OPSWAT.

SOLUTION BRIEF

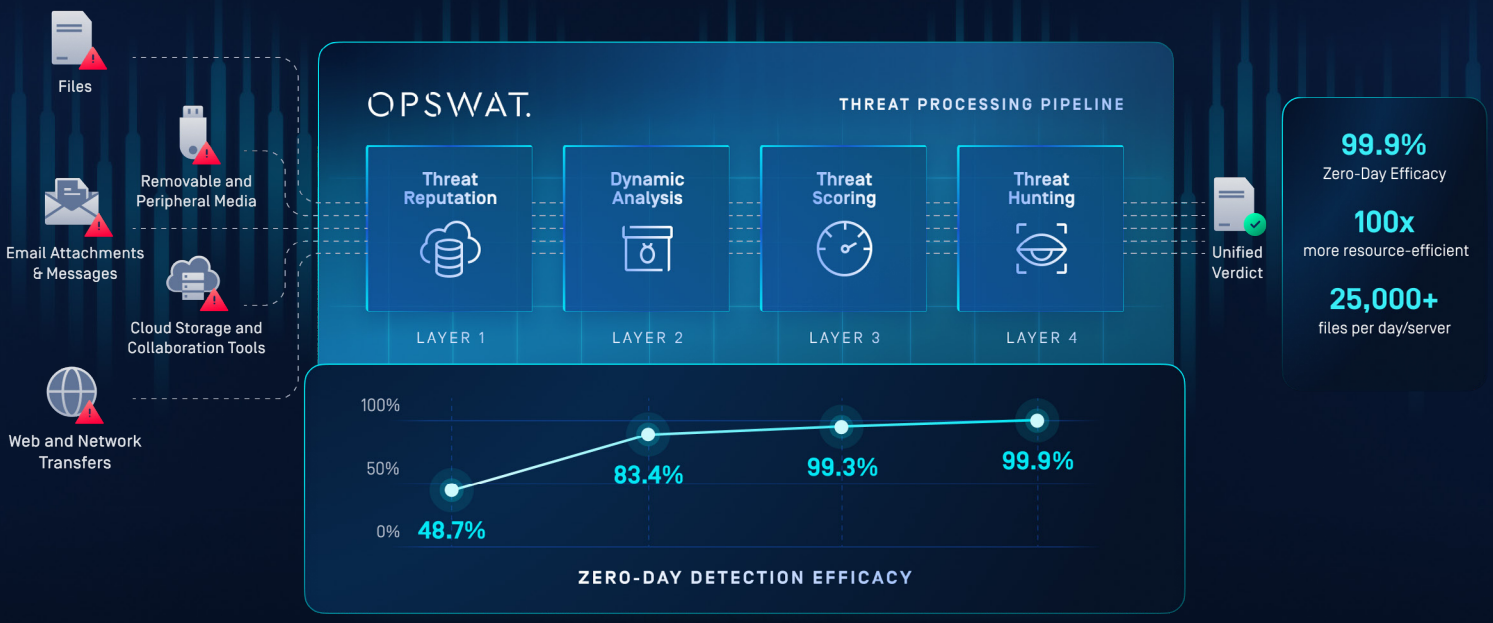
METADEFENDER™

Aether

Unified Zero-Day Detection at the Perimeter

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.

OPSWAT's zero-day detection solution combines dynamic analysis with built-in threat intelligence, achieving a 99.9% detection rate and operating 20x faster than traditional sandboxes.



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.

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.

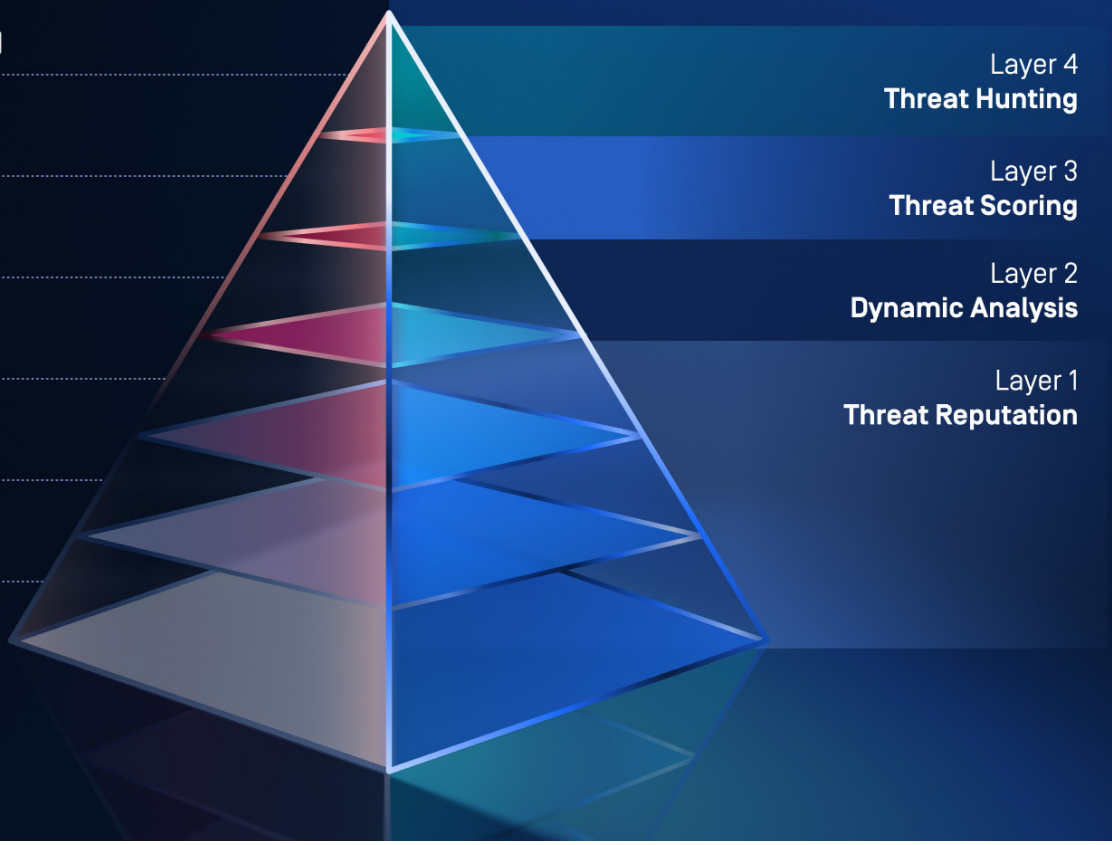
Pyramid of Pain

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

6. TTPs (highest difficulty)
5. Tools
4. Network/Host Artifacts
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 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, content / 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
- 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