

OPSWAT.

MetaDefender Storage Security™ and MetaDefender Managed File Transfer™

Protect Your Data in Storage and in Transit

Today's organizations face a complex challenge: enabling the free flow of data across diverse on-premises and cloud environments, while maintaining a secure posture. While cloud providers offer robust security measures, the shared responsibility model means you play a crucial role in protecting your own data. File-borne malware threatens even the most secure environments.

To address this, OPSWAT is integrating MetaDefender Managed File Transfer with the powerful capabilities of MetaDefender Storage Security. Combining these solutions enables your organization to leverage leading technologies to safeguard your data, both at rest and in transit.

Table of Contents

- 01 The Evolving Threat to your Files
- 02 Secure and Streamlined File Security Lifecycle with OPSWAT Solutions
- 03 Enhanced Efficiency and Security with Integrated File Transfer
- 04 How OPSWAT Secures your Files
- 05 MetaDefender StorageSecurity + Managed File Transfer: Key Features
- 06 Solutions at a Glance

01

The Evolving Threat to your Files

File-borne attacks leverage both known and unknown exploits, including zero-day threats hidden within seemingly harmless productivity files like documents, spreadsheets, and images. Traditional security methods often struggle to keep up with these rapidly evolving threats.

The consequences of a data breach can be devastating, leading to financial loss, reputational damage, and legal repercussions. Regulations like GDPR, HIPAA, and NIST demand rigorous data protection measures, and failure to comply can result in significant fines. Unfortunately, traditional storage solutions often lack the robust security features and audit trails required to meet these standards.

Furthermore, relying on outdated and unmanaged file transfer solutions can create integration challenges, hindering workflow efficiency and potentially leading to compliance issues. This often results in the rise of “shadow IT” and unapproved workarounds, which further compromise both security and operational effectiveness.

02

Secure and Streamlined File Security Lifecycle with OPSWAT Solutions

Organizations that used to face challenges in securing files both at rest and in transit can now simplify secure file management and transfers within their storage environments thanks to the seamless integration of MetaDefender Storage Security and MetaDefender Managed File Transfer. This integration uses API key authentication for enhanced security and efficiency.

Benefits

Confidently share files within your organization and with external partners, knowing that all transfers are protected.

Streamline data security management and automate file storage remediation tasks in hybrid environments.

Meet regulatory requirements for data privacy and industry standards, including GDPR, PCI, and HIPAA.

Securely back up and transfer data between platforms during system upgrades or migrations.

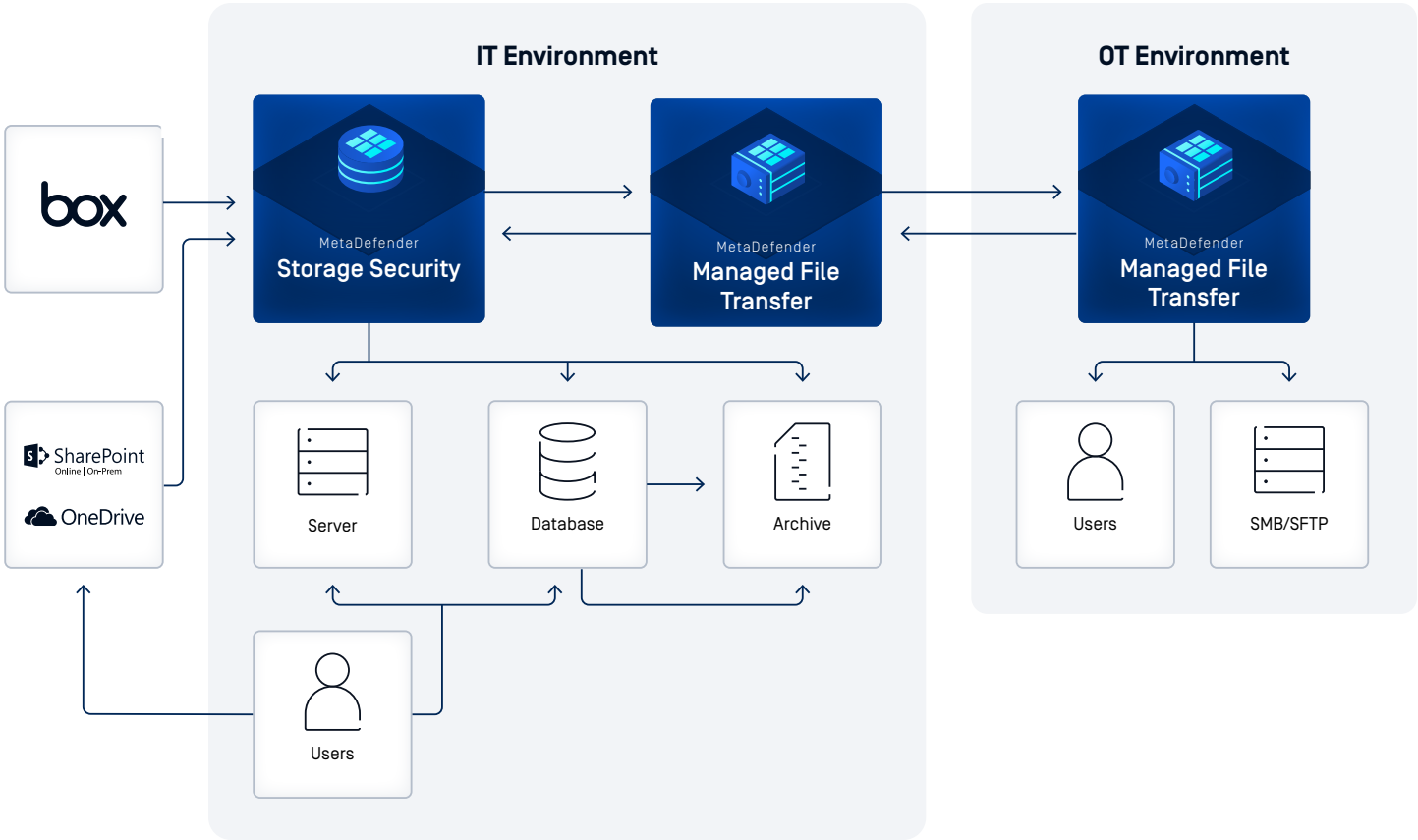
How it Works

MetaDefender Storage Security secures files shared from collaboration platforms such as Box, SharePoint, and OneDrive. Files are scanned, processed, and remediated for malware, sophisticated threats, or compliance violations. This process maintains detailed user-to-user mapping information, allowing you to:

- Monitor who uploaded a file, who it was shared with, and when.
- Easily provide audit trails and reports to prove adherence to data protection regulations.
- Rapidly identify the source of potential security breaches.
- Gain valuable insights into user activity and file access patterns.

Files are then processed through MetaDefender Managed File Transfer, ensuring secure manual and automated transfers across users, collaboration platforms, and networks with approval workflows, role-based access control, and audit logging for regulatory compliance.

This integration provides a comprehensive solution for secure file transfer and storage, maintaining operational integrity and ensuring your data remains protected throughout its lifecycle.



03

Enhanced Efficiency and Security with Integrated File Transfer

MetaDefender Storage Security integration with Managed File Transfer enforces end-to-end encryption, threat prevention, and compliance while ensuring data integrity. Automated policy-driven file transfers enhance operational efficiency. Granular access controls and secure folder and file sharing enable collaboration across networks.

Automated Workflows

Once files are transferred to MetaDefender Storage Security, administrators can configure automated remediation actions such as:



Adding informative tags about the processing each file underwent.



Sanitizing and regenerating files into new, safe-to-use versions.



Moving, copying, or deleting files based on your configurations and file status [e.g., blocked or sanitized].

Multi-Layered Data Protection

Manage your file security and security processes with OPSWAT's MetaDefender ecosystem. MetaDefender Storage Security provides comprehensive data protection, including ransomware detection, zero-day attack prevention, data loss prevention, and compliance tools. MetaDefender Managed File Transfer offers granular access controls, as well as secure folder and file sharing, enabling collaboration across users and networks.

Reports and Audit Trails

The MetaDefender Storage Security dashboard provides detailed information about blocked files, vulnerabilities, and compliance violations. It also generates in-depth scan reports and seamlessly integrates with your existing SIEM solutions for a unified security monitoring experience. The integration with MetaDefender Managed File Transfer also provides granular access control, supervisory approvals, and audit trails to ensure regulatory compliance.

04

How OPSWAT Secures your Files

Integrating MetaDefender Storage Security and MetaDefender Managed File Transfer gives you access to OPSWAT's powerful suite of MetaDefender Core™ technologies, providing comprehensive protection for your data both in transit and at rest. This easy-to-implement solution combines multiple layers of defense to safeguard your valuable information.

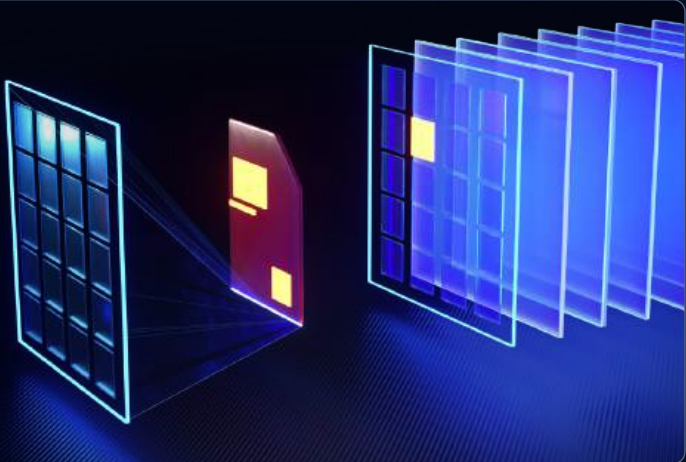
Proactive DLP™

Safeguard sensitive data and meet compliance requirements. Proactive DLP uses AI and machine learning to automatically redact, remove, watermarks, or block sensitive data within files, helping you comply with regulations like PCI, HIPAA, and more.



MetaScan™ Multiscanning

Go beyond single-engine scanning. OPSWAT Multiscanning analyzes every file with over 30 commercial antivirus engines, achieving near-perfect detection rates and maximizing your protection against known threats.



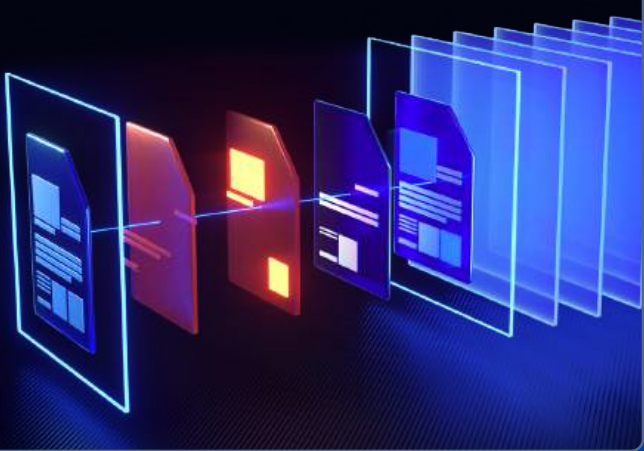
Adaptive Sandbox

Detect and analyze zero-day malware in a safe environment. Adaptive Sandbox uses advanced emulation-based technology to identify threats and extract valuable threat intelligence. It operates with 10x greater speed and 100x greater efficiency than traditional sandboxes.



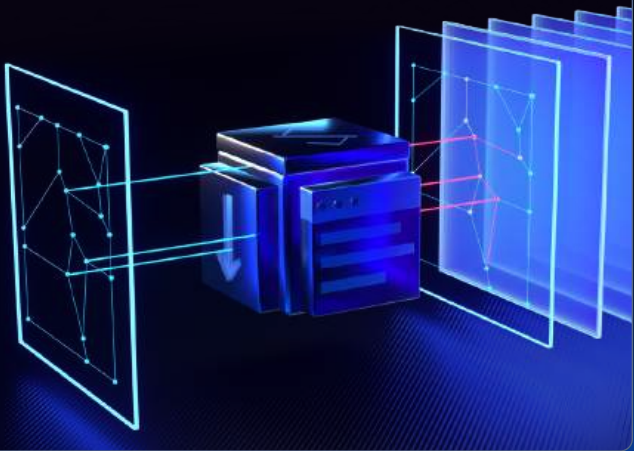
Deep CDR™

Neutralize advanced threats hidden within files. Deep CDR disarms active embedded threats and reconstructs files to prevent zero-day attacks and evasive malware. This technology supports over 180 file types and is certified 100% accurate by SE Labs.



Vulnerability Assessment

Identify vulnerabilities in software before they can be exploited. File-Based Vulnerability Assessment scans and analyzes binaries and installers to detect known application vulnerabilities, preventing them from reaching your endpoints.



MetaDefender StorageSecurity + Managed File Transfer: Key Features

Outbreak
Prevention with
Advanced
File Processing

- **Real-time Scanning:** Ensure files are processed as soon as they are uploaded. Real-time scanning supports polling & event-based handling types for file discovery.
- **Scheduled Scanning:** Automatically check your files or storage for zero-day threats or vulnerabilities at a predetermined timeand frequency.

Automated File
Remediations

- **File Tagging for Transferred Files:** Apply transfer conditions individually to each MetaDefender Managed File Transfer destination and enable detailed filtering to ensure that only files meeting your organization's criteria are transferred.
- **File Tagging for Stored Files:** Add information about file processing as tags ["Allowed," "Sanitized," or "Blocked"] for further analysis and forensics.
- **File Remediations:** Combine MetaScan Multiscanning, Deep CDR, vulnerability assessments and other remediation actions [copy, encrypt, move, delete] to tailor remediation workflows.

Comprehensive
Compliance
& Reporting

- **Regulatory Adherence** – Ensure compliance with industry standards such as GDPR, PCI DSS, HIPAA, and NIST through built-in security policies and encryption.
- **User Behavior Insights** – Gain visibility into file access patterns and detect potential security risks.
- **Granular Audit Trails** – Maintain detailed logs of system events and file lifecycles, including who uploads, shares, and accesses each file.

Integration and
Deployments

- **Easy Deployment:** Setup in minutes with a step-by-step installer.
- **Diverse Integrations:** Integrate with multiple storage repositories, such as Amazon S3, Microsoft Azure Blob Storage, NetApp, Cloudian, Dell EMC ECS, SharePoint, Box, and any S3 or SMB/NFS/SFTP-compatible storage or folders.
- **Restful API:** Integrate with SIEM systems seamlessly, customize integrations with productivity tools and automate secure file transfers.

Authentication
and Access
Control Management

- **API Key Authentication:** Ensure that only authorized systems and users can initiate file transfers using API keys, adding an extra layer of protection to your data.
- **Secure Manual & Automated Transfers:** Enforce approval workflows and role-based access controls (RBAC) to protect file exchanges across users, networks, and collaboration platforms.
- **Shared Spaces:** Upload files and collaborate among group members within a shared workspace.

Proactive Event
Notifications

- **Real-time Event Alerts** – Receive notifications for critical security events such as blocked files, compliance violations, and unauthorized access attempts.
- **Customizable Settings:** Tailor notifications to your preferences and ensure the right teams are informed.

06


Solutions at a Glance

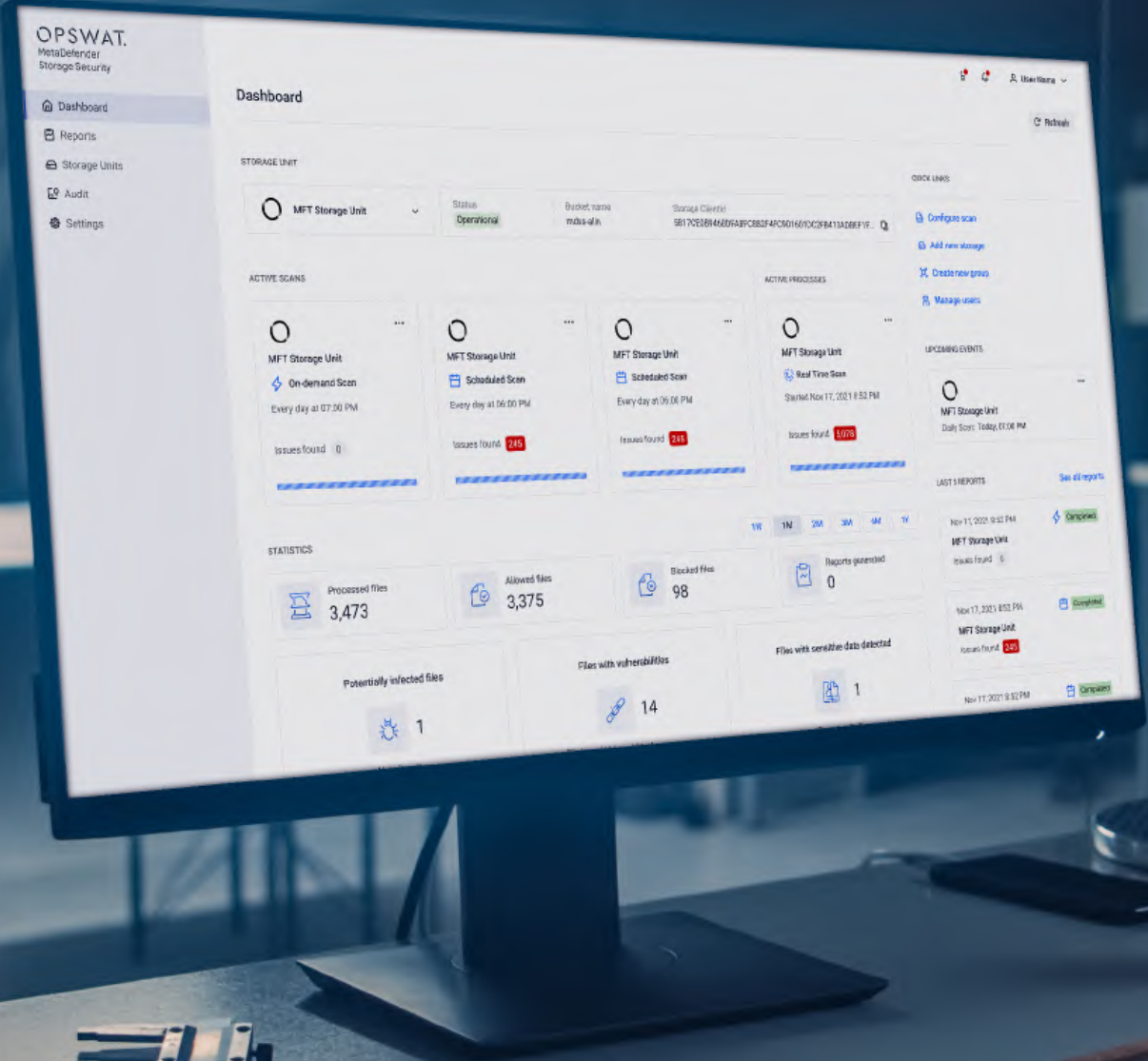
Solution	MetaDefender Storage Security™ Secure your data at rest.	MetaDefender Managed File Transfer™ Secure your file transfers.
Strengths	<ul style="list-style-type: none">• Excels with stationary datasets in enterprise storage systems• Seamless integration through APIs and robust scalability in cloud environments (especially Kubernetes)	<ul style="list-style-type: none">• Ideal for organizations with high file transfer volumes and security requirements
Key Features	<ul style="list-style-type: none">• MetaScan™ Multiscanning• Deep CDR™• Proactive DLP™• Vulnerability Assessment• Integration with storage solutions• Centralized control	<ul style="list-style-type: none">• MetaScan™ Multiscanning• Deep CDR™• Adaptive Sandbox• Vulnerability Assessment• Secure and automated workflows• Centralized control
Use Cases	<ul style="list-style-type: none">• Protecting sensitive data in storage• Preventing the spread of malware• Aiding data regulation compliance	<ul style="list-style-type: none">• Secure collaboration• Automated file transfers• Protecting data in transit• Seamless data flow across SMB, SFTP & SharePoint Online• End-to-end encryption in data in transit & at rest
Deployments	<ul style="list-style-type: none">• Integrated with storage solutions <div></div>	<ul style="list-style-type: none">• Standalone or integrated with existing infrastructure

MetaDefender Storage Security™
Secure your data at rest.



MetaDefender Managed File Transfer™
Secure your file transfers.





A Powerful Pairing for Maximum File Security

The combined capabilities of MetaDefender Storage Security and MetaDefender Managed File Transfer ensure your files are secure in transit and at rest with a defense-in-depth security strategy. This multi-layered approach, combined with powerful proprietary OPSWAT technologies, ensures your data remains secure throughout its entire lifecycle, whether it's being stored, shared, or transferred.

GET STARTED

Are you ready to put the MetaDefender Platform 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.