Securing Your Storage

Exploring OPSWAT MetaDefender Solutions

Prepared for: CIO COUNCIL CYBERSECURITY FORUM

Prepared by: Alexandru Ghioca, Solution Engineer OPSWAT

Monday, May 27, 2024

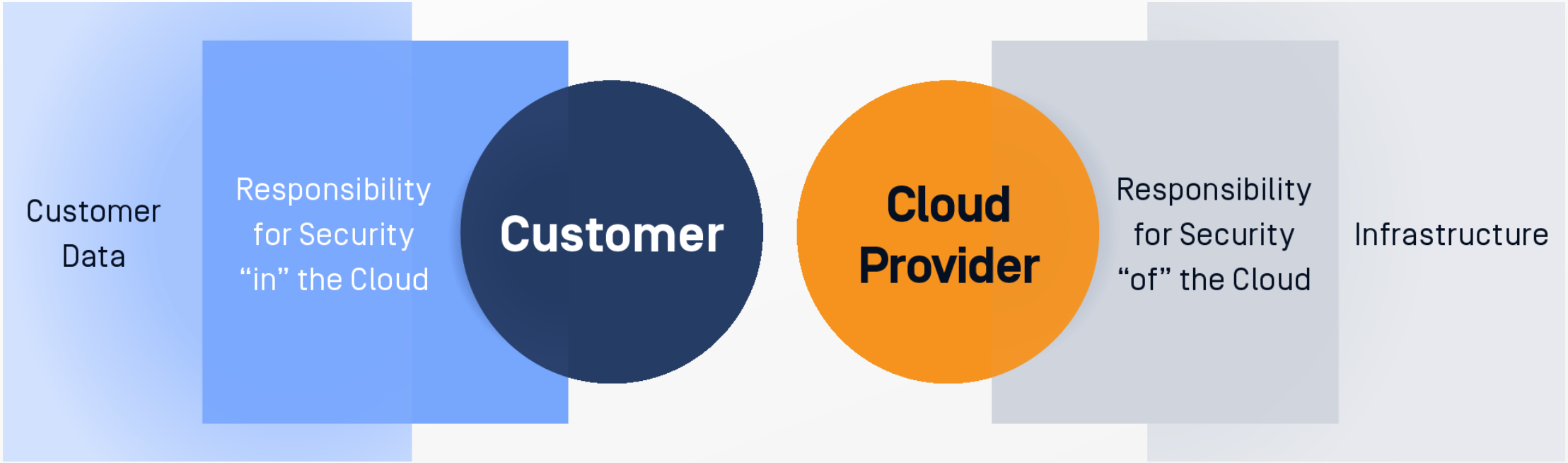
OPSWAT.

More than 90% of enterprises are multi-cloud environments.

COMPLIANCE

Shared Responsibilities

AWS: “Compliance is a Shared Responsibility”



Source: https://aws.amazon.com/compliance

CHALLENGES

Compliance & Data Privacy

53% of companies found over 1,000 sensitive files exposed to all staff

4.45M average cost of a data breach (2023)

$4.44B GDPR fines reported (2023)

74% of all breaches include the human element through Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

82% breaches that involved data stored in the cloud—public, private or multiple environments

277 days to identify and contain a data breach

32% of all Log4j vulnerability scanning occurred in the first 30 days after release

Recent Storage-Borne Attacks

Western Digital hacked: $18b storage firm's services taken offline

“[…]
The hackers who breached data storage giant Western Digital claim to have stolen around 10 terabytes of data from the company, including reams of customer information.
The extortionists are pushing the company to negotiate a ransom — of a “minimum 8 figures” — in exchange for not publishing the stolen data.
[…]"

Source: https://therecord.media/ransomware-attack-on-americold-cold-storage

Akira ransomware attacks against network-attached storage and backup devices

"[…]
Attacks deployed by Akira have been targeted at Cisco Adaptive Security Appliance and Cisco Firepower Threat Defense appliances impacted by the zero-day flaw, tracked as CVE-2023-20269, which could be leveraged to facilitate brute-force intrusions.
[…]”

Source: https://www.scmagazine.com/brief/escalating-akira-ransomware-attacks-target-finland

Major ransomware attacks have impacted Danish cloud hosting companies CloudNordic and AzeroCloud

“[…] Attackers have infiltrated certain network-linked CloudNordic and AzeroCloud servers during a migration to another data center, enabling the compromise of critical administrative systems and entire data storage silos and backup systems, which was then followed by total server disk encryption. […]”

Source: https://www.scmagazine.com/brief/cloudnordic-azerocloud-hit-by-severe-ransomware-attacks

OPSWAT.

THE PROBLEM

Malware Evades Traditional and AI/ML Anti-Malware, Sandboxes, WAFs, Next-Gen Firewalls, and Compromises Storage Systems

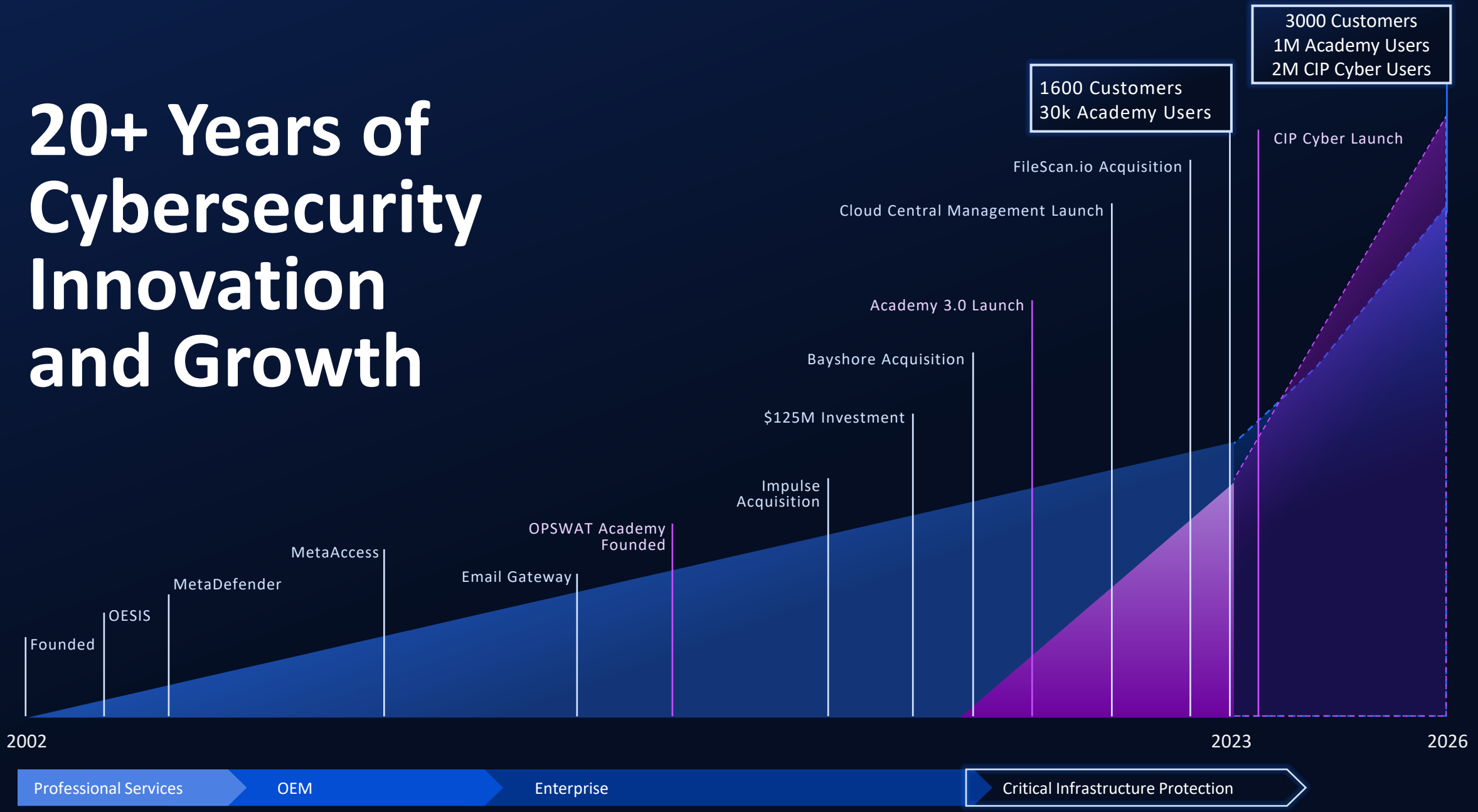
OPSWAT.

METADEFENDER STORAGE SECURITY

How We Can Help


OPSWAT.
We Protect the World's Critical Infrastructure

20+ Years of Cybersecurity Innovation and Growth



OPSWAT.

Trust no file.

In 2022, malware saw a rapid resurgence from its seven-year low in 2021 – climbing to an astonishing 1.2 billion

PDF, Word and .EXE files serve as the payload mechanism for over 62% of malware.

https://parachute.cloud/cyber-attack-statistics-data-and-trends/
https://smartdataweek-com.custommapposter.com/article/malware-statistics-in-2023-frequency-impact-cost-more#toc-14

OPSWAT.

#1 Market Leader

Multiscanning

OPSWAT.

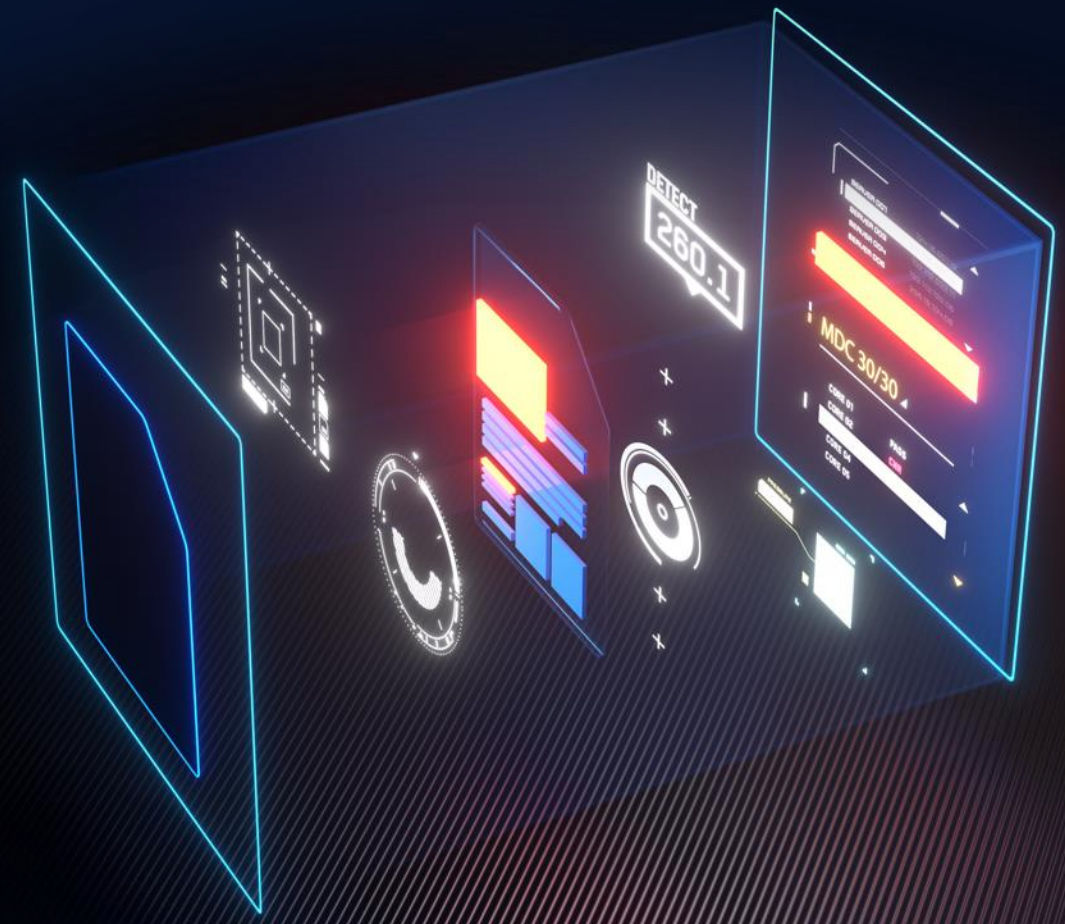
#1 Market Leader

Content Disarm and Reconstruct (CDR)

OPSWAT.

Adaptive Sandbox

Adaptive threat analysis technology enables zero-day malware detection and extracts more indicators of comprise.



OPSWAT.

What is MetaDefender Storage Security?

Secure your Enterprise Data Storage

All-in-One Platform

- Integrates effortlessly into existing workflows, providing real-time or on-demand scanning across various storage repositories.
- Guards against zero-day threats and advanced targeted attacks using leading technologies.
- Delivers real-time threat detection and prevention to ensure robust storage security.

Plug-and-Play Integrations

- Enhance cost-effectiveness with a simple plug-and-play integration.
- Configure and start scanning easily without needing storage admins.
- Seamlessly integrates with Microsoft OneDrive, SharePoint Online, Azure, Amazon S3, Box, Cloudian S3, Dell Isilon, and any SMB or S3 compatible storage.
- Begin evaluating your storage within minutes.

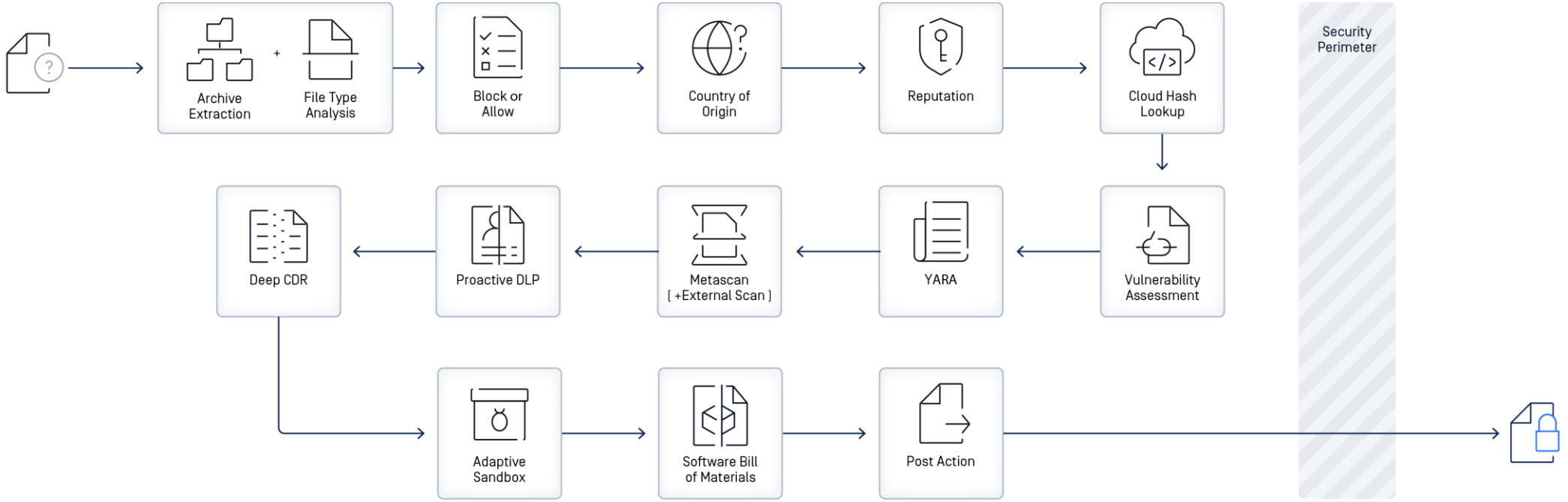
Enhanced File Privacy

- Tailor policies, workflows, and remediation actions to fit your security needs.
- Meet requirements like PCI, HIPAA, Gramm-Leach-Bliley, and FINRA.
- **P**revent sensitive data breaches by controlling data entry and exit within the organization.

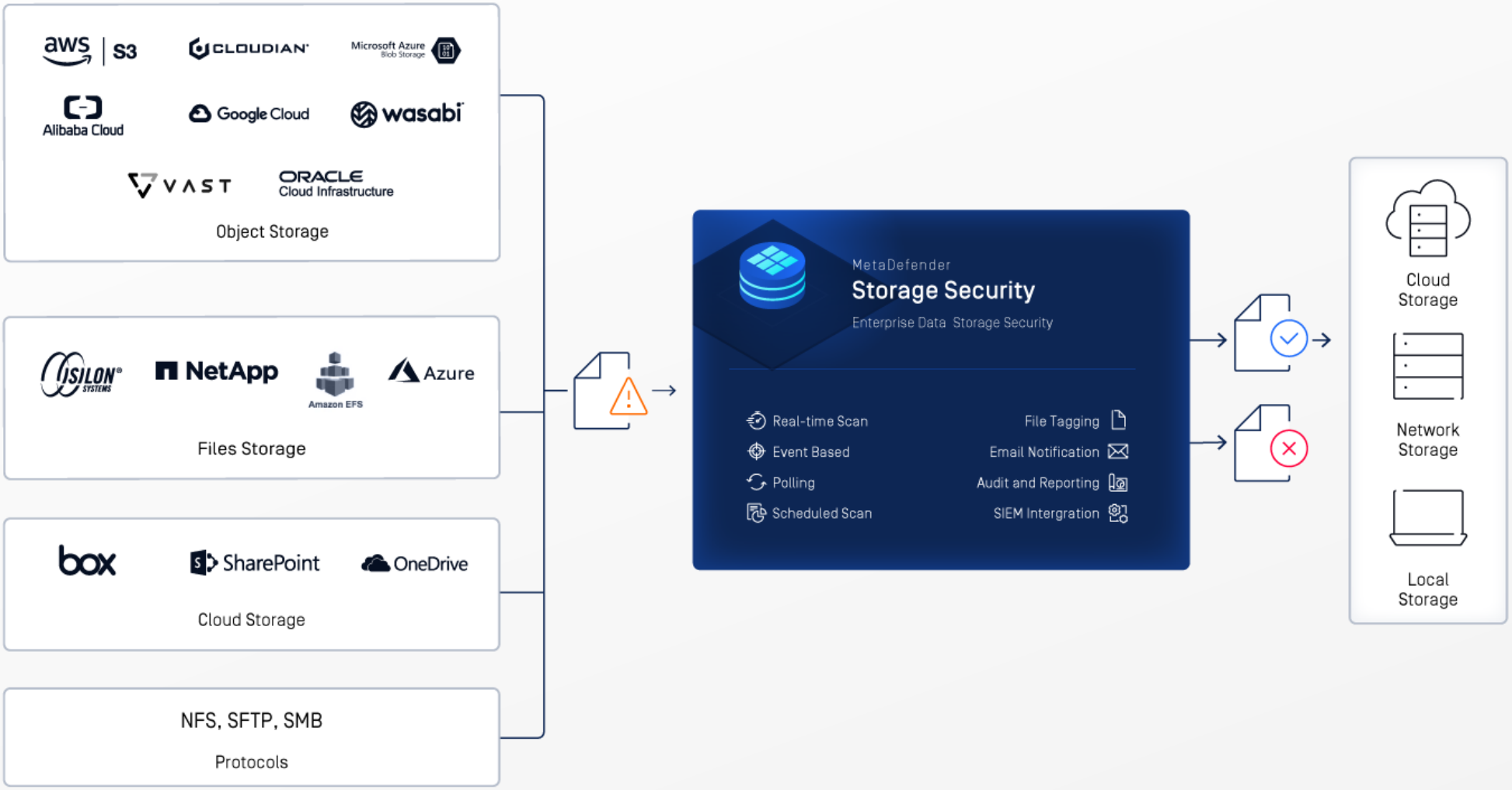
OPSWAT.

File Processing Workflow

Analyze 10 files/second per deployment for enterprise-ready performance



Available Integration Options



OPSWAT.

METADEFENDER STORAGE SECURITY

Features Overview

FEATURES

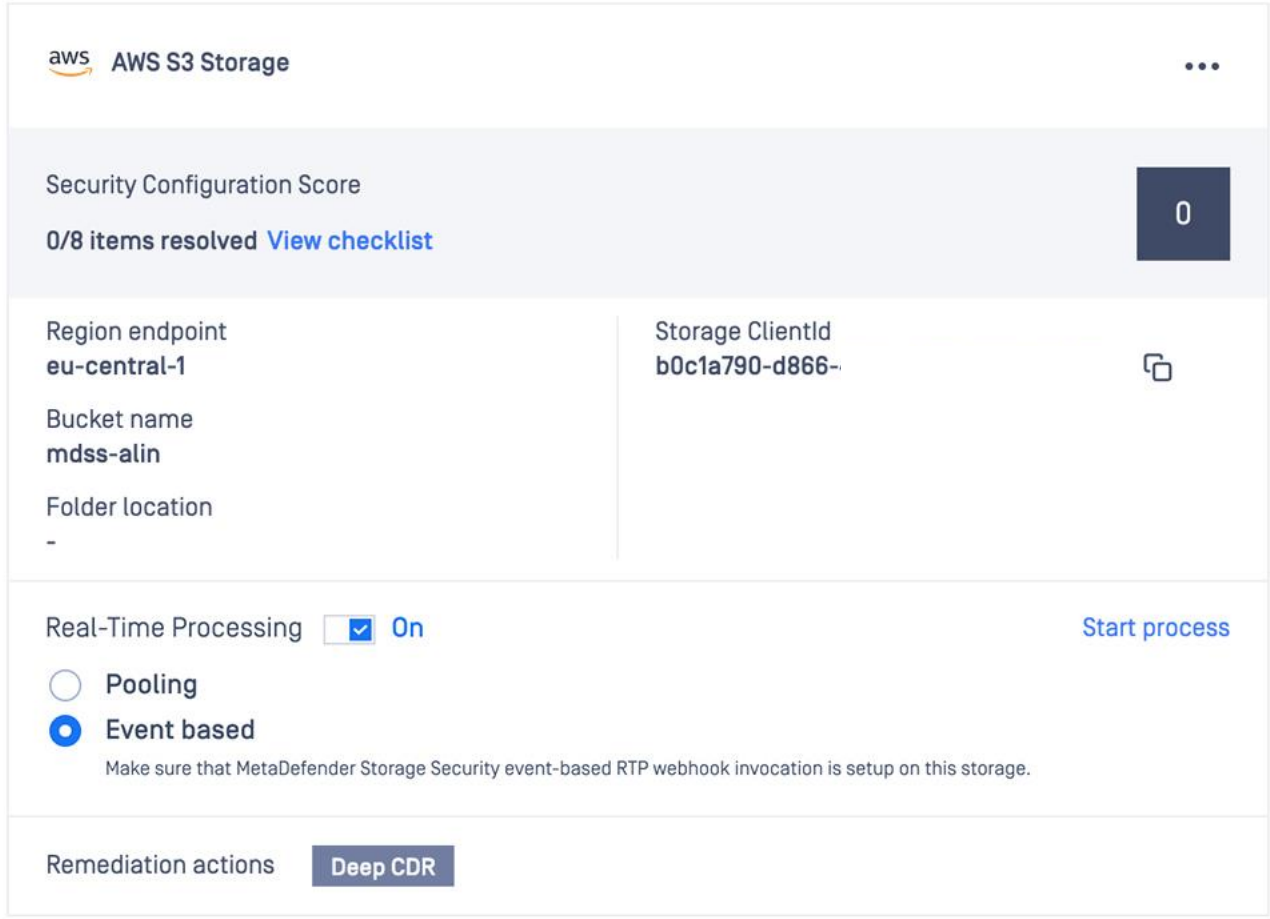
Advanced File Processing

Real-Time Scanning: Files are processed immediately upon upload, ensuring instant threat detection.

Polling Handling: Regular checks for new files to scan.

Event-Based Handling: Trigger scans based on specific events.

Scheduled Scanning: Automate scans at predetermined times to regularly check storage for threats or vulnerabilities.



FEATURES

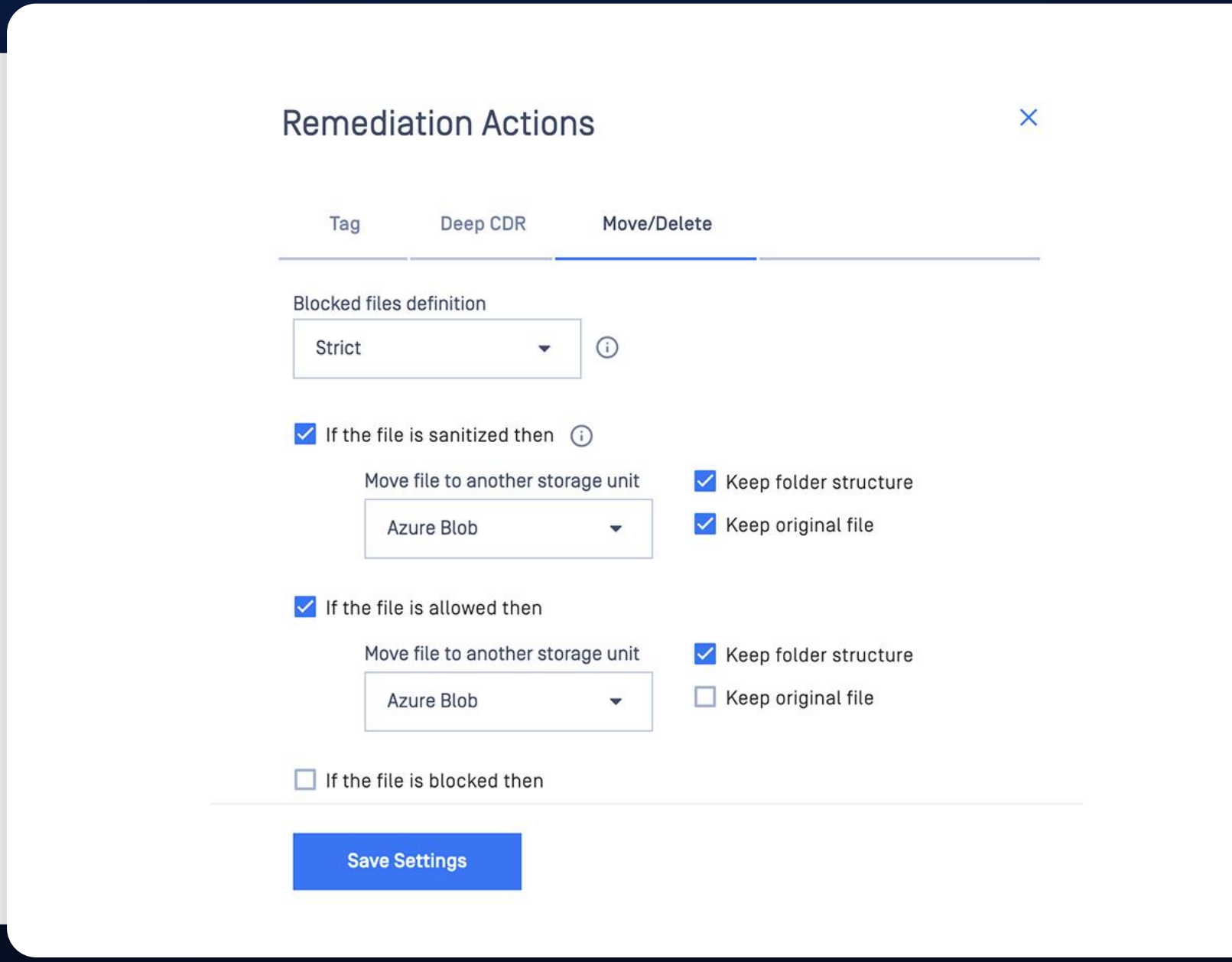
File Tagging and Management

Quickly classify file contents and identify malicious files for detailed analysis.

Choose steps based on tags like "Allowed," "Sanitized," or "Blocked."

Apply OPSWAT's Deep Content Disarm and Reconstruction (CDR) technology to sanitize files.

Copy, move, or delete files based on the set conditions after scanning.



FEATURES

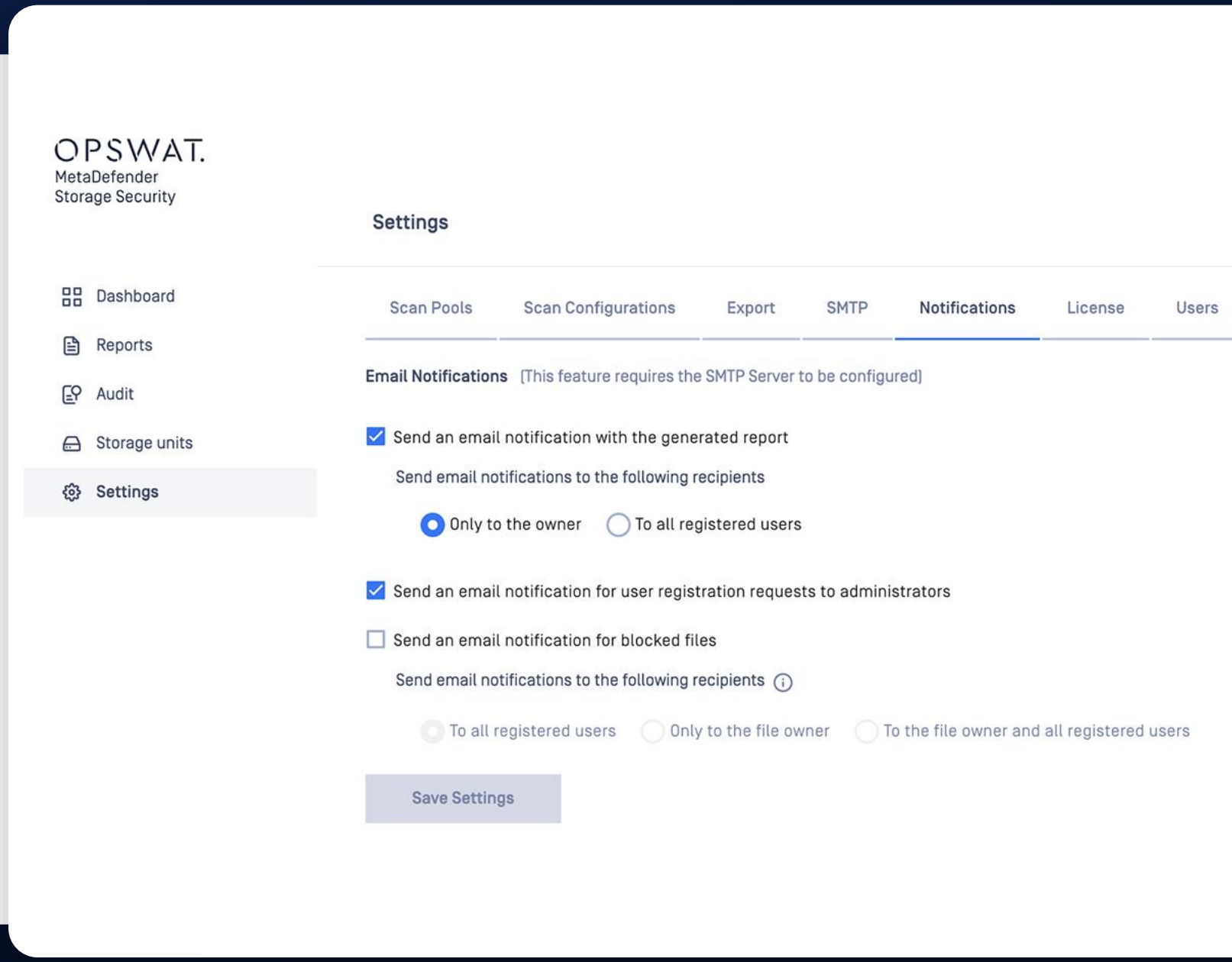
Proactive Event Notifications

Notify specific individuals when critical events occur.

Key Events include report generation, user registrations, and file blocking.

Immediate Response by ensuring timely action and improved system management.

Customizable notifications to relevant stakeholders enable swift responses and maintain operational efficiency.



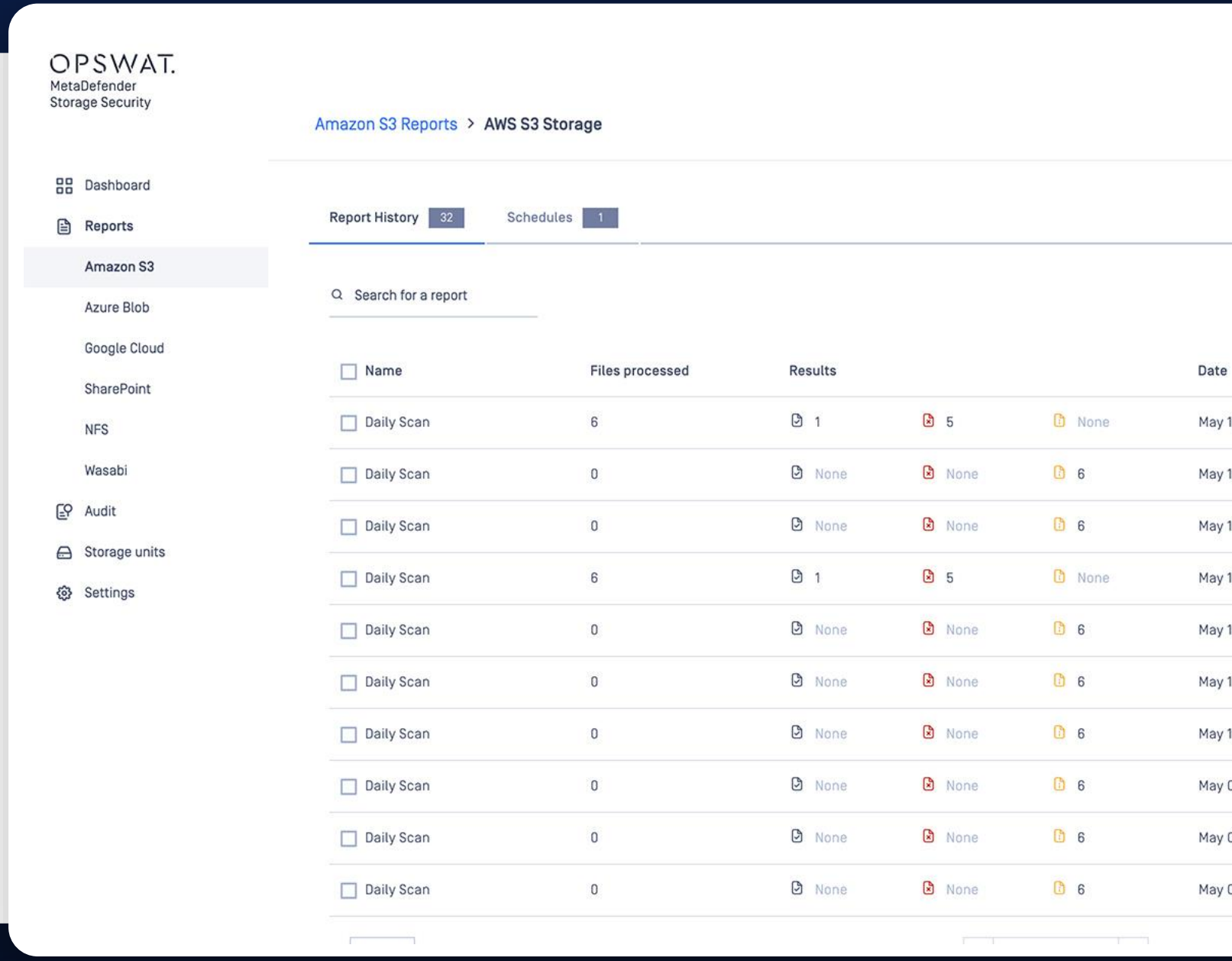
FEATURES

Streamlined Report Management

View all saved and scheduled reports in one centralized location.

Easily track health trends or meet audit requirements by periodically saving reports.

Compare key indicators from previous scans to gauge trends, ensuring informed decision-making and proactive security management.

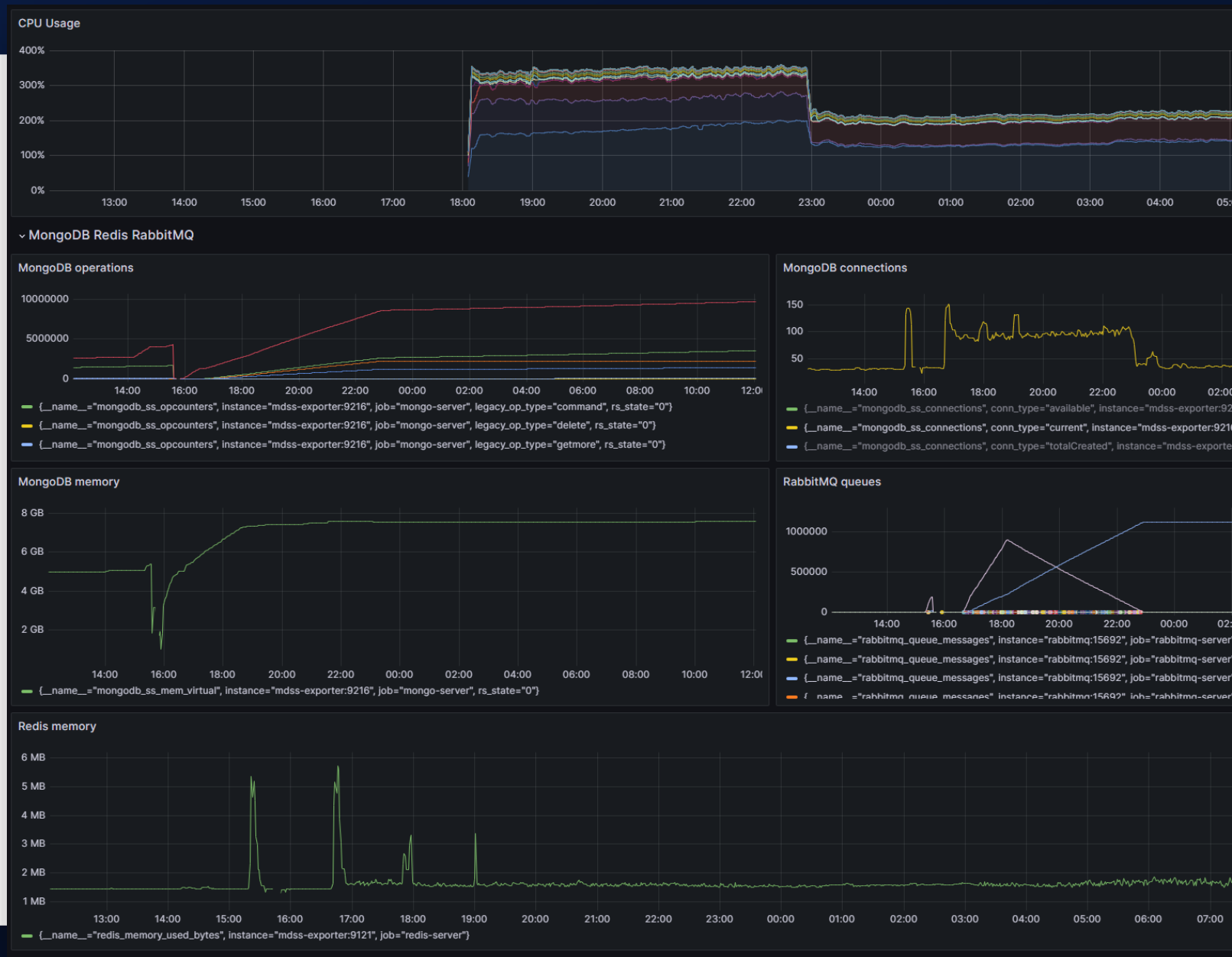


FEATURES

SIEM Integration

OPSWAT MetaDefender Storage Security integrates seamlessly with SIEM systems through an intuitive GUI and RESTful API, ensuring quick incorporation into existing workflows.

This design allows for efficient deployment and management, enhancing real-time threat detection and response without disrupting current processes.



Pain Points and Solutions

Threats & Customers' Pain Points	MetaDefender Storage Security
Difficulty detecting sophisticated malware with single AV solutions.	Utilizes multiple antivirus engines for higher detection rates, identifying and neutralizing sophisticated threats.
Challenges in preventing zero-day attacks.	Removes malicious code from files, preventing zero-day attacks while preserving file usability through Content Disarm and Reconstruction
Risk of exploitation due to unpatched vulnerabilities.	Identifies vulnerabilities in stored files and applications, enabling proactive mitigation.
Risk of intellectual property theft and non-compliance.	Detects and prevents sensitive data leakage, ensuring intellectual property compliance and protection through Proactive Data Loss Prevention
Need for seamless security integration with existing infrastructure.	Integrates with NAS, cloud, and on-premises storage, enhancing security
Necessity to meet various regulatory requirements for Regulatory Compliance.	Ensures malware-free and protected sensitive data, aiding in GDPR, HIPAA, and PCI-DSS compliance.
Complex and inefficient security management across platforms.	Central interface for monitoring and managing storage security with comprehensive reporting.
Requirement for scalable security solutions for growing storage environments.	Scales to provide consistent protection for small and extensive storage networks.

Certifications

SE Labs AAA Content Disarm and Reconstruction CDR Protection October 2023

OPSWAT Deep CDR

100% Protection Score

ISO 9001 CERTIFIED by schellman

OPSWAT has achieved ISO/IEC 27001:2013 certification.

COMMON CRITERIA

OPSWAT MetaDefender Core achieved EAL2+ (ALC_FLR. 1), meeting all Common Criteria Evaluation Assurance Level.

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations

OPSWAT was awarded SOC2 certification for MetaDefender Cloud by Schellman & Company, LLC.

Awards

CYBER SECURITY EXCELLENCE AWARDS WINNER 2022

OPSWAT's Deep CDR technology was recognized as a gold winner for the 2022 Cybersecurity Excellence Award.

CYBER SECURITY EXCELLENCE AWARDS WINNER 2023

Gold Winner in 3, 2023 Cybersecurity Excellence Awards categories — ICS/SCADA Security, Web Application Security, and CS Solution for the Energy Industry.

CYBERSECURITY BREAKTHROUGH AWARDS

OPSWAT Academy was recognized with the "Professional Certification Program of the Year" award in the 6th annual CyberSecurity Breakthrough Awards Program.

W3C WAI-AA WCAG 2.1

MetaDefender® Core Platform was determined to be compliant with Web Content Accessibility Guidelines (WCAG) 2.1 levels A and AA.

Regulation Compliance

The risks of non-compliance:

- Fines ranging up to $millions
- Penalties - higher transaction fees, termination of contracts and relationships
- Reputation loss and lawsuits
- Criminal charges or even jail
- Limits access to government-based contracts

HIPAA

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
- Medical record

GDPR

GDPR (Generate Data Protection Regulation) – The European Union guidelines mandate how organizations process and store customer data

- Email
- Date of Birth
- Phone number
- Passport number
- Social Security Number

PCI DSS

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 code
- Address

CCPA

CCPA (California Consumer Privacy Act) - Grants California consumers the right to request their personal data is not sold to third parties.

- Date of Birth
- Address
- Phone number

OPSWAT.

Thank You

Alexandru Ghioca
Solution Engineer @ OPSWAT

LinkedIn

Book a session