Don't Let Ransomware Hold You Hostage

How SecOps and disaster recovery work together to keep mission-critical applications safe

Data has become increasingly in demand, but with demand comes heightened concern over data integrity and accessibility. Malware, data exfiltration, and ransomware are prevalent and pose significant threats to data security. In a recent IDC survey, the majority of respondents indicated they had **activated a disaster response within the past 12 months, with 61% of those responses triggered by ransomware or other malware.** This alarming statistic exemplifies the growing problem businesses have protecting the applications critical to their daily operations.

There are multiple factors involved in fully protecting applications. Although quick recovery is important, proactivity is ultimately the best way to beat an unplanned disruption. That's why observability and detection, two key tools for proactively combating ransomware, are essential in any disaster recovery (DR) toolbox. A complete DR toolbox means combining the industry's best solutions for comprehensive protection.

Zerto, a Hewlett Packard Enterprise company, has teamed up with Elastic, a cloud-native enterprise search application, to provide an unmatched DR offering that protects mission-critical applications. On one side, Zerto simplifies the protection, recovery, and mobility of on-premises and cloud applications with continuous data protection (CDP), giving you industry-leading RPOs and RTOs. On the other, Elastic delivers cloud-native enterprise search, observability, and security solutions that enhance customer and employee search experiences. Together, these powerhouse applications unite to keep your mission-critical applications running smoothly and protect you against cyberthreats.

How Zerto and Elastic Work

Zerto and Elastic Security provide layers of intelligent defense and recoverability to secure all mission-critical applications against ransomware-susceptible vulnerabilities.

Elastic is a leading platform for search-powered solutions. As a proactive layer of defense intelligence, Elastic helps organizations, their employees, and their customers find what they need faster, while keeping applications running smoothly and protecting against cyberthreats. Their industry-leading SaaS platform, Elastic Security, helps users modernize SecOps through protection, investigation, and managing responses to complex threats. Elastic unifies the capabilities of security information and event management (SIEM), endpoint security, and cloud security into a single platform.

Zerto converges DR, ransomware recovery, and multi-cloud mobility into one simple, scalable solution. It provides always-on replication of even the most demanding enterprise applications, which ensures 24/7 availability and complete workload mobility and provides down-to-the second recoverability and automated replication.

Elastic Security and Zerto can work together to provide a comprehensive solution for data protection, DR, and security in a hybrid or multi-cloud environment. Here are a few ways in which Elastic Security and Zerto work together:

Threat detection and response

Elastic Security offers powerful capabilities for threat detection and response. It leverages machine learning algorithms, rule-based detection, and behavioral analytics to identify security incidents in real-time. When Zerto is integrated with Elastic Security, CDP and DR processes enhance your threat detection capabilities. Zerto can provide additional insights into potential security events by monitoring the replication and recovery activities of critical systems.

Incident investigation and forensics

Elastic Security provides a centralized platform for investigating security incidents and performing forensic analysis. It allows security analysts to search and correlate data from various sources, including logs, network traffic, and endpoint events. By integrating Zerto with Elastic Security, you can include data from Zerto's journal-based recovery and point-in-time backups during incident investigation. This integration enables security teams to gain a more comprehensive understanding of an incident's scope and impact.

Resilience and recovery

Zerto specializes in DR and business continuity solutions. It provides near-zero recovery point objectives (RPOs) and recovery time objectives (RTOs) by continuously replicating data at the hypervisor or storage level. By combining Zerto's capabilities with Elastic Security, organizations can strengthen their resilience against security incidents. In the event of a security breach or data corruption, Elastic Security can help identify the cause and contain the incident, while Zerto ensures rapid recovery and minimal data loss.

Overall, Elastic Security and Zerto together can enhance an organization's security, data protection, and recovery capabilities. They enable a more efficient and coordinated response to security incidents while ensuring business continuity in the face of disruptions.

How Zerto and Elastic Integrate

On each virtual instance, an Elastic Agent is installed and connected to the Elastic Stack in the cloud, which provides intelligent insights to proactively beat ransomware. Zerto is also installed on the virtual infrastructure and can be triggered to replicate and recover at the first signs of a ransomware attack.

Elastic and Zerto both have APIs that can “glue” them together, positioning users to take full advantage of their unique technologies. When integrated, these cloud-centric solutions empower users with an end-to-end prevention, detection, and recovery solution.

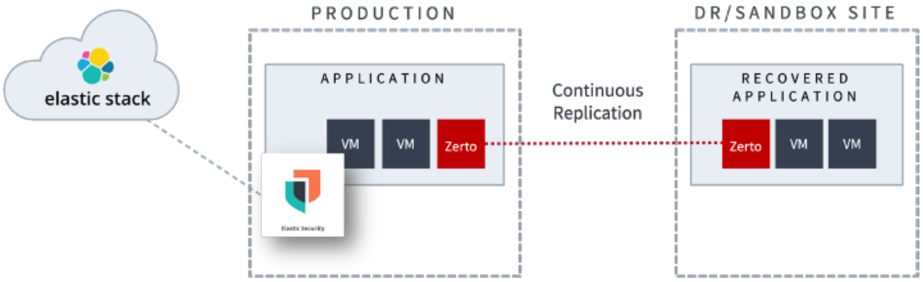

Figure 1. How Zerto and Elastic integrate to provide your virtual infrastructure with end-to-end protection.

Conquering Ransomware Together

Automated Threat Detection and Recoverability

Thwart complex attacks, block malware and ransomware, and protect applications nondisruptively.

Continuous Monitoring and Continuous Data Protection

Gain visibility across your attack surfaces and roll back to moments before a vulnerability is exposed.

Safe Sandbox for Investigation and Response Testing

Hunt for uncovered threats with ML insights in a near-second replication of the virtual instance you are seeking to protect.

Get Started

Don’t become another ransomware statistic: keep your mission-critical applications safe. Get end-to-end detection, protection, and recovery with a unique, combined offering from the industry’s best solutions. For more information, or to start understanding how Elastic and Zerto can help protect your data and applications, please reach out to sales@zerto.com.

Ready to learn more about Elastic Security? You can experience the latest version on Elasticsearch Service on Elastic Cloud for free!