OPSWAT.

METADEFENDER™

Storage Security

NetApp Integration

OPSWAT.

As enterprises spread data across on-premises and cloud storage, file-borne malware remains a persistent threat to that infrastructure. Data can appear legitimate while hiding exploits that steal sensitive data or disrupt critical operations, even in otherwise well-secured environments.

MetaDefender™ Storage Security stops these threats at the point of storage, before they ever reach users or applications. Integrated directly into NetApp ONTAP, it inspects every file and neutralizes hidden threats in real time, preserving usability while ensuring only safe, verified data moves through your environment. The result: stronger protection across NetApp storage, less operational risk, and confidence that your data stays clean.

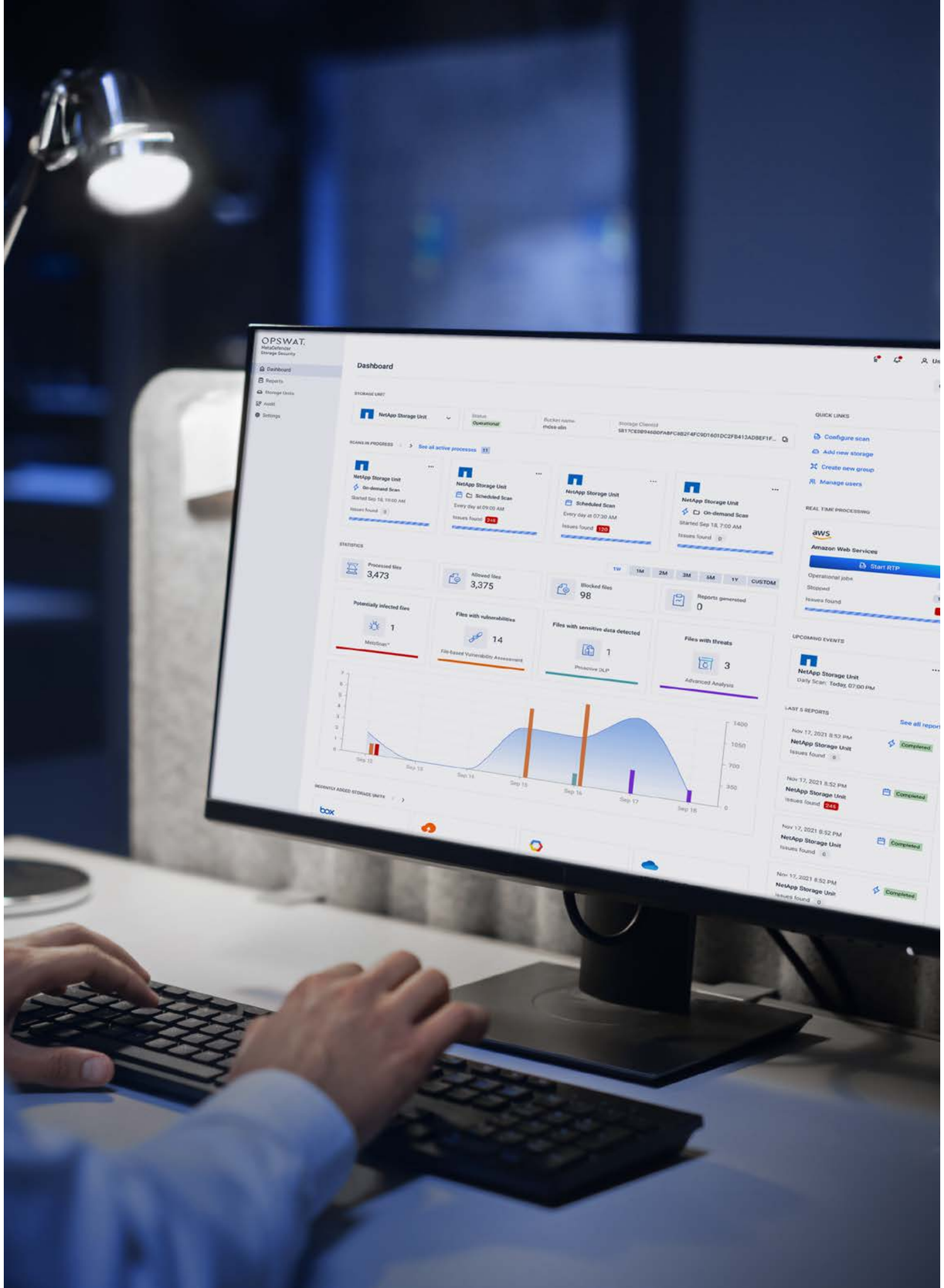


Table of Contents

01 Data Storage Challenges

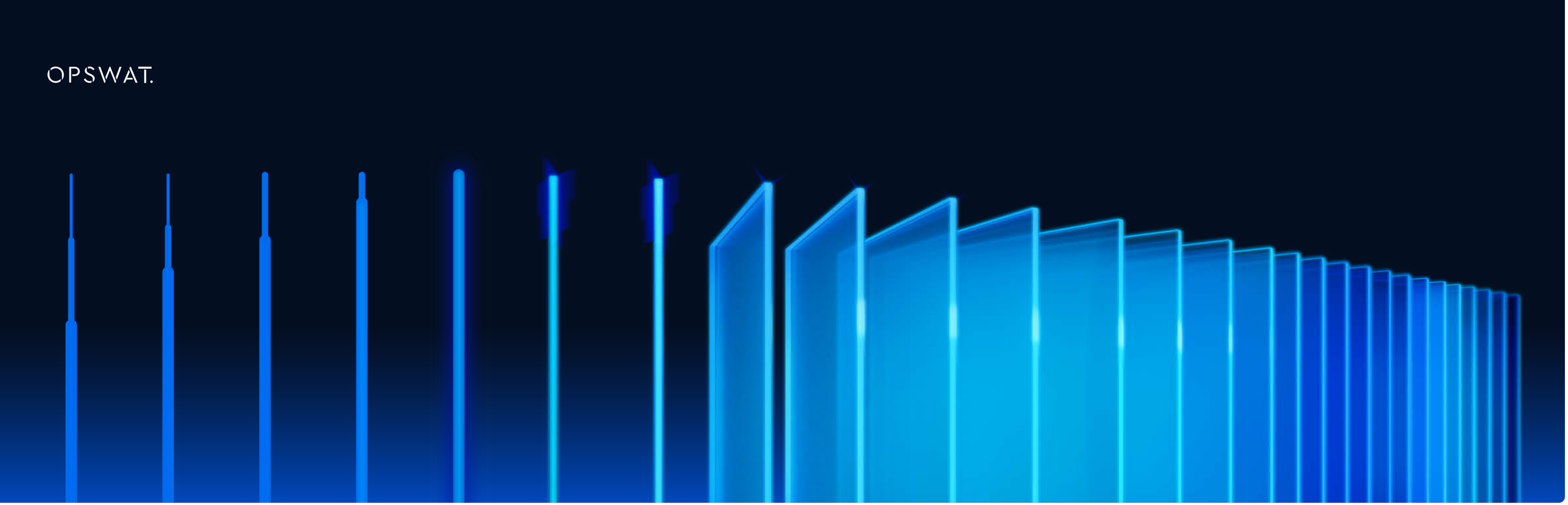
02 Secure Your NetApp Storage with MetaDefender Storage Security

03 Key Features

04 Integration with NetApp ONTAP

05 File Processing at Scale

06 All-in-One Portal



01

Data Storage Challenges

Traditional storage security strategies are struggling to keep pace with the sophistication of modern cyberthreats. Here are the most pressing challenges organizations face today.

Files as Attack Vectors

File-borne malware and ransomware are a persistent threat to storage environments. These can leverage known and unknown vulnerabilities, including zero-day exploits. File-based attacks based on productivity files are especially prevalent, since these files are broadly used, in large volumes, daily, by virtually all organizations. These files can deliver malware or ransomware via embedded macros, nested archives, images, or hyperlinks, and traditional, single-engine scanning cannot keep pace with the volume and sophistication of these evolving threats.

Data Breaches and Regulatory Compliance

Regulatory frameworks such as GDPR, HIPAA, PCI, or FINRA mandate strict data protection controls and impose significant penalties for non-compliance. Many legacy storage solutions lack the security and audit trails features needed to meet these requirements; a single data breach can trigger financial losses, reputational damage, and legal liability.

Scalability and SLAs

Enterprise file storage must scale to accommodate massive and rapidly fluctuating workloads. Usage spikes that are not handled properly can cause SLA violations, degrade system performance, and directly impact user productivity. Security scanning infrastructure must scale in parallel with storage, without becoming a bottleneck.

OPSWAT.

02

Secure Your NetApp Storage with MetaDefender Storage Security

Integrate MetaDefender Storage Security with your NetApp ONTAP instance to stop file-borne threats before they reach your data. The platform is powered by OPSWAT's proven suite of prevention-first technologies, including Metascan™ Multiscanning, Deep CDR™ Technology, Adaptive Sandbox, Vulnerability Assessment and Proactive DLP, delivering a single, easy-to-implement, storage security solution.

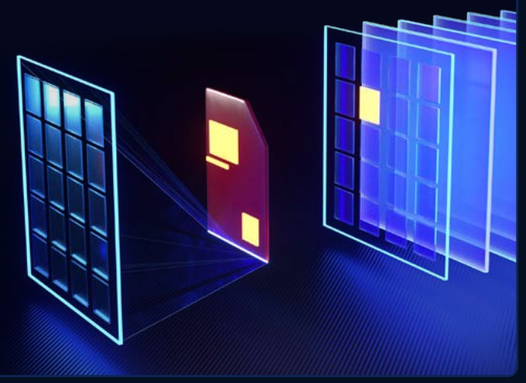
Proactive DLP™

The Proactive DLP technology helps organizations comply with data regulations by automatically redacting, removing, watermarking, or blocking sensitive and out-of-policy data in files. It supports PCI, HIPAA, Gramm-Leach-Bliley, FINRA, and others.



Metascan™ Multiscanning

Following industry best practices, Metascan Multiscanning uses 30+ anti-malware engines, to identify both known and unknown threats while reducing false positives and minimizing exposure time, achieving detection rates of +99.2%.



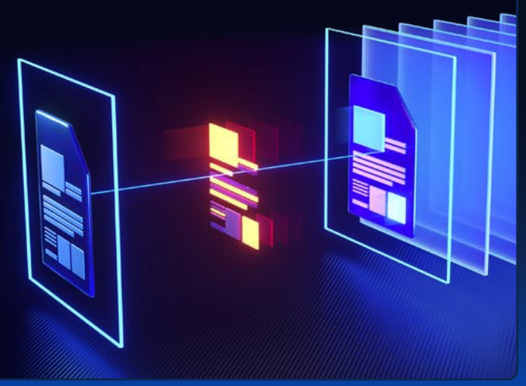
Adaptive Sandbox

Adaptive Sandbox is an emulation-based threat analysis technology that enables zero-day malware detection and extracts IOCs (Indicators of Compromise) for threat intelligence and incident response.



Deep CDR™

The Deep CDR technology disarms embedded threats from files. It does so by deconstructing files, removing active elements, then reconstructing them into a clean, usable version. Supports 200+ file types, including PDFs, nested archives, and Microsoft Office documents.



File-Based Vulnerability Assessment

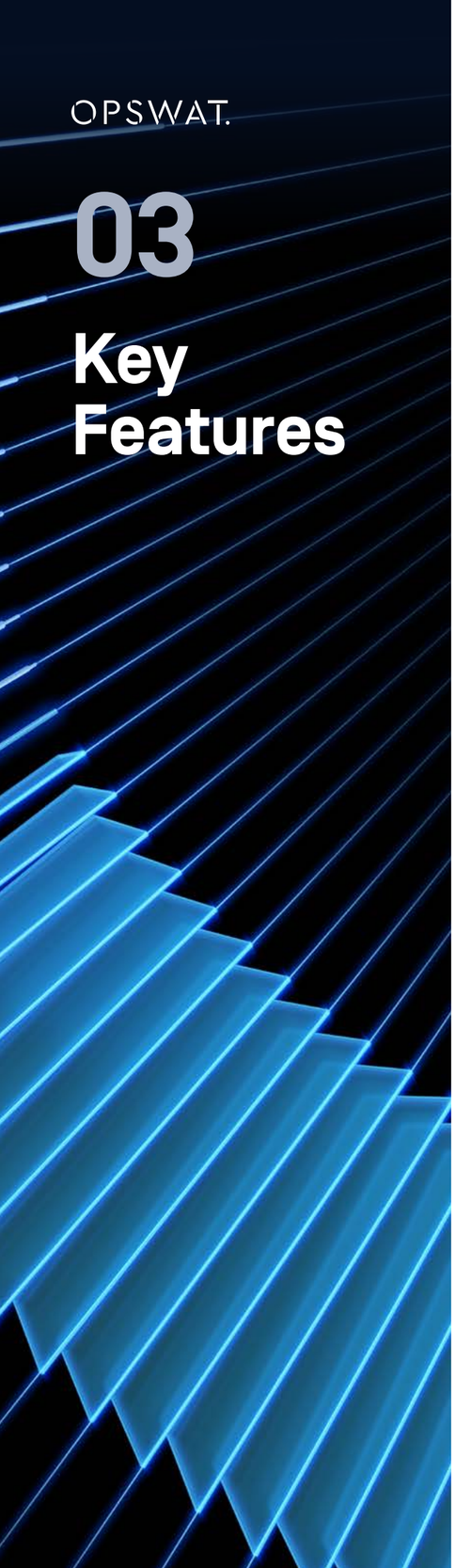
File-Based Vulnerability Assessment scans and analyzes binaries and installers to detect known application vulnerabilities before they are executed on endpoint devices.



OPSWAT.

03

Key Features



Advanced File Processing

MetaDefender Storage Security provides flexible scanning options tailored to your operational requirements:

- **Event-Based Handling:** scans are triggered when a file is written to the share (using NetApp's Vscan writes-only profile)
- **Polling Handling:** regular checks identify and scan new or modified files
- **On-Demand Scan** can be initiated immediately after configuration
- **Scheduled Scanning** automates scans at predetermined times

Automated Workflows

An automated security pipeline with five-stage processing covers the full lifecycle: Scan Configuration → Advanced Threats → Vulnerabilities → Sanitization → File Tagging. Build custom, automated file processing pipelines tailored to your organization's risk factor, without additional API development.

Cancel Scanning File

Cancel individual file scans while they are in progress, providing greater control over resource management and preventing unnecessary processing.

File Remediations

- Efficiently categorize file content and identify harmful files for investigation
- Define actions based on assigned tags such as "Allowed," "Sanitized," or "Blocked"
- Apply Deep CDR™ technology to sanitize files
- Automate file operations such as copying, moving, or deleting files based on scan results and predetermined conditions
- An optional "Delete empty folders after remediation" setting is available for SMB (Server Message Block), NFS (Network File System), and SFTP (SSH File Transfer Protocol) shares

SIEM Integration

Connect with SIEM (Security Information and Event Management) systems via an intuitive GUI (graphical user interface) and RESTful API, enabling swift integration into your established workflows.

Custom Scan Priority

Control scanning priority to match performance and throughput requirements, for each storage unit scan, allowing for tailored resource allocation.

Proactive Event Notifications

- Alert relevant teams when critical events occur
- Tailor notifications to your preferences and receive alerts for report generation, user registrations, and file blocking events
- Notify stakeholders when matters most; malware detections, blocked files, scan failures or policy violations in files

Snapshot-Based Resilience

For NetApp ONTAP deployments, MetaDefender Storage Security includes a snapshot feature that captures incremental backups of in-progress files every three seconds. This adds a resilience and failover layer to the ONTAP connector, ensuring data integrity is preserved in the event of unexpected failures during scanning.

Type-Based Storage Grouping

Combine object storage units or NAS (Network-Attached Storage) units into dedicated groups to ensure security workflows align precisely with the features and requirements of each storage integration.

04

Integration with NetApp ONTAP

Built-in Integration via Vscan

MetaDefender Storage Security integrates with NetApp ONTAP using Vscan — NetApp's built-in antivirus scanning framework. Vscan allows ONTAP storage systems to offload file scanning to external servers, enabling OPSWAT's security technologies to inspect every file written to your NetApp shares in real time.

The integration uses the SMB (Server Message Block) protocol — specifically SMB 3.1.1 — and requires the following components on a dedicated Windows Vscan Server:

- **NetApp ONTAP AV Connector:** manages communication between ONTAP and the external scanning server
- **OPSWAT ONTAP Connector:** receives file scan requests from the NetApp AV Connector and forwards them to MetaDefender Storage Security for processing

Scanning Modes Supported

MetaDefender Storage Security supports on-access scanning using the Vscan writes-only profile, which triggers scanning when new or modified files are closed. On-demand and scheduled scanning are available directly from the MetaDefender Storage Security interface.

Multiple SVM Support

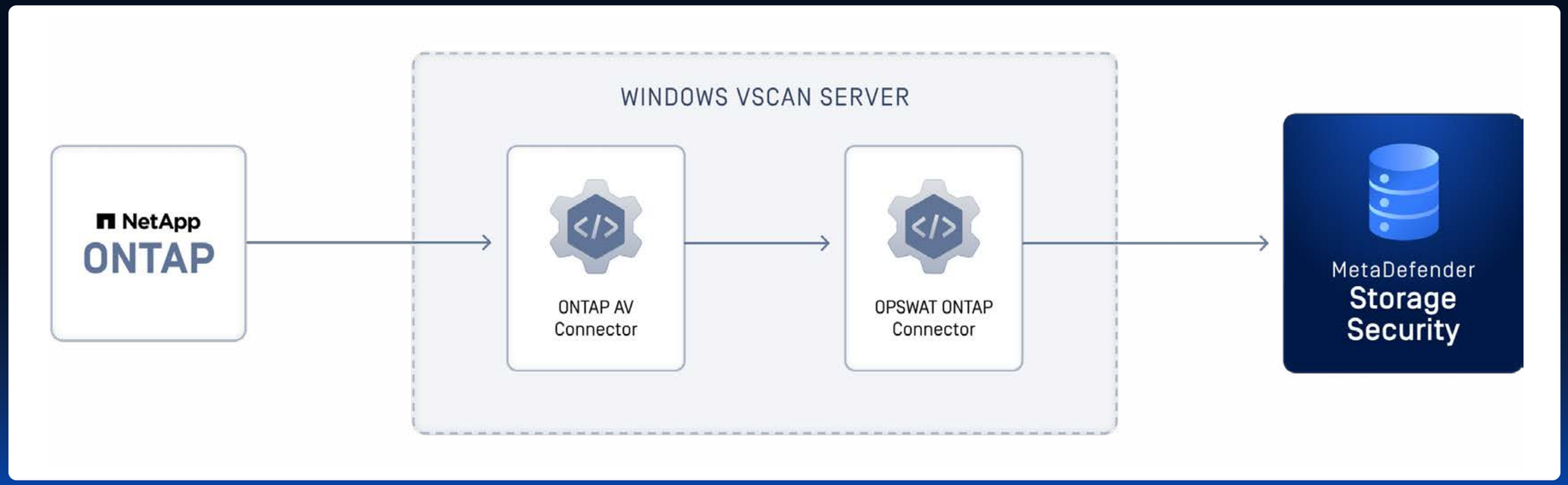
When Vscan is enabled, multiple SVMs (Storage Virtual Machines) can be connected to the same MetaDefender Storage Security instance. Each SVM is added as a separate storage unit, and the OPSWAT ONTAP Connector configuration is updated to include each SVM's details.

AWS FSx for NetApp ONTAP

MetaDefender Storage Security is fully compatible with AWS FSx for NetApp ONTAP, leveraging the same Vscan integration to scan files stored on FSxN volumes. The Windows Server running MetaDefender Storage Security must be a member of the same Active Directory domain as the FSxN SVM being scanned.

Additional Protocol Support

In addition to the Vscan-based ONTAP integration, MetaDefender Storage Security also supports SMB, NFS, and SFTP storage connections, allowing integration into diverse infrastructure environments regardless of specific deployment requirements.



OPSWAT.

05

File Processing at Scale

MetaDefender Storage Security scales as your organization's needs grow. Deployment can be sized up or down to meet your SLA requirements, delivering data security and operational resilience at enterprise scale.

For Vscan-based NetApp deployments, supported configurations include:

- **Small-scale (up to 20,000 files per hour, single SMB share)**: one Vscan Server handles scanning
- **Small-scale (up to 20,000 files per hour, multiple SMB shares)**: multiple SMB shares can connect to the same OPSWAT ONTAP Connector, or each share can connect to a separate MetaDefender Storage Security instance
- **Medium to large scale (20,000+ files per hour)**: multiple Vscan Servers can be configured for the same SMB share; files are distributed across servers using a round-robin method

Note: Throughput figures are derived from OPSWAT's sizing guide and are intended as guidelines, not performance guarantees. Actual throughput depends on file types, network configuration, and hardware specifications. For critical deployments, OPSWAT recommends site-specific benchmarking prior to production rollout.



06

All-in-One Portal

MetaDefender Storage Security delivers data security and data protection on a single unified platform — covering ransomware detection, zero-day attack protection, data loss prevention, and data compliance. From a centralized dashboard, security teams can monitor active scans, view scan reports, manage storage units, configure workflows, and respond to events. All without switching between tools.

MetaDefender Storage Security also integrates with MetaDefender™ Managed File Transfer (MFT) via API key authentication, supporting sec ure file movement and preserving user-to-user mapping for audit and compliance purposes; extending protection across transfer and storage workflows within the broader MetaDefender platform.

GET STARTED

See How MetaDefender Storage Security Works in Your Environment

Chat with an Expert 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 2,000 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.

©2026 OPSWAT Inc. All rights reserved. OPSWAT, Metascan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.