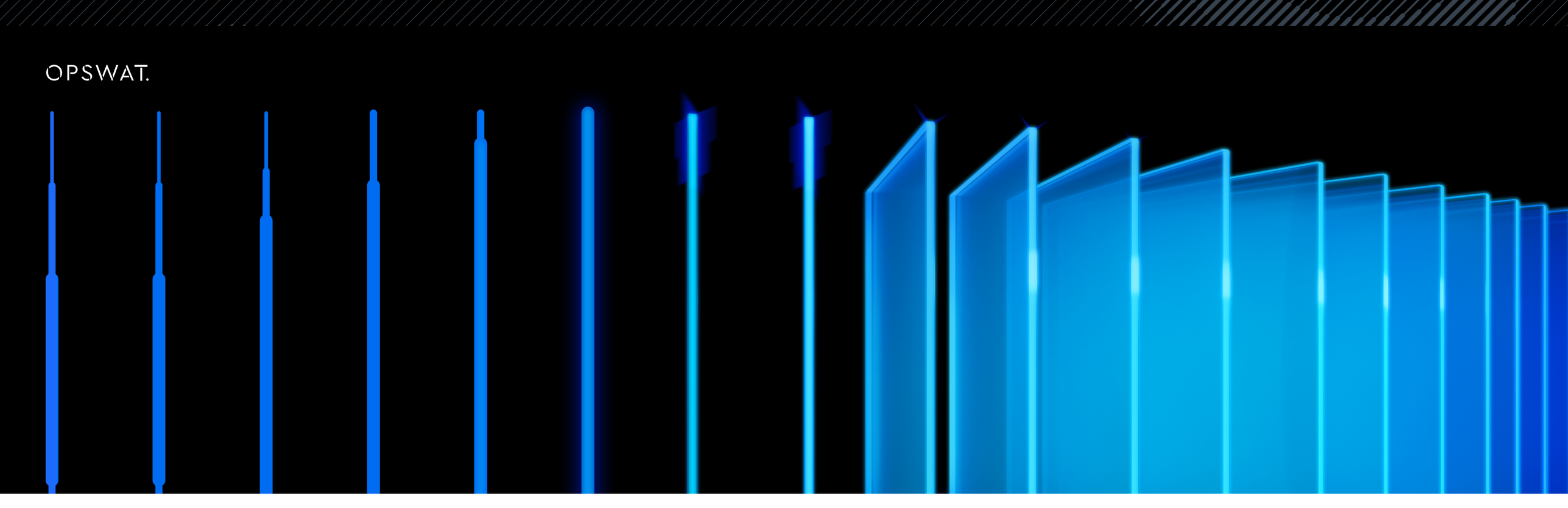
OPSWAT.

METADEFENDER™

Storage Security

Wasabi Storage Integration



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

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, detects malicious content in files, and automatically redacts or reports 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.

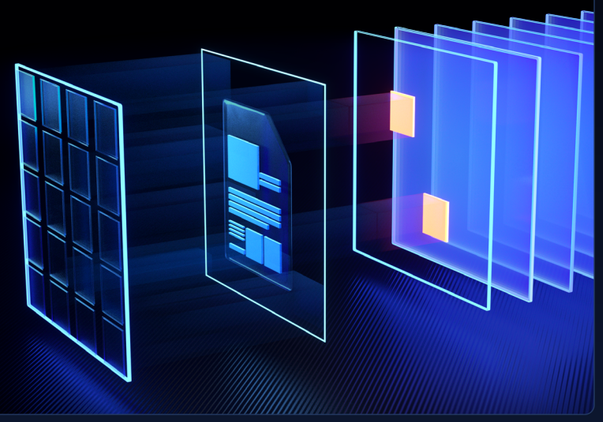
OPSWAT.

How OPSWAT Technologies Secure your Wasabi Storage

Organizations can integrate Wasabi storage with MetaDefender Storage Security to leverage OPSWAT's proprietary suite of technologies, including Multiscanning, Deep CDR and Proactive DLP, Vulnerability Assessment in one easy-to-implement solution.

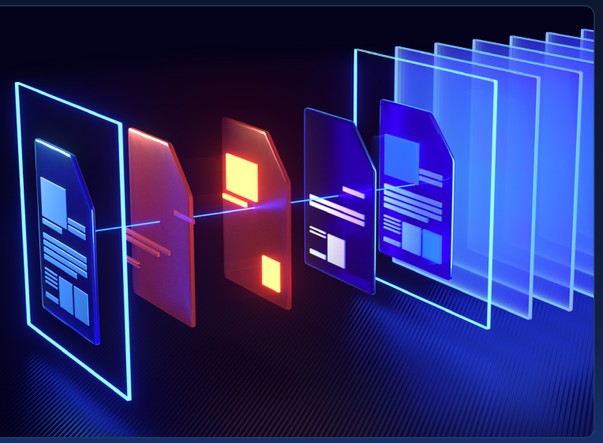
Multiscanning

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+ antivirus engines, resulting in nearly 100% detection rates.



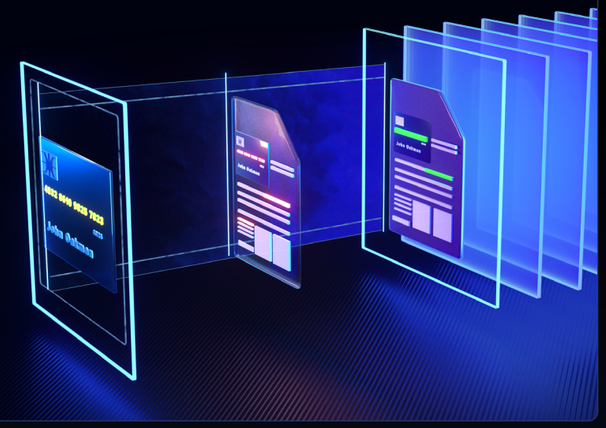
Deep CDR

Disarm active embedded threats and reconstruct every file to prevent zero-day attacks and advanced evasive malware. Supports 180+ file types, including PDFs, nested archives, Microsoft Office documents, and many other file formats, certified 100% accurate by SE Labs.



Proactive 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 and out-of-policy data in files.



Adaptive Sandbox

MetaDefender Sandbox's unique adaptive threat analysis technology enables zero-day malware detection and extracts valuable IOCs with its advanced, emulation-based approach that 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, including IoT devices.

Key Features

Custom Scan Priority

Users can control scanning priority (performance or thoroughness) for storage unit scans, allowing for tailored resource allocation.

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.

Cancel Scanning File

Users can now cancel scanning individual files while processing, providing greater control over resource management and preventing unnecessary processing.

File Remediations

- Efficiently categorize file content and pinpoint harmful files for thorough investigation.
- Define actions based on assigned tags like “Allowed,” “Sanitized,” or “Blocked.”
- Apply Deep CDR™ technology to sanitize files.
- Automate file operations such as copying, moving, or deleting files based on scanning results and predetermined conditions.
- An optional “Delete empty folders after remediation” setting is added for SMB/NFS/SFTP shares.

SIEM Integration

Seamlessly connect with SIEM systems via an intuitive graphical user interface (GUI) and RESTful API, enabling swift integration into your established workflows.

Proactive Event Notifications

- Alert designated personnel when crucial events transpire.
- Tailor notifications to your preferences and receive notifications for report generation, user registrations, and file blocking events.
- Customizable notifications to relevant stakeholders increase operational efficiency and agility.

OPSWAT.

Plug-and-Play Integration

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 integrations into the 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.

File Processing at Scale

The elastic nature of MetaDefender Storage Security deployment can be scaled up or down depending on your desired SLAs, delivering data security and operational resilience at scale for enterprise users.

All-in-one Portal

MetaDefender Storage Security provides data security and data protection solutions on a single platform, including ransomware detection, zero-day attack protection, data loss prevention and data compliance.

Detailed Dashboard and Reports

The MetaDefender Storage Security dashboard provides detailed information about all blocked files, associated vulnerabilities, and compliance violations for further analysis. A scan report also provides 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.