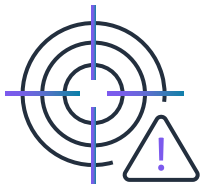
CLOUD STORAGE SECURITY | aws

Elevate Your AWS Security and Compliance with this Malware Protection Solution

Introduction

As organizations continue to migrate their workloads to the cloud, ensuring robust security and compliance becomes a critical imperative. The sheer volume of data and the complex network of cloud services pose unique challenges in protecting against malware and meeting regulatory requirements. Enter Cloud Storage Security (CSS) Malware Protection–a comprehensive solution that can help you safeguard data within your AWS environment and streamline your compliance journey. This solution has been validated by SecureIT, an independent auditor, which provides assurance that controls are designed appropriately and operating effectively when using Cloud Storage Security (CSS) Malware Protection.



Problem Statement

Navigating the cloud security landscape can be daunting. Enterprises face myriad concerns:

- Detecting and mitigating advanced malware threats targeting cloud-hosted data and applications
- Maintaining compliance with industry regulations and standards, such as NIST, HIPAA, and ISO
- Ensuring visibility, control, and auditability over cloud-based activities and security events
- Striking the right balance between security and operational efficiency

Why It Matters

The stakes are high when it comes to cloud security and compliance. A single malware incident or regulatory breach can lead to devastating consequences, including data loss, service disruptions, financial penalties, and reputational damage. Organizations must proactively address these challenges to protect their critical assets and maintain the trust of customers, partners, and stakeholders.

Recent Malware Statistics

Number of attacks

6.06 Billion

malware attacks occurred globally in 2023, which is about 190,000 attacks per second.

New malware

560,000+

new pieces of malware are detected every day.

Types of malware

6

most common types of malware attacks are worms, viruses, ransomware, trojans, and backdoor.

Entry points

31%

of ransomware attacks target cloud storage as the entry vector.

Crypto-jacking

399%

increase in crypto-jacking in 2023, which is when someone's device is infected with malware to mine cryptocurrency.

Validated by SECURE IT

Solution: CSS Malware Protection—Your Comprehensive Data Security and Compliance Enforcer

CSS's powerful malware protection solution will help safeguard your AWS environment and streamline your compliance efforts. Benefits include:

Robust Malware Protection

Flexible scanning options

Event-based, on demand, scheduled, and API-based scanning address diverse requirements, allowing you to easily insert malware detection into any workflow.

Scanning engine versatility

Leverage multiple threat detection engines from global industry leaders to detect a wide range of malware threats.

Automatic signature updates

Automatically updates virus signatures daily to stay ahead of the latest threats and reduce the risk of false negatives entering your cloud environment.

Comprehensive monitoring and alerting

Integrates with CloudWatch Logs and SNS notifications for real-time visibility and alerts.

Deployment flexibility

Choose from public, private, or hybrid deployment models to align with your security and compliance needs.

Comprehensive Compliance Coverage

Customers can run CSS on AWS storage services to address security control requirements such as:

- Malicious code protection
- Centralized management
- Automated monitoring tools and mechanisms
- Automatic updates of antivirus signatures

CSS provides appropriate scanning engines for the customer to use based on file type and size as well as the type of malware protection needed. A variety of industry-trusted engines can be enabled for scanning to improve detection rates; research shows that scanning with a few independent engines can reduce a false negative rate from ~2% (1 engine) to 0.0036% (2 engines). An optional deployment using Amazon Elastic Compute Cloud (Amazon EC2) can support scanning of extra-large files—for example, up to 5 TB for Amazon Simple Storage Service (Amazon S3). For more information, see this section from CSS on extra large file scanning.

SecureIT completed an independent assessment and validation to confirm control coverage for CSS malware solutions. The evaluation confirmed the solutions alignment with NIST 800-53 Revision 5 directly. Additional controls supported across frameworks are noted below. Details relating to the control coverage and customer configuration requirements when using CSS can be requested from CSS or the AWS GSCA team.

Validated by SECURE IT

Security Topic	NIST 800-53 Rev5	PCI-DSS v4.0	SOC II	C5	ISO 27001 Annex A (2022)	ISMAP (Japan)	CMMC	CCCS (Canada)	ISM (AUS)
Malware Protection and System Monitoring	SI-3 SI-3 (1) SI-3 (2) SI-3 (7)	5.2 5.3 11.5.1.1	CC6.8	OPS-04 OPS-05	A.8.7	12.2.1	SI.L1-3.14.2	SI-3	ISM-1288 ISM-1417

Other Compliance Frameworks Covered

The HIPAA Security Rule requires covered entities to implement controls to protect electronic protected health information (ePHI) from malware.

AWS storage services covered by CSS

Amazon Elastic Block Store (Amazon EBS)

Amazon Elastic File System (Amazon EFS)

Amazon FSx (NetApp ONTAP, OpenZFS, Luster)

Amazon Simple Storage Service (Amazon S3)

Conclusion

In today's dynamic cloud landscape, securing your AWS environment and maintaining compliance are paramount. CSS offers a robust and versatile solution that empowers you to safeguard your data in storage, strengthen your security posture, and streamline your compliance efforts. By leveraging the comprehensive controls report, provided by AWS Global Security & Compliance Acceleration Program, validated by SecureIT, you can confidently protect your cloud-hosted assets, satisfy industry regulations, and stay ahead of evolving cyberthreats.

Elevate your cloud security and compliance with CSS Malware Protection – the trusted partner in your journey to a more secure and compliant AWS environment.

Try CSS Malware Protection for AWS

aws marketplace

Cloud Storage Security and SecureIT are AWS Partners in the Global Security & Compliance Acceleration Program providing end-to-end support for your compliance requirements.

cloudstoragesecurity.com | secureit.com

Validated by SECURE IT