OPSWAT.

SOLUTION BRIEF

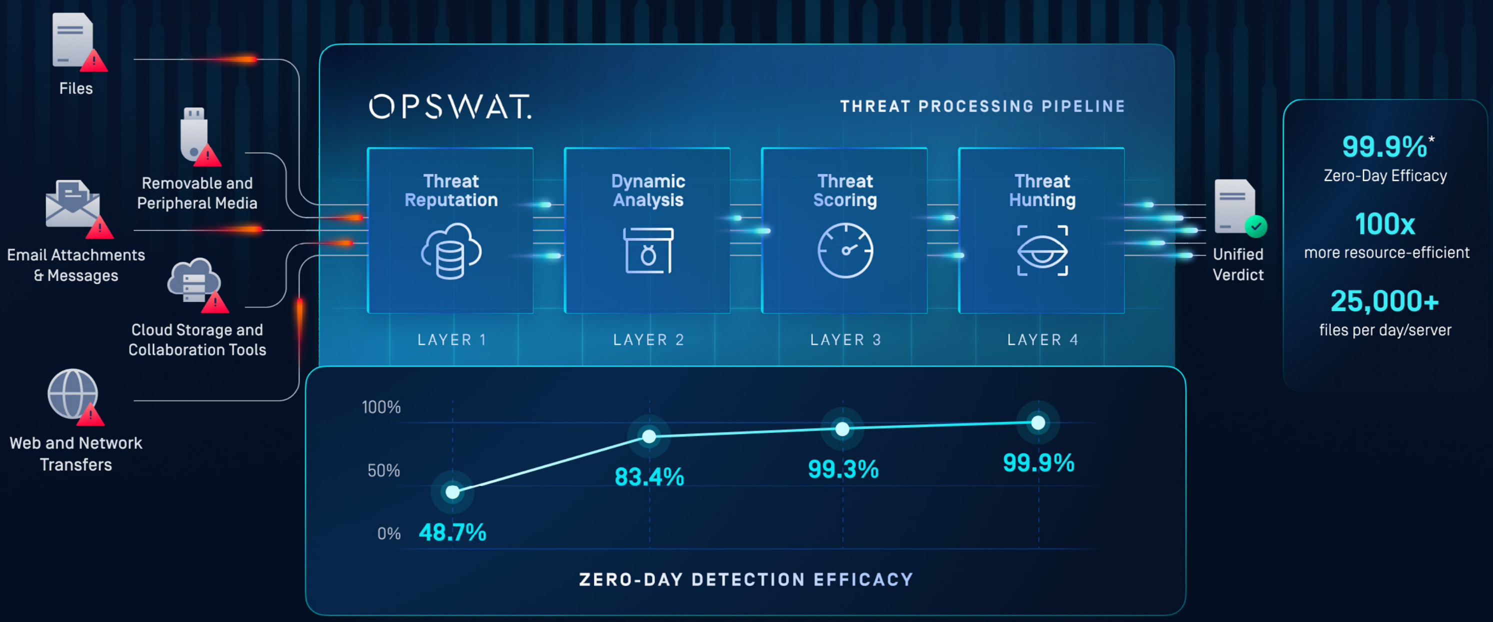
METADEFENDER™

Aether

Zero-Day Detection for MetaDefender Core

Zero-day attacks evade traditional and static 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.

Enable MetaDefender Aether's emulation-based dynamic file analysis and built-in global threat intelligence directly within your MetaDefender Core environment—no new infrastructure required. Achieve up to 99.9% zero-day detection efficacy with analysis up to 20× faster than traditional sandbox solutions.



Files
Removable and Peripheral Media
Email Attachments & Messages
Cloud Storage and Collaboration Tools
Web and Network Transfers
OPSWAT.
THREAT PROCESSING PIPELINE
Threat Reputation
Dynamic Analysis
Threat Scoring
Threat Hunting
LAYER 1
LAYER 2
LAYER 3
LAYER 4
Unified Verdict
100%
50%
0%
48.7%
83.4%
99.3%
99.9%
ZERO-DAY DETECTION EFFICACY

99.9%* Zero-Day Efficacy

100x more resource-efficient

25,000+ files per day/server

LAYER 1

- 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

- Executes unknown samples in a secure, emulation-based sandbox.
- Observes runtime behaviors to expose hidden threats.
- Extracts new IOCs & automatically feeds them back into the Reputation database.

LAYER 3

- Correlates behavioral indicators and assigns a confidence-based risk score.

LAYER 4

- Weighs persistence, injection, & C2 activity to produce an actionable verdict.
- Machine-readable results & IOCs for automated response & policy enforcement.

*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.

How MetaDefender Aether Layers Map to the Pyramid of Pain

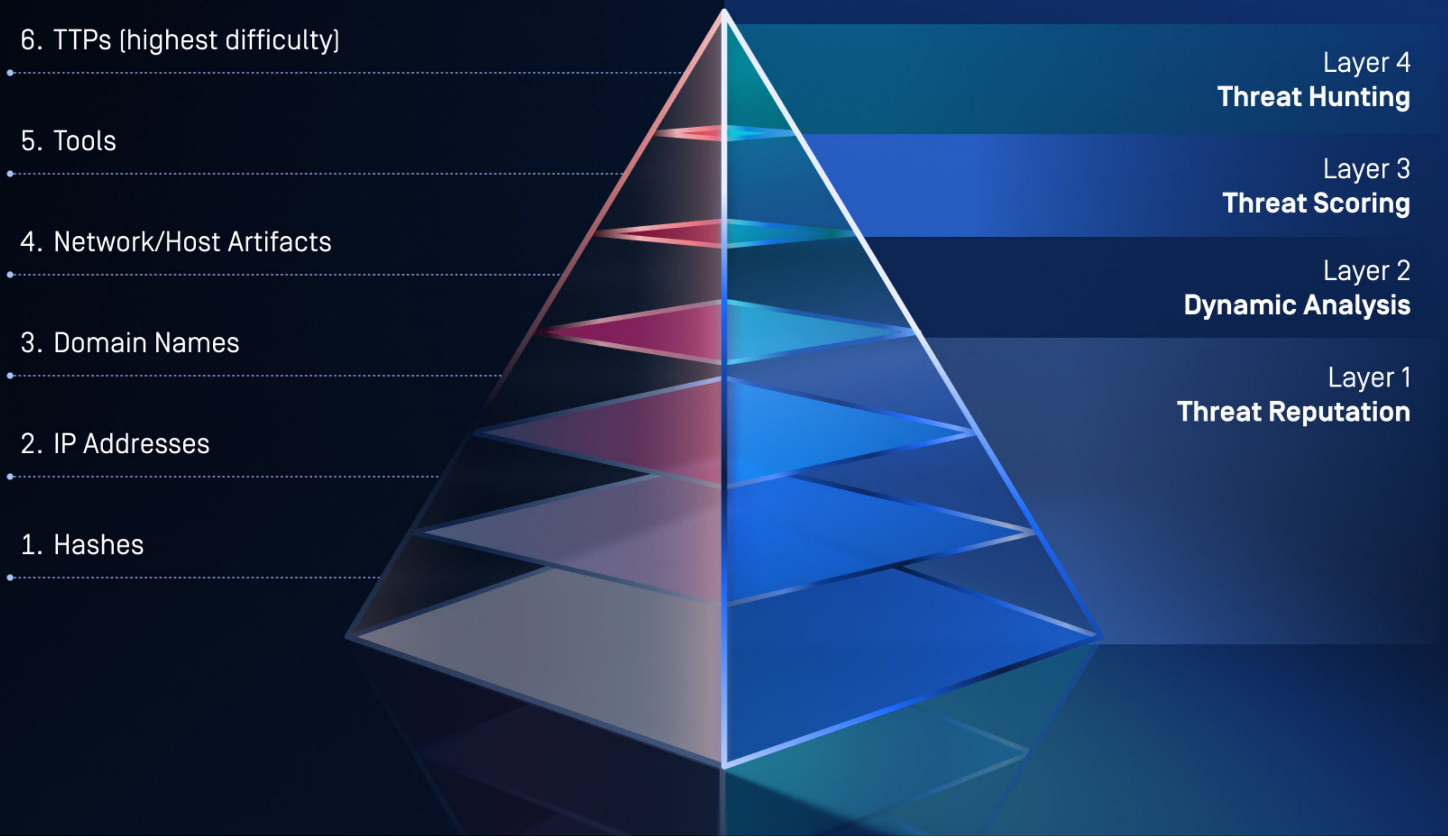
MetaDefender Aether addresses the whole Pyramid of Pain, from commodity indicators at Level 1 to advanced TTP disruption at Level 6, forcing attackers to continually rewrite their infrastructure, tools, & behaviors in order to evade detection.

Pyramid of Pain

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

MetaDefender Aether

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



6. TTPs (highest difficulty)
5. Tools
4. Network/Host Artifacts
3. Domain Names
2. IP Addresses
1. Hashes

Layer 4
Threat Hunting

Layer 3
Threat Scoring

Layer 2
Dynamic Analysis

Layer 1
Threat Reputation

LAYER 1

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

LAYER 2

Exposes artifacts, loader chains, script logic and evasion tactics. Forces tool and packer redesign.

LAYER 3

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

LAYER 4

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

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 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

- Embedded for high-level threat analysis or Remote for Low-level threat analysis
- On-premises
- 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
- 25k 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.
Protecting the World's Critical Infrastructure

For over 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.