SOLUTION BRIEF

Cloud Storage Security Antivirus

Stop malware before it lands with real-time scanning in the storage layer.

Breaches involving cloud storage often cost organizations over $5.17 million/incident[1]. Cloud Storage Security's Antivirus can scan cloud data before, as, or after it's written to storage. CSS extends the protection of application, network and endpoint solutions by scanning for, and stopping, malware and ransomware in cloud storage.

Use Cases

1 | PREVENT MALWARE FROM ENTERING CLOUD STORAGE

Desired Outcome: Stop malware from reaching production data or backups.

Solution: Cloud Storage Security's Antivirus scans every file before, as, or after it's written to storage. This is completed entirely in-tenant across AWS, Azure, and Google Cloud so data never leaves your environment. Malware and ransomware are detected, blocked, quarantined and deleted before they enter your storage, infect your workloads, or reach your downstream applications and users.

2 | ENSURE CLEAN BACKUPS AND RESTORE POINTS

Desired Outcome: Prevent reinfection through legacy or restored data.

Solution: Malware and ransomware can hide in dormant files and return during recovery. CSS Antivirus automatically scans new and existing data for malware and ransomware before it's backed up and again before it's restored. Only clean files enter backups and return to active storage.

3 | AUTOMATE & EXPEDITE YOUR STORAGE LAYER INCIDENT RESPONSE

Desired Outcome: Reduce manual investigation and remediation time.

Solution: CSS Antivirus automatically tags, quarantines, and deletes infected files. Response workflows can trigger through SNS, Lambda, or your SIEM. Automated tagging and notifications expedite responses to malware and ransomware incidents, so your storage remains clean and your operations run without disruption.

4 | SUPPORT COMPLIANCE AND AUDIT READINESS

Desired Outcome: Show malware protection is in place for stored data.

Solution: Malware and ransomware scanning is required in many compliance frameworks, including PCI DSS 4.0, HIPAA, and ISO 27001. CSS Antivirus provides policy enforcement and reporting to satisfy audit requirements and keep your data scanned and secure.

#1 Most Subscribed Container Solution on AWS Marketplace

Award winner in three 2024 Cybersecurity Excellence Award categories: Cloud Native Data Security, AWS Cloud Security, and Antivirus.

Learn more:

Cloudstoragesecurity.com

Cloudstoragesecurity.com/av

[1]IBM Cost of a Data Breach Report 2024

SOLUTION BRIEF

DataDefender by Cloud Storage Security

Prevent breaches and resource misuse with control in storage layer.

Breaches involving cloud storage often cost organizations over $5.17 million/incident[1]. DataDefender, by Cloud Storage Security, offers environment-wide inventory, over 90 security checks on misconfigurations, and activity monitoring that answers the who, what, where and how much of all your data in cloud storage.

Use Cases

1 | PREVENT MISCONFIGURATIONS AND DATA EXPOSURE

Desired Outcome: Proactively reduce risk by identifying and fixing insecure storage configurations.

Solution: DataDefender runs over 90 automated checks across AWS storage services—including S3, EBS, FSx, and EFS—to detect public buckets, missing encryption, and other misconfigurations. Security issues are categorized by severity so teams can take action intelligently.

2 | LOCATE SENSITIVE DATA IN UNEXPECTED PLACES

Desired Outcome: Prevent accidental exposure of regulated or high-risk data.

Solution: DataDefender tags sensitive content (SSN, PII, PHI, confidential). When teams know how much sensitive data they have, what type it is, where it resides and who can access it, remediating storage insecurities becomes a breeze for security teams.

3 | MAP STORAGE RESOURCES AT SCALE

Desired Outcome: Eliminate blind spots across distributed, multi-account cloud environments.

Solution: DataDefender continuously inventories every storage resource across AWS—including accounts, buckets, volumes, and shares—delivering a holistic, live view of your storage landscape. Knowledge of your entire environment enables quicker incident response, easier auditing, and control over data sprawl.

4 | ACCELERATE INVESTIGATIONS AND AUDIT READINESS

Desired Outcome: Quickly answer access-related questions and pass audits with confidence.

Solution: DataDefender's Query Tool allows teams to investigate who accessed, modified, or deleted data across cloud storage, without digging through raw logs. Results are exportable and immutable, supporting audit documentation, incident response, and forensic workflows.

Beta onboarding open now for our Second Class!

Built by the team that won three 2024 Cybersecurity Excellence Awards for cloud data security, AWS security, and antivirus.

Learn more:

Cloudstoragesecurity.com

Cloudstoragesecurity.com/DataDefender

[1]IBM Cost of a Data Breach Report 2024