OPSWAT.

DATASHEET

MetaDefender Sandbox

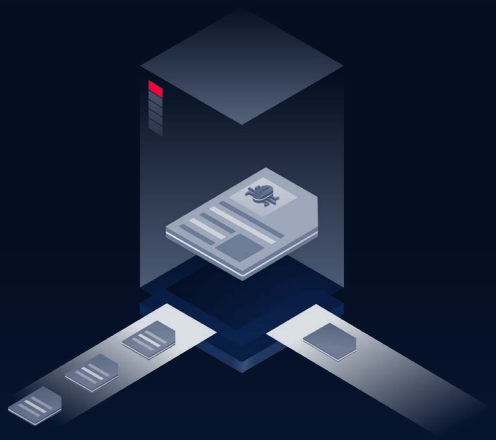
Advanced Threat Analysis Platform

MetaDefender Sandbox platform combines static and dynamic analysis with machine learning powered threat intelligence for highly accurate and rapid malware analysis. Our platform can analyze 25K+ files per day per machine. Enhance defensive capabilities, save time, and effectively hunt threats with advanced threat analysis.

Overview

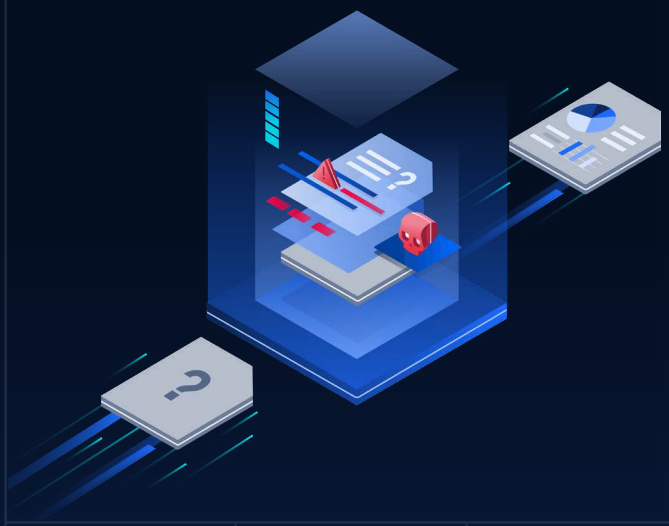
- Static analysis uses 30+ antivirus engines, Yara rules, and threat patterns for high-volume processing.
- Dynamic analysis virtually detonates malware with adaptive threat analysis to expose highly evasive malware and zero-day threats.
- Threat analysis accesses 50 billion+ hashes, IPS and domains, and includes threat actor attribution.
- Fully automated, zero-trust threat detection platform.

Traditional Sandbox



- Slow
- High resource use
- Detectable

Emulation Sandbox



- Fast
- Small Memory Footprint
- Adapts to multiple environments

OPSWAT.

MetaDefender
Sandbox

Analysis Workflow

Stage 1
Deep Structure Analysis

Initial static file assessment and extract embedded active content.

- Analyzes 50+ different file types
- Extracts artifacts, images, and more
- Automated decoding, decompilation, and shell code emulation
- Extracts VBA macro code from DWG
- Compiled Phyton unpacking and decompilation for PyInstaller, Nuitka, and py2exe

Stage 2
Threat Detection and Classification

Detect and classify threats using machine learning and decades of experience.

- Detects 290+ brands for ML-based phishing detection
- Extracts and correlate a wide range of IOCs
- Detects malicious intent with 400+ generic behavior indicators
- ML-based similarity search detects unknown threats and malicious clusters
- Identify and extract configuration data from more than 18 malware families

Stage 3
Adaptive Threat Analysis

Perform dynamic analysis on active content using adaptive threat analysis. Detect and classify threats using machine learning and decades of experience.

- Detonates targeted attacks via specific application stacks or environments
- Bypasses a wide range of anti-evasion checks
- Emulates JavaScript, VBS, PowerShell scripts
- Automatically adapts the control flow to detect unknown threats

Stage 4
Threat Intelligence and Automation

Perform automated threat hunting and real-time threat identification using a wide range of integrations.

- Exports to MISP & STIX report formats
- Queries MetaDefender Cloud reputation service
- Integrates with other open-source intelligence vendors
- Automatically generates YARA rules on a per threat basis
- Scans all artefacts with 8000+ YARA rules

Platform Features

OPSWAT
- MetaDefender Core
- MetaDefender Cloud
- MetaDefender Threat Intelligence

SOAR
- Splunk SOAR
- Palo Alto XSOAR
- Assemblyline 4

Others
- Virus Total
- Python CLI
- SIEM (CEF Syslog)

Others Cont.
- Chrome Extension
- Passive Email Scanning (IMAP)
- OpenAPI Specification (OAS)
- ChatGPT Executive Summary
- CIS Level 1 Compatible

Flexible Deployments

On-Premises (Example)
- Intel Xeon-E 2136 (12M Cache, 3.30 GHz)
- RAM 32GB DDR4 ECC 2666 MHz
- 2x SSD NVMe 256GB RAID

Note: example system processes 25K files/ day with a retention period of 10 days.

Cloud
- 5000 scans/day: t3a.2xlarge
- 10000 scans/day: c4.4xlarge
- 25000 scans/day: c4.8xlarge

Learn more about the technical requirements technical requirements

OPSWAT.
Protecting the World's Critical Infrastructure