OPSWAT.

DATASHEET

MetaDefender Core™

Advanced Threat Protection for Trusted File Workflows

MetaDefender Core stops file-borne threats, including ransomware, zero-day exploits, and embedded malware, before they reach users or systems. It integrates seamlessly into existing infrastructure, securing uploads, downloads, email attachments, and file transfers without disrupting workflows.

Key Features

Evasive & Zero-Day Threat Prevention
Removes scripts, macros, and out-of-policy content from 200+ file types to prevent zero-day attacks.

Multi-Engine Malware Scanning
Uses 30+ anti-malware engines, as well as heuristics and machine learning, to achieve 99%+ malware detection.

True File Type Detection
AI-based identification prevents file spoofing and malware evasion.

Archive Scanning
Extracts and scans 30+ compressed formats, including encrypted archives.

File-Based Vulnerability Assessment
Identifies exploitable vulnerabilities before execution.

Adaptive Threat Analysis
Detects IOCs using emulation-based sandboxing.

Dynamic Threat Intelligence
Real-time detection of evasive, file-based threats.

Data Loss Prevention
Redacts or watermarks sensitive data; detects adult content and offensive text.

Country of Origin and Vendor Detection
Flags files from restricted or untrusted origins.

SBOM Generation
Creates software bills of materials and finds vulnerabilities in code and containers.

Executive Dashboard & SIEM Integration
Delivers insights, logs, and reports for compliance and visibility.

Deployment Flexibility

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.

For more information on MetaDefender Core, visit OPSWAT website.

Use Cases

Secure File Uploads
Scan and sanitize files from customers, partners, and vendors to block known and unknown threats.

Email Attachment Protection
Remove embedded threats and enforce DLP before delivery.

Safe Downloads
Sanitize files from the internet, cloud, or email links before opening.

Secure Internal/External Transfers
Prevent malware spread between networks, including air-gapped systems.

Accelerated Threat Analysis
Streamline SOC investigations with fast, detailed threat insights.

Data Leak Prevention
Detect and remove sensitive data before files leave your network.

Why MetaDefender Core

- **Risk Mitigation**: Stops advanced file-borne threats before impact.
- **Data Protection**: Safeguards sensitive and regulated data in transit and at rest.
- **Seamless Integration** : Fits into existing portals, storage, and email systems without workflow disruption.
- **Operational Efficiency**: Automates scanning and enforcement to reduce workload.
- **Infrastructure Flexibility**: Works in on-premises, offline, and hybrid environments.
- **Lower TCO**: Modular, agentless architecture reduces long-term costs.

OPSWAT.
Protecting the World's Critical Infrastructure