OPSWAT.

DATASHEET

METADEFENDER™

Threat Intelligence

AI-Driven Malware Analysis for Evasive Threats

Make your organization more resilient to file-based attacks by combining our adaptive sandbox and reputation service to ensure robust detection with an efficacy of 99.6% - enabling fast, informed responses to zero-day threats and evasive malware.

Quickly Respond to Evolving Threats

Modern threats are evolving rapidly. Zero-day attacks and evasive malware can stay hidden, avoiding detection by conventional solutions. Organizations are under pressure to quickly identify these threats to reduce breakout time.

Sophisticated Threats

Modern malware is designed to evade detection at every turn, lurking in your environment long enough to inflict serious damage and harvest sensitive data. At the same time, sophisticated adversaries employ targeted attacks and Advanced Persistent Threats (APTs) to infiltrate high-value networks, maintaining stealthy, long-term access that's difficult to uncover.

Breakout Time

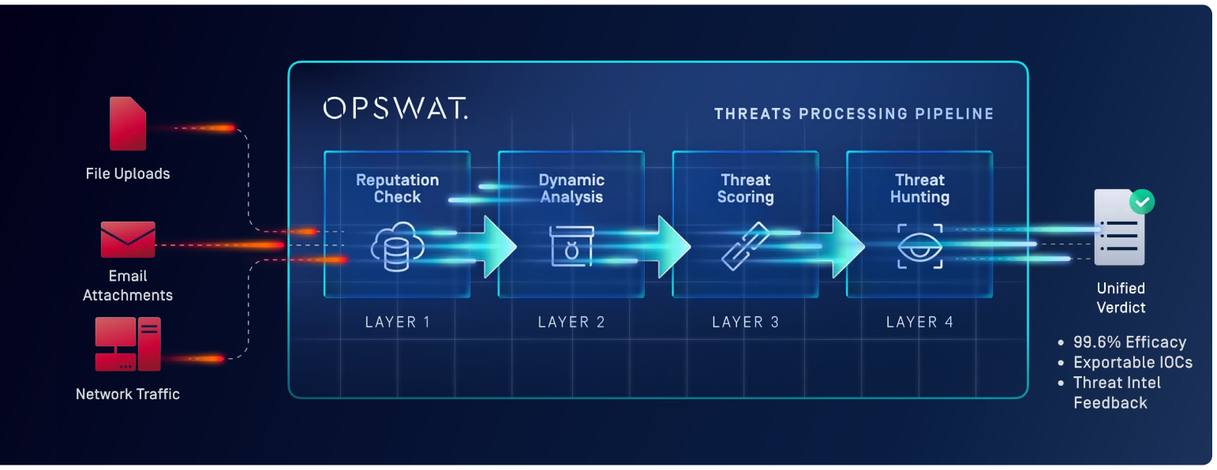
Once inside your network, attackers move laterally with alarming speed - escalating privileges, spreading to critical assets, and exfiltrating data before traditional defenses can react. Rapid detection and automated response are essential to contain threats early and prevent widespread disruption.

Disconnected Tools & Workflows

Relying on disparate security solutions forces analysts to manually correlate indicators of compromise, creating critical blind spots and slowing down investigations. A unified platform with integrated workflows eliminates gaps, streamlines threat hunting, and accelerates incident response.

Actionable Threat Intelligence

OPSWAT's MetaDefender Threat Intelligence is enriched with sandbox-derived IOCs and ML-powered similarity scoring, combining behavioral analysis, file reputation, and global threat feeds into a unified solution. It enables detection of both known and unknown threats-including zero-days-at machine speed.



Threat Hunting: Empowers analysts to identify campaigns or attack clusters

- Attribution & Classification
- Identify Threat Clusters
- Extract all Correlated IOCs & TTPs

Threat Scoring: Quickly prioritize alerts based on behavioral similarity

- Powered by Machine Learning
- Trained on Millions of Phishing Threats
- Air-gapped Compatible

Dynamic Analysis

- Powered by Adaptive Sandbox
- Full Attack Chain Analysis
- Extracts Embedded IOCs
- Behavioral Analysis & Zero-day Threat Detection

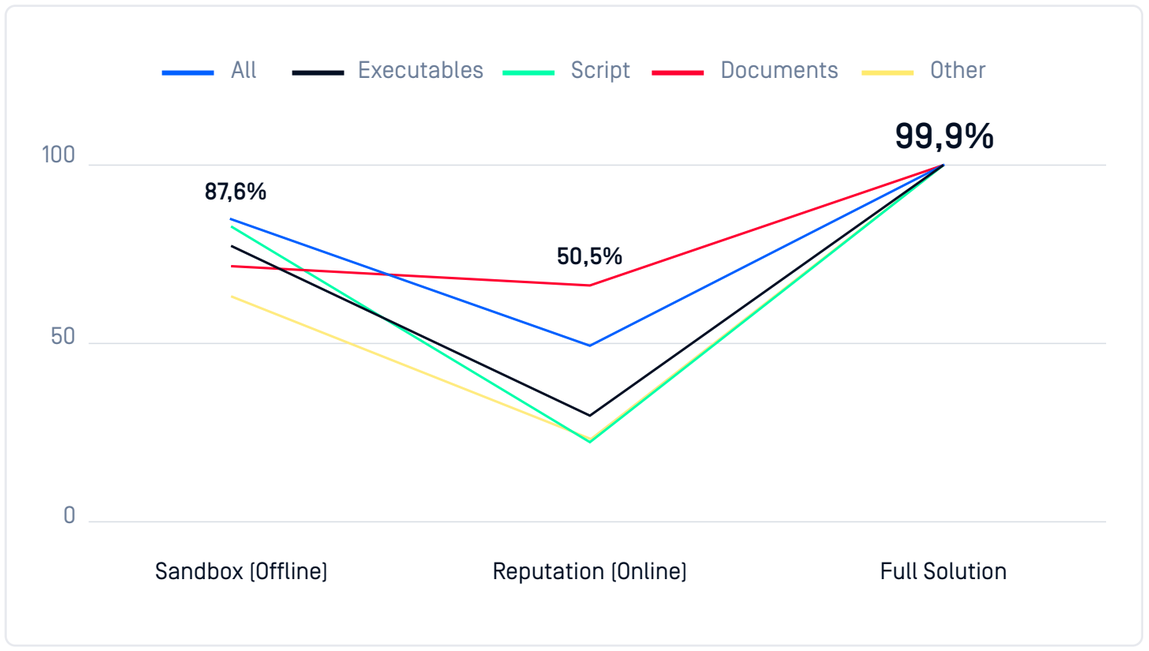
Reputation Check

- Instant Threat Checks
- 50 Billion Artifacts
- Continuously Enriched by IOCs & TTPs

Threat Intelligence Solution Efficacy

Boost Efficacy Rates to 99.9%, Combining MetaDefender Sandbox™ & MetaDefender Reputation Service™ API.

MetaDefender Reputation Service API checks the reputation of hashes, IPs, domains, and URLs, while Sandbox extracts and dynamically inspects IOCs. These technologies work together to achieve a near 100% detection rate.



Reputation Services

Checks the reputation of hashes, IPs, Domain, and URLs.

Sandbox Analysis

Extracts and dynamically inspects hidden IOCs.

Combined Strength

Achieves 99.9% threat detection rate for a robust defense system.

OPSWAT.

DATASHEET

Maximize Threat Actor Pain

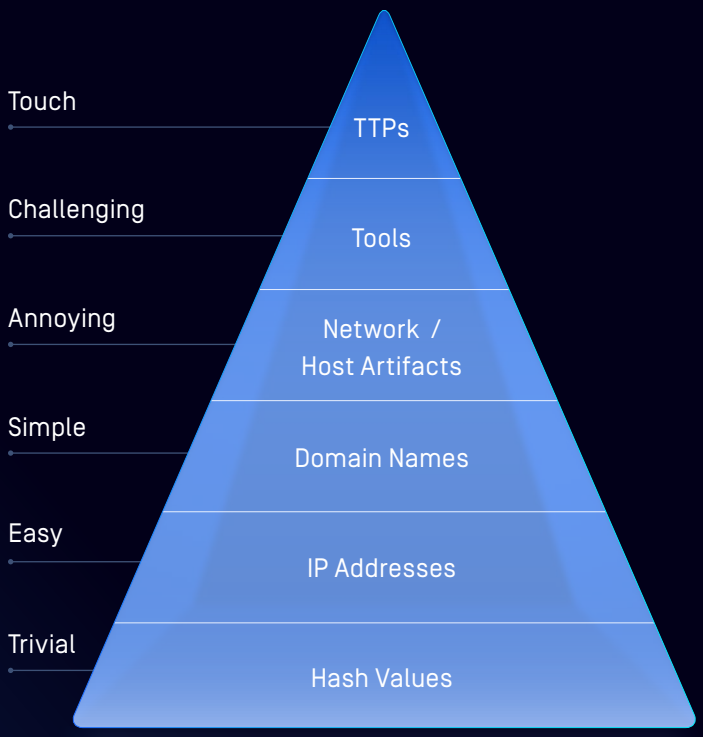
Reach Higher on the Pyramid of Pain

MetaDefender Sandbox and Threat Intelligence work together to detect and disrupt threats at the most impactful levels of the Pyramid of Pain. While conventional solutions only address basic indicators like file hashes or IPs - easily altered by attackers - our approach goes further:

Adaptive Sandbox dynamically detonates suspicious files to extract hidden Indicators of Compromise (IOCs), uncovering behaviors, techniques, and tactics.

Threat Intelligence enriches these findings with real-time data across 50+ billion IOCs - including domains, IPs, and behavior patterns - correlated using advanced machine learning.

Combined, they allow your security team to detect and respond not only to known threats but also to emerging, evasive malware by identifying similarities in behavior and tactics. This makes it harder for attackers to reuse infrastructure or tactics undetected, delivering meaningful pain at the top of the pyramid where it counts.



Request a Live Demo

See a Sample Threat Report

Try the Reputation API Today

OPSWAT.