

OPSWAT.

METADEFENDER

Storage SecurityTM

Secure Your Enterprise Data Storage

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

From local servers to cloud platforms like Amazon S3, Microsoft Azure Blob Storage, NetApp, Cloudian, Dell Isilon, SharePoint, Box, and any S3 or SMB/NFS/SFTP-compatible storage, MetaDefender Storage Security safeguards enterprise data and files against breaches, reducing downtime and helping prevent compliance violations. Its seamless integration with leading storage and collaboration solutions ensures minimal disruption to existing workflows and technology stacks.



Table of Contents

- 01 Scan. Sanitize. Store.
- 02 Benefits
- 03 Features
- 04 Integrations
- 05 Deployments Options
- 06 How does OPSWAT minimize your compliance risk?

01

Scan. Sanitize. Store.

Files from users within 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.

Share data within your organization confidently and securely with MetaDefender Storage Security™.

02

Benefits

All-in-One Platform

- MetaDefender Storage Security offers seamless integration with existing workflows, enabling real-time, on-demand or scheduled scanning across multiple storage repositories, including on-prem, hybrid, and cloud-native environments.
- Guard against zero-day threats and advanced targeted attacks using leading technologies from OPSWAT.
- Multi-layered solutions deliver real-time threat detection and prevention to ensure comprehensive storage security.

Plug-and-Play Integrations

- Deploy easily and cost-effectively into your existing infrastructure. Configure and start scanning in minutes, with no need for extensive setup or storage administration. The SaaS-native solution makes this even more effortless by providing ready-to-use protection right in the cloud.
- Seamlessly integrate with Amazon S3, SharePoint Online, Azure, any SMB/NFS/SFTP or S3 compatible storage.

Enhanced File Privacy

- Tailor policies and workflows to comply with stringent regulations like PCI, HIPAA, GLBA, and FINRA. MetaDefender Storage Security’s cloud-native solution provides automatic compliance with no manual oversight required.
- Prevent sensitive data loss or leakage by controlling data entry and exit within the organization.

Flexibility and High Availability

- MetaDefender adapts to your storage environment, from local systems to fully cloud-native architectures, ensuring protection at any scale.
- Ensure continuous protection with support for redundant and distributed architectures, minimizing downtime and maintaining service reliability.

03

Features

Advanced File Processing

- **Real-time Scan** ensures that files are processed as soon as they are uploaded. Real-time processing supports two handling types for files discovery
 - **Event-Based Handling:** Triggered scans based on specific events.
 - **Polling Handling:** Regular checks for new files to scan.
- **On-Demand Scan** is a manual scanning process that can be initiated immediately after configuration. Users have the flexibility to specify a scan name, set scan priority and select preferred scan configurations tailored to specific security requirements.
- **Scheduled Scan:** Automatically check your storage for threats or vulnerabilities at a predetermined time and frequen

Custom Scan Priority

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

Remediation Actions

- Add information about file processing as tags to classify the contents of files quickly and find all malicious files with a <tag> for further analysis and forensics.
- Choose conditional steps to move files tagged as “Allowed,” “Sanitized,” or “Blocked”.
- Apply Deep CDR™ technology to sanitize files.
- Copy, move, and delete files after processing according to the configuration [e.g. if the file is blocked or after it is sanitized].
- An optional “Delete empty folders after remediation” setting is added for SMB/NFS/SFTP shares.

Cancel Scanning Fie

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

Streamlined Report Management

- View all saved and scheduled reports in one centralized location.
- Easily track health trends or help meet audit requirements by periodically saving reports.
- Compare key indicators from previous scans to gauge trends, ensuring informed decision-making and proactive security management.
- Remediation data is included in scan details, providing a comprehensive remediation overview.
- Generate actionable reports with dynamic charts, and detailed PDF audits, streamlining compliance and audit processes.

SIEM Integration

Integrate with SIEM systems seamlessly and quickly through an intuitive GUI and RESTful API.

Proactive Event Notification

- Notify specific individuals when critical events occur.
- Key Events include report generation, user registration, and file blocking.
- Ensure an immediate response with timely action and improved system management.
- Customizable notifications to relevant stakeholders increase operational efficiency and agility.

04

Integrations

Setup and configure multiple storage units from multiple vendors in minutes [in the cloud or on-premises] 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.








Seamlessly integrate all your Dell Isilon or any SMB/NFS/SFTP - compatible on- premises storage units.

Secure all your data stored in Microsoft OneDrive, SharePoint, Azure Files, and Azure Blob Storage.

Easily configure all your storage units from Box and other collaboration solutions.



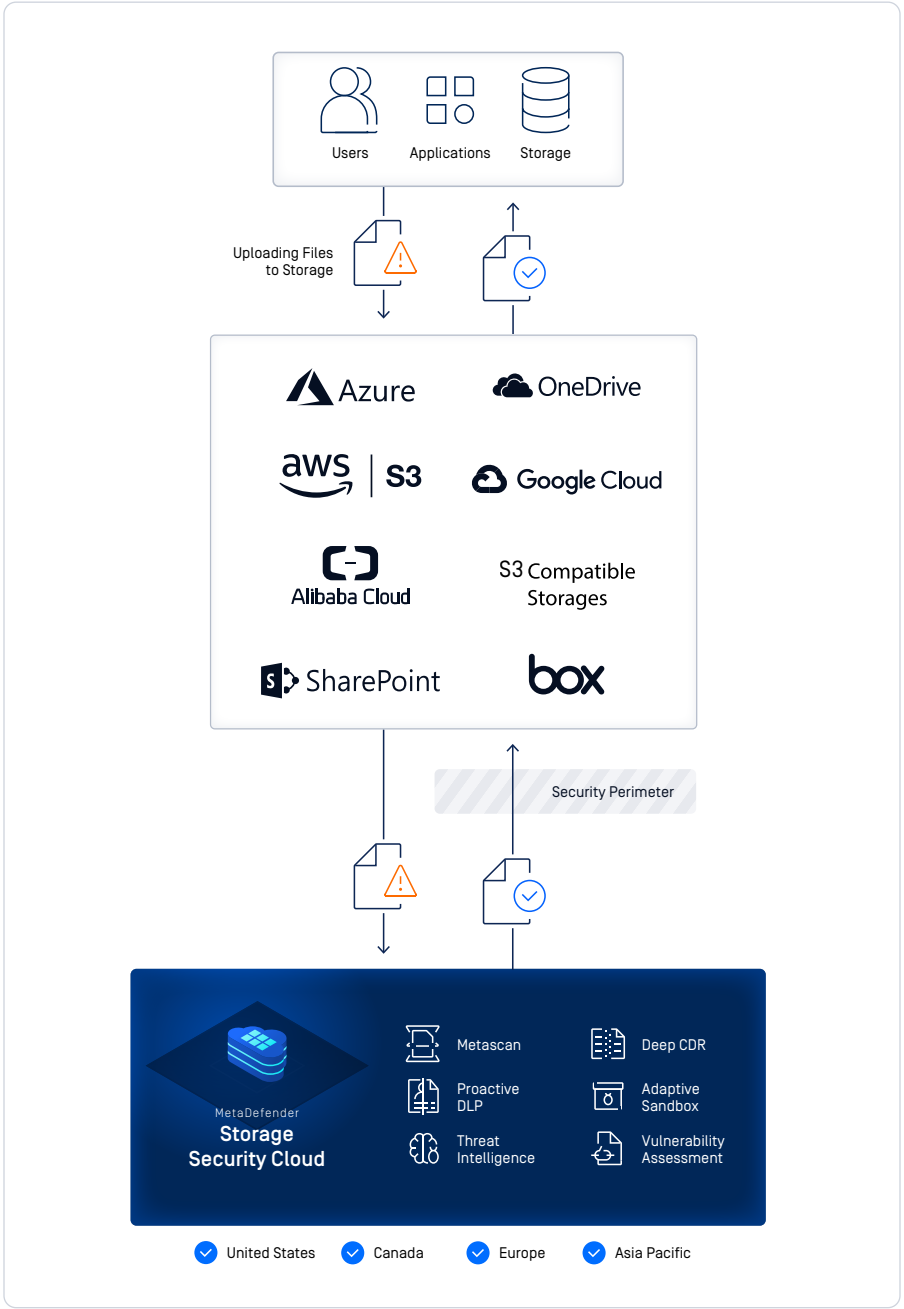
Storage Name	Integration Type
 S3	Native
	S3 Compatible
	S3 Compatible
 Cloud Infrastructure	S3 Compatible
	S3 Compatible
	S3 Compatible
 Blob Storage	Native
	Native
	Native

Storage Name	Integration Type
	NFS
 Files	Native
	SMB/NFS/SFTP
	Native/SMB/NFS/SFTP
	Native
	Native
 Online On-Prem	Native
OPSWAT. MetaDefender Managed File Transfer	Native

Deployments Options

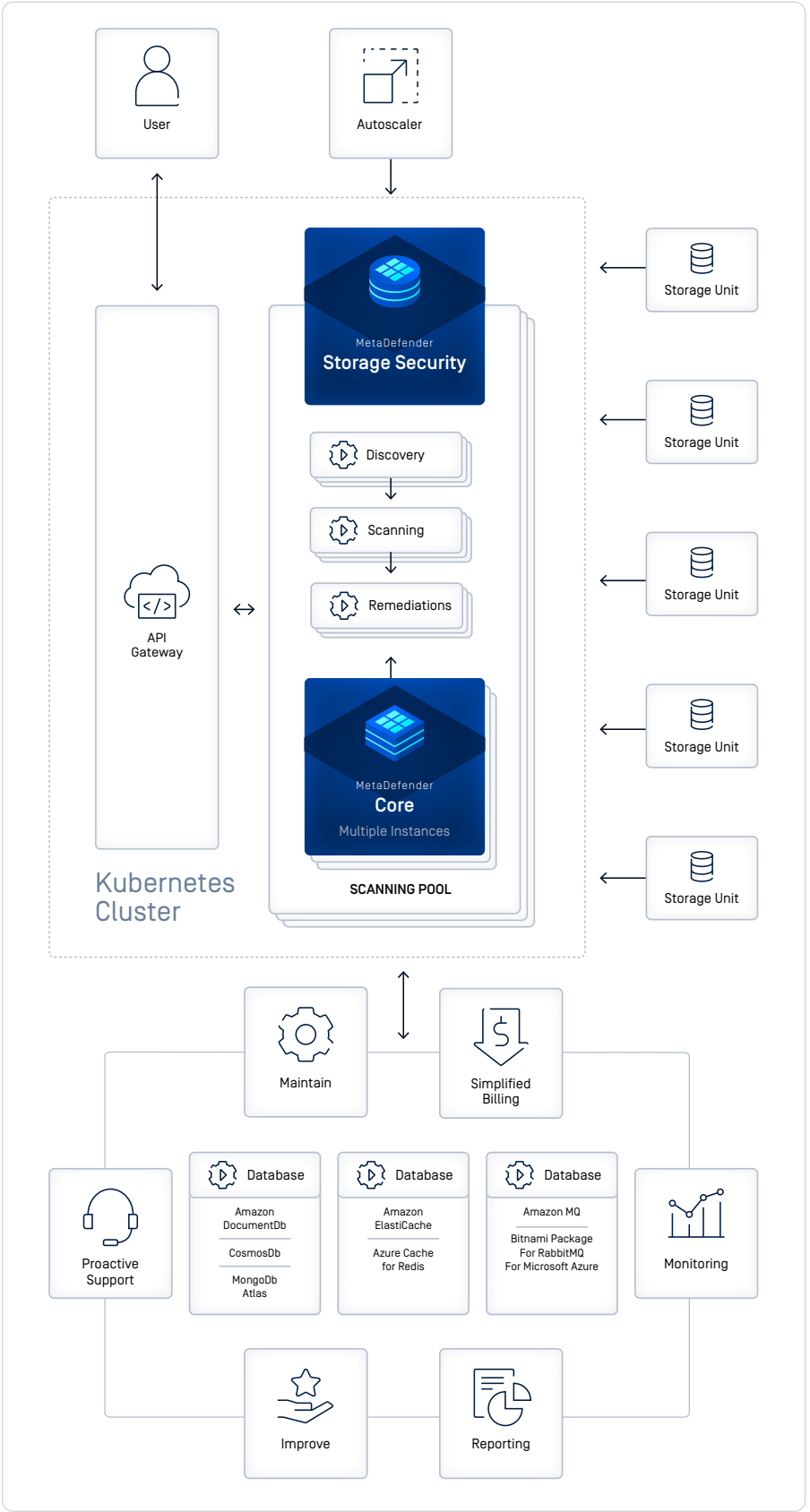
Cloud: SaaS [Software as a Service]

- Streamlined for the Cloud: Perfect for businesses prioritizing ease of use and cloud-first strategies.
- Hassle-free Management: No need for dedicated IT staff. OPSWAT handles everything from setup to updates.
- Flexible Integration: Works seamlessly with popular cloud platforms and your existing on-premises systems.
- Cost-Effective: No hardware investments needed. Pay only for what you use.
- Secure & Compliant: Built-in features ensure your data stays protected, aiding compliance with industry regulations.



Kubernetes: On-Premises and Hybrid

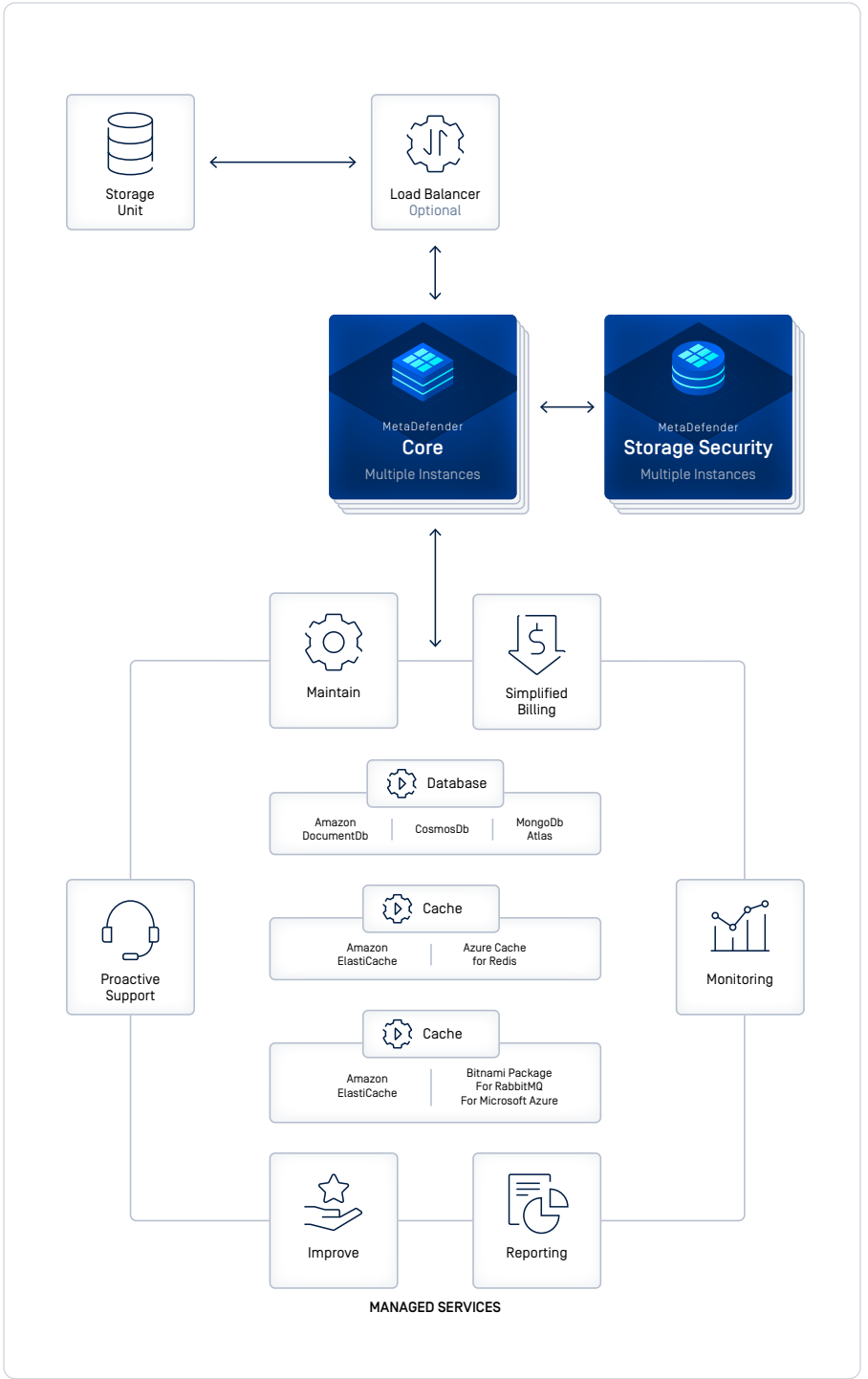
- Perfect for modern enterprises running large-scale, distributed applications in containers, both on-premises and in hybrid cloud environments.
- Handles daily workload fluctuations efficiently, while optimizing costs.
- Helm support is available for popular cloud Kubernetes services like EKS, AKS, and GKE.



Virtual Machines:
On-Premises & Hybrid

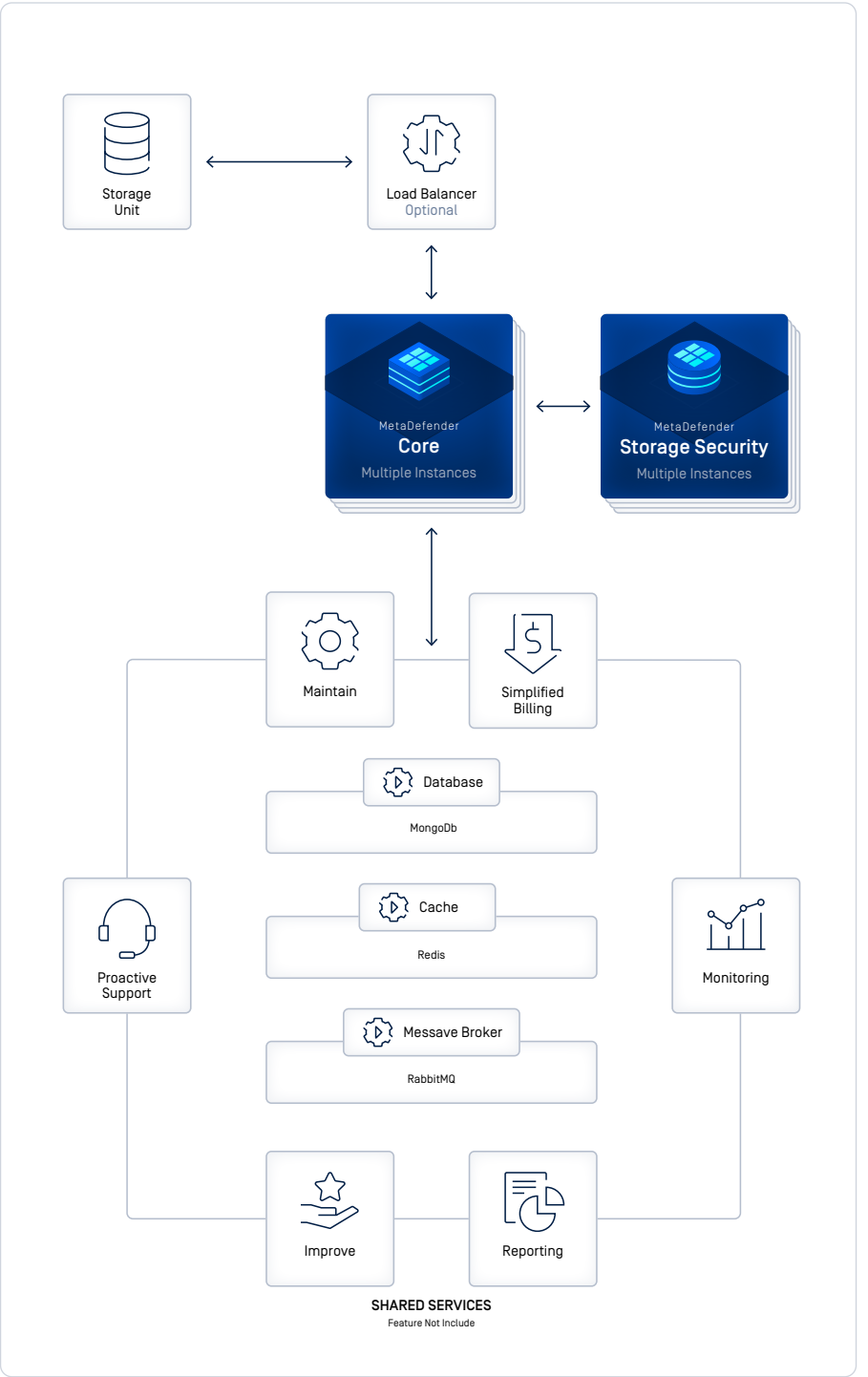
Advanced deployment with
self-hosted shared services.

- Enhanced control and customization.
- Improved reliability and scalability for shared components.
- Capable of processing up to 100,000 files per hour with sufficient resources allocated to database, cache, and message broker services.



Advanced deployment with
managed services.

- Ideal for medium to large workloads without the need for auto-scaling.
- Can efficiently handle up to 100,000 files per hour with a minimum of two MetaDefender Storage Security instances and four MetaDefender Core instances.



06

How does OPSWAT minimize your compliance risk?

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

MetaDefender Storage Security 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 solution alerts you to misuse, giving you visibility into suspicious or careless activity by your users.

OPSWAT’s advanced suite of technologies—including industry-leading MetaScan™ Multiscanning with 30+ antivirus engines, Deep CDR™ for sanitization of all files, and Proactive DLP™ to detect and block sensitive data—helps to meet and exceed mandated regulatory requirements.

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 evaluates storage security risks and mandates best practices for the entire life cycle of securing data and information stored in physical and Virtual storage. 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 Associ- ation]	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 Manage- ment 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.

Compliance Type	Regulation / Standard	Types of Data Protected
Privacy laws and regulations require organizations to guard against the unauthorized access, storage, and misuse of personal data.	GDPR [General Data Protection Regulation]	<ul style="list-style-type: none">• Social Security Number• Date of Birth• Phone Number• Address
	CCPA [California Consumer Privacy Act]	<ul style="list-style-type: none">• Date of Birth• Phone Number• Address
	The BDSG [German Bundesdatenschutzgesetz]	<ul style="list-style-type: none">• Name• Identification Number• Location Data• Medical History or Other Health-Related Information• Biometric Data/ Genetic Data
Industry-specific regulations have specific requirements to protect sensitive data from unauthorized access	PCI DSS [Payment Card Industry Data Security Standard]	<ul style="list-style-type: none">• Credit Card Number• Security Codes• Address
	HIPAA [The Health Insurance Portability and Accountability Act of 1996]	<ul style="list-style-type: none">• Email• Date of Birth• Phone Number• Passport Number• Medical Record Number
	NERC CIP [North American Electric Reliability Corporation Critical Infrastructure Protection]	<ul style="list-style-type: none">• Security Procedures or Security Information About BES Cyber Systems• Collections of Network Addresses• Network Topology of The BES Cyber Systems
	FINRA [Financial Industry Regulatory Authority]	<ul style="list-style-type: none">• Social Security Numbers;• Brokerage, Bank, or Other Financial Account Numbers;• Taxpayer Identification Numbers; and Medical Records.
	GLBA [The Gramm-Leach-Bliley Act]	<ul style="list-style-type: none">• Name• Address• Social Security Number• Account Numbers• Credit Card Numbers• Income or Investments• Medical History or Other Health-Related Information

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.