OPSWAT.

SOLUTION BRIEF

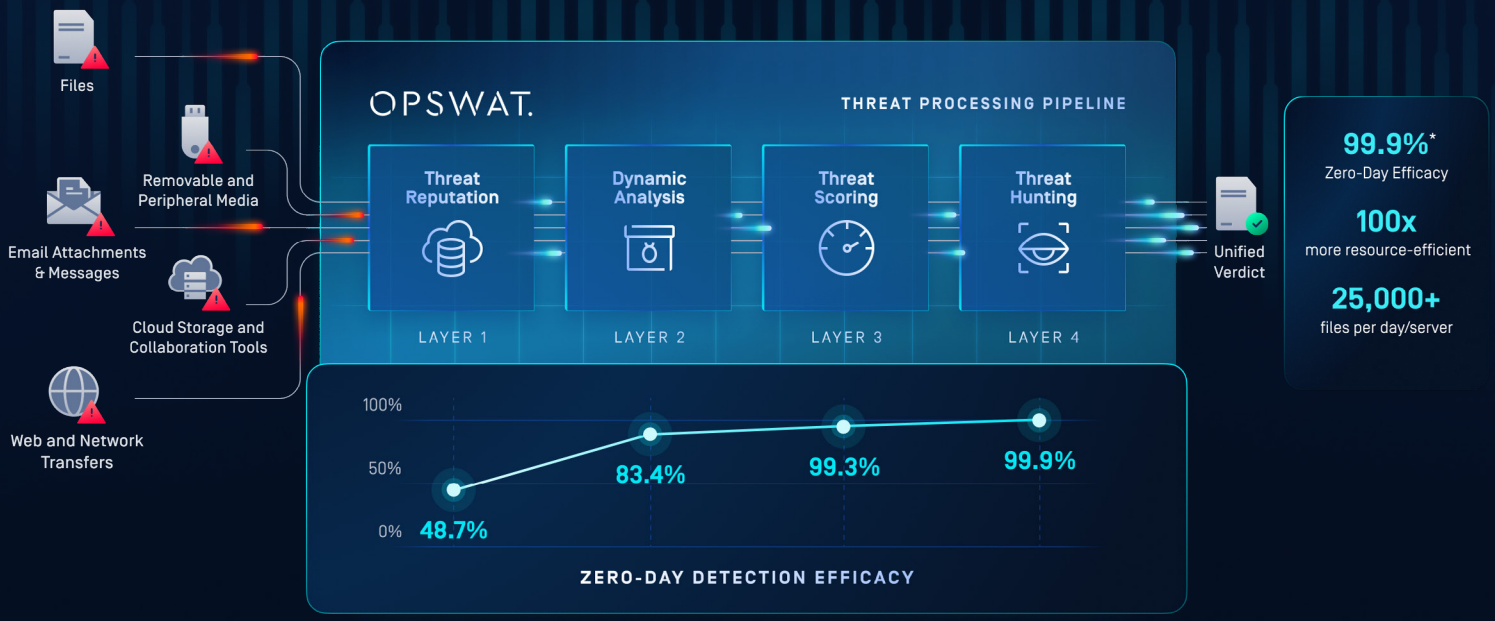
METADEFENDER™

Aether

Zero-Day Detection for MetaDefender Cloud

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.

MetaDefender Aether's Adaptive Sandbox detonates evasive malware in a secure cloud environment and feeds results into threat intelligence to shrink time-to-insight. Achieve a 99.9% detection rate with 20X faster processing over 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.

*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.

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 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

MetaDefender Aether's Adaptive Sandbox Integrations for MetaDefender Cloud

Large-scale, cloud-native detonation for files and UxqRLs, perfect for email security/OEMs and teams that need elastic capacity without running their own sandbox farm. Auto-scaling with fast emulation keeps latency low while avoiding VM overhead. Policy routing ensures you only detonate what's necessary—so you control volume and spend.

Inside OPSWAT / SaaS Ecosystem

- MetaDefender Cloud public APIs (files, hashes, URLs, domains)
- Reputation and threat intelligence APIs (URL, domain, IP, hash lookups)
- Other OPSWAT cloud modules and services

Cross-Environment / Hybrid

- Private file processing / scanning options for sensitive environments
- On-prem MetaDefender Core using Cloud reputation and threat intelligence services

External / 3rd-Party Integrations

- REST API for file, URL, IP, and domain submissions with sandbox analysis results
- SIEM / logging platforms through API or event export
- Developer tools (CI/CD pipelines, repositories, SDKs, plugins)
- SOAR / orchestration platforms through API integration
- Support for Ubuntu 24.04, Red Hat Offline (RHEL 9), Rocky Linux

Setup & Performance Specs

- 25k scans per day
- Average processing time of 10s
- Setup wizard for simplified deployment

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.