OPSWAT.

METADEFENDER™

Storage Security

Microsoft Azure Integration

Table of Contents

01 Protect Data in the Cloud

02 How OPSWAT Technologies Secure your Wasabi Storage

03 Key Features

04 Use Cases

05 Easily Integrate with Microsoft Azure Storage

06 Detailed Dashboard and Reports

07 Scale-Out Architecture

MetaDefender Storage Security provides multi-layered protection for your Azure storage environment. It leverages near real-time, on-demand, or scheduled scans to identify vulnerabilities, zero-day threats, and sensitive data within your cloud files. This proactive approach significantly enhances the security posture of Azure storage users by shielding data and systems from malicious file uploads, and by helping fulfill the shared responsibility model for security and compliance.

01

Protect Data in the Cloud

With Microsoft Azure, customers are entrusted with securing their information and data, endpoint devices, and management of accounts and identities. The specific division of responsibility on Microsoft's side further depends on the deployment model – Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS) – or whether it's hosted on-premises.

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.

OPSWAT.

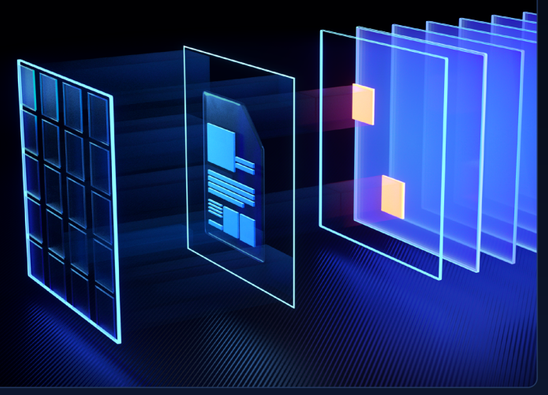
02

How OPSWAT Technologies Secure your Azure Storage

Organizations can integrate NetApp 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.

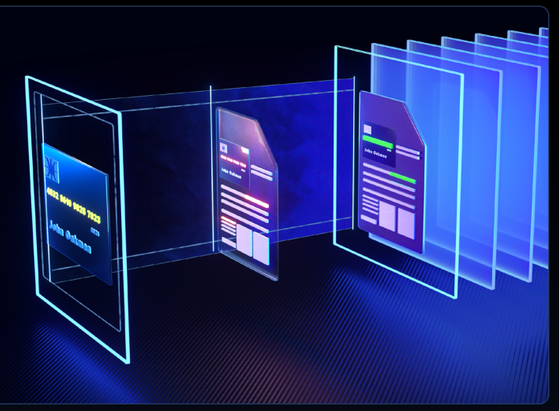


Deep CDR

Disarm active embedded threats and reconstruct every file to prevent zero-days 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.

03

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.

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.

Custom Scan Priority

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

Cancel Scanning File

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

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.

SIEM Integration

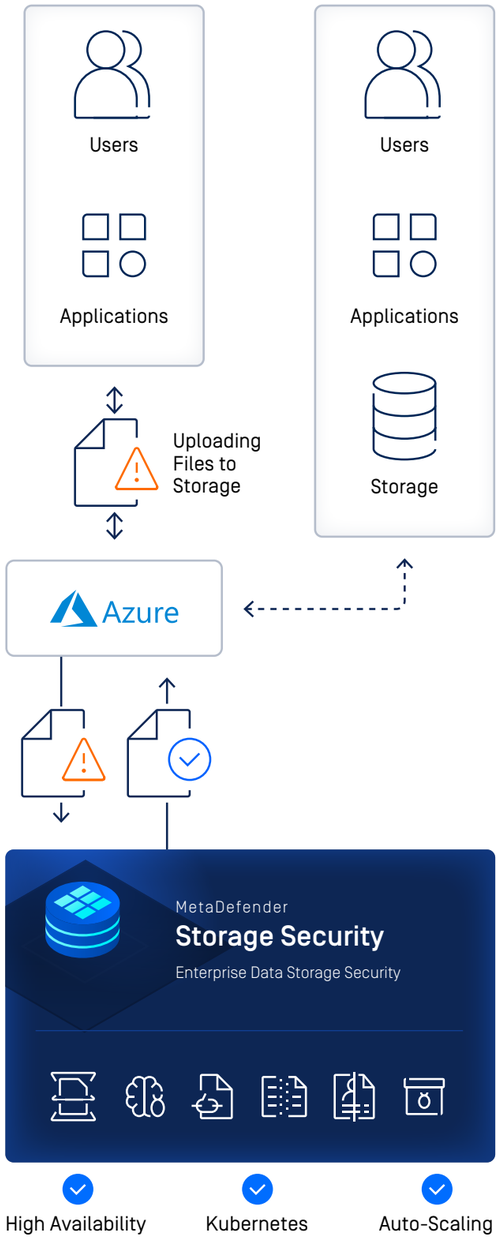
Seamlessly connect with SIEM systems via an intuitive graphical user interface (GUI) and RESTful API, enabling swift integration into your established workflows.

04

Use Cases

A Typical Workflow for Azure File Upload Scenario:

- B2C file uploads to cloud – Insurance claims, KYC (Know Your Customer), and other similar use cases.
- B2B file uploads to cloud – Suppliers' portals, invoicing, insurance agent claims to insurance companies, and other similar use cases.
- Citizens' file uploads to Federal/State/ Local governments.



05

Easily Integrate with Microsoft Azure Storage

Microsoft Azure storage has 2 storage modes:

- Azure Blob which is an object storage type like AWS S3.
- Azure File Type which is similar to a shared folder storage (SMB compatible).

Users can integrate Azure Blob or Azure File Type storage in MetaDefender Storage Security to provide multi-AV malware scanning, data sanitization, sensitive data loss protection, and other advanced vulnerability assessment and threat prevention features.

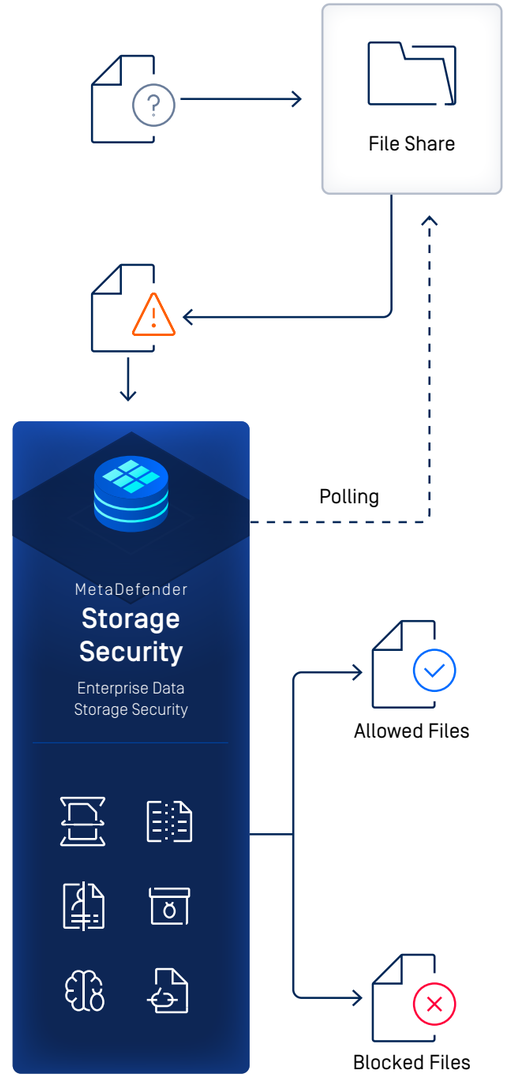
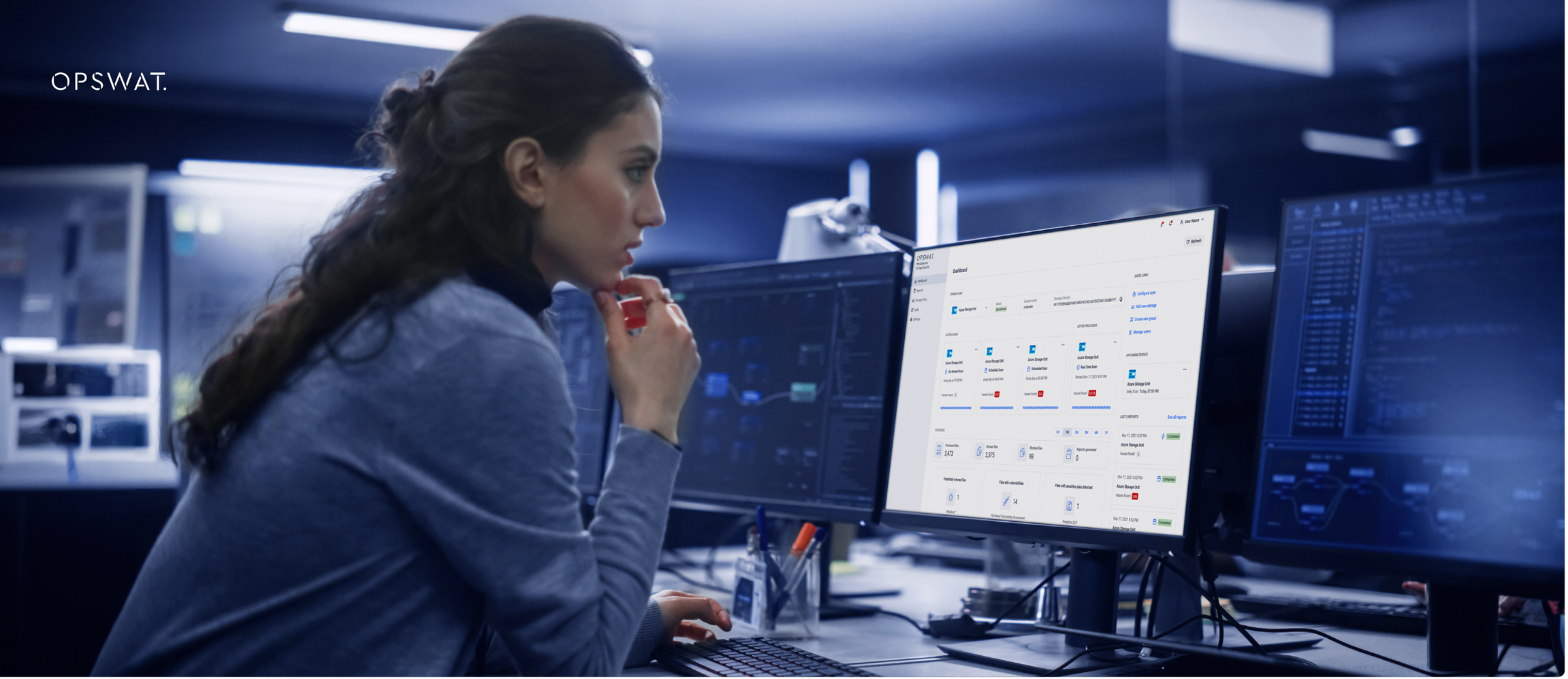


Diagram of Azure Blob for Azure Files



06

Detailed Dashboard and Reports

MetaDefender Storage Security includes an intuitive and feature-rich dashboard that 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 individual files. Complement existing SIEM solutions by ingesting logs in syslog format for a single pane of glass user experience.

07

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.

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.
Protecting the World's Critical Infrastructure

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.