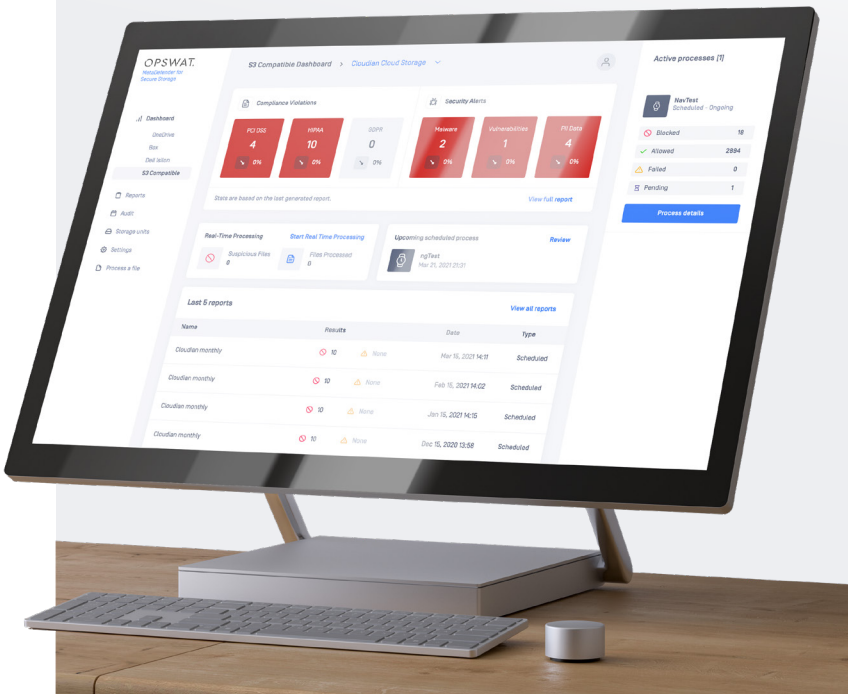
OPSWAT.

DATASHEET

MetaDefender® for Secure Storage

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 for Secure Storage 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.

Analyze. Remediate. Report.

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 for Secure Storage 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

Multi-scanning from 5-35 leading antimalware engines (Mcafee, ESET, Avira, K7, Crowdstrike, TrendMicro, 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 for Secure Storage

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).

Full auditibility

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.

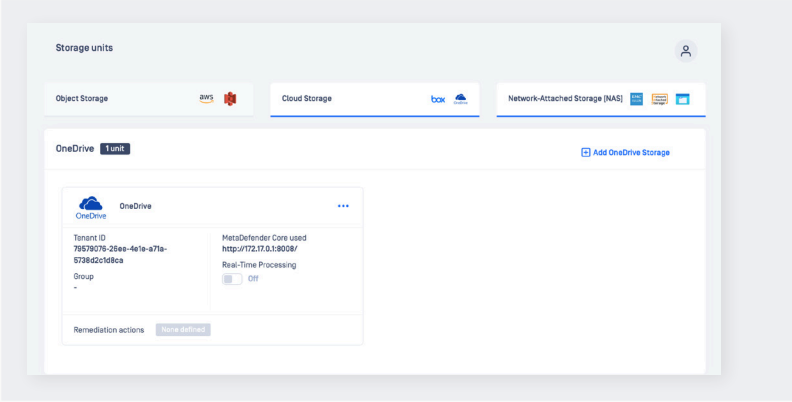
User Management

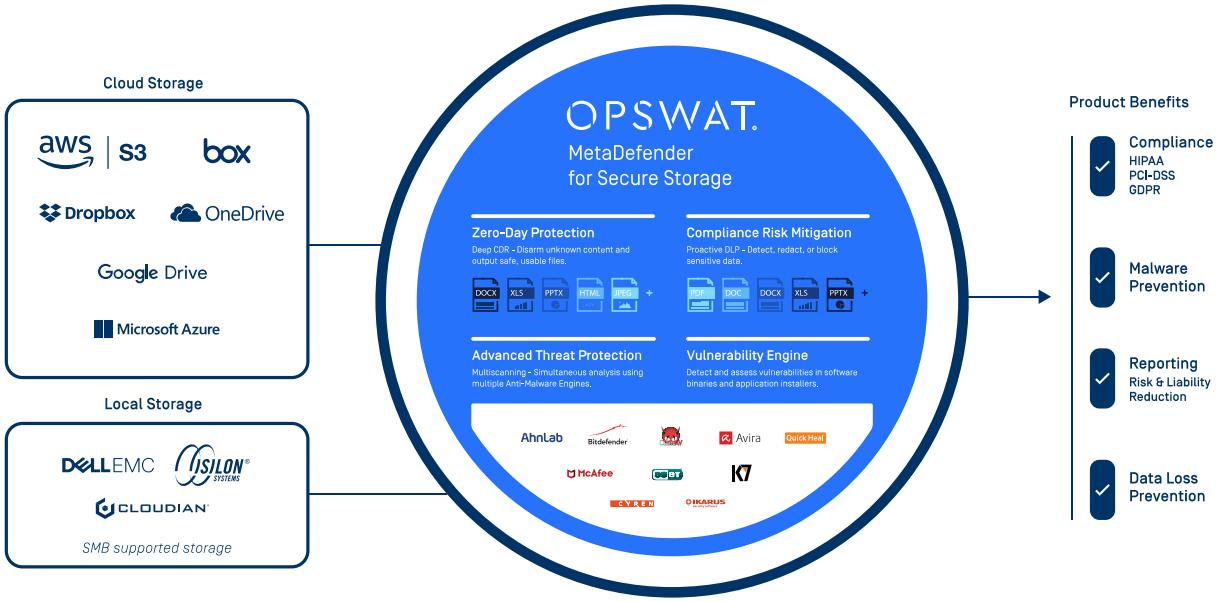
Enable your IT department to effectively manage compliance and data breach risks by giving role based (including 'read only') access to multiple administrators.

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.

MetaDefender for
Secure Storage

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 from 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.

Types of data that OPSWAT protects

- to meet **Payment Card Industry (PCI) Data Security Standards (DSS)** guidelines:
  - **Credit card number**

Risk of Non-compliance

According to PCI Compliance Blog (pcicomplianceguide.org/faq/#15) the penalties for non-compliance are:
The payment brands may, at their discretion, fine an acquiring bank $5,000 to $100,000 per month for PCI compliance violations. The banks will most likely pass this fine along until it eventually hits the merchant. Furthermore, the bank will also most likely either terminate your relationship or increase transaction fees. Penalties are not openly discussed nor widely publicized, but they can be catastrophic to a small business.

- to meet **General Data Protection Regulation (GDPR)** regulations:
  - **Personally identifiable Information (PII) of data subjects**
    - email
    - date of birth
    - phone number
    - passport number

Risk of Non-compliance

There are two tiers of administrative fine for non-compliance with the GDPR:
- Up to €10 million, or, in the case of an undertaking, 2% of annual global turnover – whichever is greater
- Up to €20 million, or, in the case of an undertaking, 4% of annual global turnover – whichever is greater

Fines for GDPR breaches are discretionary rather than mandatory. They must be imposed on a case-by-case basis and should be "effective, proportionate and dissuasive".
ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

- to prevent **Health Insurance Portability and Accountability Act (HIPAA)** violations:
  - **Social Security number**
  - **date of birth**
  - **phone number**
  - **address**

Risk of Non-compliance

Penalties for non-compliance are based on the level of negligence and can range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for violations of an identical provision. Violations can also carry criminal charges that can result in jail time.

hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.htmlw

OPSWAT.

Trust no file. Trust no device.