Data Security for Cloud Storage

Protection that evolves to meet expanding threats so you're never left behind.

The Need for a Ongoing Security

Managed storage services like Amazon S3 help organizations store vast amounts of data and build scalable, cost-effective data lakes. As these services improve, businesses adoption grows across industries.

However, organizations must take responsibility for securing their cloud-stored data. The AWS Shared Responsibility Model makes it clear: businesses using AWS storage services must protect their own data, including safeguarding it against malware.

Effective data security requires continuous adaptation to evolving threats. Robust security practices depend on ongoing scanning to prevent costly breaches. A single scan isn't enough—every week, cybercriminals introduce dozens of new malware variants that can lie dormant in your data, waiting to execute.

Cloud Storage Security (CSS) provides comprehensive cloud protection with Antivirus for Amazon S3—a solution designed and priced to make continuous scanning easy and effective.

Cybercriminals don't stop after one attempt—your security strategy shouldn't either.

7 Reasons Customers Love Us

Defends Against Malware
Identifies and removes incoming malware regardless of delivery method.

Multi-cloud Environment Protection
Protect your entire environment with a solution designed and priced for scale.

Ongoing Compliance and Safety
Live, on-demand and scheduled scanning evolve alongside threats.

Offers Visibility into Configurations
Identifies secure and insecure permission policies. Reports on encryption.

Deploys Quickly
Can be found and deployed from AWS Marketplace in under 15 minutes.

Flexible Subscription Plans
Four subscription tiers for every organization size.

Maintain Reputation, Money & Effort
Improves security posture; prevents malware transmissions, data leaks, services disruptions, and fines.

CloudStorageSecurity.com/aws

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

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

Features	Scan Models

Features

- Automated serverless security solution

- Runs in-tenant, data only leaves your environment if you want it to

- Alerts you in-console, over AWS SNS/CloudWatch and 3rd-parties like email and Slack

- 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

- Supports Amazon S3, Amazon FSx, Amazon EFS, Amazon EBS, Multi-Cloud

- Scan engines include Sophos, CSS Premium Engine and ClamAV

- Static and Dynamic Analysis through SophosLabs Intellix

- Integrated with AWS Transfer Family

Scan Models

Flexible scanning options fit into any workflow without disruption

API | scans files inside or outside of the cloud before being written

Event | scans new data in real time when dropped into storage

Retro | scans existing data on demand or via schedule

Antivirus Pricing
Enterprise, Unlimited Licenses

		Tier 1	Tier 2	Tier 3	Tier 4
Eligibility (lesser of)	Number of Employees	0 - 30	31 - 100	101 - 1,000	1,001+
	Monthly AWS Spend	$0 - $35,000	$0 - $200,000	$200,001 - $1 million	>$1 million
Pricing per Month		$750	$3,000	$5,000	$10,000
Add-ons			+10% for CSS Premium Engine +15% for Sophos Discounts are available for MSPs, please inquire *All subscriptions include CSS Secure scanning engine*		

See Listing for PAYG pricing.

aws **Available in AWS Marketplace**

30 Day FREE TRIAL

CLOUD
S T O R A G E   S E C U R I T Y

011025