



# Recover In Minutes, Not Months

## With Ransomware and Malware Scanning for **S3 Backups**

### Why do you need ransomware and malware scanning for S3 Backups?

Cyber attacks can use S3 as a gateway and distribution point for ransomware or malware, posing a serious threat to your organization, as well as to third parties and consumers. If this malware finds a host to run on, the impact can be devastating.

Security best practices, as well as leading compliance standards such as NIST, SWIFT, and UK Government protocols, all stress the importance of scanning files in cloud storage before they are accessed by human users or applications. Scanning your S3 backups with AWS Backup restore testing ensures that your backups are clean, uncompromised, and recoverable.

### Use cases

**Compliance requirements:** Adhering to standards like NIST, SWIFT, and GDPR demands robust security postures, including malware scanning. This is especially critical for highly regulated industries.

**Content protection:** Assets like photos and videos shared internally or externally pose malware risks; CDN and content hubs are common distribution points.

**Web uploads:** Ensure that content from web uploads in cloud applications is safe before downloading by performing a ransomware scan.

**Third-party integrations:** Third-party data can come from a wide variety of sources, and not all of them will have robust security practices, necessitating ransomware scans.

**Data pipelines:** Data moving through ETL processes (e.g., for AI models) can come from multiple sources, increasing the risk of malware. Scanning for malware can help ensure the integrity of these pipelines.

### Key features and capabilities

#### Integration with AWS Backup restore testing capability

Elastio integrates seamlessly with the AWS Backup restore testing policy and sends the results into your recovery testing.

#### Intelligent, scalable ransomware/malware scans on AWS S3 Backups

Auto-scales worker instances using on-demand instances based on the size and number of objects.

#### Threat visibility across all AWS data

Gives a holistic picture of threats across your storage assets, including EC2, EBS, S3, ECS, EKS, EFS, and AWS Backup Recovery Points.

#### 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.

#### Full and partial S3 bucket scans

Customize scans to scan either an entire bucket or specific objects based on prefixes, paths, and globs.

#### Integration with SIEM e.g., AWS SecurityHub

Get alerts on malware and ransomware findings pushed into AWS SecurityHub 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).

Learn more and get a free ransomware scan at [www.elastio.com](http://www.elastio.com) or contact [sales@elastio.com](mailto:sales@elastio.com).

