CLOUD STORAGE SECURITY

Antivirus for Amazon S3

Prevent threats from infiltrating Amazon Simple Storage Service (S3) and Amazon WorkDocs and reduce the risk of sharing malware with others

The Blind Spot in Cloud Storage

A growing number of organizations are using Amazon S3 and Amazon WorkDocs as the object store for files uploaded by application users or as a data lake to cost-effectively build, scale and analyze data.

Since data may come from external sources and can eventually enter an environment where they become executable, uploading objects without first scanning them for advanced threats could become a vector for virus payloads.

Yet, AWS does not scan objects going into or out of storage for advanced threats. In line with the AWS Shared Responsibility Model, it's up to the customer to ensure that their data are free of malware. What's more, many regulations *require* organizations to implement procedures that protect against infection.

Traditionally, organizations have had to purchase an expensive and complicated data security platform or build their own solution in house. Now organizations have the option of using Antivirus for Amazon S3 by Cloud Storage Security.

https://CloudStorageSec.com/AWS

6 Reasons Customers Love This Product

Prevents Malware Intrusion

Easily identify and remove malware by scanning all files no matter how they arrive in storage, for files up to 5TB in size

Helps Meet Compliance

Near real-time and scheduled scanning meet malware scanning compliance requirements

Automated Assurance at Your Fingertips

Proof of data protections and controls that can be shared with executive teams, auditors, and customers

Gain Visibility into Misconfigurations

Quickly identify all S3 buckets with secure and insecure permission policies

Only Pay for What You Need

Don't break the budget on an entire data security platform when all you need is a dedicated, easy-to-use solution that scans storage for malware

Maintain Reputation, Money & Effort

Improve storage security posture to prevent costly and embarrassing infection transmissions as well as service disruptions

aws PARTNER

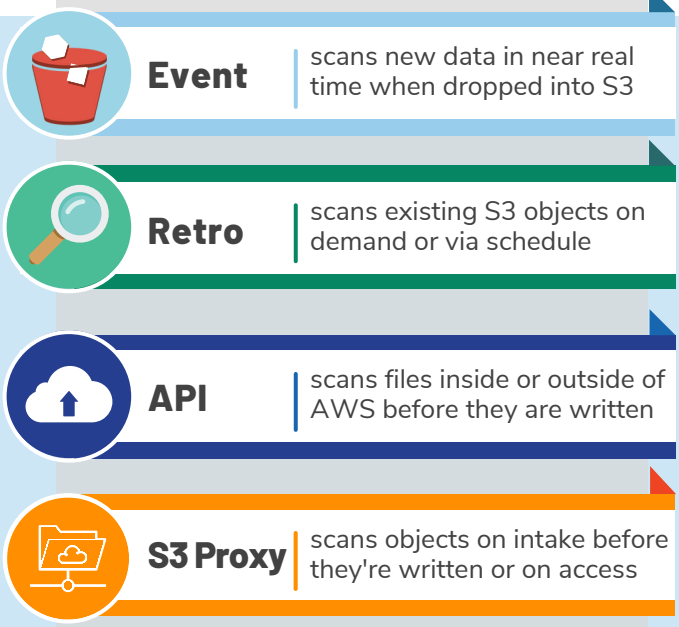
- Public Sector
- Authority to Operate
- Security Software Competency

Antivirus for Amazon S3 Features

Our modern, cloud-native malware scanner:

- Runs in tenant, meaning data never leaves your account
- Installs in minutes via AWS Fargate Containers and CloudFormation Templates
- Uses multiple virus detection engines including ClamAV and Sophos
- Auto discovers all Amazon S3 buckets across multiple accounts and regions
- Provides almost immediate visibility into the prevalence of malware
- Remediates problem files (e.g., quarantine, tag, delete)
- Integrates with SIEM and workflow tools, such as AWS Security Hub

Scan Models



Simple Consumption-Based Pricing

PAYG (USD)

Unit Type	Cost/GB
Free Trial	$0
Monthly Subscription - includes 100GB of premium engine scanning	$49.00
Scan 101 - 500 GB per month	$0.40
Scan 501 - 1,500 GB per month	$0.35
Scan 1,501 - 3,000GB per month	$0.30
Scan >=3,001 GB per month	$0.25
Scan pre-existing objects	$0.25
Premium Engine per GB Add-on - Sophos	$0.10
Premium Engine per GB Add-on - pre-existing objects - Sophos	$0.10
Cloud Detonation - Static Analysis (Per File)	$0.05
Cloud Detonation - Dynamic Analysis (Per File)	$0.50

Scan up to 500 GB in 30 days with a FREE TRIAL in AWS Marketplace

Either Amazon EC2 or AWS Fargate is required. For infrastructure costs, please refer to Amazon EC2 and Amazon Fargate pricing.

Start a trial in AWS Marketplace or contact us to learn about our prepaid license option, which can significantly reduce costs.

CLOUD STORAGE SECURITY

aws Qualified Software