Real-Time Ransomware Detection

Most modern businesses know they need to combat ransomware by deploying a multi-layered proactive and reactive security solution stack—what's known as defense-in-depth. But which solutions, and how do you layer them to maximize your chances at every step of the security chain?

Preventive cybersecurity tools can be excellent at detecting and stopping attacks, but ransomware can still break through despite all the barriers. Recovery solutions can be critical in these scenarios, but how do you know what data to restore: which recovery points are clean and unencrypted, and which are compromised?

Challenges of Periodic Detection

Unfortunately, traditional methods to determine clean recovery points aren't fast enough to keep up with the pace of today's rapidly evolving security landscape. Existing solutions typically scan backup copies, so the data is already hours old to start with (likely from last night's backup job) and the malware scanning process itself takes quite a few hours added on top. Worse, you might be locked into a vendor's own security scanning tools—all at added cost to you—that they've either bolted on to an existing product or licensed from a third party.

Moving to Real-Time Detection

Zerto, a Hewlett Packard Enterprise company, has innovated new technology to bring real-time encryption detection to the market. Zerto's software-only solution applies algorithmic intelligence to alert you within seconds when there's an encryption anomaly that could signal the start of ransomware's detonation phase. Since you no longer need to wait hours or days to know when recovery is necessary, you'll be able to radically reduce data loss and downtime following an attack—and do so without paying any ransoms.

> *"Zerto 10 will play a key role in delivering effective data protection and disaster recovery in an environment of increased cyberthreats. Its 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 and achieve the business goals we have in place."*
>
> —Steve Smith, Network Administrator at Unverferth Manufacturing

Key Differentiators

The proprietary Encryption Analyzer in Zerto 10 is dramatically different than other alternatives in the data protection and recovery industry:

- **Real-Time, Not Periodic:** Inline, streaming detection is continuously monitoring all data that flows into your digital environments. Be alerted near-instantly so IT or SecOps teams can take action mid-attack rather than being hours or days late to the scene of the crime.
- **No Production Impact:** Lightweight components—both small footprint and low overhead—combined with unique architectures means your production workloads aren't slowed down or taking performance hits. These same components perform the always-on, continuous replication that's essential to recovery, so there's nothing new to deploy to support this powerful real-time detection technology.

- **API-First Approach:** Avoid the black box that's all too common with competitors by leveraging Zerto's open REST APIs, based on Swagger, to integrate our encryption analyses with your existing security or observability stack. Stream the real-time detection and all associated alerts to the SIEM or SOAR of your choice, including powerful visualizations using open-source software such as Prometheus and Grafana; a free example is available on GitHub.

- **No Added Cost:** Zerto's real-time encryption detection is included out of the box. No paid add-ons; no extra subscriptions; no additional software to buy, install, config, and manage. The threat is too real for encryption detection to stay locked behind an add-on paywall instead of being core to recovery and ransomware resilience.

"As businesses continue to focus on resilience and continuous availability, the real-time ransomware detection capabilities offered by Zerto 10 are increasingly important to both maintaining an effective security posture and minimizing the risk of data loss and downtime. Our research shows that ransomware is not a matter of if, but a matter of when. In focusing on rapid detection and recovery, Zerto is offering key must-have capabilities designed to help organizations with the identification, mitigation, and remediation of ransomware threats."

—Christophe Bertrand, Practice Director, Enterprise Strategy Group (ESG)

Key Business Outcomes

Reduce Data Loss and Downtime: Leverage the earliest warning system to minimize the total ransomware impact by rejecting ransoms and rapidly recovering your data.

Minimize Risks and Costs: Avoid paying extra for security in your data protection solution, not to mention avoiding the cost of ransoms, the damage to your brand and reputation, and loss of productivity.

Maximize Operational Efficiency: Unify the efforts of security and infrastructure teams by detecting malicious encryption within seconds and enabling recovery within minutes.

Accelerate Time to Value: Complement your existing security stack by detecting anomalies immediately without deploying new infrastructure, adding new costs, or deploying separate solutions.

Learn more about how real-time encryption detection can combine with real-time data protection to enable ransomware resilience with Zerto.

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**

RITM0095279