Data Sheet

Recover In Minutes, Not Months

With Elastio's True Ransomware Detection and Malware Scanning

Why do you need true ransomware detection and malware scanning?

While existing perimeter and endpoint security tools are necessary, they are not enough to stay safe in today's cyber landscape because:

EDR and XDR solutions are reactive, not proactive: They can only detect and respond to ransomware attacks after they have already occurred. Scanning snapshots and data help identify and isolate ransomware *before* it encrypts data.

EDR and XDR solutions can be bypassed: Attackers are constantly developing new techniques to evade detection. Scanning snapshots can help identify ransomware even when it is able to bypass EDR and XDR solutions.

Reinfection after post-attack recovery can happen: Undetected malware can reinfect newly rebuilt systems that had XDR deployed on them, demonstrating the limitations of relying solely on perimeter defenses.

Elastio uniquely supports enterprises pre- and post-ransomware attacks. Our data integrity scans detect ransomware down to the individual file and specific strain pre- and post-detonation and enable quick post-attack recovery from the last-known clean copy.

Use cases

Post-attack business continuity: Minimize downtime and ensure a quick recovery in the event of an attack by preventing ransomware-infected backups from being inadvertently restored.

Threat intelligence integration: Enhance security measures by integrating threat intelligence into scanning processes, allowing for real-time identification of emerging threats and proactive defense against evolving ransomware strains.

Recovery testing: Conduct regular scanning as part of data resilience testing to verify the effectiveness of recovery security measures and identify vulnerabilities in the production and backup environments.

Compliance requirements: Standards like NIST, SWIFT, and GDPR demand advanced recovery procedures for timely restores in the event of an attack.

Key features and capabilities

File-level ransomware detection: Elastio's behavioral and deterministic engine, based on 2200+ and counting ransomware encryption strains, can detect encryption pre- and post-detonation in your data and snapshots.

Malware scanning: Offline scans for known and unknown ransomware and malware to prevent detonation in your data.

Retain full data custody: Data never moves out of your VPC, during and after the scan. Only the scan metadata is shown in the Elastio Tenant, so the customer maintains complete data custody.

Over-time analysis: Over-time analysis complements the model to unmask ransomware encryption that is evasive with slow encryption techniques.

Intelligent, scalable scans: Auto-scales worker instances using on-demand or spot instances based on the size and number of objects. Compute costs are optimized as the instances scale back after performing agentless scans.

Recovery assurance: Optionally store mission critical data backups in Elastio's ScaleZ Vault, with global data deduplication & compression, to ensure that you always have a clean recoverable copy of your data.

Integration with SIEM e.g., AWS SecurityHub: Get alerts on malware and ransomware findings pushed into AWSSecurityHub or other SIEM and ticketing tools.

Elastio detects and precisely identifies detonated and undetonated ransomware in your data and assures rapid post-attack recovery.

You can protect your data in AWS (EC2, EBS, ECS, S3, EKS, EFS and AWS Backup Recovery Points); Azure (VM backups and disk snapshots in Azure Recovery Service vault and Azure Backup vault); and VMware (Veeam, Commvault backups).