OPSWAT.

DATASHEET

METADEFENDER

Storage Security™

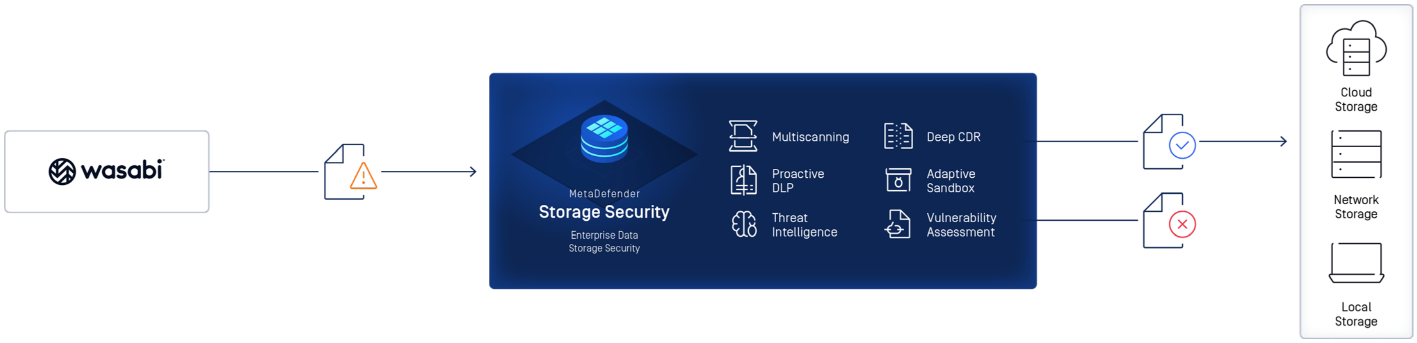
Multi-Layered Protection for Your Wasabi Data

MetaDefender Storage Security secures your Wasabi files and data at rest across any storage environment—on-premises, hybrid, or cloud—preventing breaches, downtime, and compliance violations with comprehensive, multi-layered protection.

99.2%	Detection Rate Utilizing 30+ AV Engines
100%	Protection Rating in SE Labs & Secure IQ Lab's Content Disarm & Reconstruction Test
500,000+	Objects Processed per Hour for Large Scale Deployment

Plug and Play Integration with Wasabi Storage

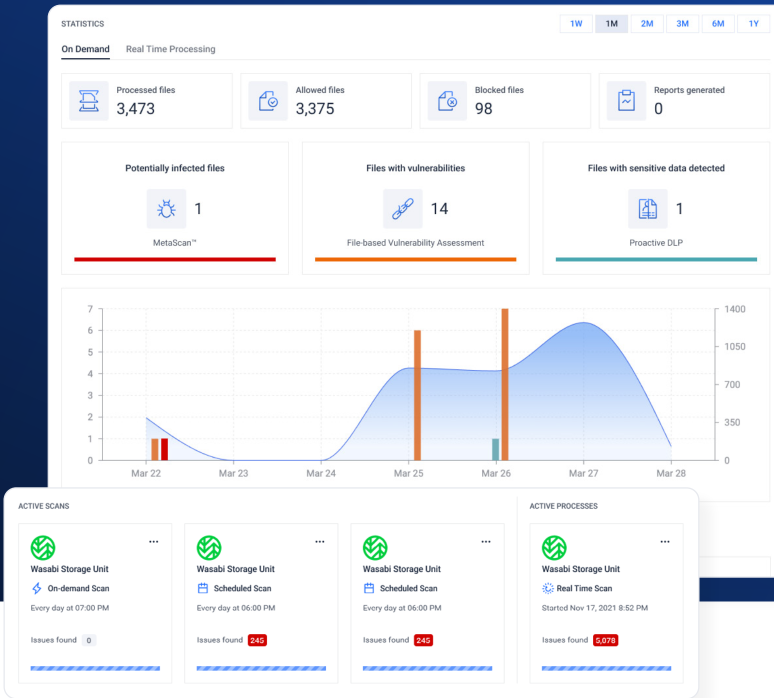
MetaDefender Storage Security easily integrates with Wasabi to provide real-time file scanning. Our solution provides enterprise-class features to protect at scale with an easy-to-use GUI and RESTful API interface for quick integration into existing workflows.



Files are inspected and analyzed during scans for vulnerabilities, zero-day threats, and compliance violations. Additionally, you can schedule on-demand file scans using the polling process.

Benefits

- Unified security platform with broad coverage
- Enhanced file/ data privacy and regulatory compliance
- Comprehensive security by utilizing OPSWAT's industry-leading proprietary technologies
- Performant and scalable
- Rapid deployment within your existing infrastructure
- Single-pane-of-glass interface to integrate, monitor, and secure



Processed files 3,473

Allowed files 3,375

Blocked files 98

Reports generated 0

Potentially infected files 1 MetaScan™

Files with vulnerabilities 14 File-based Vulnerability Assessment

Files with sensitive data detected 1 Proactive DLP

Wasabi Storage Unit
On-demand Scan
Every day at 07:00 PM
Issues found 0

Wasabi Storage Unit
Scheduled Scan
Every day at 06:00 PM
Issues found 245

Wasabi Storage Unit
Scheduled Scan
Every day at 06:00 PM
Issues found 245

Wasabi Storage Unit
Real Time Scan
Started Nov 17, 2021 8:52 PM
Issues found 5,078

Features

Advanced File Processing

- Real-time scanning, on-demand scanning and scheduled scanning.

Automated File Remediations

- Add information about file processing as tags for further analysis and forensics with File Tagging.
- Combine file sanitization with Deep CDR™ and other remediation actions (copy, encrypt, delete files/ empty folders, etc.) to customize prevention and remediation workflows.

Custom Scan Priority

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

Automated Workflows

New automated security pipeline with 5-stage processing (Scan Configuration) → Advanced Threats → Vulnerabilities → Sanitization → File Tagging).

Cancel Scanning File

Users can cancel an individual file's scanning while processing.

Type-based Storage Grouping

Users can combine Object Storage units into dedicated groups and do the same for Network Attached Storage units.

Proactive Event Notifications

Customize notifications to your preferences and receive timely notifications for critical events like report generation, user registrations, and file blocking.

Centralized Report Management

Analyze historical scan data to monitor security trends, meet audit requirements, and identify potential risks in one location.

Seamless SIEM Integration

Integrate quickly and easily with SIEM systems via an intuitive GUI and RESTful API.

Broad Storage Integration

Integrate with a wide range of storage vendors, including:

Alibaba Cloud
aws | S3
CLOUDIAN
wasabi
ORACLE Cloud Infrastructure
Azure
OneDrive
box
Cubbit
ISILON SYSTEMS
OPSWAT. MetaDefender Managed File Transfer
Amazon EFS
NetApp
SharePoint Online | On-Prem
MINIO
Google Cloud

OPSWAT.

Storage Security Solution Page
opswat.com/solutions/storage-security

MDSS Page on Wasabi Website
docs.wasabi.com/v1/docs/how-do-i-use-opswat-mdss-with-wasabi