Data Sheet

elastio®

Secure Backups

With Advanced Ransomware and Malware Protection

Why do you need ransomware detection and malware scanning for backups?

Scanning backups for ransomware is critical because:

Simple air-gapping and immutability do not eliminate ransomware risk, as threat actors are crafting ransomware that can sit hidden and dormant for months before activating.

Anomaly detection alone does not eliminate ransomware risk, as sophisticated ransomware can make file activity appear normal.

Perimeter defenses alone do not eliminate ransomware risk, as ransomware often enters networks through social engineering, phishing emails, or insider threats.

For comprehensive ransomware protection, backups require advanced file and folder inspection in order to detect ransomware encryption, scan for malware signatures, check for file system corruption, and enable faster post-attack recovery.

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.

Data protection and integrity: Ensure the integrity of backups by scanning for ransomware, safeguarding against potential corruption or encryption that could compromise the ability to restore critical information.

Recovery testing: Conduct regular scanning as part of data resilience testing to verify the effectiveness of backup 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.

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

You can protect your data in EC2, EBS, ECS, S3, EKS, EFS, AWS Backup Recovery Points and VMware backups.

Learn more and get a free ransomware scan at www.elastio.com

Key features and capabilities

Scan AWS Backup recovery points and EBS snapshots
Seamlessly integrates with AWS Backup policies and EBS snapshots to scan for detonated and undetonated ransomware in your recovery points, keeping track of last-known-clean copies of your backups.

File system corruption check
Identifies integrity and consistency of the file systems data within a backup to ensure that the backups are indeed easily recoverable.

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.

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

Flexible automated and on-demand scans
You can perform automated and on-demand scans of S3 buckets based on your business needs.

Recovery assurance
Optionally store the 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 ransomware and malware findings pushed into AWS SecurityHub or other SIEM and ticketing tools.

Scan on-prem backups
Scan VMware backups taken by third-party backup tools like Veeam and Commvault to ensure the recoverability of your on-prem workloads.

Infra costs

Our analyses show the following results:

Feature	*Cost
Elastio IScan	$ 0.00007 per GB
Elastio IScan + ScaleZ Vault	$ 0.023 per GB/month

*Scan cost includes all AWS costs including compute and storage costs

Example: 10TB of EBS snapshots would cost $0.70 to scan. The same volume would cost $230 to scan and backup in the ScaleZ vault.