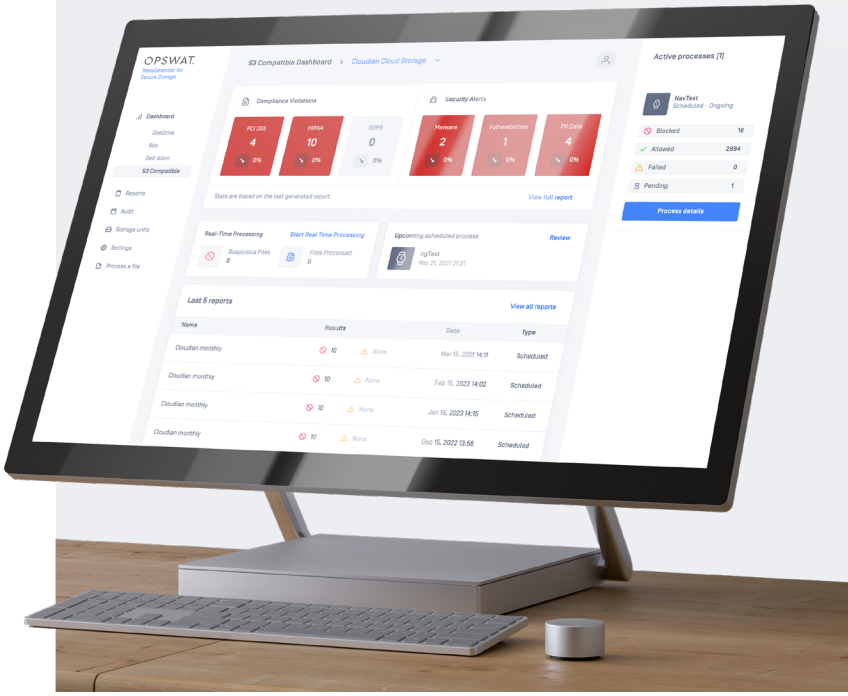
OPSWAT.

DATASHEET

MetaDefender® Storage Security

Secure Your Storage



Storage solutions facilitate access, sharing and collaboration. However, they leave the IT and security departments in a blind spot when it comes to malware and sensitive data loss. This is a critical security hole, as per a 2020 report, 80% of companies experienced a cloud data breach.

MetaDefender Storage Security offers a robust layer of protection for securing stored enterprise data such as files and images. It helps you prevent data breaches, downtime, and compliance violations in your cloud and on-premises storage.

Scan. Sanitize. Store.

Files from users in the organization are scanned for malware and analyzed for potential data loss or unsolicited privacy data. Suspicious files can be sanitized, while sensitive data from files can be reported and redacted automatically.

Native integration with many cloud and on-premises storage services makes this solution easy to deploy. Automated and actionable audit reports give IT professionals full visibility into potential risks associated with users and services for quick remediation.

MetaDefender Storage Security lets you trust the data shared within your organization.

Benefits

Zero-Day Threat Prevention

Disarm unknown content and output safe, usable files. OPSWAT's Deep CDR technology is focused on preventing an attack before it occurs. It can sanitize hidden or unknown malware from 100+ file types.

Advanced Threat Detection

Multiscanning with 30+ anti-malware engines (Mcafee, ESET, Avira, K7, Crowdstrike, Sophos etc.) combining all detection mechanisms (signatures, heuristics, AI/NGAV) leaves little room for error.

Compliance Risk Mitigation

Detect, redact, mask or block sensitive data. OPSWAT's Proactive DLP technology provides automated reporting and remediation for sensitive data loss to keep you in line with regulatory requirements such as HIPAA, PCI-DSS and GDPR.

Broad Integration Coverage

Microsoft OneDrive, Sharepoint Online and Azure, Amazon S3, Box, Cloudian S3, Dell Isillon, and any SMB compatible or S3 compatible storage; can all be seamlessly integrated so that you can start evaluating their health within minutes.

OPSWAT

MetaDefender Storage Security

Features

Processing at Scale

With one click - process the entire storage, new files only, or customize for specific files.

Automatic Reporting

See the status of your cloud and on-premises storage solutions at a glance through automated reports emailed directly to you and your organization's stakeholders; or see it real-time via the comprehensive dashboard.

Flexible Scheduling

Choose a combination of real-time processing and scheduling options that fit your organization's needs to keep your storage secure from zero-day threats and advanced persistent threats (APTs).

Facilitate Audits

Monitor and log a history of user actions that can be easily exported for full transparency to facilitate corporate audits.

Automated Workflow

In addition to manual and automated scheduling options, you have the ability to integrate processing into your business workflow via REST API.

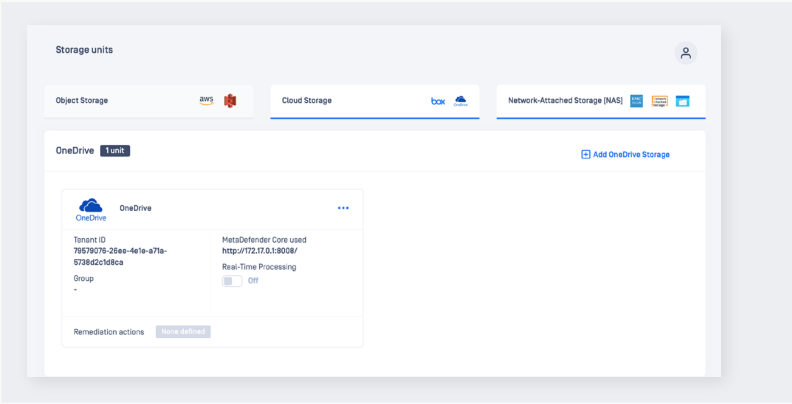
User Management

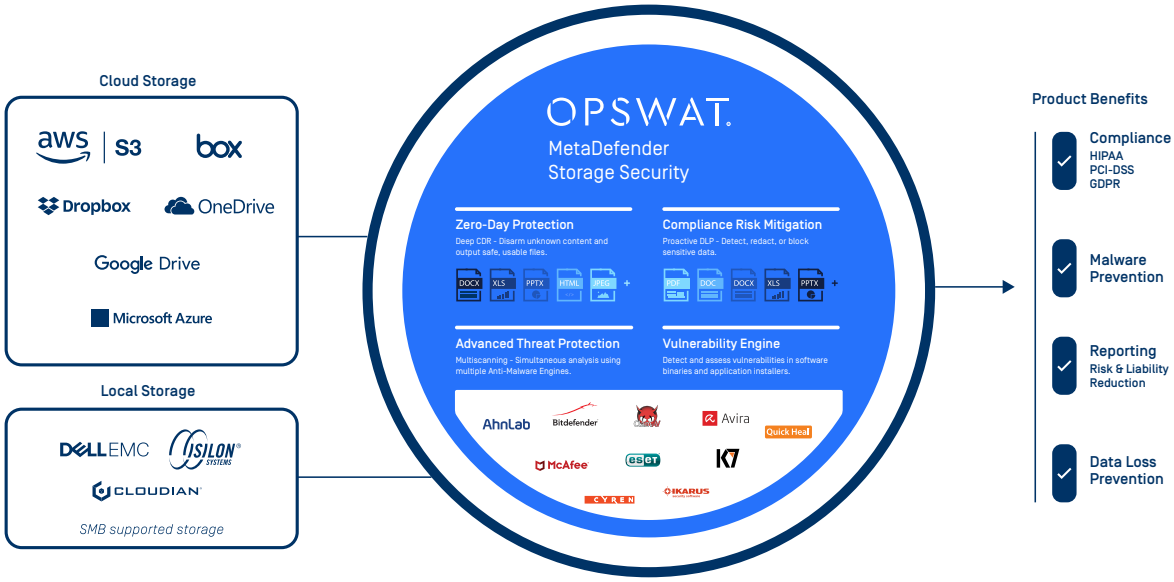
Enable your IT department to effectively manage compliance and data breach risks by giving role based (including 'read only') access to multiple administrators.

Integrations (Amazon S3, Dell and more)

Setup and configure multiple storage units from multiple vendors (whether in the cloud or on-premises) within minutes to manage and secure all your data in one view. We provide native API integrations to minimize your overhead.

- Integrate with all your Amazon S3 instances or any S3 compatible storage.
- Secure all your data stored in Microsoft OneDrive, SharePoint online, Azure File type, and Azure blob storage.
- Seamlessly integrate all your Dell Isilon or any SMB compatible on-premises storage units.
- Easily configure all your storage units from Box and other collaboration solutions.





OPSWAT.

Trust no file. Trust no device.

OPSWAT

MetaDefender Storage Security

How does OPSWAT minimize your compliance risk?

Regulatory requirements mandate the privacy and security of sensitive customer data.

- OPSWAT checks for any sensitive data that might be inadvertently exposed or maliciously targeted. Role based need to know access (including 'read only') minimizes violations of data privacy laws. Our products alert you to misuse, giving you visibility into suspicious or careless activity by your users. If this activity went undetected, it could put your organization at risk and result in significant regulatory fines and reputational loss.
- OPSWAT's advanced suite of technologies; including industry-leading Mutliscanning with 30+ anti-virus engines, Deep Content Disarm and Reconstruction for sanitization of all files, and Proactive Data Loss Prevention to detect and block sensitive data; helps to meet and exceed the mandated regulatory requirements.

Compliance type	Regulation / Standard	Types of data protected
Industry-specific regulations have specific requirements to protect sensitive data from unauthorized access	PCI DSS (Payment Card Industry Data Security Standard) - Any entity that processes, stores or transmits cardholder data, such as merchants or payment card processors, is required to comply with PCI-DSS.	▪ credit card number ▪ security codes ▪ address
	HIPAA (The Health Insurance Portability and Accountability Act of 1996) - Healthcare providers, insurance providers and their business associates with access to patient health information (PHI) are required to comply with HIPAA.	▪ email ▪ date of birth ▪ phone number ▪ passport number ▪ medical record number
	NERC CIP (North American Electric Reliability Critical Infrastructure Protection) - Out of the dozen plus NERC standards developed to protect critical infrastructure, the Critical Infrastructure Protection (CIP) standard is the most relevant for secure storage of critical systems information.	▪ security procedures or security information about BES Cyber Systems ▪ collections of network addresses ▪ network topology of the BES Cyber System
Privacy laws and regulations require organizations to guard against the unauthorized access, storage, and misuse of personal data	GDPR (Generate Data Protection Regulation) – The European Union guidelines mandate how organizations process and store customer data.	▪ social security number ▪ date of birth ▪ phone number ▪ address
	CCPA (California Consumer Privacy Act) - Grants California consumers the right to request their personal data is not sold to third parties.	▪ date of birth ▪ phone number ▪ address

Storage industry specific standards and **Non-profit industry watchdogs** provide in depth guidance for a wide variety of storage systems.

NAME	DESCRIPTION
ISO27040 (a subset of ISO27001 for Storage Security developed by the International Organization for Standardization)	This standard explores storage security risks and provides best practices for the entire life cycle of securing data and information stored in Physical and Virtual storages. It provides controls for designing and auditing storage virtualization, data confidentiality and integrity, data retention, data reliability, and data availability and resilience.
SNIA (Storage Networking Industry Association)	The mission of SNIA is "to lead the storage industry in developing and promoting vendor-neutral architectures, standards and educational services that facilitate the efficient management, movement and security of information."
FISMA (Federal Information Security Management Act of 2002)	Requires federal agencies to implement a cybersecurity program that promotes a set of high-level best practices, such as creating an inventory of IT assets, utilizing security controls, and continuously monitoring for risks.

OPSWAT.
Trust no file. Trust no device.

NEWCOM
Authorized Partner

Contact **NEWCOM** for more information or a quote!
781.826.7989 | sales@newcomglobal.com
NEWCOMGlobal.com