OPSWAT.

DATASHEET

METADEFENDER

# Sandbox™

AI-Driven Malware Analysis for Evasive Threats

MetaDefender Sandbox is a multi-layered, AI-powered malware analysis solution designed to detect and classify even the most evasive threats. By combining deep static analysis, advanced threat intelligence, and high-speed emulation, it delivers actionable insights to protect critical assets from zero-day attacks.

## Key Features

### Advanced Threat Detection

- Multi-layered detection: Static analysis, emulation, dynamic analysis
- 30+ AV engines, YARA rules, heuristic scanning
- Detects evasive malware and sandbox-aware threats
- Analyze broken Office files used in zero-day attacks

### 10x Faster Adaptive Emulation

- Results in ~10 seconds, 10x faster than traditional sandboxes
- Automatically defeat evasion techniques without manual tuning
- Uncover hidden payloads and unpacks obfuscated threats with precision

### Flexible Deployment and API-First Design

- On-prem, hybrid, or cloud-native deployment
- REST API for seamless integration
- SIEM/SOAR support: Splunk, Cortex XSOAR, CEF Syslog
- Setup Wizard for Simplified Deployment

### Actionable Reputation Insights

- 50B+ hashes, IPs, domains for enhanced threat attribution
- MISP and STIX integration for automated sharing
- Custom generated YARA rules for in-depth threat profiling with tagging, naming and metadata
- Brand Detection Model with additional brands added, as well as further support for OCR Capabilities

### Threat Hunting and Forensics

- MITRE ATT&CK mapping and similarity search
- Config extraction for 18+ malware families
- Embedded file and script decoding (e.g., VBA, PowerShell, AutoIT, JavaScript)
- AI-powered phishing and URL threat detection
- OpenAI-powered Decompiler: “Automatic RE” generates AI-assisted decompiled code with inferred names and comments

## Speed and Accuracy Across the Entire Malware Analysis Pipeline

| **Analysis Stage** | **Key Capabilities** |
|---|---|
| **Step 1:**<br>**Threat Intelligence** | Reputation analysis, OSINT lookups, hash/IP reputation |
| **Step 2:**<br>**Deep Static Analysis** | YARA scanning, unpacking, decompilation |
| **Step 3:**<br>**Dynamic Fast-Pass**<br>**(Avg. 10s)** | Emulation-based detonation, evasive malware detection |
| **Step 4:**<br>**Adaptive Threat Analysis** | Deep behavior analysis, IOC extraction, ML clustering |

## Technical Specifications

### Deployment Options

- On-Prem: 32GB RAM, 256GB SSD
- Cloud: AWS m6a/c6a instances, up to 25K scans/day
- API & GUI-based integrations
- Support for Ubuntu 24.04

### Integration and Reporting

- SIEM/SOAR: Splunk, Cortex XSOAR, Assemblyline 4
- Threat Intel Feeds: MISP, STIX 2.1
- Data Export: JSON, PDF, HTML

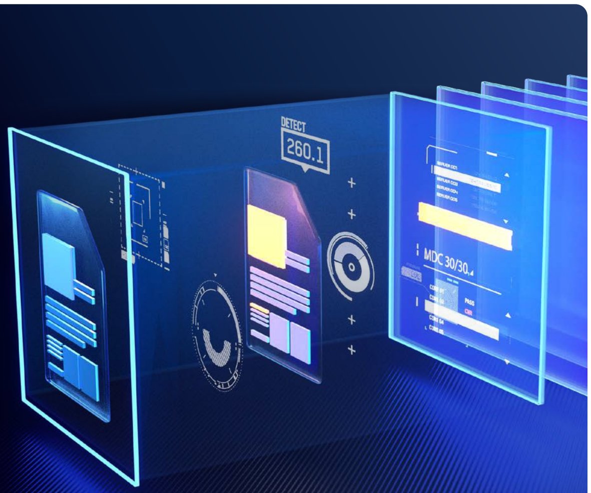
## Why MetaDefender Sandbox?

**Fastest Malware Analysis**
Verdicts in seconds, not minutes

**Seamless SOC Integration**
REST API, SIEM & SOAR support

**Low Resource Consumption**
10x more efficient than traditional VM-based sandboxes

**Unparalleled Threat Visibility**
IOCs, malware family detection, MITRE ATT&CK mapping



OPSWAT.
Protecting the World's Critical Infrastructure

**Defend What's Critical**

Talk to an OPSWAT expert today:
opswat.com/get-started
sales@opswat.com