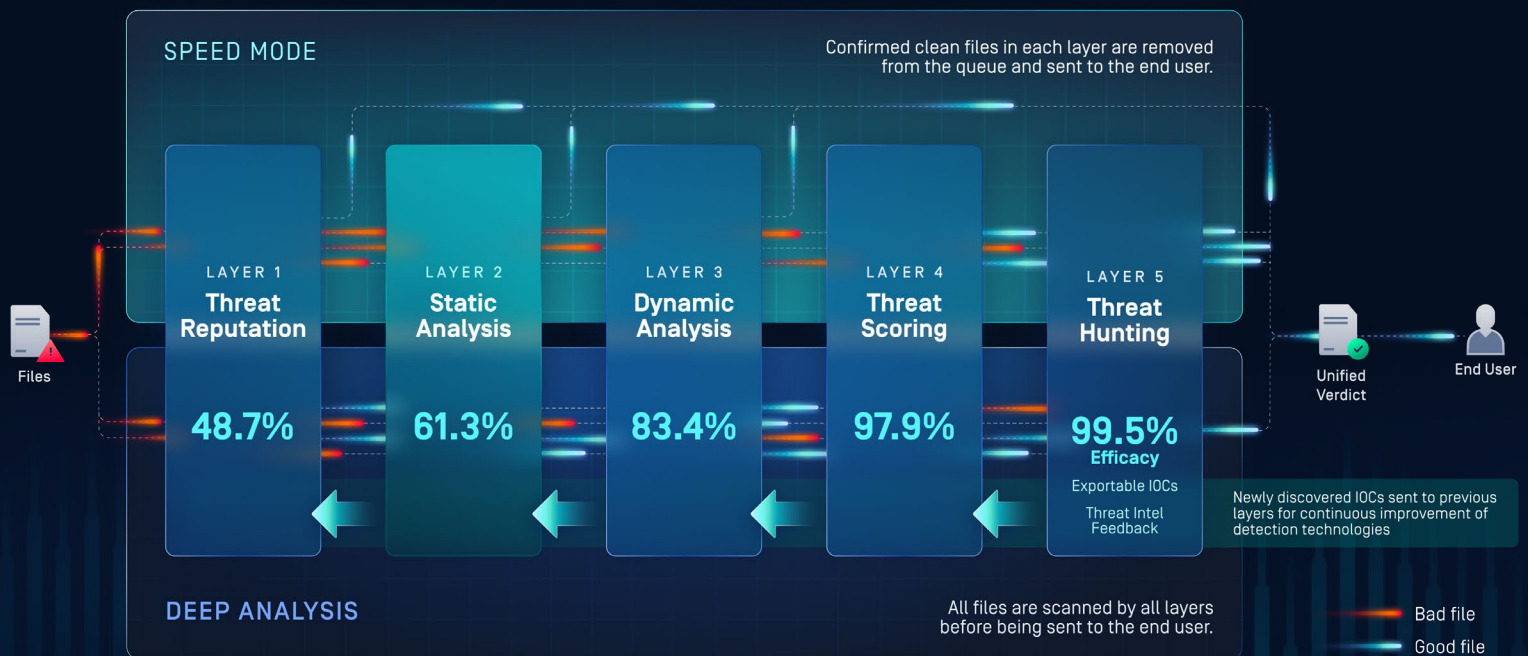


METADEFENDER

Aether™

Unified Zero-Day Detection at the Perimeter



Zero-day attacks evade traditional signature-based defenses, quickly moving through networks to inflict the most devastating impact. But trying to stop these new attacks with yesterday's tools just slows down file flows and floods threat analysts with false positives.

MetaDefender Aether™ combines a next-gen, adaptive sandbox with built-in threat intelligence

to achieve a 99.5% detection rate at 40X faster speed than traditional sandboxes. By using pre-execution Predictive Alin AI technology, clean files are deflected out of the sandbox queue while machine learning scans file structure to detect evasive malware and unknown threats that traditional AV engines miss.

*Based on OPSWAT's internal benchmark of randomly selected, in the wild file samples collected from the community-driven filescan.io website in cooperation with sample sharing agreements.

LAYER 1: THREAT REPUTATION

- Checks URLs, IPs, & domains in real time or offline to detect malware & phishing.
- Flags suspicious or unknown files for deeper analysis.
- Continuously updated with new indicators discovered by Dynamic Analysis.

LAYER 2: STATIC ANALYSIS

- Deflection: Clears high-confidence clean files in milliseconds [P90: 50ms | P99: <100ms].
- Detection: Predicts and blocks malicious files before execution that AV engines miss.
- AI model scanning: Detects embedded threats in model files without executing their code.

LAYER 3: DYNAMIC ANALYSIS

- Executes unknown samples in a secure, emulation-based sandbox.
- Probes live LLMs for prompt injection and sensitive data disclosure.
- Extracts new IOCs & automatically feeds them back into the Reputation database.

LAYER 4: THREAT SCORING

- Correlates static and dynamic analysis signals into a confidence-based risk score.
- Weighs behaviors such as persistence, process injection, payload delivery, and command-and-control activity.
- Produces a consolidated verdict that can be used for automated policy enforcement and response.

LAYER 5: THREAT HUNTING

- Weighs persistence, injection, & C2 activity to produce an actionable verdict.
- Generates machine-readable results & IOCs for automated response & policy enforcement.
- Links related samples, malware families, and campaigns through ML-powered similarity search.

How MetaDefender Aether Layers Map to the Pyramid of Pain

MetaDefender Aether addresses the whole Pyramid of Pain, from commodity indicators at Level 1 to advanced TTP disruption at Level 6, forcing attackers to continually rewrite their infrastructure, tools, & behaviors in order to evade detection.

Pyramid of Pain

The higher the level, the more painful it is for the adversary to change.

6. TTPs [highest difficulty]

5. Tools, TTPs

4. Artifacts, Tools

3. Domain Names

2. IP Addresses

1. Hashes

MetaDefender Aether

The only unified zero-day detection solution that addresses all layers of the pyramid to challenge attackers.

Layer 5
Threat Hunting

Layer 4
Threat Scoring

Layer 3
Dynamic Analysis

Layer 2
Static Analysis

Layer 1
Threat Reputation

LAYER 1

Blocks reused infrastructure & commodity malware. Forces attackers to rotate basic indicators.

LAYER 2

Prevents network and host artifacts from emerging by predicting malicious intent Pre-Execution.

LAYER 3

Observes the actual network and host artifacts created during execution.

LAYER 4

Identifies malicious behavior patterns. Forces attackers to rewrite behavioral techniques.

LAYER 5

Uncovers malware families and campaigns. Forces complete tactic/ infrastructure overhaul.

Key Features

Reputation Service

- Scans IP Addresses, URLs, and domains using up to 30 providers
- Correlates hashes to millions of known applications and CVEs
- Continuously updates its Threat Intelligence Database
- Supports bulk and individual searches via REST API
- Enhances visibility with comprehensive intelligence

Dynamic Analysis

- YARA & Malware Config Extraction for the most prevalent malware families
- Detects evasive malware & sandbox aware threats through our inhouse Threat Indicator Library
- Detection of .NET loaders & suspicious binary anomalies
- Brand Detection Model, identifying phishing impersonation attempts, with OCR capabilities
- Supporting wide array of file types for analysis

Static Analysis with Predictive Alin AI

- Predicts malicious intent Pre-Execution by analyzing structural and behavioral file characteristics without signatures or detonation
- Deflects high-confidence clean files in milliseconds, reducing unnecessary downstream analysis
- Blocks high-confidence malicious files before execution while escalating uncertain files for dynamic analysis
- Continuously improves using sandbox-confirmed zero-day intelligence from MetaDefender Aether
- Operates online or offline, including regulated and air-gapped environments

AI Model & LLM Scanning

Detect embedded threats in model files and test live LLMs for prompt injection and sensitive data disclosure. Use MITRE ATLAS-mapped findings to guide model approval and remediation.

Advanced Emulation

- Powered by Next-Gen Advanced PE Emulator Beta - purpose-built to outpace traditional sandboxes
- Defeats Anti-VM, anti-debug, and time-based evasion - no manual tuning required
- Unpacks multi-stage payloads, decrypts runtime packers, and reveals hidden IOCS
- Detects fileless malware, customer loaders, and sandbox-aware threats missed by legacy tools
- Shellcode execution, memory dump integration, and event tracking for deeper behavioral insights

Threat Indicator Repository

- 50B+ Hashes, IPs, domains for enhanced threat attribution
- MISP & STIX integration for automated extraction and sharing
- Custom generated YARA rules for in-depth threat profiling with tagging, naming and associated metadata

Threat Hunting & Forensics

- MITRE ATT&CK mapping and machine learning similarity search
- Web threat detection with ML-based multi-label classification, including content and style analysis

Deployments & Integrations

Flexible Deployment & API First Design

- On-premises, hybrid, or cloud-native deployment
- REST API for seamless integration
- SIEM / SOAR support: Splunk, Cortex XSOAR, CEF Syslog
- Setup Wizard for Simplified Deployment

Deployment Options

- On-premises: 32GB RAM, 256GB SSD
- OPSWAT cloud-hosted
- 50k Scans per day
- API & GUI-based integrations
- Support for Ubuntu 24.04, Red Hat Offline (RHEL 9), Rocky Linux
- Average Processing time of 10s

GET STARTED

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



OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, protects public and private sector organizations and enterprises with an AI-powered end-to-end cybersecurity platform that secures complex networks, critical devices, and ensures compliance.