

Malware Detection Made Easy

Cloud storage services are used for applications and data ingestion pipelines to cost-effectively collect, store 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 malicious code. What's more, security frameworks and regulations require organizations to protect against malware. Traditionally, organizations have had to purchase an expensive and complicated data security platform or build their own solution in house. Today, they can rely on Cloud Storage Security (CSS).

Why Customers Love Us



Supports AWS and Microsoft

Amazon S3, Amazon EBS, Amazon EFS, Amazon FSx, Azure Blob Storage.



Protects Against Malware

Detect and remediate ransomware and other types of malware no matter how data arrives in storage.



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.



Assists with Audits

Proof of data protections and controls that can be shared with c-suite, auditors, and customers.



Deploys Quickly

Can be procured in AWS Marketplace and automatically added to AWS billing. Get started 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

Proven Benefits

Complete Security Risk Assessment in 24 Hours

A company completed a baseline scan of 120+ million existing objects within a few hours; within 24 hours all objects were scanned.

Stop Malware

A customer scanned more than 300 million objects and found over 1,400 malicious files.

50% Less Expensive

Through CSS's custom pricing and modern, Fargate container-based solution, a customer's total cost of ownership would be 50% lower than other solutions.

Dozens of Hours of Maintenance Eliminated

CSS automation eliminated dozens of hours of maintenance time while meeting real-time scan requirements.

98% Reduction of Resources

CSS shortened a security review process from 2 days to 1 hour by automatically scanning terabytes of data across multiple AWS accounts and streamlining reporting in a single dashboard.



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

Helps with SOC & ISO

Antivirus for Amazon S3 plays a key role in maintaining our SOC 2 certification and ISO 27001 compliance, integrating easily into our application workflow and our SOC operations. It is also helping us win new business, assuring security conscious customers that all user uploaded files are scanned and secure before they are shared with other users.

Darragh Duffy, Software and Infrastructure Engineering, [Workvivo](#)

Meets every requirement we have



This solution completely met our expectations and requirements. API scanning and totally private deployment to be precise. We have scanned thousands of objects so far without any problems or complications. Our clients can trust us with our solution thanks to Cloud Storage Security.

Ivan Tsenov
Review verified by AWS Marketplace

We were about to give up.

We found Cloud Storage Security through an AWS referral. We had already evaluated Kaspersky, TrendMicro, and Sophos and were about to give up. Super happy with the solution.

Business Services, Information &

Document Management Customer

Simple Amazon S3 Antimalware Scanner and Dashboard



I couldn't find an enterprise class solution for some time and I finally found *Antivirus for Amazon S3*... Simple, scalable deployments and I was scanning buckets in minutes. To date, I have scanned over 1 million files and scaling up and down scanning agents as required. We thought about creating a solution ourselves, but this solution exceeded our expectations!

Steve, VP IT Operations
Review verified by AWS Marketplace

Features

- Automated serverless security solution
- Runs in tenant--data never leaves your account
- Installs in minutes using AWS CloudFormation Template or Terraform
- Automatic discovery and scaling across multiple accounts and regions
- Multiple premium detection engines
- Integrates with SIEM systems you already have in place
- Automated remediation of problem files (e.g., quarantine, tag, delete)
- Static and Dynamic Analysis
- Private VPC endpoint deployment option
- Scans any size file or volume

Scan Models

Flexible scanning options fit into any workflow without disruption



Event

scans new files in near real time when dropped into storage



Retro

scans existing files on demand or via schedule



API

scans files inside or outside of AWS before they are written



FREE TRIAL



Available in
AWS Marketplace

Contact us for custom pricing





Built For and Powered By AWS

Built Using:

- AWS CloudFormation
- AWS Fargate
- Amazon ECS
- Amazon DynamoDB
- AWS AppConfig
- AWS IAM
- Amazon Cognito
- AWS Lambda

Integrates With:

- AWS Security Hub
- Amazon SNS
- Amazon SQS
- Amazon CloudWatch
- AWS Control Tower
- Amazon EventBridge
- AWS CloudTrail
- AWS Transfer Family

Available for:

- AWS GovCloud
- Commercial AWS Regions



Most Viewed Article on AWS

About CSS

Cloud Storage Security (CSS) protects data in the cloud so that businesses can move forward freely and fearlessly. Its robust malware detection and data loss prevention solutions are born from a singular focus on, and dedication to, securing the world's data, everywhere.

Serving a diverse clientele spanning commercial, regulated, and public sector organizations worldwide, the company solves security and compliance challenges by identifying and eliminating threats, while reducing risk and human error. CSS's modern, cloud-native solutions are streamlined and flexibly designed to seamlessly integrate into a wide range of use cases and workflows, while complementing and bolstering existing infrastructure and security frameworks.

CSS holds certifications including SOC2, AWS Public Sector Partner with an AWS Qualified Software offering, AWS Security competency, and AWS Authority to Operate.

