OPSWAT.

METADEFENDER™

Storage Security

AWS S3 Integration

OPSWAT.

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.

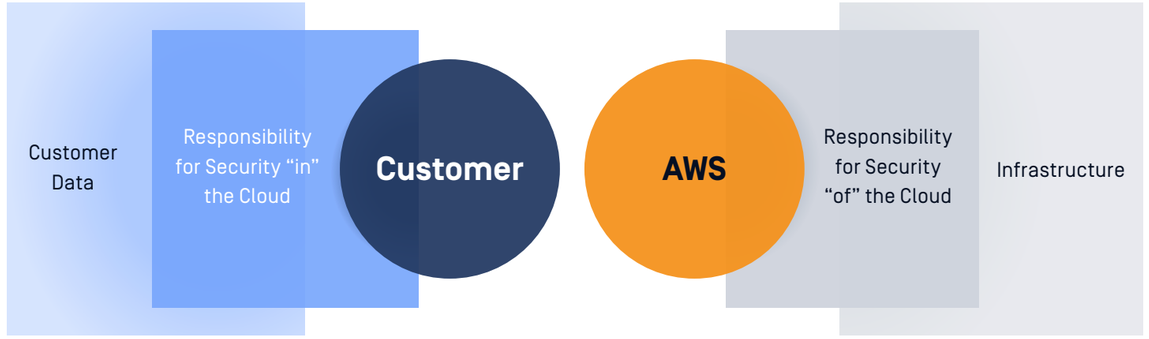
MetaDefender Storage Security stops malicious content from infiltrating your Amazon S3 bucket by conducting real-time, on-demand, or scheduled inspections for file-borne malware, vulnerabilities, zero-day threats, and sensitive data in files stored in the cloud.



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.



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 ondemand 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).

Metascan™ Multiscanning

Many enterprises scan with only a single anti-malware engine. Industry best practices recommend simultaneous scanning with as many engines as possible to maximize detection rates. With OPSWAT, you can choose to scan every file with 30+ commercial antivirus engines, resulting in nearly 100% detection rates.

Deep CDR™

Disarm active embedded threats and reconstruct every file to prevent zero-day attacks and advanced evasive malware. Supports 200+ file types, including PDFs, nested archives, Microsoft Office documents, and many other file formats, certified 100% accurate by SE Labs.

Proactive DLP™

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 and out-of-policy data in files.

Adaptive Sandbox

Adaptive Sandbox is a unique adaptive threat analysis technology, enabling zero-day malware detection and extracting valuable IOCs with its advanced, emulation-based approach. Adaptive Sandbox operates 10x faster and 100x more efficiently than traditional sandboxes.

Vulnerability Assessment

File-Based Vulnerability Assessment technology scans and analyzes binaries and installers to detect known application vulnerabilities before they are executed on endpoint devices.

OPSWAT.

Key Features

Advanced File Processing

Tailored Scanning Options:

- **Real-Time Scanning** offers instant detection as files are processed immediately upon upload, which can be achieved through:
  - **Event-Based Handling:** Triggered scans based on specific events.
  - **Polling Handling:** Regular checks for new files to scan.
- **On-Demand Scan** can be initiated immediately after configuration.
- **Scheduled Scanning** enables automated scans at predetermined times.

Partition-Based Real-Time Scanning

Configure multiple scanning policies across different partitions within individual storage units.

Custom Scan Priority

Users can control scanning priority (High, Medium, Low) for storage unit scans.

Automated File Remediations

Customize remediation workflows by combining Deep CDR™, and actions like copy, encrypt, block, move, or delete files. An optional “Delete empty folders after remediation” setting is added for SMB/NFS/SFTP shares.

Automated Workflows

Automated security pipeline with 5-stage processing (Scan Configuration → Advanced Threats → Vulnerabilities → Sanitization → File Tagging). Build custom, automated file processing pipelines tailored to your organization's unique needs, all without additional API development.

Multiple Workflow Destinations

Remediation policies can specify up to five copy/move destinations, supporting complex data handling requirements common in regulated industries while ensuring business continuity through multiple backup locations.

Type-based Storage Grouping

Combine Object Storage units or Network Attached Storage units into dedicated groups to ensure security workflows perfectly match the features and requirements of the specific storage integrations within the group.

Seamless SIEM Integration

Connect to SIEM systems quickly using an intuitive GUI or RESTful API to ensure quick incorporation into existing workflows.

Cancel Scanning File

Stop processing individual files during active scans.

Dual View Modes

Dual view system (Groups and Accounts) allows organizations to organize storage units through Groups and Accounts perspectives, accommodating different operational models and organizational structures.

Immediate Alerts and Proactive Incident Notification

Get instant alerts for critical system events so you can respond immediately. Customize notifications to relevant stakeholders for increased operational efficiency and agility.

Simplified HTTPS Configuration

Enable HTTPS directly through the Security settings interface, incorporating real-time certificate validation and comprehensive error reporting.

Enhanced Integration Capabilities

Include individual file webhooks, and secure syslog with TLS, enabling automated response procedures and meeting enterprise compliance requirements for secure audit data transmission to centralized log management systems.



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.



GET STARTED

Are you ready to put MetaDefender Storage Security on the front lines of your cybersecurity strategy?

Talk to one of our experts today.

Scan the QR code or visit us at:
opswat.com/get-started
sales@opswat.com

OPSWAT.

For the last 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats.

Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and device access with zero-trust solutions and patented technologies across every level of their infrastructure. OPSWAT is trusted globally by more than 1,700 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations.

Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com.

©2025 OPSWAT Inc. All rights reserved. OPSWAT, Metascan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc. Rev. October 15, 2025 10:34 AM