

# Data Classification for AWS Storage

Know what type of data exists and where it exists so you can protect the sensitive data you're storing

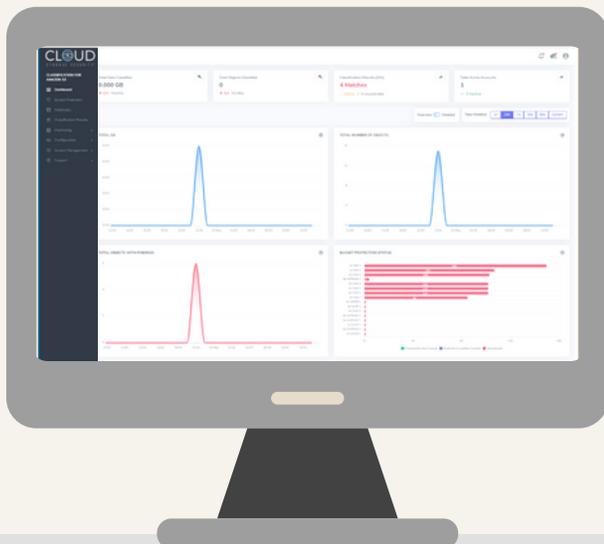
## The Blind Spot

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.

When data comes in from third parties, you may not realize that it includes sensitive data, which requires additional safeguards to prevent compliance violations, meet data privacy requirements, and ensure security.

Yet, 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 platform or build their own solution in house. Now organizations have the option of using Cloud Storage Security's Data Classification solution.



<https://CloudStorageSec.com/aws-data-classification>

## 5 Reasons Customers Love Us



### Supports Most All AWS Storage Services

Amazon S3, Amazon EBS, Amazon EFS, Amazon FSx (NetApp ONTAP)



### Simplifies Classification

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



### 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

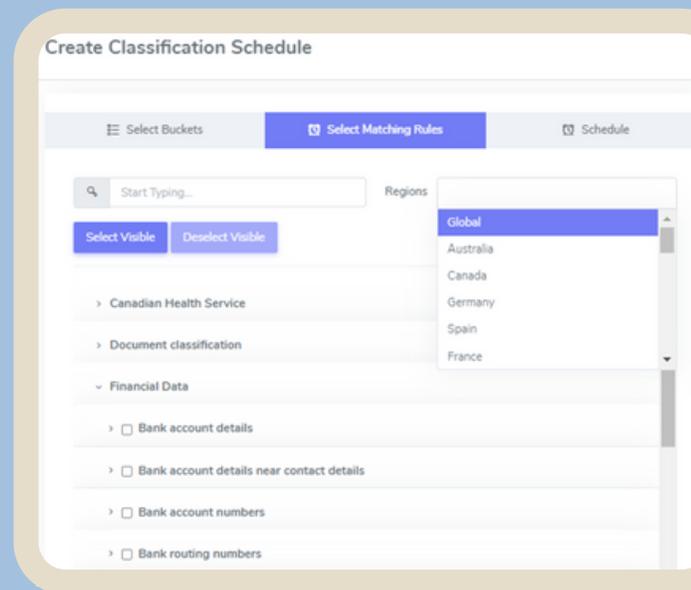
Improves operational efficiency and security posture; prevents costly and embarrassing data leaks, services disruptions, and fines.



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

## Features

- Automated serverless solution
- Runs in tenant, meaning data never leaves your account
- Installs in minutes using AWS CloudFormation Template or Terraform
- Private VPC endpoint deployment option
- Automatic discovery and scaling across multiple accounts and regions
- Real-time and scheduled scanning that leverages SohposLabs
- Scans files up to 195 GB across range of file formats
- Identifies hundreds of sensitive data types
- Covers 11 regional localizations
- Remediates problem files
- Integrates with SIEM and workflow tools such as AWS Security Hub



## Consumption-Based Pricing

Unit Type	Cost/GB
Free Trial	\$0
Monthly Subscription - includes 100GB	\$49.00
Scan 101 - 500 GB per month	\$0.40
Scan 501 - 1,500 GB per month	\$0.35
Scan 1,501 - 3,000GB per month	\$0.30
Scan >=3,001 GB per month	\$0.25

AWS Fargate is required; for infrastructure costs, please refer to [Amazon Fargate](#) pricing.

*Custom pricing is available for large data sets.  
We also offer prepaid licensing and private offers.*

 Available in  
AWS Marketplace

**Scan 500 GB  
in 30 days  
with a  
FREE TRIAL**



**Let's Connect**  
+1 385 376-3838  
sales@cloudstoragesec.com