CLOUD STORAGE SECURITY

Data Security for Healthcare & Life Sciences Organizations

Protect patient data, medical research, and intellectual property. Operate securely and enable innovation in the cloud.

The Problem

Healthcare and life sciences is consistently the most targeted vertical in terms of ransomware attacks. With an **average cost of $9.77 million**[1] and an average systems recovery time of **287 days**[2], ransomware cripples healthcare organizations, causing headaches for months, and most importantly, **disrupting patient care**. Healthcare organizations also lose the most amount of data during a ransomware attack, with an estimated impact of **five times more sensitive data lost** than the global average.

Complicating the problem of data security is the fact that healthcare organizations ingest an immense amount of data from multiple sources, much of which is regulated under different compliance requirements. This data, if inadvertently made publicly accessible, or copied into a forgotten test environment for application development, could result in a data breach.

Given these challenges, it can be difficult to protect data and maintain compliance. So how do healthcare and life sciences organizations operate securely and enable innovation in the cloud? With simple, easy-to-implement solutions that don't have to move your data in order to scan it for ransomware and sensitive information, and that can also report on configuration and permission issues across all of your accounts.

How We Help

Cloud Storage Security (CSS) protects data so that businesses can move forward freely and fearlessly.

Prevent Ransomware Intrusion

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

Prevent Data Loss

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

Maintain Compliance

Provide proof of data protection and controls via summarized reports.

Gain Visibility into Configurations

Identify secure and insecure permission policies. Report on public access and encryption.

Support For

Amazon S3

Amazon EBS

Amazon EFS

Amazon FSx

Microsoft Azure Blob

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

Key Features

- Runs in tenant; all data remains under your sovereignty and control
- Private VPC endpoint deployment option without public internet connections
- Two-bucket configuration that only allows clean files into production/staging
- Event-based, retro and API scan models
- Ability to scan files before they are written to storage
- Multiple scanning engines

Proven Benefits

Security Risk Evaluated and Quantified in 24 hours

A company completed a baseline scan of 120+ million existing objects within a few hours; within 1 day all objects were scanned.

Malware Stopped

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

Dozens of Hours of Monthly Maintenance Eliminated

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

Simple Yet Robust

One customer reviewed multiple solutions but decided to go with CSS because the solution was so simple to set up yet robust to use.

How It Works

CSS provides a container-based solution. One container houses CSS's management console and the other more prevalent set comprises scanning agents. Deployment into the your account is simplified and automated through IaC provisioning tools, taking 15 minutes or less. Data is auto-discovered and cataloged for any connected cloud accounts. Newly-created data is automatically found and protected through tagging.

Organizations use CSS to baseline scan existing data on demand or schedule as well as scan new data in real time. When a scan completes, the results are generated and an alert is shared via a notification service. Real-time notifications can be sent to the SIEM systems and tools you already have in place.

If data is found to be infected or have sensitive information, it may be automatically quarantined, tagged, deleted, or kept in place. Reporting shows the scan outcome and type of data as well as where the data resides. Security attributes such as whether a bucket is publicly accessible or if the data is encrypted are also provided.

Getting Started

Healthcare organizations of all sizes turn to Cloud Storage Security (CSS) to meet compliance requirements and manage data security. Take advantage of a free trial in AWS Marketplace or contact us for more information including how to get started with a POC.

1. Cost of a Data Breach Report, IBM 2024
2. CSA Report: Ransomware in the Healthcare Cloud, Cloud Security Alliance 2021

100124