OPSWAT.

Storage Security Buyer's Guide

Protecting the World's Critical Infrastructure

Introduction

Storage security encompasses the protection of data throughout its lifecycle, from creation and storage to access and disposal. With data breaches costing organizations an average of millions of dollars and regulatory compliance requirements becoming more stringent, implementing robust storage security measures is no longer optional - it's essential for business continuity and reputation management.

Nowadays, organizations face an unprecedented volume of data and sophisticated cyberthreats targeting stored information. Whether businesses rely on cloud storage, hybrid infrastructures, or distributed file systems, securing data at rest has become a critical priority. This buyer's guide examines modern storage security challenges and demonstrates how OPSWAT MetaDefender Storage Security provides comprehensive protection for enterprise data across multiple storage platforms.

Table of Contents

01

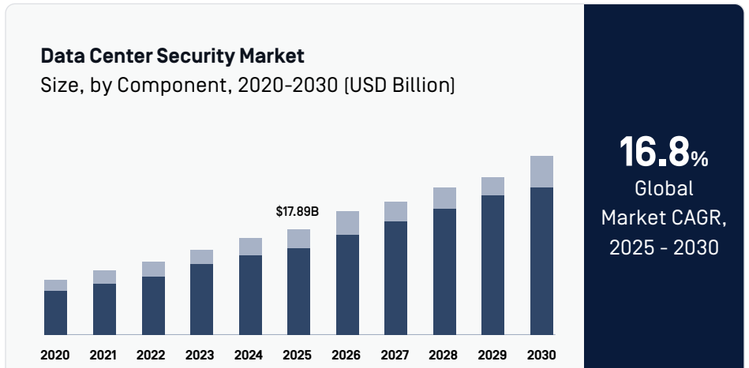
The State of Modern Storage Security

Storage security is a significant and growing segment within the cybersecurity market. Recent reports highlight substantial growth projected for related sectors:

Data Center Security Market

The global data center security market is worth US $17.89 billion in 2025 and is forecasted to reach around $49.08 billion by 2034, accelerating at a compound annual growth rate (CAGR) of 16.8% from 2025.

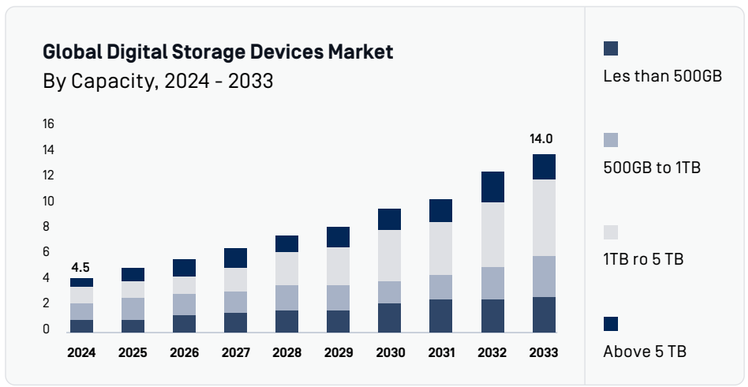
Grand View Research



Digital Storage Devices Market

The global digital storage devices market is projected to grow from US $4.5 billion in 2024 to $14.0 billion by 2033, at a CAGR of 13.4%.

Dimension Market Research



02

Challenges in Storage Security

Securing data storage in complex IT environments presents numerous challenges. These challenges stem from evolving threats, the increasing volume and diversity of data, and the distributed nature of modern storage infrastructures. Key challenges include:

03

How to Choose a Data Storage Security Solution

Choosing the right storage security partner is a critical decision that can significantly impact your organization's ability to protect its data assets. Here is a checklist of key factors to consider when evaluating potential partners:

Comprehensive Threat Prevention Capabilities

- Does the solution offer multi-layered threat detection and prevention (e.g., multiscanning, CDR (content disarm and reconstruction), and sandboxing)?
- Can it effectively detect and mitigate zero-day threats and APTs (advanced persistent threats)?
- Does it provide robust ransomware protection?

Deployment Flexibility and Scalability

- Does the solution support your existing and planned storage environments (on-premises, cloud, or hybrid)?
- How does the solution perform at enterprise scale, and what capabilities does it offer for managing petabte-scale deployments across large, distributed environments?
- Does it offer flexible deployment options (e.g., virtual machines, containers, or SaaS)?

Integration Capabilities

- Can the solution seamlessly integrate with your existing storage infrastructure (e.g., NAS, SAN, object storage, cloud storage platforms like AWS S3, or Azure Blob Storage)?
- Does it integrate with other security tools, such as SIEM systems, for centralized visibility and management?
- Are APIs available for custom integrations?

Management and Reporting

- Is there a centralized management console for easy configuration, monitoring, and policy enforcement?
- Does the solution provide comprehensive reporting and analytics for security events, compliance, and threat intelligence?
- Are alerting and notification mechanisms robust and configurable?

Ease of Use and Administration

- Is the solution intuitive and easy to deploy, configure, and manage?
- Does it require specialized expertise, or can existing IT staff manage it effectively?

Data Sanitization and Disarm Capabilities

- Does the solution include advanced data sanitization (CDR) to remove potentially malicious active content from files while preserving usability?
- What file types are supported for sanitization?

Future Roadmap and Innovation

- Does the vendor have a clear vision and roadmap for future product development and innovation?
- Are they committed to adapting to evolving threats and customer needs?

Vendor Reputation and Support

- Do they have a proven track record and positive customer testimonials?
- What level of technical support and customer service is offered?
- Is there a strong research and development team dedicated to staying ahead of emerging threats?

Compliance and Regulatory Support

- Does the solution help meet relevant industry regulations and data privacy mandates (e.g., PCI DSS, NIS2, ISO/IEC 27001, GDPR...)?
- Does it provide audit trails and documentation to support compliance efforts?

Performance and Efficiency

- What is the performance impact of the solution on storage systems and user access?
- Does it offer optimized scanning and processing to minimize latency?

By carefully evaluating potential partners against this checklist, organizations can make informed decisions and select storage security solutions that best meet their specific requirements and enhance their overall security posture.

When evaluating data storage security solutions, organizations should prioritize vendors that offer comprehensive capabilities across all these areas while providing proven track records, strong customer support, and transparent pricing models. **A thorough proof-of-concept deployment can validate solution effectiveness in your specific environment before making a final selection.**

04

The Need for a Multi-Layered Approach

Storage security cannot rely on single-point solutions or traditional signature-based detection methods. A multi-layer approach enables balanced security depth with performance and user experience through strategies including:

Comprehensive Threat Coverage

Different security layers are designed to address different types of threats. For example, anti-malware engines are detection-based and mostly specialize in identifying known threats, while CDR is preventative and disarms any potentially malicious content embedded in files. Sandboxing can safely detonate and analyze suspicious files for malicious behavior, and DLP (data loss prevention) prevents sensitive information from leaving the organization.

Threat Sophistication

Modern cyberthreats utilize multiple attack vectors and evasion techniques that can bypass single-layer defenses. A multi-layered approach allows organizations to adapt by adding or updating specific security layers without overhauling their entire security infrastructure. This agility is crucial for staying ahead of cybercriminals.

Compliance Requirements

Many regulatory frameworks and industry standards now implicitly or explicitly require a multi-layered security approach to protect sensitive data. Implementing such a strategy helps organizations meet their compliance obligations.

Business Continuity

Multi-layered security reduces the risk of successful attacks that could disrupt business operations, ensuring organizations can maintain productivity while protecting critical data.

Risk Mitigation

Different security layers address different types of risks, from technical vulnerabilities to human factors, providing comprehensive risk mitigation across the entire storage security spectrum.

05

The OPSWAT Solution for Storage Security

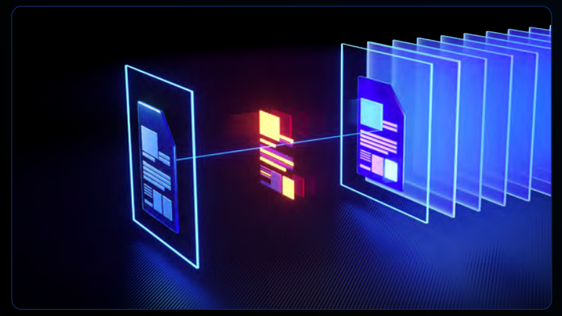
MetaDefender Storage Security™ is a multi-layered solution designed to provide comprehensive protection for enterprise data stored across various environments, including on-premises, hybrid, and cloud-native storage.

MetaDefender Storage Security can quickly and seamlessly integrate with major platforms like Amazon S3, Microsoft Azure, NetApp, Dell EMC, Wasabi, and SMB/NFS/SFTP or S3-compatible storage through standard connectors.*

***Disclaimer:** Lightning-fast integration performance depends on having the appropriate API access rights and network permissions. Additional network configuration and policy adjustments within your existing security framework may be required during the implementation process.

Market-Leading Technologies

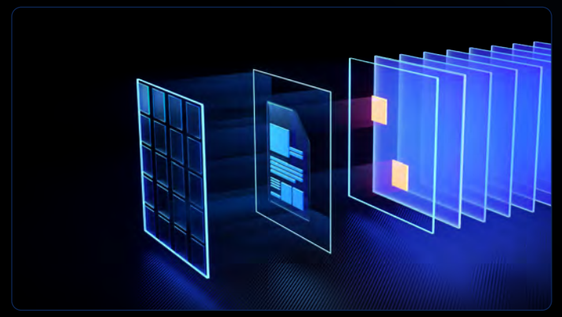
MetaDefender Storage Security leverages several core OPSWAT technologies to stop threats:



Deep CDR™

This technology proactively sanitizes files by disarming potential threats and reconstructing safe, usable files. It supports 200+ file types, including PDFs, archives, and file formats that support archives, with a 100% Protection Score verified by SE Labs.

Learn more about Deep CDR



MetaScan™ Multiscanning

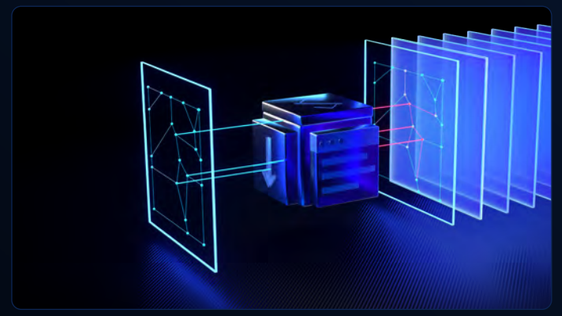
Utilizes over 30 commercial anti-malware engines to detect known file-borne threats, resulting in over 99% detection rates. MetaScan also uses machine learning and heuristics to help detect unknown threats.

Learn more about MetaScan Multiscanning

Proactive DLP™

Helps prevent sensitive data from leaving the organization. This technology detects sensitive data in 110+ supported file types that might be inadvertently exposed or maliciously targeted, including credit card numbers, PII, and PHI.

Learn more about Proactive DLP



Vulnerability Assessment

Detects application and file-based vulnerabilities before they are installed. We use our patented technology [U.S. 9749349 B1] to correlate vulnerabilities to software components, product installers, firmware packages and many other types of binary files, which are collected from a vast community of users and enterprise customers.

Learn more about Vulnerability Assessment

Adaptive Sandbox

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. It offers organizations scalable solutions, flexible deployment options, and enhanced resource efficiency for comprehensive malware analysis.

Learn more about Adaptive Sandbox

Key Features and Capabilities

Type-based Storage Grouping

Users can combine Object Storage units into dedicated groups and do the same for Network Attached Storage units.

Advanced File Processing

Real-time scanning, on-demand scanning and scheduled scanning.

Broad Storage Integration

Integrate with a wide range of storage vendors, including S3 compatible storage and SMB/NFS/SFTP storage.

Cancel Scanning File

Users can cancel an individual file scan while processing.

Proactive Event Notifications

Customize notifications to your preferences and receive timely notifications for critical events like report generation, user registrations, and file blocking.

Custom Scan Priority

Users can control scanning priority (High, Medium, Low) for storage unit scans.

SharePoint Historical Version Scanning

Scan all historical versions of SharePoint files.

Centralized Report Management

Analyze historical scan data to monitor security trends, meet audit requirements, and identify potential risks in one location.

Seamless SIEM Integration

Integrate quickly and easily with SIEM systems via an intuitive GUI and RESTful API.

Cancel Scanning File

Users can cancel an individual file scan while processing.

Proactive Event Notifications

Customize notifications to your preferences and receive timely notifications for critical events like report generation, user registrations, and file blocking.

Simplified HTTPS Configuration

Enable HTTPS directly through the Security settings interface, incorporating real-time certificate validation and comprehensive error reporting.

Automated Workflows

Create an automated security pipeline with 5-stage processing (Scan Configuration → Advanced Threats → Vulnerabilities → Sanitization → File Tagging).

Automated File Remediations

- Add information about file processing as tags for further analysis and forensics with File Tagging.
- Combine file sanitization with Deep CDR™ and other remediation actions (copy, move, delete...) to customize prevention and remediation workflows. Remediation policies can specify up to five copy/move destinations.
- An optional "Delete empty folders after remediation" setting for SMB/NFS/SFTP shares.

Automatic File Tagging with Scan Metadata

Enable to implement automated file routing policies that move, copy, or organize files based on security scan results across both AWS S3 and Google Cloud Platform environments.

Partition-Based Real-Time Scanning

Configure multiple scanning policies across different partitions within individual storage units.

Dual View Modes for More Clarity and Control

Dual view system (Groups and Accounts) allows organizations to organize storage units through Groups and Accounts perspectives.

Enhanced Integration Capabilities

Include individual file webhooks, and secure syslog with TLS.

Deployment Options

MetaDefender Storage Security offers flexible and scalable deployment options to fit various IT infrastructures:

Virtual Machines

Supports on-premises and hybrid IT environments.

Kubernetes

Compatible with modern architecture and containerized environments for enterprises.

Cloud (SaaS/IaaS)

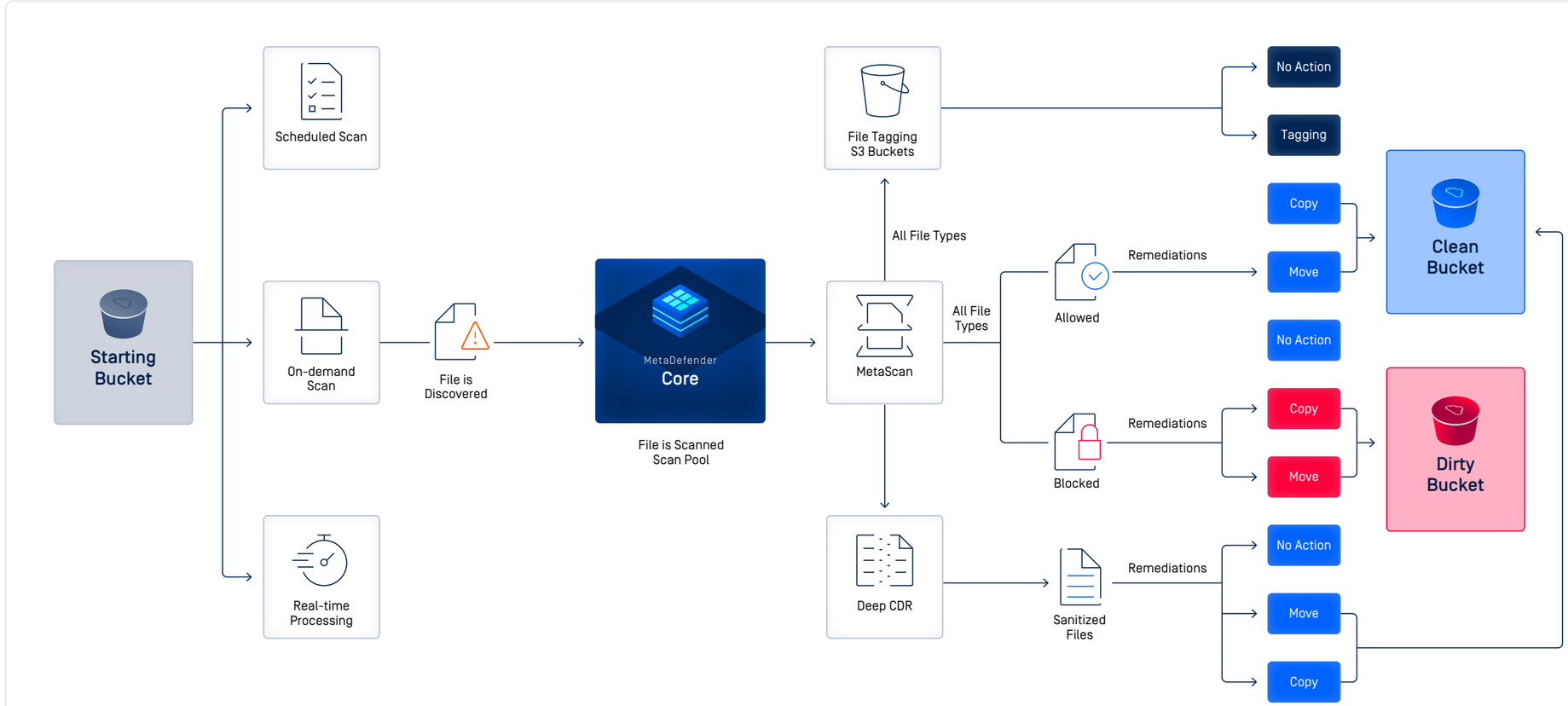
Provides a scalable, seamless, and cost-efficient cloud-based storage security solution.

06

Storage Security Uses Cases

Malware Remediation & Compliance

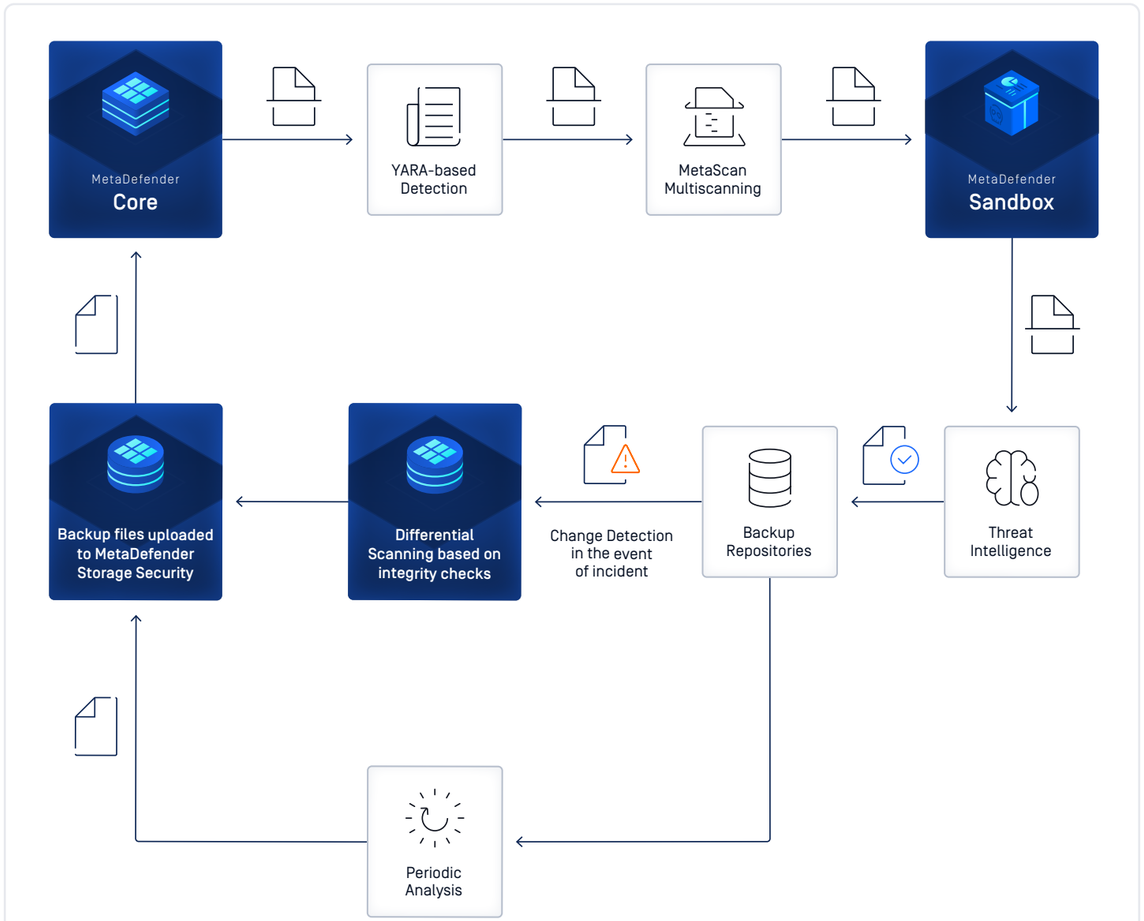
Organizations require comprehensive malware detection and removal capabilities to protect stored files while maintaining regulatory compliance through audit trails and documentation. Advanced remediation ensures infected files are safely sanitized or quarantined without disrupting business operations or compromising compliance requirements.



Backup Protection

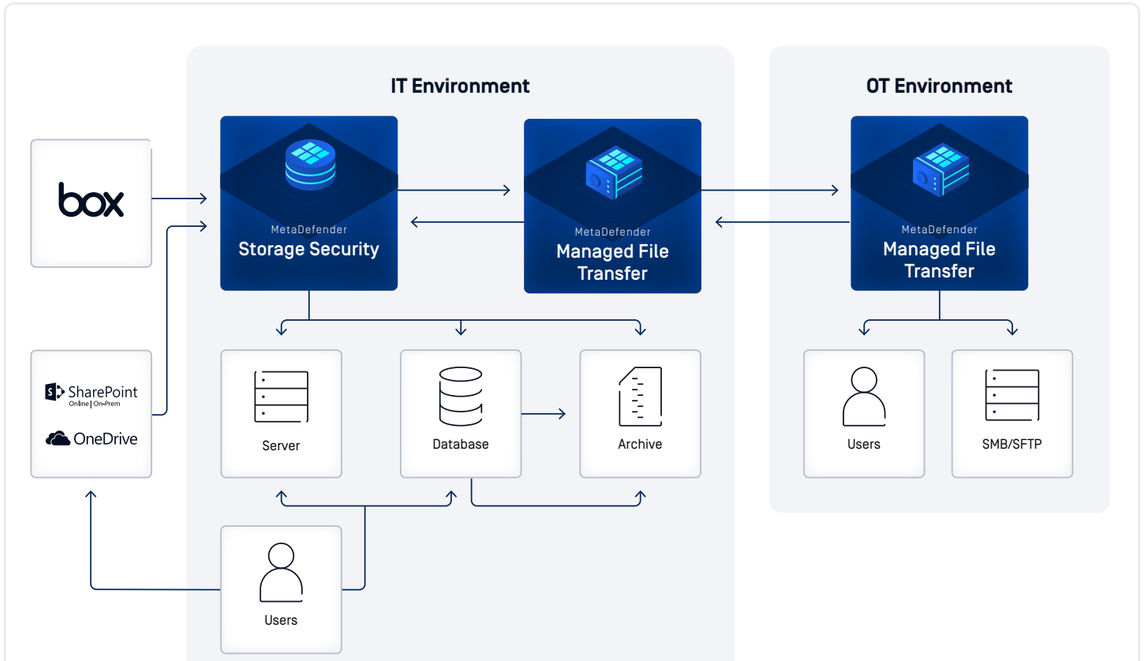
Protects your backup files by regularly checking them for viruses, malware, and other threats using multiple security technologies. The system scans files when they're backed up and when you need to restore them, preventing dangerous software like ransomware from infecting your backup storage.

This continuous protection helps ensure your backups stay clean and secure, so when you need to recover important data after a cyberattack or system failure, you can trust that the restored files are safe to use. The solution also helps your organization meet industry security requirements and provides detailed reports for compliance purposes.



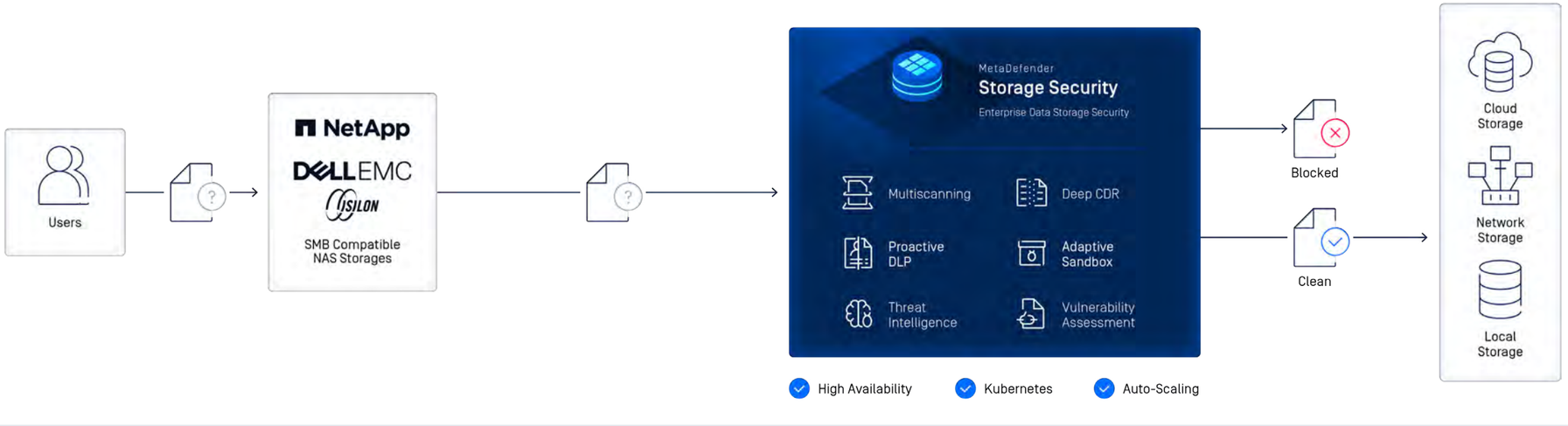
Collaboration Platform Security

File sharing and collaboration platforms like SharePoint, Box, and Google Workspace need real-time threat protection to prevent malware distribution among users. Advanced scanning and content sanitization ensure safe collaboration while maintaining productivity and user experience.



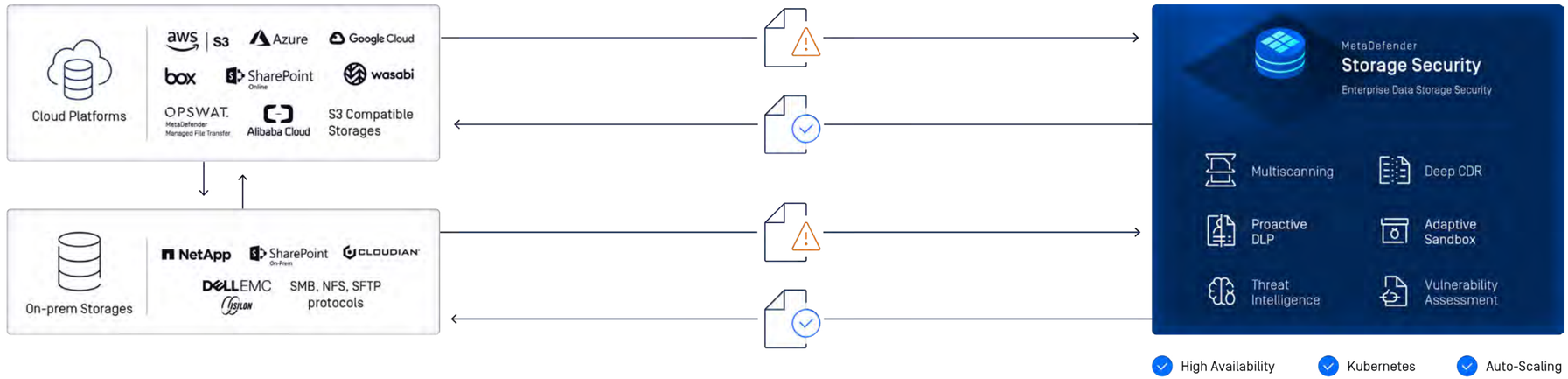
NAS (Network Attached Storage) Security

NAS systems serving multiple users and applications require continuous monitoring and threat detection to prevent malware propagation across the network. Automated scanning and remediation capabilities protect shared storage resources without impacting performance or accessibility.



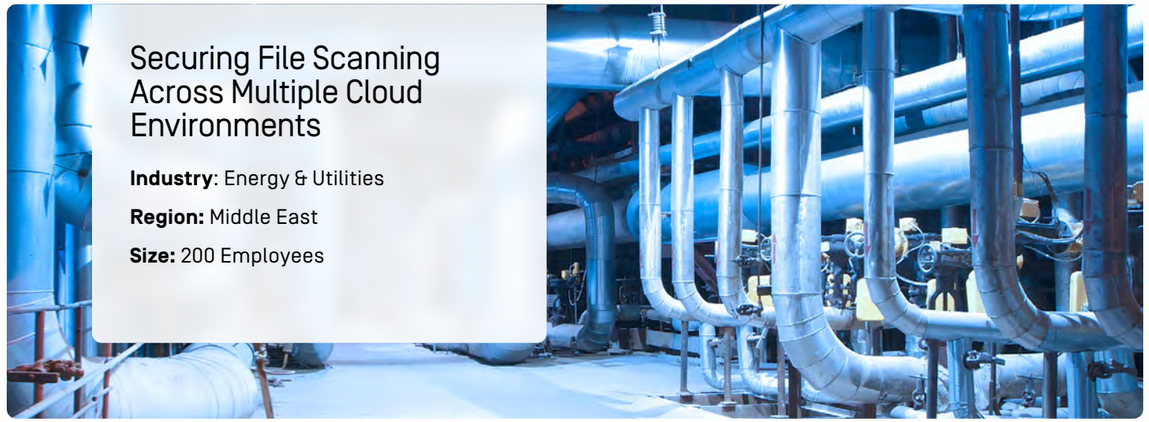
Hybrid Cloud Workflow Protection

Organizations operating across on-premises and cloud environments require consistent security policies that protect data as it moves between platforms during automated workflows. Seamless integration ensures files remain protected regardless of their location in hybrid infrastructure deployments.



07

Success Stories



Securing File Scanning Across Multiple Cloud Environments

Industry: Energy & Utilities

Region: Middle East

Size: 200 Employees

Challenges

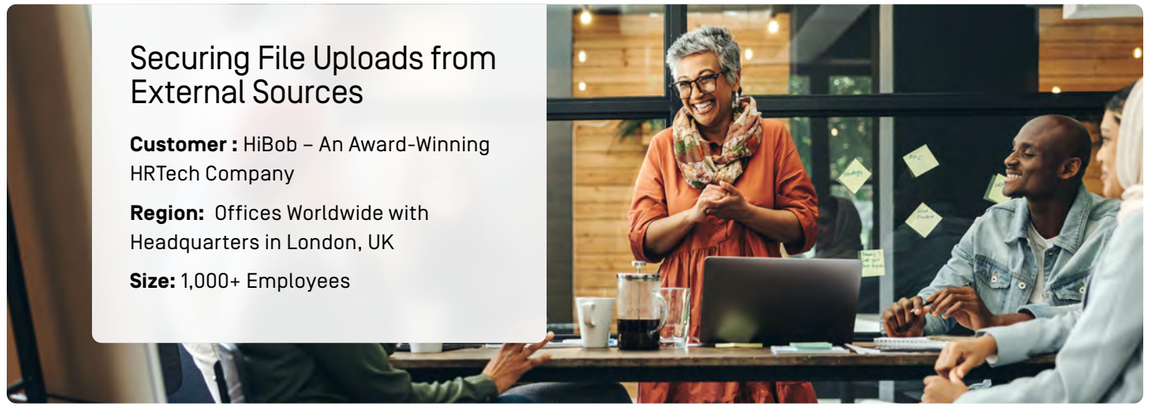
The client needed a flexible solution which could:

- Scan file uploads from both external resources and internal repositories to prevent any malware from infiltrating the network.
- Adapt to different policies so the organization stays compliant across different environments
- Seamlessly integrate with their existing Palo Alto firewalls.

Solutions

OPSWAT delivered a tailored approach to address the client's specific needs:

- The limitations of real-time upload scanning in all environments were overcome with a post-upload scanning strategy.
- The ICAP incompatibility was addressed by only implementing ICAP-enabled devices in compatible environments.
- For incompatible environments, storage workflow was adjusted to facilitate secure file scanning without relying on direct ICAP integration with the firewalls.



Securing File Uploads from External Sources

Customer : HiBob – An Award-Winning HRTech Company

Region: Offices Worldwide with Headquarters in London, UK

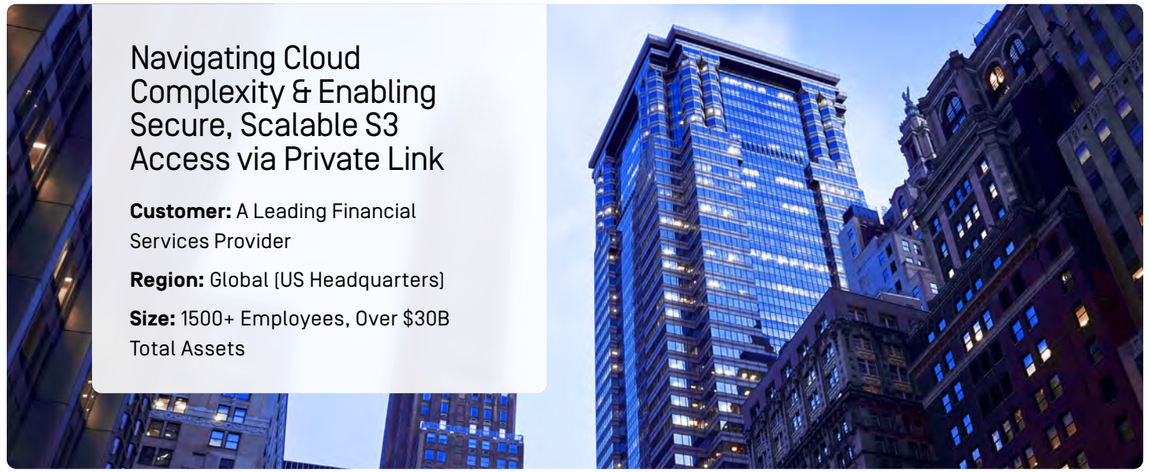
Size: 1,000+ Employees

Challenges

- **Security Challenge**: HiBob needed to secure application documents from external candidates, addressing malware threats and maintaining data integrity to protect against security breaches through file uploads.
- **Sanitization Requirement:** The solution required effective sanitization of incoming files to remove any malware while preserving data integrity.
- **Integration with AWS S3:** It was crucial for the security solution to integrate seamlessly into HiBob's existing AWS S3 cloud infrastructure without disrupting their operations.

Solutions

- By deploying MetaDefender Storage Security, HiBob achieved a comprehensive, zero-trust approach to file-upload security, significantly reducing the risk of malware and other threats.
- MetaDefender Storage Security solution seamlessly integrated with HiBob's AWS environment, ensuring minimal disruption to existing workflows while enhancing security measures.
- With Deep CDR deployed, HiBob can confidently sanitize files uploaded by external entities/customers to maintain data integrity, mitigate the risk of data breaches, and protect their platform and customers.



Navigating Cloud Complexity & Enabling Secure, Scalable S3 Access via Private Link

Customer: A Leading Financial Services Provider

Region: Global (US Headquarters)

Size: 1500+ Employees, Over $30B Total Assets

Challenges

- **Private Link Limitations:** AWS S3 has limited support for Private Link integration, which can make direct secure access to buckets through this preferred method challenging.
- **Multi-Account Complexity:** The bank managed multiple AWS accounts and regions, complicating access management and resource allocation.
- **Scalability Requirements:** A planned shift from EC2 to ECS/EKS required a flexible, modern deployment approach.
- **Manual Configuration Risks:** Hardcoded connection URLs and inconsistentvaccess policies increased the risk of error and misconfiguration.

Solutions

Recognizing the need for a modern, resilient solution, the bank partnered with OPSWAT to reimagine its approach. OPSWAT deployed MetaDefender Storage Security in a tailored configuration that addressed every concern, enabling secure S3 access through Private Link, automating policy enforcement, and easing the move to containerized environments.

- **IAM Role Integration with Private Link:** Engineered a solution that securely accessed S3 buckets via Private Link by leveraging IAM roles, bypassing the limitation for native Private Link support.
- **Centralized Resource Management:** Recommended consolidating operations under a single S3 account to reduce complexity and streamline governance.
- **Containerized Deployment:** Transitioned MetaDefender Storage Security from EC2 to ECS/EKS, enabling elastic scaling and better resource efficiency.
- **Validated QA Environment:** Conducted rigorous testing in QA environment to ensure Private Link functionality and S3 compatibility.
- **Flexible Deployment Strategy:** Explored region- and account-specific configurations to meet future scalability demands.

Protecting Government Data Centers with Advanced File Security from OPSWAT

Customer: A Government Defense Agency in Southeast Asia

Region: Southeast Asia

Size: Confidential

Challenges

- **Stringent Security Requirements:** This project presented a unique chance to implement cutting-edge technologies. Any proposed technology would need to meet rigorous security standards and undergo extensive technical validation to ensure minimal operational disruption.
- **Limited Information Sharing:** The sensitive nature of the project made it difficult to provide detailed system specifications, requiring OPSWAT to adapt and prove its value with limited initial data.
- **Complex System Integration:** This new data center required seamless integration of advanced security solutions from the ground up, necessitating a careful, phased approach to maintain strict compliance standards.

Solutions

To address these challenges, OPSWAT implemented a multi-phase deployment strategy:

Phase 1: Establishing a Strong Foundation

- Deployed four MetaDefender Storage Security instances and 30 MetaDefender Core MSW8 instances to enable robust file processing and protection.
- Integrated a tailored antivirus solution (McAfee) to meet the organization's unique security needs.

Phase 2: Enhancing Threat Analysis Capabilities

- Expanded the deployment with eight additional MetaDefender Core instances to support increased security demands.
- Integrated four embedded sandbox solutions for advanced threat analysis, enhancing the organization's ability to detect and respond to sophisticated cyber threats.
- Throughout both phases, OPSWAT's security teams worked closely with the technology contractor, ensuring seamless implementation, ongoing support, and optimized security performance.

Getting Started with OPSWAT

Ready to secure your storage with MetaDefender Storage Security?

Reach out to OPSWAT experts or our channel partners to discuss your specific requirements and get a quote.

Leverage OPSWAT's professional services team for implementation planning, deployment assistance, and ongoing support.

Learn More

OPSWAT is here to help.

Contact us today to schedule a demo and learn how we can help you secure every file, everywhere.

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 1,900 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.