OPSWAT.

METADEFENDER™

Storage Security

SharePoint Integration

Scan, sanitize, and protect your SharePoint libraries, including existing content and new uploads.

OPSWAT.

SharePoint is where files come to rest. Much of that content arrived before current policies existed, and no one has gone back to inspect it under current standards. MetaDefender™ Storage Security scans both existing and newly uploaded content and applies current security policies across your SharePoint environment. Each deployment uses its own authentication and connectivity path. A single, unified interface manages file handling policies and embeds file security directly into your SharePoint libraries.

Table of Contents

01

Key Challenges

Files from Uncontrolled Sources

Authorized users can upload files into SharePoint libraries, from multiple devices and locations. Every file becomes an entry point for malicious content which can spread across entire libraries.

Compliance-Driven Scanning

Regulated industries need to document and audit their file scanning policies to meet compliance frameworks.

Libraries Outside Default Scope

Unless addressed during initial setup, some document libraries are not scanned by default, creating visibility gaps.

Ransomware Propagation

File-driven ransomware can spread rapidly across teams and devices thanks to SharePoint's real-time sync and sharing feature.

Lateral Movement via Infected Files

Attackers can take advantage of SharePoint’s collaboration features to move between systems via infected files.

Files Inherited from Teams Channel

Files shared on Teams are stored on that team's SharePoint site, located in the Documents library, in a folder named after the channel. Users mistakenly view Teams as a separate problem for later, when it is the same content, carrying the same risks.

02

Bringing Multi-Layered Storage Security into SharePoint

MetaDefender Storage Security is designed to protect data at rest across on-premises, hybrid, and cloud environments. Key technologies, delivered through OPSWAT's MetaDefender™ Core, and key capabilities, include:

Metascan™ Multiscanning

The Multiscanning Technology runs files against 30+ anti-malware engines, achieving close to 100% detection rates, 99.4% to be precise.

Deep CDR™

The Deep CDR Technology disarms and regenerates files, so only safe, clean and useable content reaches your systems; effective against evasive malware and zero-days.

Proactive DLP™

With Proactive DLP, MetaDefender Storage Security identifies payment, health, and personal data in files, supporting compliance through data visibility.

Adaptive Sandbox

The Adaptive Sandbox enables zero-day malware detection and extracts IOCs with its advanced, emulation-based approach.

Vulnerability Assessment

Scan and analyze binaries and installers to detect known application vulnerabilities before they execute.

File Type Verification

Detects true file types and blocks mismatched extensions, stopping disguised, malicious files from entering your organization.

Version History Scans

Since version history is typically outside the scope of security scans, it often survives incident cleanup. MetaDefender Storage Security scans file versions, showing both the total version count and whether any are blocked.

(Available for SharePoint On-Prem only)

Autodiscovery

Autodiscovery automatically finds and adds SharePoint Online sites, eliminating the need to enter site URLs manually. It can also be enabled for existing deployments, making it easy to bring newly created sites under protection. For tenants with hundreds of sites, this saves significant admin time.

Note: Storage Security does not perform file analysis itself; files are passed to OPSWAT's MetaDefender Core for scanning. Adaptive Sandbox, Proactive DLP, and Vulnerability Assessment require the corresponding engine package to be licensed in your MetaDefender Core deployment; availability depends on your license.

What Happens with Flagged Files

Actions can be configured per verdict: keep, copy, move, delete, or sanitize with Deep CDR sanitization. The options are set/verdict, up to five destinations. When Replace Original is enabled, the sanitized file overwrites the original. Users simply open the document from its usual location, without changing how they work.

03

Deployment Models and Integration Requirements

SharePoint Online

- Supported via Microsoft Graph API, using an app registration in Microsoft Entra ID (Azure Portal).
- Compatible with commercial and standard GCC (Government Community Cloud) environments.
- GCC High and DoD environments are supported via a dedicated configuration option.

Required credentials

- Tenant ID — from Microsoft Entra ID overview
- Client ID — Application ID from app registration
- Client Secret — generated under Certificates & Secrets; must remain valid for the duration of use

Required API permissions (Microsoft Graph, Application type)

- Files.ReadWrite.All
- Sites.Read.All

Admin consent must be granted for both permissions in the Azure Portal.

SharePoint On-Premises

- Supported via domain credential authentication.
- Available exclusively on Windows deployments of MetaDefender Storage Security.

Required credentials

- Site URL
- Domain and username in DOMAIN/USERNAME format
- Password for the configured account

Required permissions

- The configured account must have at minimum Contribute permissions on the target site

Deployment requirement

- MetaDefender Storage Security must be deployed on Windows

04

Configuration Workflow

SharePoint Online

Navigate to Storage Units, select **Add Storage** Unit, and choose **SharePoint**. Provide the following:

1. Account name and storage unit name
2. GCC High/DoD flag — enable only for Microsoft 365 GCC High or DoD environments; leave unchecked otherwise
3. Tenant ID, Client ID, and Client Secret
4. Site URL
5. Document Library (optional)
6. Folder Location (optional — only available after a Document Library is specified)
7. Select Continue — valid credentials create the storage unit; invalid credentials return an error message

Note on temporary files: When a file upload takes more than a few seconds, SharePoint creates a temporary zero-byte file with the same name. MetaDefender Storage Security discovers and lists this file by default. Once the upload completes, the actual file is discovered and processed. To skip discovery of empty files, refer to the How to Handle Empty Objects in Discovery page in the OPSWAT documentation.

SharePoint Online Autodiscovery

Automatically discover and add all SharePoint Online sites during setup, without configuring each Site URL individually. Choose between automatic discovery of all sites or manual selection of specific sites. Autodiscovery can also be enabled for existing storage units.

SharePoint On-Premises

Add a new storage unit and select **SharePoint On-Premises**. Provide the following:

1. Storage unit name
2. Site URL
3. Domain and username in DOMAIN/USERNAME format, and password
4. Document Library (optional)
5. Folder Location (optional — only available after a Document Library is specified)
6. Scan all subsites (optional — see Scanning Scope)

05

Scanning Scope and Configuration Options

MetaDefender Storage Security supports ad hoc, scheduled, and real-time scanning, allowing you to scan files on demand, at recurring intervals, or automatically as new and modified files are detected.

For SharePoint Online, your MetaDefender Storage Security instance must be publicly accessible over HTTPS with a valid TLS certificate to receive Microsoft file event notifications.

Option	Status	Behavior
Site URL	REQUIRED	Defines the target SharePoint site. When no document library is specified, all public document libraries within the site are processed.
Document Library	OPTIONAL	Restricts processing to a single named library within the configured site.
Folder Location	OPTIONAL	Restricts processing to a specific folder within the configured document library. Requires a document library value to be entered first.
Scan all subsites	ON-PREM ONLY	When enabled, processes files from all document libraries across the full subsite hierarchy. Applies only when no document library is specified; specifying a library overrides this setting.

06

Operational Considerations

01 Authentication for SharePoint Online

The Client Secret must remain active for as long as the integration is in use. An expired secret will break the connection.

02 Authentication for SharePoint On-Premises

The configured account must maintain at least Contribute permissions on the target site for the integration to remain functional.

03 Throttling for SharePoint On-Premises

SharePoint Server limits the number of concurrent requests per user. Remediation actions against large file sets will cause operations to queue until the server frees resources, resulting in extended processing times.

MetaDefender Storage Security includes configurable error handling and retry mechanisms for this scenario. Refer to the Configuring Error Handling and Retry Mechanisms for SharePoint On-Premise page in the OPSWAT documentation for configuration details.

04 GCC High/DoD for SharePoint Online

Enable the Azure Government (GCC High/DoD) option only for organizations using Microsoft 365 GCC High or DoD environments. Leave unchecked for commercial or standard GCC environments.

Note: Document libraries whose display name differs from their URL name do not receive event notifications; real-time scanning is not supported for those libraries.

Real-time scanning, meaning files are processed automatically as they're added or modified, is available for SharePoint Online only. SharePoint On-Premises relies on on-demand and scheduled scans.

Bring File Security into Your SharePoint Environment.

SharePoint Online
Scan a SharePoint site through MetaDefender Cloud and get visibility into the files, threats, and sensitive data stored in your environment.

SharePoint On-Premises
Chat with an Expert

Windows deployment required. Contact Sales to discuss deployment requirements and licensing.

opswat.com/get-started
sales@opswat.com

Review the official OPSWAT documentation to configure MetaDefender Storage Security for:

SharePoint Online
SharePoint On-Premises

OPSWAT.

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.