OPSWAT.

METADEFENDER CORE™

Platform Guide

OPSWAT.

Table of Contents

01

Getting Started

MetaDefender Core provides advanced threat prevention and file security capabilities designed for organizations that require strict control over file-based workflows across IT, OT, and air-gapped environments. It enables organizations to sanitize, scan, analyze, and govern every file that enters, exits, or moves within their environment, whether from a public-facing portal, internal transfer, or third-party source.

MetaDefender Core is designed to:

- Detect known and unknown threats using MetaScan™ Multiscanning with 30+ anti-malware engines, as well as heuristics and machine learning
- Neutralize embedded threats with Deep CDR™
- Enforce data loss prevention and content compliance through file-level inspection with Proactive DLP™
- Analyze and enrich file intelligence using Adaptive Sandbox, Threat Intelligence, and File-Based Vulnerability Assessment
- Integrate easily via REST API with portals, file shares, email systems, and DevOps pipelines

The platform is modular. You can start with core file analysis capabilities and scale up with additional modules for advanced detection, prevention, and analysis based on your use case and risk profile.

02

Understanding MetaDefender Instances

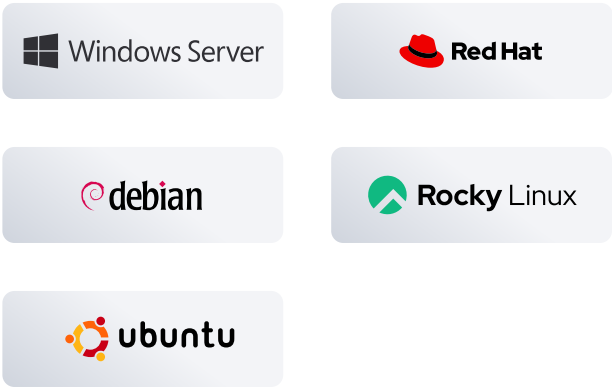
A MetaDefender Instance refers to a single deployment of the MetaDefender Core application running on an operating system. Each instance can be installed across diverse environments, including bare metal servers, VMs (virtual machines), workstations, tablets, or Docker containers.

Once activated with a MetaDefender Core license, that deployment is considered a licensed instance. Whether it's used standalone or as part of a larger distributed architecture, each activated system requires its own license.

MetaDefender Core is licensed per instance and offered as an annual subscription. This flexible model supports everything from single-use deployments to large-scale, multi-instance configurations across global infrastructure.

03

Select an OS for MetaDefender Integration



04

Start with the MetaDefender Platform

File Analysis

- True file type verification – Verify thousands of file types.
- Archive Extraction – Archive scanning for over 30 types of compressed files.
- Custom Workflow Configuration - Create multiple workflows to handle different security policies.
- Reputation Check - Remediate false positives faster with file hash matching against a huge database.

Integration and Scalability

- Integration available via REST API.
- External Scanner – Integrate with your own analysis tools.
- Offline & Automated deployment and templates for Autoscaling.
- Docker container support.

Administration

- Integration with SSO, OpenID Connect, LDAP, Active Directory.
- Define custom roles and profiles for users/groups.
- Supports multi-tenant environments.
- Containerized configuration and monitoring via My OPSWAT™ Central Management.

05

Add Detection Modules

Simply add modules and choose which ones to implement based on your needs.

MODULE 1

MetaScan Multiscanning

Select a MetaScan package on Windows or Linux.

MetaScan Package		
MAX - Over 30 Engines	✓	
20 Engines	✓	
16 Engines	✓	
12 Engines	✓	
10 Engines		✓
8 Engines	✓	
5 Engines		✓
Custom Engines*	✓	✓

[*] Custom engines can be added to any package except MAX, which includes all available engines.

MODULE 2

File-Based Vulnerability Assessment

- Detect known vulnerabilities in binaries with over 3M hashes covering over 20,000 products.
- Support for applications, patches, IoT Software, firmware, and installers.

MODULE 3

Software Bill of Materials

- Generate SBOMs and quickly find vulnerabilities in source code and containers.
- Supports 10+ languages including Java, JavaScript, Go, PHP, and Python, and over 5M third-party open-source software components.

MODULE 4

Country of Origin

- Identify file origin and vendor to block high risk files, enforce regional policies, and strengthen software supply chain defenses.
- Detects file provenance and vendor identity using static inspection and certificate validation.

06

Choose Prevention Modules

MODULE 1

Deep CDR

- Remove potential threats and regenerate 200+ common file types including PDF, Microsoft Office, HTML, and many image files.
- Verify thousands of file types using AI to combat spoofed file attacks and detect complex files posing as simpler ones.
- Customize file processing workflow for different file entry points for fast scanning and regeneration of safe-to-use files in milliseconds, without affecting performance.
- Access detailed reports with sanitized objects and their embedded scripts.

MODULE 2

Proactive DLP

- Detect and redact sensitive information, including PII, PHI, DICOM, etc.
- Aid compliance with data regulations and industry-standard security requirements such as PCI DSS, HIPAA, Gramm-Leach-Bliley, FINRA and more.
- Locate and classify unstructured text into predefined categories with machine-learning powered AI.
- Establish custom policies to meet specific requirements.

07

Choose from Advanced Analysis Module Options

MODULE 1

Threat Intelligence

- Analyze and detect both known and unknown threats while gaining real-time insights into emerging threats.
- Use Pattern and Similarity Search to hunt threats.
- Access billions of hashes through Reputation API.

MODULE 2

Adaptive Sandbox

- Conduct threat-agnostic analyses of files and URLs using Adaptive Sandbox technology.
- Focus on identifying actionable IOCs (indicators of compromise) for incident response.
- Detect targeted attacks bypassing anti-analysis tricks (e.g. geofencing).

08

Choose from OPSWAT Support Options

View Plan Details

	Silver	Gold	Platinum	Managed Service
Case via My OPSWAT	12 hours (business days)	24 hours (business days)	24 hours (7 days per week)	24 hours (7 days per week)
Via AI Chatbot	24 hours (7 days per week)	24 hours (7 days per week)	24 hours (7 days per week)	24 hours (7 days per week)
Via Live Agent Chat	Not included	24 hours (business days)	24 hours (business days)	24 hours (business days)
Via Phone	Not included	Not included	24 hours (7 days per week)	24 hours (7 days per week)
Blocker Severity (S1 & S2)	Within 4 hours	Within 2 hours	Within 1 hours	Within 1 hours
Lower Severity (S3 & S4)	Within 1 business day	Within 8 business hours	Within 4 business hours	Within 4 business hours

Are you ready to put OPSWAT 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

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

OPSWAT.
Protecting the World's Critical Infrastructure