OPSWAT.

Protecting the World's Critical Infrastructure

MetaDefender Storage Security

AWS S3 INTEGRATION

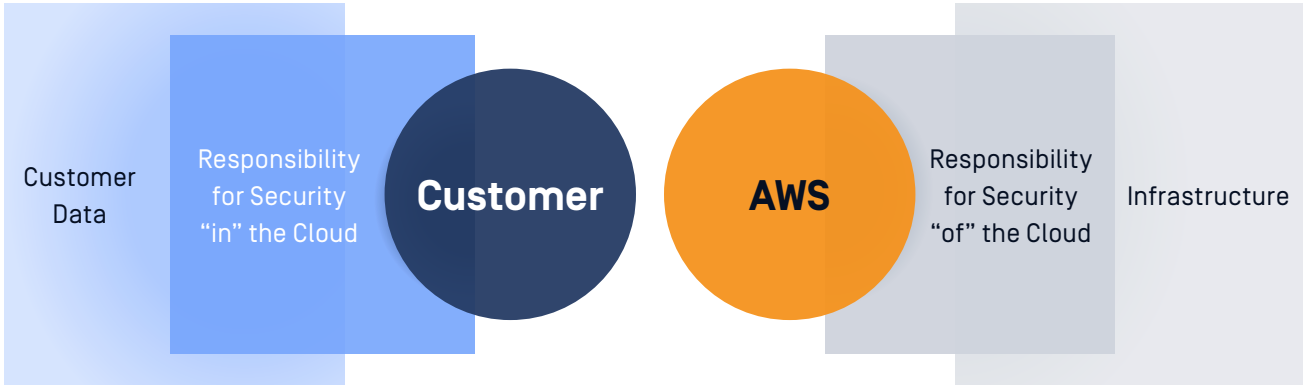
Amazon Web Services (AWS) and its customers share responsibility for the security and compliance of files stored in the cloud. While there is nothing inherently insecure about Amazon Simple Storage Service (Amazon S3), its flexibility and scalability open it to abuse by attackers who may upload malware-infected files or unwanted objects into S3 buckets.

MetaDefender Storage Security stops malicious content from infiltrating your Amazon S3 bucket by conducting near real-time, on-demand, or scheduled inspections for vulnerabilities, zero-day threats, and sensitive data in files stored in the cloud.

OPSWAT.

Protect Data “in” the Cloud

There are numerous security measures customers must consider when securing their S3 buckets. MetaDefender Storage Security is a powerful tool that adds a file security layer to scan user-uploaded files for malware, detect suspicious files for malicious content, and automatically redact or report sensitive data in files. It integrates easily with cloud and on-premises storage services and provides IT professionals with automated audit reports for quick remediation.

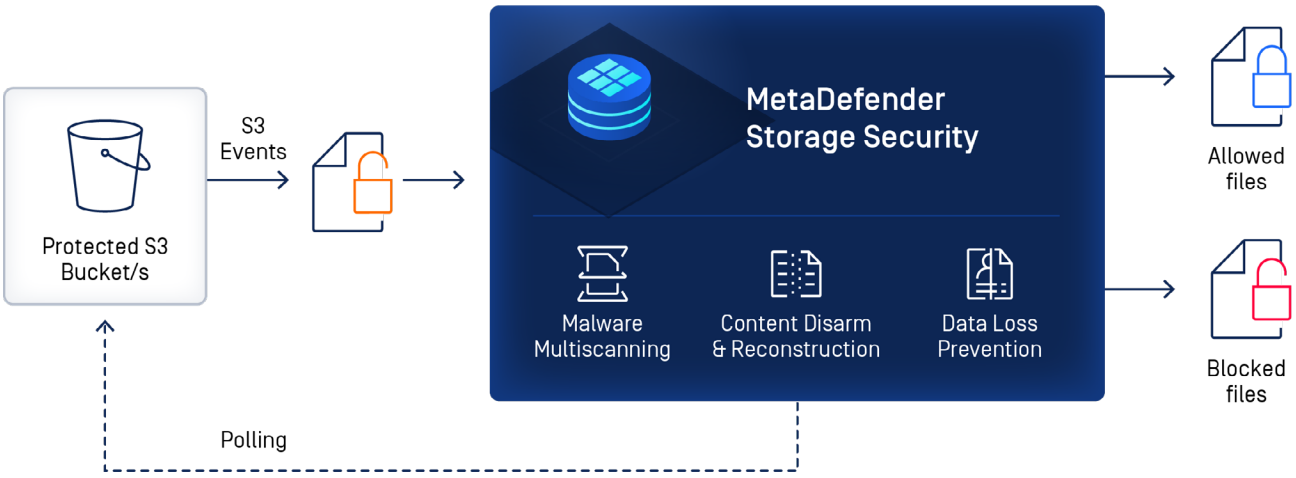


Features	Benefits
Near Real-Time File Scanning	MetaDefender Storage Security triggers an S3 event to scan files uploaded to an S3 bucket quickly. You can configure scheduled or on-demand file scanning depending on your needs.
Scale-Out Architecture	Enterprise-class scalability leverages Amazon EKS to add MetaDefender instances to meet file scan time service level agreements (SLAs).
Multiscanning	Leverage 30+ anti-malware engines to detect over 99% of known threats.
Deep Content Disarm and Reconstruction (CDR)	Disarm active embedded threats and reconstruct every file to prevent zero-days and advanced evasive malware.
Proactive Data Loss Prevention (DLP)	OPSWAT Proactive DLP helps you comply with data regulations and security requirements such as PCI, HIPAA, Gramm-Leach-Bliley, FINRA, and many more by automatically redacting, removing, watermarking, or blocking sensitive data in files.

OPSWAT.

Easily Integrate with S3 Buckets

MetaDefender Storage Security easily integrates with AWS to provide near real-time file scanning. When you upload files to an S3 bucket, an S3 event is triggered. The file is inspected and analyzed during the scan for vulnerabilities, zero-day threats, and compliance violations. Additionally, you can schedule on-demand file scans using the polling process. Below is an example of how MetaDefender Storage Security integrates into the Amazon EKS cloud.



Scale-Out Architecture

The scale-out architecture of the MetaDefender platform allows adding multiple instances of MetaDefender Core to meet the file scan-time service level agreements (SLAs). All potentially harmful files are sent to the blocked bucket.

Detailed Dashboard and Reports

Furthermore, MetaDefender Storage Security's dashboard provides detailed information about all blocked files, associated vulnerabilities, and compliance violations for further analysis. A scan report can also provide a deeper dive into each file. Complement existing SIEM solutions by ingesting logs in syslog format for a single pane of glass user experience.

Are you doing everything you can to secure your cloud storage from threats?

Talk to one of our specialized cybersecurity experts today to discover how OPSWAT can level-up your security posture.

Talk to an expert today to learn more.

opswat.com/get-started

OPSWAT.
Protecting the World's Critical Infrastructure