

OPSWAT.

DATASHEET

METADefENDER

Storage Security™

Secure Your Enterprise Data Storage

MetaDefender Storage Security provides comprehensive, multi-layered protection for your data at rest across on-premises, hybrid, and cloud-native storage environments.

MetaDefender Storage Security safeguards enterprise data and files against breaches, downtime, and compliance violations. Its seamless integration with leading storage and collaboration solutions ensures minimal disruption to existing workflows and technology stacks.

Benefits

- Real-time comprehensive threat detection and prevention to protect data storage from malicious files
- Protect storage data against malware, zero-day threats, advanced targeted attacks, and sensitive data leakage
- Customize policies, workflow and remediation actions to meet your unique security needs
- Achieve the optimal balance of security, system performance, and user experience through a zero-trust, multi-layered security approach
- **Low False Positives**
- Supports **on-premises, hybrid, and cloud deployments**, with architecture designed to scale beyond single-instance specifications
- Enable distributed, multi-site deployments and secure petabyte-scale storage environments with high availability and performance
- Single pane of glass to integrate, monitor, and secure

Key Technologies



MetaScan™ Multiscanning

Detects nearly 100% of malware by simultaneously scanning files with 30+ leading commercial AV (anti-virus) engines.



Deep CDR™

Zero-day exploits are neutralized by removing any potentially harmful and out-of-policy objects in files and regenerating new, safe-to-use files. Deep CDR has achieved a 100% Protection Rating in SE Labs & SecureIQ Lab's Content Disarm & Reconstruction Test.



Proactive DLP™

Proactive DLP detects and blocks confidential or out-of-policy data, then automatically redacts the identified sensitive information in 110+ file types. Supports image-to-text recognition.



File-Based Vulnerability Assessment

Identify vulnerabilities in software before they can be installed and exploited. File-Based Vulnerability Assessment scans and analyzes binaries and installers to detect known application vulnerabilities, preventing them from reaching your endpoints.

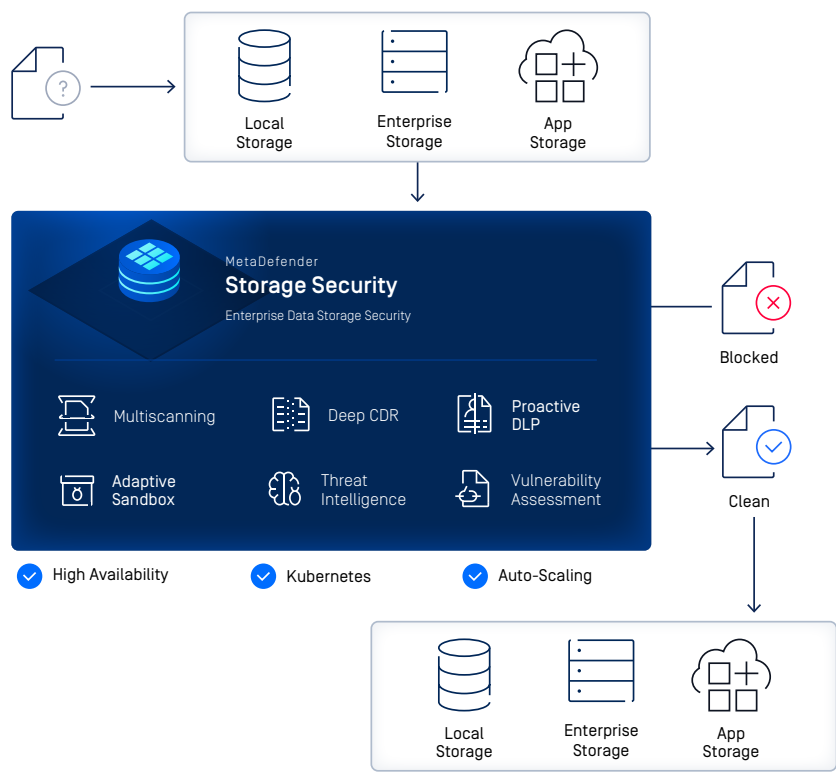


Adaptive Sandbox

Adaptive Sandbox dynamically detects complex and evasive malware threats using threat agnostic analysis of files and URLs, emulation of targeted applications, IOC (Indicator of Compromise) extraction, and Rapid Dynamic Analysis.



METADEFENDER STORAGE SECURITY™



Storage Integrations



Features

- Advanced File Processing¹: Real-time scanning, on-demand scanning and scheduled scanning
- Custom scan priority
- Inline scanning to secure network traffic, inspect files and data in real time to detect and stop threats².
- Cancel scanning files
- Centralized dashboard
- Automated File Remediations: File tagging, Deep CDR, copy, encrypt, move, delete files/empty folders
- Automated workflows
- Type-based storage grouping
- Comprehensive logging with detailed audit trails
- Proactive alerts and notifications

1. Storage scanning operations may temporarily impact system performance and user access. To minimize disruption, consider scheduling scans during off-peak hours when possible.

2. This approach is particularly effective when using event-based real-time scanning, as it prevents user access to uploaded files during file processing. By blocking access to files undergoing security, this method helps preserve both business productivity and organizational security. [Learn more.](#)

OPSWAT.

Protecting the World's Critical Infrastructure

Specifications

Supported Operating Systems

Windows	Windows Server 2019, 2022 and 2025
Linux	CentOS 9.0+ Red Hat Enterprise Linux 7.0+ Debian 10.0+ Ubuntu 18.04+ Amazon Linux 2

Supported Browsers

Microsoft Edge, Google Chrome, Firefox, Safari

CLI and API alternatives for critical operations are also available

Installation Components*

Name	Version	Type
MongoDB	v6.0	Database
RabbitMQ	v3.13	Message Broker
NGINX	v1.23.3	Web Server

*The customer is solely responsible for maintaining, patching, and updating all underlying components related to their environment. OPSWAT does not assume liability for any issues arising with the database or message broker infrastructure.

Deployment Models

On-premises	
Cloud	
Physical/ Virtual deployment	Amazon Machine Images (AMI) Azure VMs Vscanner
Containers	Kubernetes Helm support is available for Amazon EKS (Elastic Kubernetes Service), AKS (Azure Kubernetes Service), and GKE (Google Kubernetes Engine)

Visit <https://www.opswat.com/docs/mdss/installation/types-of-deployment#deployment-options> to learn more about the requirements and specific limitations for each deployment model.