtualization offers extraordinary capabilities and benefits, but they cannot be fully realized unless and until other technologies within the data center evolve to enable them. Managing a virtual or hybrid environment from the physical storage layer inhibits the move to the cloud and makes it harder to fully leverage the benefits of virtualization.

So, because array-based and agent-based replication methods are designed for physical IT environments, they have critical limitations in a virtual context. They undermine the investment made in virtualization and limit its functionality. To fully benefit from virtualization without compromising on BC/DR, a new approach is required.

That's why Zerto realized the need to move replication up the stack—above the resource abstraction layer—into the hypervisor layer. And that's how hypervisor-based replication was born.

Zerto Architecture: Simple, Effective, and Scalable

Zerto provides an enterprise-class replication solution that's purpose-built for virtual environments. Our innovative, hypervisor-based replication solution is currently the first and only solution that delivers enterprise-class, virtual replication and DR capabilities for the data center and the cloud.

At the heart of this replication technology are components that are easily deployed:

- **Zerto Virtual Manager (ZVM)**—The ZVM plugs directly into the virtual management console (such as VMware’s vCenter), enabling visibility into the entire infrastructure. The ZVM is the nerve center of the solution, managing replication for the entire vSphere domain, tracking moving applications and information in real time.
- **Virtual Replication Appliance (VRA)**—The VRA is a software module automatically deployed on the physical hosts. The VRA continuously replicates data from user-selected VMs, compressing and sending that data to the remote site over WAN links.

Because it’s installed directly inside the virtual infrastructure (as opposed to on individual machines), the VRA integrates with the hypervisor to replicate any protected VM’s data change. Each time the VM writes to its virtual disks, the write command is captured, cloned, and sent to the recovery site. This is much more efficient, accurate, and responsive than storage-based methods.

Unlike some replication technologies that primarily offer data protection through cumbersome snapshots and backups, Zerto provides continuous replication with zero impact on application performance.

Hypervisor-based replication is fully agnostic to storage source and destination. It natively supports all storage platforms and the full breadth of capabilities made possible by virtualization, including high availability, clustering, and locating and replicating volumes in motion.

Finally, hypervisor-based replication installs seamlessly into the existing infrastructure. The carefully architected application configuration doesn’t need to be changed in any way, and IT administrators don’t have to modify their approach to get Zerto up and running.

Journal-Based Recovery

With Zerto, all replicated changes are stored in a journal for up to 30 days, providing incredible recovery granularity through checkpoints inserted every few seconds. This reduces data loss to just seconds by recovering files, VMs, applications, or entire sites to specific points in time. You can recover either to the latest point in time or, for example, to a point in time before a VM was attacked by a virus or ransomware.

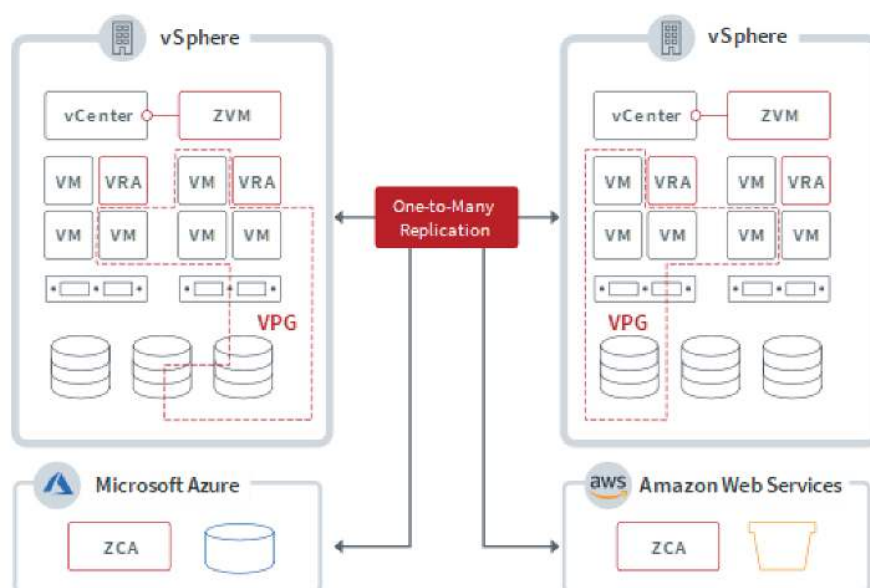


Figure 3. Hypervisor-based replication aligns the production and BC/DR strategy, extending all the benefits and flexibility of virtualization to the data protection and data mobility strategies.

Application-Centric Protection: Another Important Differentiator

Today's applications rarely run on a single VM. Instead, most applications have multiple VM dependencies, but traditional methods of protecting VMs individually impede quick application recovery. Zerto resolves this by protecting VMs in Virtual Protection Groups (VPGs). VPGs allow you to protect multiple VMs together in a consistent fashion, ensuring every point in time inserted into the Zerto journal is identical for all VMs within the VPG. This method recovers an entire application and all its VM dependencies to the same point in time.

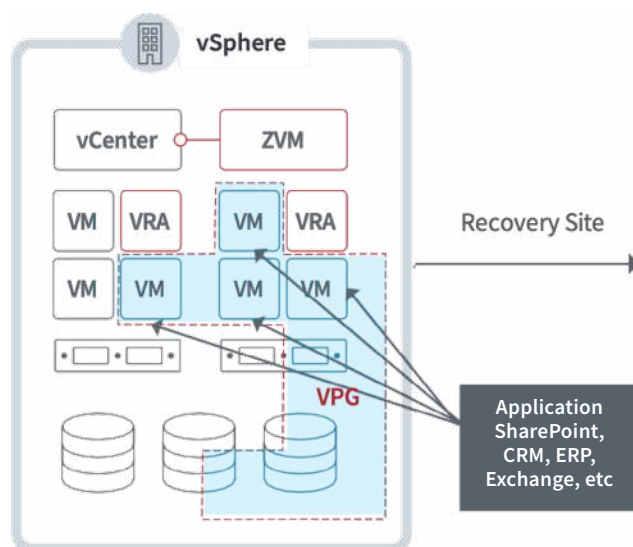


Figure 4. The Virtual Protection Group is a group of VMs that comprise an application. Zerto recognizes and preserves these relationships even as the VMs are moved throughout the environment with VMware DRS, vMotion, etc.

“When I first heard about Zerto, I was skeptical. Now that we have it deployed, I call it a miracle for BC/DR. We have very aggressive service levels to meet – we must have our mission-critical applications up in 15 minutes. With Zerto, we can recover our Microsoft SQL Server database, Exchange, File servers, and other applications well within our SLA.”

— Uzah Chinedu Infrastructure Manager, Leadway Pensure PFA Limited

Granularity

Replicating at the correct level of any virtual entity, whether that's a single VM or group of VMs, is critical. Zerto can replicate all VMs consistently, along with all metadata, to recover the entire application infrastructure from a disaster.

A typical enterprise application includes multiple servers for the web, applications, databases, etc., and each server has its respective disk. Today, administrators tend to put all those disks in a single logical unit in storage so they can replicate the entire application at once without having to search for its individual components. But this means the entire logical unit must be replicated even when its other applications don't need replication. That lack of granularity—where administrators can't identify specific applications and application components to replicate—is inefficient.

For example, a given CRM application may span eight VMs deployed on four physical servers that use five different data stores located on three different logical units. With hypervisor-based replication (and only with hypervisor-based replication), centralized management through the hypervisor layer enables the solution to find what it's looking for, no matter where it is located. That granularity is simply impossible with prior replication technologies that aren't virtual ready.

In today's virtualized environments, the goal is full consistency among all application components. With hypervisor-based replication, that goal is achieved.

Scalability

“We believe that the virtual machine is the new atomic unit for replication strategies. Zerto works at the virtualization level, which allows us greater flexibility in the type of storage we replicate to and removes the limitations around LUN-based consistency groups. This solution adds a deeper level of control of recovery time objective (RTO) and recovery point objective (RPO) in a virtual environment than traditional replication methods.”— R. Todd Thomas, Chief Information Officer, ARA

There are two aspects of scalability: deployment and management. As a virtual infrastructure grows, an organization's DR capabilities must grow with it seamlessly, without having to purchase, install, and configure additional proprietary hardware. Zerto's hypervisor-based replication solution is software based, so it can be deployed and managed easily, no matter how fast the infrastructure expands. The solution also enables administrators to perform operations and configure policies at the level of the VMs or applications.

Ease of Management

With no guest-host requirements or additional hardware footprint, Zerto is easy to manage.

It simply resides in the hypervisor, enabling centralized management from the virtual management console (such as VMware vCenter). Organizations can now manage everything from the same console. Because Zerto is software based, it installed by users (the VRA install process itself is automated), configured by users, and scaled automatically and without hassle.

Server and Storage Motion

“Our customers are running their businesses 24 hours a day, seven days a week, and they require short outage windows for migrations to minimize disruptions. With Zerto, we are able to cut over applications in just 15 minutes. The setup is very simple and does not require customers to change anything in their environments. Within minutes we are replicating the applications to the new location with no disruption to the environment. We will be using Zerto for our next migration project.”

— TJ Tran Platform Architect, Fujitsu

One of the great advantages of the virtual environment is the ability to quickly move VMs around from one physical server or array logical unit (data store) to another. This might be done for load balancing or other strategic data management reasons. With VMware, this is accomplished manually through vMotion or automatically using Distributed Resource Scheduler (DRS). Only hypervisor-based replication supports this capability, continuing to locate and replicate data no matter where it resides or where it is moved.

“[Zerto’s] real-time ransomware detection puts us in a much stronger position to both identify and mitigate ransomware attacks. This gives us confidence that we can proactively meet the risks presented by ransomware.”— Network admin at manufacturing customer

Zerto’s granular, hypervisor-based replication identifies what servers/files were first encrypted and then rolls back to the last known write operation before ransomware started encrypting. Such granularity allows businesses to recover and quarantine in the best possible way, with the least amount of risk and disruption.

Hardware Agnostic

Hypervisor-based replication is hardware agnostic and supports all storage arrays, so organizations can replicate from anything to anything. In today’s increasingly heterogeneous IT environment, this allows users to mix storage technologies like Storage Area Network (SAN) and Network-Attached Storage (NAS), as well as virtual disk types like Raw Device Mapping (RDM) and VMware File System (VMFS).

“The flexibility and usability of Zerto was the deciding factor for us. Because the technology is hardware- and storage-agnostic, it provides us superior protection encompassing our entire environment, without the need for vendor- specific solutions. The singular management interface allows us to seamlessly manage our replication groups within the vSphere client and provides excellent visibility of the replication statistics and process. Setup and configuration were quick, painless, and completed within only a few hours. Zerto has proven to be indispensable in our environment and we are very pleased with the results we’ve seen.” — Erik Rasmussen System Administrator

RPOs and RTOs

In DR, the two key metrics are recovery point objective (RPO) and recovery time objective (RTO). RPO refers to the amount of data at risk of being lost between data protection events and how long until all the data at risk is recovered. RTO defines the time needed to recover from a data loss event and return to normal operation and availability. Zerto’s hypervisor-based replication solution achieves RPO in seconds and RTO in minutes.

Ransomware Detection

Ransomware is a sophisticated technology that inconspicuously infiltrates systems to compromise data and coerce end users into paying money. It targets backup software and antivirus solutions with precision, subverting them with a filter driver that operates behind the scenes to encrypt and decrypt data.

Because the filter driver is hidden, users remain unaware of the ongoing encryption process. Eventually, the attackers trigger the ransomware and demand a ransom in exchange for the decryption key.

Interestingly, ransomware assailants often refrain from tampering with backup systems, opting instead for a gradual encryption strategy. By allowing a span of time to pass—say, several months—before presenting the ransom demand, attackers capitalize on organizations’ reluctance to revert to potentially outdated backups.

The implications of succumbing to such data compromise are dire, particularly for businesses that may be unable to weather the extensive loss. While the main goal of cybersecurity is to preemptively thwart ransomware attacks through multifaceted defense mechanisms, a comprehensive cybersecurity framework includes strategies for swift detection of and recovery from intrusions. This final line of protection necessitates vigilant measures and robust recovery protocols to counteract the potentially crippling aftermath of a ransomware assault.

Because Zerto replication operates at the hypervisor-level, encryption detected from write I/O streaming to the journal allows for a granular, real-time detection of anomalies potentially infesting VMs. As such, potential anomalous encryption rates follow data-adaptive techniques. This dynamically calculates trigger thresholds, verifying that what appears as anomalous truly is. Zerto has the enormous advantage of combining real-time detection and recovery to combat modern threats.

When combating ransomware, Zerto's hypervisor-based replication and encryption detection feature allow you to:

1. Automatically detect an attack in near real-time and recover in minutes, with an incredibly tight RPO.
2. Detect ransomware activity even in already compressed data or data made to look like text after base64 encoding and (in the future) legitimate, user-encrypted data.
3. Detect encryption even when very small amounts are encrypted in each file.
4. Identify the infection's source (down to volumes in a specific server), accelerating response time and quarantine protocols.
5. Avoid data set size limitations with a solution that relies completely on real-time streams.
6. Move beyond signature-based detection with a solution that doesn't require malware signatures.
7. Ditch computationally expensive deduplication/compression engines to determine uniqueness or heavy calculations in general (the latency of the detector is only 1-2 microseconds per sample).
8. Scan without snapshots, backups, and the delays they cause—they don't provide enough granularity for recovery.
9. Go agent-free to implement easily and guard against malware that targets backup agents.

Conclusion

If you have a virtual or hybrid environment, realizing the full benefits and promise of virtualization means your replication solution must be virtual-aware and ready. Zerto's hypervisor-based replication technology is the first and only solution that delivers virtual replication and DR capabilities for the data center and the cloud.

As your information and virtual initiatives grow over time, Zerto's purpose-built hypervisor-based replication solution will position you for growth and optimize your business continuity and data protection needs.

To see how Zerto can work in your environment, schedule a demo.

[Get a Demo](#)

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

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