Data Sheet

elastio

Recover In Minutes, Not Months

With Ransomware and Malware Scanning for **S3**

Why do you need ransomware and malware scanning for S3 buckets?

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.

Use cases

Cloud migration: When migrating to the cloud, it is crucial to scan the data to make sure that it is clean before setting up the environment.

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

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.

Intelligent, scalable scans for very large buckets

Auto-scales worker instances using on-demand 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-demandscansofS3 buckets based on your business needs.

Full and partial S3 bucket scans

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

Scan new or existing objects

Create policies to scan new objects as they are uploaded, to scan existing objects that are created within a specific period, or to scan all objects.

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).

Learn more and get a free ransomware scan at www.elastio.com or contact sales@elastio.com.

vmware aws Azure