Why Zerto for Ransomware Resilience

> Ransomware attacks have become increasingly common in recent years, targeting organizations of all sizes and industries. The consequences of a ransomware attack can be devastating, with organizations losing access to critical data and systems, even facing financial losses and reputational damage.

Continuous Data Protection and Journal-Based Replication

To combat the ever-growing threat of ransomware, Zerto, a Hewlett Packard Enterprise company, uses a combination of advanced technologies and best practices. Chief among these are continuous data protection (CDP) and journaling technology. CDP enables organizations to continuously capture and store changes to virtualized data in near real time, allowing for near-instant recovery after data loss or corruption. Even if ransomware manages to encrypt data on a system, the CDP journal can quickly restore the data from one of thousands of recovery checkpoints. Each of these checkpoints are only 5 to 15 seconds apart, enabling very granular restores instead of reverting back to a nightly backup copy that is hours and hours behind production.

Journal-based replication is another core Zerto technology. Journal-based replication creates multiple, consistent copies of data across different storage systems, ensuring that even if one data copy is lost or corrupted, other copies can be used for recovery. This method also prevents ransomware from spreading, since multiple copies of data provide multiple points of entry where ransomware can be isolated and removed.

Zerto enables organizations to easily protect and restore their data anywhere they need to with its one-to-many journal-based replication. This easily allows data to be copied from a production site to multiple target locations either on-premise, in the public cloud, or co-location. This allows organizations to easily protect their data beyond the traditional 3-2-1 data protection rule.

Granular Recovery and Seamless Integration

A major benefit of these technologies is granular recovery. Organizations can choose to recover specific files or folders rather than restore an entire system or data set. This targeted and efficient recovery reduces downtime and minimizes the impact on the organization.

Organizations also benefit from Zerto's seamless integration with other security and data management systems. Using Zerto's APIs can provide an easy way to interface with existing infrastructure and technology investments—including SIEMs and EDRs—to gain further value though automation. This can improve an organization's overall security posture and help them respond to and recover from security events rapidly.

Zerto is a powerful solution for organizations looking to reduce the risk and impact of a ransomware attack. By using CDP, journal-based replication, data mobility, and a range of secure technologies, Zerto helps organizations recover from attacks and protect their critical data and systems with efficiency and speed.

Why Make the Switch to Zerto?

From the features of CDP and journal-based replication to the benefits of granular recovery and seamless integration, there are many reasons to pick Zerto for ransomware resilience. Here are the top reasons:

Recover everything from files to datacenters.

With Zerto, organizations can recover not only individual files and folders, but entire virtual machines, applications, and datacenters as well.

Match the pace of today's digital business environment.

Zerto offers near real-time replication and data protection through CDP. This is critical in today's fast-paced business environment, where even the smallest amount of downtime can be costly and disruptive.

Leverage—rather than replace—what you already own.

Zerto integrates seamlessly with existing IT infrastructure through open APIs. Organizations can easily incorporate Zerto into their existing disaster recovery plans with automated processes.

Benefit from a resilience strategy tailored to your needs.

Zerto offers flexible recovery options. Instead of modifying infrastructure to meet the demands of an inflexible solution, organizations can tailor Zerto to meet their unique needs—whether that's recovering data to the same location, a different location, or a cloud-based platform.

Simplify your infrastructure and management overhead.

Zerto is easy to use. It's intuitive and user-friendly. Even organizations with limited IT expertise can use Zerto to successfully recover from ransomware attacks—no additional datacenters or personnel required.

Offsite immutable journal copies.

Zerto has the capability to create additional immutable copies from the journal that can be stored on Azure Blobs, Amazon S3, or any S3-compatible platform. This ensures that you can have a copy of your data that can't be modified or changed—allowing you to restore that copy to any available Zerto infrastructure for recovery.

Zerto for ransomware resilience provides comprehensive recovery capabilities, uses real-time replication and synchronization, integrates seamlessly with existing IT infrastructure, offers flexible recovery options, and is easy to use. With Zerto, organizations can protect their data from ransomware attacks and recover from those attacks without incident when they do occur.

Product Tour **On-Demand Labs**

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

RITM0077112