OPSWAT.

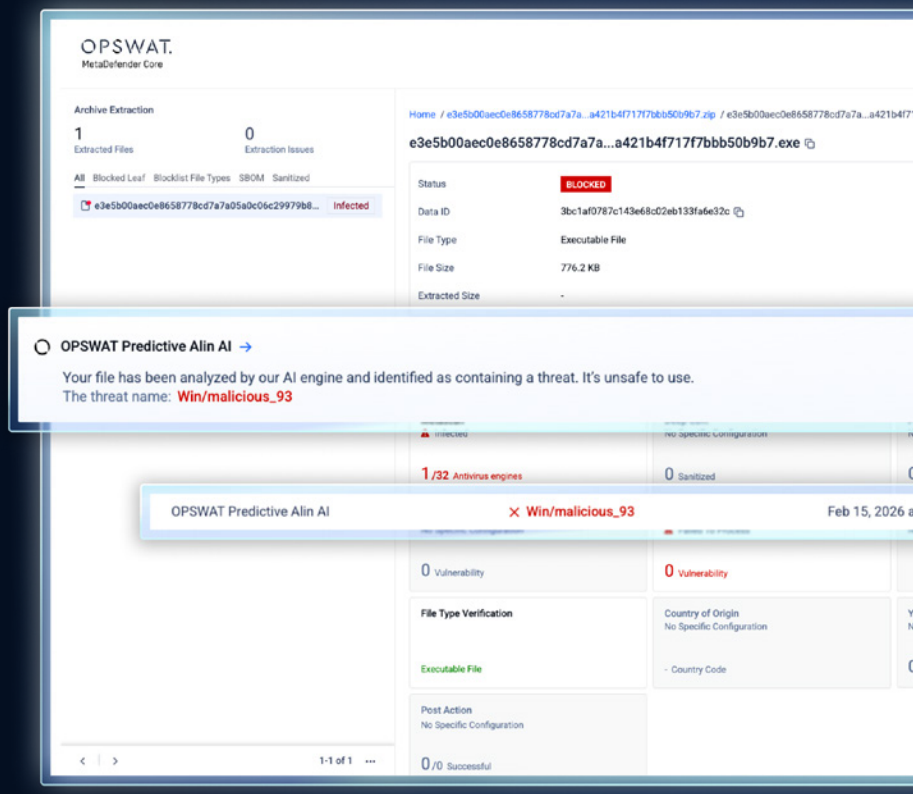
DATASHEET

Predictive Alin AI

Pre-Execution Zero-Day Detection at the Perimeter

Zero-Day malware moves faster than traditional defenses and antivirus engines. Security teams are overwhelmed by thousands of alerts per day, yet still risk missing the one file that matters.

OPSWAT Predictive Alin AI changes the antivirus engine's static analysis model to predict malicious files, using file feature extraction for behavior analysis before execution. With real zero-day intelligence and machine learning, verdicts are delivered in milliseconds.



Why Predictive Alin AI

Pre-Execution Zero-Day Prediction

Detects malicious files before execution by analyzing structural and behavioral indicators of compromise rather than relying on signatures or sandbox detonation.

Radically Lower False Positives

Delivers verdicts approximately 50 milliseconds at P90 and under 100 milliseconds at P99, enabling real-time inline protection with minimal resource impact.

Millisecond Level Performance at Scale

Trained on curated, enterprise grade, privacy safe datasets that reflect real enterprise file flows, significantly reducing alert noise and wasted analyst time.

Continuously Retrained on Real Zero-Days

Improves detection accuracy over time through a retraining loop powered by sandbox confirmed zero days from MetaDefender Aether.

Enterprise Ready Anywhere You Operate

Runs online or offline, on premises or in regulated environments, and integrates seamlessly across the MetaDefender platform.

PREDICTIVE ALIN AI

Key Features

Pre-Execution Intelligence Layer

Operates at the perimeter, providing predictive signals where multiscanning engines may be silent. Detects threats without detonation, reducing exposure and latency.

Zero-Day Retraining Loop

Leverages validated zero-day discoveries from MetaDefender Aether dynamic analysis to continuously refine and strengthen predictive models. Each confirmed threat enhances future detection capability.

Optimized for Enterprise Content Flows

Machine learning models are trained on privacy safe, enterprise grade datasets that replicate real world file movement patterns across email, web uploads, removable media, and collaboration platforms.

High Accuracy with Low Noise

Early testing demonstrates 90 percent detection on executable files with 0.1 percent false positives, helping SOC teams focus on real threats instead of triaging noise.

Lightweight and Resource Efficient

Designed with a small memory footprint and minimal CPU impact to support high throughput environments without degrading performance.

Focused High Risk File Coverage

Optimized for high-risk executable formats, with expanded file type support on the roadmap.

Deployments & Integrations

Flexible Deployment Models

- Available now in MetaDefender Core for on premises and regulated environments on Linux and Windows
- Cloud integrated via MetaDefender Cloud

Platform Integration

- Integrated across the MetaDefender platform including Core, Cloud, MFT, ICAP, Security Supply Chain, Cloud Email Security, Endpoint, Security Storage and Kiosk
- Enhances Metascan multiscanning by adding predictive detection where traditional AV engines lack visibility
- API driven architecture for seamless integration into existing workflows

Designed for Regulated and Air-Gapped Environments

- Operates fully offline with consistent performance
- Suitable for critical infrastructure, government, defense, and high compliance sectors

OPSWAT Predictive Alin AI

Fast. Accurate. Enterprise-ready.