OPSWAT.

METADEFENDER STORAGE SECURITY™ FOR AWS

Keep Your S3 Buckets Malware-Free and Audit-Ready

Continuously scan every file that lands in S3 for threats, remove malicious content, and redact sensitive data; with the audit trail to prove it.

Block
Malware before it spreads

Redact
Sensitive data automatically

Prove
Compliance with a full audit trail

aws PARTNER

- Amazon RDS Ready
- Amazon Linux Ready
- AWS PrivateLink Ready
- Security Software Competency

OPSWAT.

You Own the Data. We Secure It.

AWS is responsible for securing the cloud infrastructure, while customers are responsible for securing the data they place in the cloud. MetaDefender Storage Security ensures that data residing in the Cloud Storage environment is protected against breaches, downtime, and compliance violations.

Security Gaps Covered by MetaDefender Storage Security

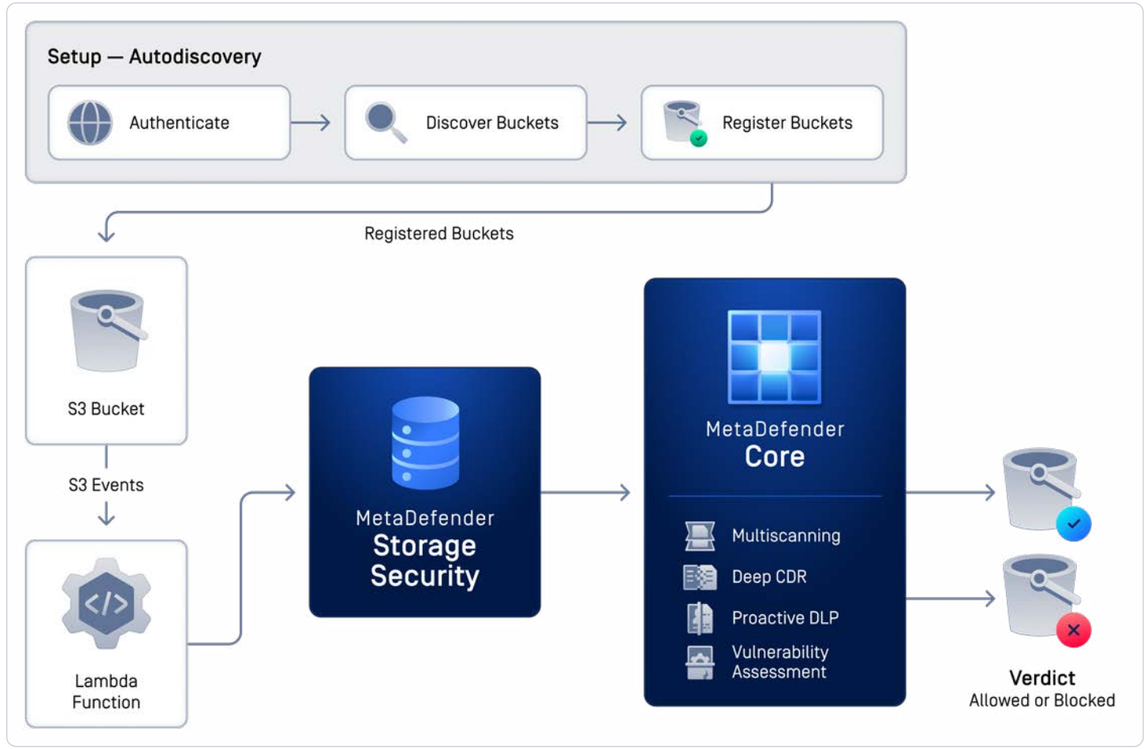
- Infected files entering S3
- PII, PHI, PCI, and regulated data at risk
- Malicious files propagating across repositories
- High-risk files introducing exploitable weaknesses
- Lack of insight into file activity and scan results
- Unmanaged data creating regulatory challenges

AWS-Native Features

- Automatic S3 bucket discovery
- Event-driven scanning with S3 and Lambda
- Support for encrypted buckets
- Cross-account deployment support
- REST API and dashboard management
- Centralized audit reporting

How It Works on AWS

MetaDefender Storage Security automatically discovers and registers Amazon S3 buckets, then uses AWS Lambda integrations to enable event-based scanning. Uploaded files are analyzed by MetaDefender Core™ using multilayered threat detection and sanitization technologies. In workflows configured for sanitization, Deep CDR™ Technology reconstructs clean versions of files and writes them to a designated destination bucket while malicious or non-compliant files are blocked.



Flexible Deployment

- AWS Marketplace AMI
- EC2-based deployment
- Kubernetes deployment via EKS and Helm

Native AWS Integration

- IAM role or access keys
- AWS KMS and Secrets Manager support
- CloudWatch and SIEM connectivity

Operational Control

- Centralized dashboard and REST API
- Real-time, scheduled, on-demand scanning
- Audit reporting and policy-based governance

OPSWAT.

Compliance Support

PCI DSS, HIPAA, CCPA, GDPR, FINRA, GLBA, NYDFS Part 500

30+
Anti-malware engines

99%+
Detection rate

20+
Storage platforms

Industries

Trusted by the world's most security-conscious organizations across:

- Financial Services
- Healthcare Organizations
- Federal & Government
- OT & Critical Infrastructure

Take the Next Step

Find Us on AWS Marketplace

Deploy from the AWS Marketplace listing in minutes. Annual or hourly pricing on consolidated AWS billing.

Talk to an Expert

Book a working session with an OPSWAT solutions architect. Walk away with a deployment plan tailored to your AWS estate.

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 2,000 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.