Zerto

a Hewlett Packard Enterprise company

Zerto for Ransomware Resilience

How Continuous Data Protection Helps Combat Cyberthreats

Zerto
a Hewlett Packard Enterprise company

The Global Threat of Ransomware

Ransomware is one of the biggest threats organizations worldwide face today. With the frequency and severity of attacks increasing, executives and leaders worry about the negative impact ransomware can have on their organization. Organizations need to plan their response strategy to potential ransomware attacks before they suffer data loss and downtime.

As we discuss ransomware resilience in this white paper, we'll explore how ransomware operates, the NIST framework for protecting against it, and how Zerto, a Hewlett Packard Enterprise company, combines the industry's leading technology to give you true resilience.

What Is Ransomware?

Ransomware is a type of malware that maliciously encrypts data, locking out the owner. Similar to having a storage unit where someone else changed the lock, you still own your assets but cannot access them without the new key. When data is locked and inaccessible, the owners are faced with a choice: negotiate with criminals and pay the ransom—which could be millions of dollars—or try to recover the last good copy of data, bringing their organization online with minimal disruption and effort. This second option, while preferable, is much easier said than done.

Without data, most organizations become paralyzed and cannot function. The attackers play on this to create a state of panic and force quick payment. Many attacks come from either phishing or exploiting known vulnerabilities in systems. After the malware is planted, it's usually triggered by a random event or a date strategically planned to maximize damage, such as a fiscal year-end at a financial services company or Black Friday for a US retailer.

Unfortunately, ransomware is here to stay and is only on the rise. By 2031, the ransomware market will be worth an estimated $265 billion. As long as attackers are paid, the ransomware attacks will continue to grow and increase in severity.

> The ransomware market is expected to reach $265 billion by 2031.

Stopping Ransomware in Its Tracks

To end this perpetual loop of criminal activity, we must stop paying ransoms. We need to demonstrate to cybercriminals a robust recovery plan that limits downtime and reduces data loss, mitigating and eliminating the impact of ransomware attacks. This means you can avoid paying large ransoms and ultimately stop funding these criminal organizations—all without having to tolerate high levels of data loss.

In this white paper, we will explore how Zerto can help you achieve an uninterrupted business and recover within minutes to a clean state that's only seconds prior to an attack.

A Multi-Layered Approach for Ransomware Resilience

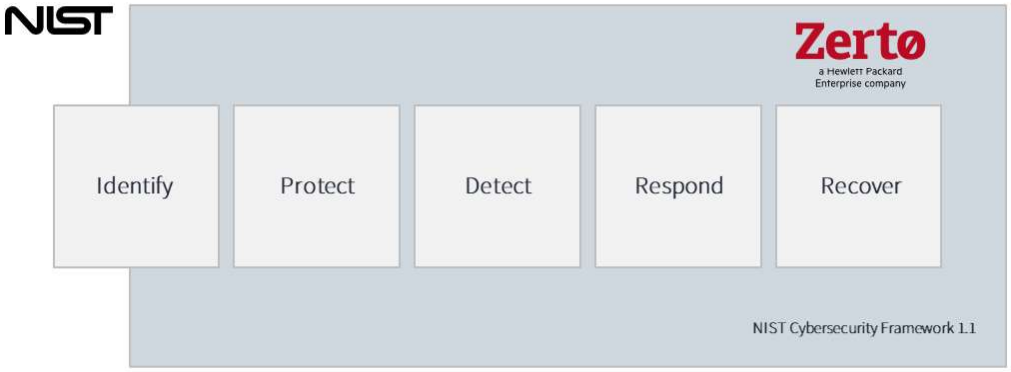
Although there are many different facets to a robust ransomware response, what resonates with experts and across industries is a multi-layered, multi-pronged approach that includes both proactive and reactive elements. We call this approach resilience. Rather than rely on a single piece of technology or process to mitigate ransomware, a resilient approach leverages specialist tools that provide industry-leading results in their area of expertise.

[1]*Cybersecurity Ventures "Market Ransomware Report"*

The ideal approach layers these best-of-breed tools rather than attempting to find one silver bullet that can do all tasks marginally but none of them well. For example, backup solutions are vital parts of every IT organization, but the speed and complexity of ransomware recovery means backup is more suited for compliance and long-term retention than cyber resilience. On the other hand, the modern security stack is well-equipped to prevent and stop ransomware, but these preventive solutions are not designed for data recovery after a malicious payload has detonated and encrypted production systems.

Zerto brings the best of both: it interoperates and complements both backup and cybersecurity solutions by enabling organizations to protect, detect, respond, and recover during ransomware attacks. The NIST Cybersecurity Framework can help demonstrate how continuous data protection (CDP) with Zerto unlocks these options for cyber resilience.

The NIST Cybersecurity Framework



Identify

An important part of any cybersecurity strategy—especially around ransomware—is identifying weaknesses and gaps in protection and recovery methods or strategies. Tools such as vulnerability scanners, automated penetration testing, phishing testing, etc. can all form a good basis for understanding what your organization is lacking. Zerto helps identify these gaps in infrastructure protection through nondisruptive ransomware recovery testing that requires minimal effort. Zerto allows you to spin up and test a simulated recovery from a ransomware attack in just minutes, providing valuable insights into how well your organization is prepared and if any critical infrastructure is missing from the recovery plan.

Protect

The cybersecurity industry is built on protection. As it relates to the NIST framework, protection revolves around security policies, roles and responsibilities, processes, and procedures. Protection ensures IT practices such as scheduled patching, backup configurations, and disaster recovery plans are in place and regularly tested and reviewed to ensure they are working and meet an organization's needs on an ongoing basis. Recently, many analysts and regulators have suggested that isolated recovery environments (IREs), or clean rooms, play a role in protecting organizations from the full impact of a cyberattack by ensuring data is isolated and locked away from harmful events.

An IRE ensures there is true isolation from production environments. It provides a trusted location to recover data and applications in the event of a ransomware attack. When combined with immutable copies in a vault, IREs ensure data is untouchable.

Normally IREs and vaults are based on backup technologies, which pushes the boundaries of backup capability. As a result, organizations lose more data and take far longer to restore than they would from a disaster recovery solution designed to recover at scale and with speed.

Zerto's Cyber Resilience Vault solves this problem by pairing Zerto with best-in-breed technology from the HPE portfolio—storage from HPE Alletra, compute from HPE ProLiant, and switches from HPE Aruba Networking—to create an IRE different from anything on the market. The Cyber Resilience Vault enables rapid air-gapped recovery in a trusted, secure environment to minimize data loss and downtime after an attack. See also: Zerto Cyber Resilience Vault solution brief for more details.

> "Isolated recovery environments with immutable data vaults provide the highest level of security and recovery against insider threats, ransomware, and other forms of hacking."
>
> *– Jerry Rozeman and Michael Hoeck, Gartner*

Data immutability with Zerto is also available when using the extended journal. Copies from the journal can be made immutable when stored on Azure Blobs, Amazon S3, or S3-compatible storage that leverages S3 Object Lock.

Detect

Detection is a critical piece of any cybersecurity and ransomware strategy. The NIST framework states that anomalous activity must be detected in a timely manner. What constitutes a "timely manner" may vary from organization to organization; however, every organization should make it their goal to detect in the shortest possible amount of time possible. Detecting encryption in real time is the best way for organizations to minimize the impact and spread of ransomware inside their environment.

Zerto's encryption detection enables organizations of all sizes to accelerate their ransomware response by alerting immediately if anomalous write activity is taking place inside their virtual environment. This block-level detection is then used to flag a potential compromise at the volume, VM, or application level when using Zerto Virtual Protection Groups (VPGs). Zerto automatically tags suspicious checkpoints as well as the last known clean recovery point to enable rapid action mid-attack. The Zerto encryption analyses are also available via API to unlock integration with an organization's existing SIEM, SOAR, or other security and observability solutions.

Zerto's streaming, inline detection can also be combined with other related technologies, like those available from HPE (e.g., Aruba IntroSpect) or an HPE alliance partner (e.g., Fortinet or RackTop). This multifaceted interoperability—what's sometimes called "composable security"—allows a business to build a complete, well-rounded ransomware detection strategy that is scanning for known malware signatures or other indicators of compromise (IOCs), as well as detecting the likely catastrophic encryption event that signals a ransom demand is imminent.

If we use traditional methods for detection, such as periodic scanning (which scans backups every 24 hours), we open the door for ransomware to spread through our environment before we detect it. Hours of scanning on an already aging backup copy likely means that a vast amount of damage has already been done.

Although long idle dwell times in environments do occur, recent reports by Mandiant show that the average global median dwell time for ransomware attacks is 5–9 days. This means that organizations can plan to recover with solutions like Zerto, which are focused on short-term retention. With a user-defined journal of one hour up to 30 days, Zerto offers far greater granularity than backup or archive options. This drastically reduces data loss to ranges as low as 5–10 seconds.

According to Mandiant's M-Trends Reports, median dwell time for ransomware is 5–9 days, with 69% of incidents having a dwell time under 30 days.

Respond

Whether an organization understands how to respond to a cyberattack or ransomware attack dramatically alters their ultimate outcome. Ensuring everyone in the business knows their role and responsibility and that they can execute it without hesitation or delay will speed up the end goal of recovery.

Zerto has an incredibly simple method for IT teams to roll back infrastructure within minutes to seconds before an attack. You can do it in just four clicks. Simple rollback gives the IT department confidence in their roles, responsibilities, and ability to take swift, decisive action at any time.

If a ransomware attack has occurred, many teams inside and outside the organization will likely be involved in the overall resolution. These teams include legal, crisis response, marketing, customer service, etc. You should also inform any necessary authorities and governing bodies. Once all teams are aware of their roles and duties in this event, you will need to ensure the infection has been stopped and infected systems have been quarantined, likely off-network. The recovery teams will also need to know what to recover, where to recover it, and from when.

Proving protection and practicing incident response can be done via nondisruptive testing with Zerto. It can be executed on demand with no impact to production applications or the protection of those apps. This allows organizations to test these plans thoroughly and regularly without interrupting their mainstream activities or needing to conduct tests outside of normal working hours. Regular testing instills higher confidence in your plans and a better understanding of how to respond to an incident when one does occur.

Recovery Phase

Resilient cybersecurity cannot assume preventive measures will never fail. As such, recovery is the most critical part of reacting to a ransomware attack for any organization. All other stages of the NIST framework lead toward a seamless recovery and, ideally, no ransom payment. Zerto is the industry leader in ransomware recovery. Let's dig into the recovery phase in a little more detail.

Data Loss. Data is now the world's most valuable asset. On-demand, 24/7 data access ensures organizations from every sector and every geography can continue operations and deliver the outcomes they exist to achieve. However, as soon as that data becomes unavailable, many organizations grind to a halt.

The same applies to data loss. If we allow data loss to stretch into hours, days, or even weeks, this will impede the organization's ability to function. Additionally, some data can never be replaced, so we need to take action that minimizes data loss as much as we possibly can.

Zerto recovers data from only seconds before a ransomware attack or any other data loss event, such as a logical failure or a bad actor deleting data. This means organizations suffer minimal impact from data loss and organizational operations can resume without a hitch.

Downtime. According to a recent IDC study, downtime costs organizations $250,000 per hour on average. Imagine this number multiplied across days or weeks—the total cost could be astronomical. Therefore, responding quickly and recovering data to a usable state to get systems operational is vital to everyone.

When we think about ransomware recovery, we need to think about disaster recovery rather than backup and restore. Restoring systems quickly and at scale is not something backup systems do well—they serve a different role in IT operations and are simply not designed for these use cases. Backup solutions may be able to recover at a small scale relatively quickly; however, when you need to recover your whole IT infrastructure in a matter of minutes, individual backup jobs will not cut it.

In this instance, organizations need to ensure that recovery times are as low as possible. This requires automation, orchestration, and a solid test plan to rehearse the procedure. Orchestration and automation will not only speed up the recovery process, but also eliminate human errors and minimize any ongoing impact.

Zerto has built-in orchestration and automation synced with the data path. In other words, the same tool that replicates and protects your data also orchestrates and automates your recovery. This is important because as recovery systems become more complex, the knowledge becomes more specialized, and fewer people can actually recover the data. Zerto avoids this with consumer-level simplicity at enterprise scale, allowing full recovery of whole IT estates with only a few clicks.

A Deep Dive into Real-Time Ransomware Detection

As discussed earlier, detection is a key pillar of minimizing the impact that ransomware has on an organization. Zerto has the unique ability to detect encryption in real-time as the blocks of data stream in, while adding no additional overhead to your production workloads. As data is replicated during normal operations, Zerto's unique method for detecting ransomware inspects each and every changed block, looking for anomalous encryption. Zerto uses a combination of both common and proprietary algorithms to inspect and assess the data writes, and it does so without requiring agents or additional infrastructure components. This allows organizations to catch any suspicious activity in real time and enables them to take swift and decisive action to stop the ransomware before it spreads widely.

Real-time ransomware detection takes place inside the Zerto Virtual Replication Appliance (VRA), a component that already exists in the Zerto architecture. Therefore, customers do not need to deploy any additional components to benefit from real-time ransomware detection from Zerto. Detection is completed at the source/production site—there is no delay or need to wait for data to be written to disk and scanned before it can be inspected for anomalous behavior.

A Deep Dive into Recovery

Using CDP, Zerto has the unique ability to recover data after a ransomware attack within just minutes and with only seconds' worth of data loss. Zerto is the only vendor that offers a proprietary, patented CDP engine for hybrid and multi-cloud environments at any scale. Let's review what makes up the CDP that powers Zerto to deliver industry-leading SLAs.

Near-Synchronous Replication

Zerto utilizes near-synchronous replication to achieve RPOs of seconds. Near-synchronous replication is built on taking the best parts of both synchronous and asynchronous replication and leaving the negatives of each behind. For instance, near-synchronous replication has the speed and agility of synchronous replication but not the latency, bandwidth, and cost concerns. It has the efficiency and rewind capabilities of asynchronous replication without lengthy delays and storage overheads.

Near-synchronous replication works inside the technology stack of your choosing and not at the storage layer. For example, inside a VM infrastructure, Zerto replicates at the hypervisor level, which means it's completely agnostic about storage, compute, and even cloud vendor choices.

Zerto's replication is completely agentless and doesn't rely on snapshots of your production environment. As a result, Zerto has no impact on production workloads. This means replication is continuous, always on, and never scheduled, giving you the peace of mind that your applications and data are always protected.

Application-Centric Protection

Most enterprise applications are made up of many component parts. Whether those parts include multiple VMs or other resources and services, each component is vital to the application and requires protection. Traditional data protection methods focus on the component parts themselves as individual items, ensuring each component part is protected. But, without any real understanding of where those components live and what they relate to, focusing on the component parts leads to longer recovery times and inconsistent data between application components when recovering.

Zerto customers perform 50,000 failovers per month with an average RTO of only two minutes and 25 seconds.

Zerto leads the way with application-centric protection. This means that an administrator of a virtual estate can logically group all the components that make up your application to be protected, replicated, and recovered together. Combine this with write-order fidelity, and every component inside the logical group is recovered to the exact same point in time. Zerto gives administrators the ability to recover the whole application as it stood at a particular point in time rather than having to try and rebuild the app from disparate data, which could span hours. The end result is a rapidly improved recovery time objective (RTO) and mean time to recover (MTR), saving valuable time and resources during an attack.

Unique Journal

Zerto stores data checkpoints in its unique journal, giving users the ability to restore from thousands of points in time, all only seconds apart. Organizations can limit data loss to just seconds after what could be a catastrophic ransomware attack. The Zerto journal can store data for any time between one hour and 30 days, giving customers flexibility with each application-centric protection group. Combined with real-time encryption detection, the Zerto journal allows organizations to identify known clean checkpoints to avoid recovering infected data, which wastes valuable time and resources.

"The big benefit against ransomware [with Zerto] is that we can easily just go back in time to the point before the attack."

– Infrastructure manager, government customer

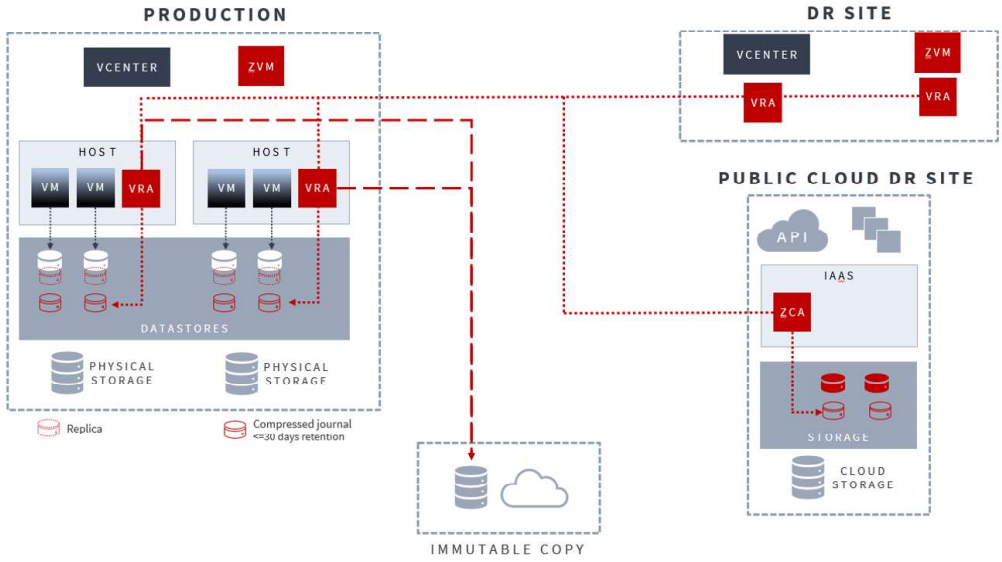
Zerto can recover full sites, individual applications, single VMs, and even files and folders from inside the VMs—all from the journal. This fast, flexible recovery allows users to choose not only the exact point in time from which they wish to recover, but also the exact item they want to recover.

Zerto Recovery Scenarios

Ransomware recovery is rarely a simple exercise. Each attack can impact IT infrastructure and applications in a different way. Therefore, it is crucial to have a flexible, fast, and trusted recovery mechanism for your data and applications. At Zerto, we give users the ability to recover exactly what they need to, to the exact point in time that they need it.

> *See also: our full walkthrough of ransomware recovery scenarios, explaining more about the different ways Zerto can help organizations recover from ransomware.*

The Zerto reference architecture below demonstrates resilience across the complete range of ransomware scenarios.



This Zerto architecture includes recovery options that span a variety of scenarios, including:

1. **File Infection** If the ransomware blast radius is limited to files and folders on a VM, these can be near-instantly restored back to their source location from a timestamp only 5–10 seconds before the infection. If needed, these can also be restored to a clean room prior to being put back in production.
2. **VM Infection** If one or more VMs are encrypted with ransomware, Zerto can near-instantly restore back to production with no intermediate steps (e.g., storage vMotion in vSphere). This recovery can also apply to all VMs that comprise a multi-VM application stack, including using the exact same point in time, separated by seconds, for the restore instead of timestamps staggered across a nightly backup window.
3. **Full Workload Contamination** If all VMs in the production/source site have been infected, a live failover to a secondary site can ensure operations are back up and running in minutes. Some customers run automated tests of this process daily, including security scans on the test VMs in an isolated bubble network—in case of infection, it is then easier to roll back to a tagged checkpoint that is known and verified as clean. If recovery from the Zerto journal is not possible for any reason, this architecture enables using storage snapshots as a copy of last resort.
4. **Full Site Contamination** If the production site has been badly compromised, simultaneous one-to-many replication to an additional cloud site can help mitigate the damage. Recovery can be to a hyperscaler such as

AWS or Azure or in an MSP's cloud. Access to the production site's hypervisor, let alone Zerto itself at production, is not required for this scenario, and failback to that primary site is simple if/when it is backed up and verified as clean.

5. **Full Source and Target Contamination—Immutability in Public Cloud** In a worst-case scenario, if the production site is fully down, the primary DR site is down, and the third site in the cloud is also compromised, recovery from offsite immutable copies is still available. These immutable copies are portable, so they can be reattached to a fourth site even if that site wasn't an original replication target. This new clean room can also be on-premises or with an MSP. Using clean and/or rebuilt infrastructure, it re-attaches the immutable repository and restores from there—this is particularly helpful since these will be restores of entire applications from a single consistent point in time rather than on a VM-by-VM basis.

6. **Full Source and Target Contamination—Air-Gapped Data Vault Coupled With a Zero Trust Isolated Recovery Environment** When ransomware snares your whole IT estate, having data copies that are not only immutable but also always accessible is imperative. A data vault that sits inside your own data center where only you have access will be a critical recovery step. Immutability or vaults in cloud environments can be beneficial, but to mitigate the worst attacks (where access to cloud or even the whole internet may be restricted), use data that is already patriated to the correct place. It can be recovered into a known clean environment, which will not only speed up recovery but also mitigate the impacts of a widespread attack. With the Zerto Cyber Resilience Vault, you will be implementing the only combined data vault and IRE in the market that utilizes journal-based recovery and all the other benefits that come with recovering with Zerto.

> "If we had to deal with a ransomware event, Zerto would be one of the first things I would use, because it is going to be the fastest to restore data to a certain point."
>
> *– IT director, manufacturing customer*

Post-incident Analysis

Recovery is the lifeline that organizations need to survive ransomware attacks. Examining an attack after recovery is vital to understanding it fully. This will highlight potential weaknesses and vulnerabilities inside the organization, which can then be rectified to strengthen your defense and avoid future attacks. Ideally, this examination would be done in an isolated environment, away from production workloads to ensure reinfection doesn't occur.

Zerto facilitates post-incident analysis with the ability to restore from multiple locations, including our unique 30-day journal, an environment of your choice, an isolated network of your choice, or into the Zerto Cyber Resilience Vault. This will allow forensic experts to look at the data and applications while they are infected. This environment can be spun up in as little as four clicks to run within minutes. In addition to simplifying the process, quick spinup speeds your efforts to fully understand any vulnerabilities and weaknesses, allowing for a faster response to ransomware.

Best Practices and Considerations

To achieve ransomware resilience and reliable recovery, follow the best practices below.

1. Protect the Zerto control plane and use role-based access control (RBAC) and multifactor authentication (MFA). Deploying strong local accounts to the hardened Zerto Virtual Manager Appliance (ZVMA) will ensure that only a small number of trusted users can access your last line of ransomware defense.

2. If possible, do not set hard limits on the Zerto journal inside of Zerto itself—set as unlimited, then manage space through your storage provider's tools and settings. In the case of mass encryption, this ensures steady state operations even as the write load dramatically spikes. Monitoring in Zerto Analytics will also reflect these write spikes.
3. If any infection is suspected, pause replication and test VMs inside a clean room. Zerto can manage this process, including spinning up test VMs and remove from inventory afterward. If integrating Zerto with a best-of-breed security tool, as is recommended, use alerts and alarms from that platform with Zerto's REST API to automatically pause replication and disconnect NICs when infection is detected.
4. Leverage one-to-many replication to place data on disparate infrastructures and reduce the chance of a single ransomware variant being able to encrypt every single target. Keep in mind that Zerto already separates journals and replicas, another advantage during an attack. Place an additional offsite copy of the journal on immutable storage in Azure, Amazon S3, or other S3-compatible storage (e.g., Scality).
5. In addition to the cloud, deploy a vault solution. Immutability in the cloud will help with less severe cyberattacks; however, the worst attacks will likely compromise access to cloud environments and the networks needed to repatriate data. This could further delay recovery and may even increase data loss. Vaults ensure that not only data but also the control plane, authentication, and network are controlled, accessible, and secure. An on-premises vault and isolated recovery environment will give you the best last line of defense against ransomware that has spread rapidly and reaches far across your environment.

Achieving Resilience with Zerto

Ransomware resilience is a complex topic, and there is no single solution that can solve for all use cases. Some specialty vendors can bolster your defense and attempt to stop ransomware in the first place, while others can identify and alert your SOC teams or specialize in recovery.

For over a decade, Zerto has been hyper-focused on recovery. The solution is renowned as the market leader in delivering the best RPOs and RTOs at scale, mitigating even the worst disasters—ransomware included. Zerto's battle-tested solution has been proven in the most demanding environments, including Fortune 10 companies and organization protecting over 10,000 VMs, by providing CDP for all workloads across private, public, and hybrid clouds. Zerto can neutralize the threat of ransomware and deliver maximum data retention and uptime for organizations of all sizes and sectors across the globe.

LEARN MORE

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

RITM0090537