CLOUD STORAGE SECURITY

Antivirus for Amazon S3

Malware Detection Made Easy

AWS storage services are used by applications and data ingestion pipelines to cost-effectively collect, scale and analyze data. Ingesting objects from external sources without scanning them for advanced threats can become a vector for virus payloads.

In line with the AWS Shared Responsibility Model, it's up to the customer to ensure that their data is free of malware; AWS does not scan objects going into or out of storage for advanced threats. 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, organizations can use Antivirus for Amazon S3 by Cloud Storage Security.

5 Reasons Customers Love Us

Prevents Malware Intrusion

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

Meets & Maintains Compliance

On demand and scheduled scanning meet malware scanning requirements.

Provides Visibility into Configurations

Identifies all buckets with secure and insecure permission policies. Reports on encryption.

Quick Deployment

Procured in AWS Marketplace and automatically added to your monthly 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

Proven Benefits

Fast & Efficient

MindEdge completed a baseline scan of 120+ million existing objects within a few hours. Within 24 hours all objects were scanned.

Stopped Malware

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

50% Less Expensive

Because Antivirus for Amazon S3 is a modern, Fargate Container based solution, ADEC Innovations determined that their total cost of ownership for the product would be 50% lower than the other Lambda and EC2 based solutions.

Dozens of Hours of Maintenance Eliminated

Antivirus for Amazon S3 eliminated dozens of hours of maintenance time that was required to keep the former solution running and able to meet Poka's real time scan requirements.

Simple Yet Robust

ADEC Innovations reviewed multiple solutions but decided to go with Antivirus for Amazon S3 because it was so simple to set up yet robust to use.

aws PARTNER

- Public Sector
- Authority to Operate
- Security Software Competency

Features

- Runs in tenant, meaning data never leaves the customer's AWS account
- Installs in minutes via AWS Fargate Containers and CloudFormation Templates
- Uses multiple virus detection engines including ClamAV, Crowdstrike and Sophos
- Auto discovers all Amazon S3 buckets across multiple accounts and regions
- Scans files up to 5TB in size
- 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

How it Works

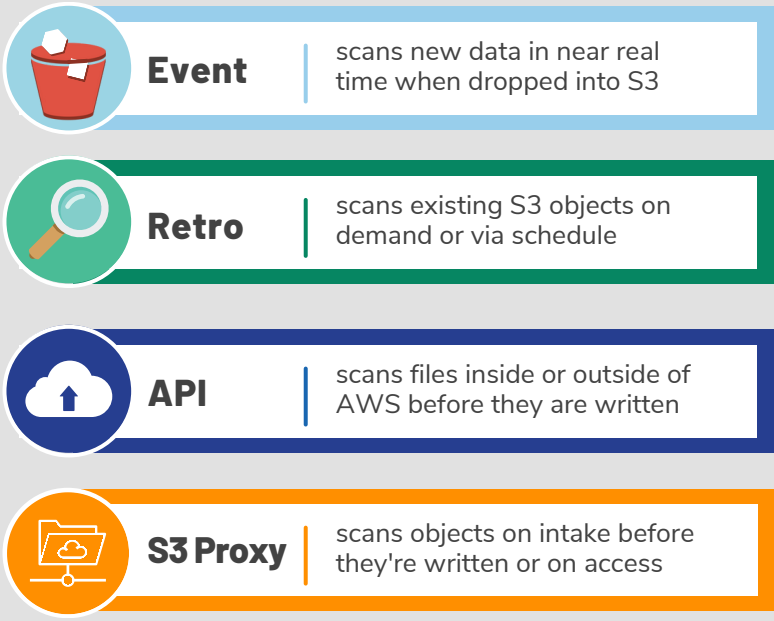
Antivirus for Amazon S3 is different from other solutions because its scan models accommodate any type of workflow without interruption:

- Scan new data in real time when dropped into Amazon S3 or WorkDocs, on intake before it is written, or on access when it is retrieved.
- Scan existing data on demand or via schedule.

When a scan completes, a verdict is returned. If an object is found to be infected, you're alerted and may quarantine it, delete it or decide to keep it in place.

If additional investigation is warranted, we've harnessed the power of the SophosLabs Intelix Platform to offer Static Analysis and Dynamic Analysis.

Scan Models



Built on AWS to Support AWS-Managed Services

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 (Account Factory Customization)
- Amazon EventBridge
- AWS CloudTrail (CloudTrail Lake)

Support For:

- Amazon Simple Storage Service (Amazon S3)
- Amazon WorkDocs

Available In:

- AWS GovCloud
- Commercial AWS Regions

“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

Getting Started

15 minutes and a few straightforward steps is all it takes:

1. Subscribe to Antivirus for Amazon S3 in AWS Marketplace.
2. Deploy the software as an ECS container and set of resources. Antivirus for Amazon S3 is installed using a CloudFormation Template. You will be asked a series of questions to install the software.
3. Configure scanning with a few clicks of your mouse via an easy-to-use dashboard; no need to write scripts.

Read the AWS Blog

One of the most viewed APN Blog Posts in 2022.

About CSS

Agencies and enterprises of all sizes turn to Cloud Storage Security (CSS) to extend data privacy, meet compliance requirements, and manage data security. Specifically, they turn to CSS to prevent the spread of malware, locate sensitive data, and assess their storage environment. CSS solutions are used worldwide for applications and data lakes built on cloud storage because they fit into any workflow and data never leaves the customer’s account. Take advantage of a 30 day free trial or contact CSS for more information.

CLOUD STORAGE SECURITY

aws Qualified Software