OPSWAT.

MetaDefender Core™

Advanced Threat Protection for Trusted File Workflows

Protecting the World's Critical Infrastructure

Overview

With the growing threat of sophisticated, multi-layered, and zero-day attacks, businesses can no longer rely solely on detection-based cybersecurity systems to provide adequate protection for their most valuable business assets. Enterprises need to take more comprehensive and preventive approaches to combat advanced file-borne attacks.

MetaDefender Core integrates advanced threat detection and prevention capabilities into your existing IT solutions and infrastructure to handle common attack vectors by securing web portals from malicious file attacks, augmenting cybersecurity products, and developing malware analysis systems that adhere to company-specific policies.

OPSWAT.

Key Features

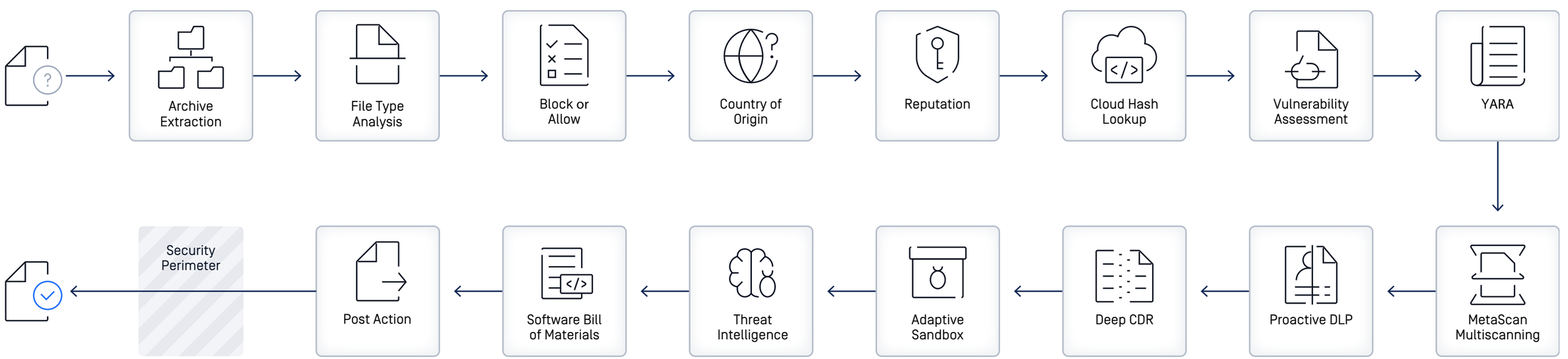
Deep File Sanitization	Recursively sanitizes over 200 file types using Deep CDR™ technology. Removes embedded potential threats such as scripts, macros, and out-of-policy content. Regenerates safe and usable files to prevent zero-day attacks without disrupting workflows.
Multiple Anti-Malware Engines	Detects over 99% of malware using MetaScan™ Multiscanning leveraging 30+ leading anti-malware engines. It combines signatures, heuristic analysis, and machine learning for comprehensive protection.
File Type Verification	Leverages AI to identify true file type based on its content rather than extensions to effectively prevent spoofing and evasive threats.
Recursive Archive Extraction	Scans more than 30 types of compressed files. Supports encrypted archives with configurable extraction options.
File-Based Vulnerability Assessment	Analyzes and assesses known file and application vulnerabilities before they are executed on endpoint devices, including IoT devices.
Adaptive Threat Analysis	Uses emulation-based sandbox technology to detect IOCs (indicators of compromise) in files and URLs. Provides threat agnostic insights that support effective incident response.

Dynamic Threat Intelligence	Detects and responds to evasive file-based threats including zero-day attacks using AI driven analysis, adaptive sandboxing, and real time threat intelligence.
Sensitive Data Protection	Removes, redacts, or watermarks sensitive data in files before they enter or leave your network using Proactive DLP™. Detects adult content in images and offensive language in text using machine learning, computer vision, and AI.
Country & Vendor Detection	Country of Origin detection identifes file origin and vendor by analyzing digital fingerprints and metadata. Flags files from restricted regions and untrusted sources.
SBOM Generation	Generates SBOMs (Sofware Bills of Materials) and quickly finds vulnerabilities in source code and containers.
Blocked File Quarantine	Holds blocked files in a secure environment to enable further investigation and analysis.
Executive Dashboard	Delivers high-level system insights with downloadable reports and continuous health monitoring.
Custom Workflow Rule	Allows administrators to define and manage file handling policies based on organizational security requirements.
Tailored File Submission	Accepts files through multiple input methods including direct upload, URL, and file path for file scanning.
SIEM Support (Audit Log Reports)	Provides detailed scan logging with manual and scheduled options. Supports syslog format for integration with SIEM platforms.
Flexible Integration	Offers both synchronous and asynchronous API options for seamless integration with existing tools and workflows.

OPSWAT.

Custom File Processing Workflow

- Analyze 10 files per second, per deployment
- Customize multiple workflows based on file security policies
- Pick and choose features without further API integration



OPSWAT.

Use Cases

1

Protect File Uploads from Threats and Compliance Risks

MetaDefender Core helps organizations secure any file upload workflow, whether from customers, partners, or third-party vendors. By automatically scanning and sanitizing files before they enter your environment, it eliminates threats like ransomware, embedded malware, and disguised executables. Organizations can confidently accept uploaded files through web portals, partner integrations, and internal systems without compromising security or regulatory compliance.

2

Sanitize Email Attachments Before They Reach Users

Files shared via email remain one of the most common and exploited threat vectors. MetaDefender Core strengthens your email defenses by removing embedded threats from inbound attachments and enforcing data protection policies on outbound content. Clean files are delivered in real time, supporting uninterrupted business communications while reducing the risk of malware infection or data leakage.

3

Ensure Safe Downloads from External Sources

Files downloaded from the internet, email links, or cloud storage often bypass traditional security controls. MetaDefender Core scans and sanitizes downloaded files before they're opened, stopping ransomware, trojans, and zero-day attacks before impact. Its MetaScan Multiscanning engine delivers high-accuracy malware detection, while Adaptive Sandbox reveals evasive behavior in suspicious files. Dynamic Threat Intelligence is enriched with sandbox-derived IOCs and ML-powered similarity scoring, combining behavioral analysis, file reputation, and global threat feeds. This approach delivers safer, compliant file access without delaying business workflows.

4

Secure File Transfers Across Internal and External Networks

Files moving between departments, branches, or segmented networks (such as IT and OT) can transmit malware across trusted zones, including air-gapped environments. MetaDefender Core ensures that all transferred files are clean, trusted, and policy-compliant before reaching critical systems. It reduces the risk of internal malware propagation and supports secure collaboration across complex infrastructures.

5

Accelerate Malware Triage and Response for Security Teams

Security analysts often spend valuable time investigating suspicious files with limited visibility. MetaDefender Core simplifies malware triage by delivering fast, accurate insights into file-based threats without relying on single-point detection. By streamlining analysis and providing actionable threat context, security teams can resolve alerts faster and improve detection fidelity across the SOC.

6

Prevent Data Leaks with File-Level Content Control

Files often carry more risk than their appearance suggests, especially when they contain sensitive data. MetaDefender Core helps prevent data loss by inspecting and redacting sensitive information before files are shared externally or stored in regulated environments using Proactive DLP. This supports compliance with data protection standards while reducing the operational burden on security and compliance teams.

OPSWAT.

Deployment Flexibility

DEPLOYMENT OPTION	BEST FOR
On-Premises	Environments with predictable file volumes and centralized operations.
Cloud	Teams looking for managed infrastructure and easy integration with cloud-based solutions.
Cloud Image	Pre-configured template to launch MetaDefender Core instance in the cloud including AWS, Azure, and GCP for quick setup and scanning.
Containerized	Kubernetes-native or containerized workflows with dynamic scaling needs.
Distributed Cluster	Large-scale, high-availability environments requiring parallel processing and centralized control.

Why MetaDefender Core

Risk Mitigation	Prevents file-based malware, ransomware, and zero-day threats from reaching users or systems. Enhances overall security posture across all file flows.
Data Protection	Ensures the security of sensitive data and confidential information by securing files in transit or at rest from file-borne attacks.
Seamless Integration	Deploys easily into existing infrastructure including email systems, file portals, storage platforms, and APIs. Improves security without disrupting workflows.
Operational Efficiency	Reduces manual workload for IT and security teams. Automates file scanning, threat prevention, and policy enforcement at scale.
Infrastructure Flexibility	Supports deployment in on-premises, offline, air-gapped, and hybrid environments. Ideal for regulated industries and Zero Trust initiatives.
Lower TCO	Simplifies implementation and management through a modular, agentless architecture. Delivers long-term value with reduced maintenance overhead.

GET STARTED

Are you ready to put MetaDefender Core 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 1,900 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