

Data Security for Cloud Storage

Know and protect the sensitive data you're storing. Reduce the risk of ingesting and sharing malware. Assess your storage environment.

The Blind Spot

Given the flexibility and performance of managed storage services such as Amazon S3, a growing number of organizations use them as object stores for files uploaded by application users or to build data lakes to cost-effectively scale and analyze data.

Ingesting files from external sources without scanning them for advanced threats can become a vector for virus payloads. According to the AWS Shared Responsibility Model, the organization using the storage service is responsible for the security of the data. This includes ensuring that the data is free of malware; AWS does not automatically scan for advanced threats.

What's more, the data may contain sensitive information, which requires additional safeguards to meet data privacy requirements, prevent compliance violations, and ensure security. But finding and tagging sensitive data is not an easy task when you store a lot of data and don't know where it is.

Traditionally, organizations have had to purchase an expensive and complicated data security platform or build their own solution in house. Today, organizations have the option of using Cloud Storage Security's malware protection and data loss prevention (DLP) solutions.



CloudStorageSecurity.com/aws

7 Reasons Customers Love Us



Easily Prevents Malware Intrusion

Identifies and removes malware no matter how objects arrive in storage.



Simplifies Data Loss Prevention

Classify and protect sensitive data in a complex environment by gaining visibility and control of structured and unstructured data at scale.



Meets & Maintains Compliance

Real-time, on demand and scheduled scanning meet requirements.



Provides Visibility into Configurations

Identifies secure and insecure permission policies. Reports on encryption.



Deploys Quickly

Can be procured in AWS Marketplace and automatically added to AWS billing. You're up and running in 15 minutes or less.



Only Pay for What You Need

- Pay-as-you-go pricing, BYOL, prepaid discounts and private offers
- Smart Scan and scheduled scanning
- Less expensive than a homegrown solution or a platform with extra features that you don't need but have to pay for



Maintain Reputation, Money & Effort

Improves operational efficiency and security posture; prevents costly and embarrassing infection transmissions, data leaks, services disruptions, and fines.



- Public Sector
- Authority to Operate
- Security Software Competency
- AWS Marketplace Seller

Features

- Automated serverless security solution
 - Runs in tenant, meaning data never leaves your account
 - Installs in 15 minutes or less using AWS CloudFormation Template or Terraform
 - Remediates problem files based on user-defined policies (e.g., quarantine, tag, delete)
 - Integrates with SIEM and tools such as AWS Security Hub
 - Automatic discovery and scaling across multiple accounts and regions
 - Private VPC endpoint deployment option
- ### Malware Protection
- Supports Amazon S3, Amazon FSx, Amazon EFS, Amazon EBS, Azure Blob
 - Scan engines include Sophos, CrowdStrike and ClamAV
 - Static and Dynamic Analysis through SophosLabs Intellix
 - Integrated with AWS Transfer Family
- ### Data Loss Prevention
- Supports Amazon S3, Amazon FSx, Amazon EFS, Amazon EBS
 - Leverages Sophos engine
 - Identifies hundreds of sensitive data types

Scan Models

Flexible scanning options fit into any workflow without disruption



Event

scans new data in real time when dropped into storage



Retro

scans existing data on demand or via schedule



API

scans files inside or outside of the cloud before being written

New Data Pricing

Monthly Scan Volume	PAYG
Free Trial	\$0
1 - 100 GB	\$99/mo
101 < GB	\$0.80/GB
Premium Engine - Add-on (AV only)	+\$0.10/GB

Custom pricing is available for large data sets and when using both malware protection and data loss prevention solutions. We also make private offers.

Cloud Detonation (AV Only)

Analysis Type	Cost/File
Static Analysis	\$0.05
Dynamic Analysis	\$0.50



Available in
AWS Marketplace

**Scan 100 GB in 30 days
on us with a FREE TRIAL**

AWS Fargate is required; for infrastructure costs, please refer to Amazon Fargate pricing.



[Learn More](#)

