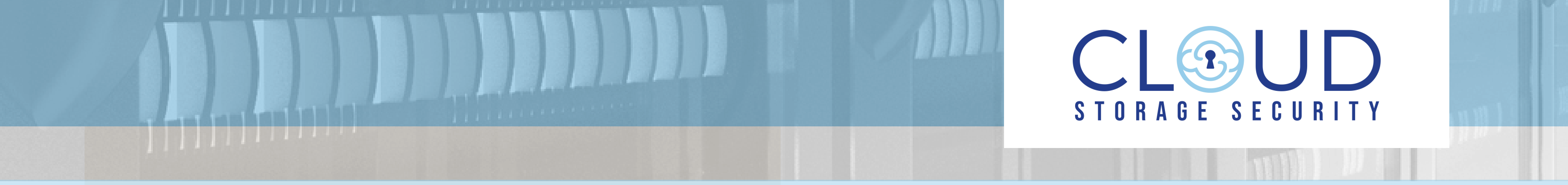

CLOUD STORAGE SECURITY

Data Security for Cloud Storage

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

The Need for a Secure Cloud

Organizations use managed storage services like Amazon S3 to store files and build data lakes which scale cost-effectively. The adoption of managed storage services across verticals has grown significantly as these services' flexibility and performance improves.

When storing data in the cloud, it is crucial that organizations understand their risks and responsibilities. According to the AWS Shared Responsibility Model, organizations using AWS storage services are responsible for securing their own data. This includes defending against malware.

To avoid the monetary, reputational and time costs of compliance violations or remediation in malware and ransomware events, organizations must adopt comprehensive data security solutions. Comprehensive security is especially important for organizations who handle sensitive data and face strict requirements.

Where organizations previously relied on expensive in-house solutions or patchwork point solutions, they can now trust in Cloud Storage Security's (CSS) comprehensive environment protection through Antivirus for Amazon S3.

CloudStorageSecurity.com/aws

7 Reasons Customers Love Us

Defends Against Malware

Identifies and removes incoming malware regardless of delivery method.

Simplifies Environment Protection

Protect your entire environment with a solution designed and priced for scale.

Ensures Ongoing Compliance

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

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

Three enterprise subscription tiers purpose priced for small, medium and large organizations.

Maintain Reputation, Money & Effort

Improves security posture; prevents malware transmissions, data leaks, services disruptions, and fines.

aws PARTNER

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

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

Malware Scanning

- Supports Amazon S3, Amazon FSx, Amazon EFS, Amazon EBS, Microsoft Azure Blob
- 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
Eligibility (lesser of)	Number of Employees Monthly AWS Spend	0-100 $0 - $200,000	101-1,000 $200,001 - $1 million	1,001+ >$1 million
Pricing per Month		**$3,000**	**$5,000**	**$10,000**

Add-ons	+10% for CSS Premium Engine +15% for Sophos All subscriptions include CSS Secure scanning engine.
	+20% for Premium Support

See Listing for PAYG pricing.

CLOUD STORAGE SECURITY

aws Available in AWS Marketplace

30 Day FREE TRIAL