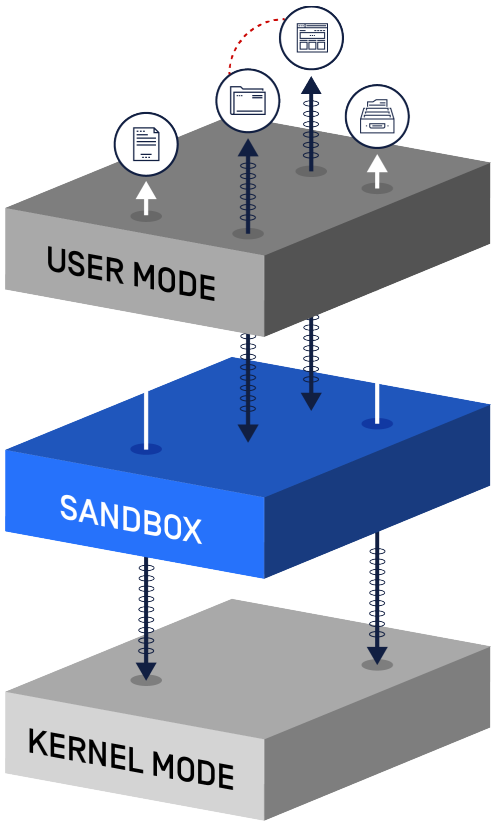
OPSWAT.

DATASHEET

OPSWAT Sandbox

Smarter, Faster Sandbox to Security Analysts and Incident Responders



The explosive growth in evasive and targeted malware makes it ever more challenging to analyze and classify new malware before they cause harm. These advanced malware can easily circumvent legacy sandboxing technologies and signature-based detection tools, putting organizations at risk. Security teams need better detection and analysis capabilities to reduce the likelihood and potential impact of attacks.

OPSWAT Sandbox delivers the latest innovations in dynamic analysis capabilities, in both speed and accuracy, and increases detection rates in both IT and operational technology (OT) environments.

Key Features

Undetectable Kernel-Mode Agent

Reveals malware's full malicious nature by deceiving malware into executing its full range of intended functionality and revealing its true malicious nature, intent, and capabilities.

Ultra-Fast and Deep Scanning Options

Derives quick, statistically accurate verdicts in approximately one minute, 3X (three-times) faster than existing contemporary sandboxes.

Deep Learning and AI-driven Analysis

Applies deep learning and multi-vector detection by channeling static, dynamic and network inputs through an AI engine for faster and more accurate results.

Environment-Specific CIP Profiles

Provides dynamic analysis across the entirety of critical infrastructure, supporting profiles across both IT and OT environments such as Windows and specific industrial control systems (ICS) platforms.

Scalability across On-Premises and Private Cloud

Supports clustering of analysis resources to scale processing capacity to over 100K (one-hundred thousand) files per day.

OPSWAT.

Benefits

Reduce Analysis Time

Reduces Mean Time to Detect (MTTD) by simplifying the process of analyzing malware across security engineering, operations, and analysis, and accelerating incident response.

Deliver Complete Visibility

Provides a single platform to assess risk across both IT and OT environments, and uniquely protects critical infrastructures against targeted, zero-day attacks particularly as these attacks span both networks.

Decrease Analysis Costs

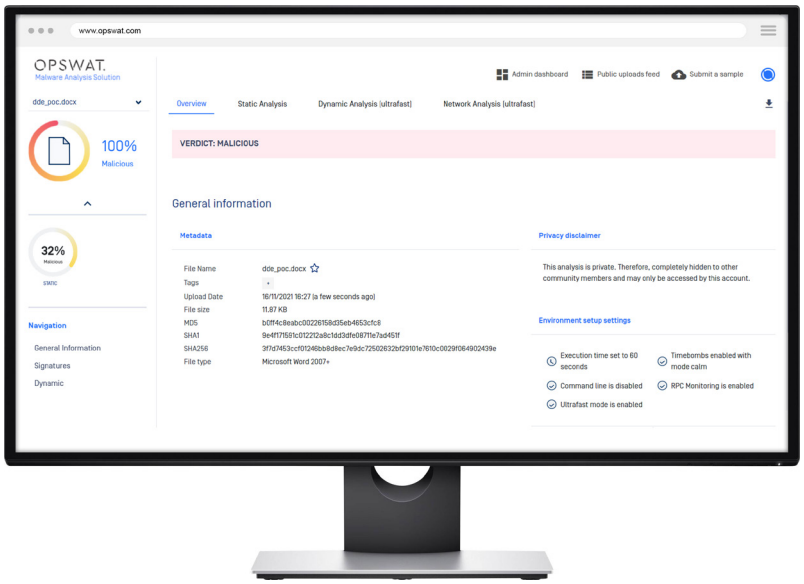
Simplifies overall security operations and reduces costs by consolidating IT and OT-related malware analysis within a single solution.

Improve Efficiency and Scale

Supports real-time business operations by executing and analyzing evasive malware in about one minute, applying ultra-fast analysis and multi-vector, AI-derived verdicts.

Gain Greater Threat Visibility

Delivers security teams unprecedented levels of visibility into malware behaviors via easy-to-interpret analysis results which are available to third-party security solutions.



Capabilities

Apply Advanced Deception

Takes a smarter approach to malware analysis by remaining undetectable to attackers and capturing behaviors as if in a live environment, including command and control (C2) server communications.

Accelerate Dynamic Analysis

Searches for key anomalies in behavior indicative of malware and channels observables through AI to quickly derive verdicts and IOCs on IT and OT-based malware.

Deliver Accurate Conclusions

Deciphers volumes of data from kernel-level monitoring and leverages AI-derived analysis for more accurate outcomes.

Support Critical Infrastructure Protection

Supports malware analysis across the entirety of the critical infrastructure, offering dedicated profiles for specific ICS platforms as well as IT systems.

Integrate with Malware Analyzer

Available as an integral component of MetaDefender Malware Analyzer to be factored into automated malware analysis workflows.

Summary

OPSWAT Sandbox offers a unique approach to reduce malware detection times and mitigate risks associated with targeted attacks. At a time when conventional dynamic analysis solutions are slow or being evaded by sophisticated attackers, OPSWAT Sandbox introduces new innovations to avoid detection, and support greater throughput, scalability, as well as accuracy into malware, regardless of whether IT or OT infrastructures, to play a key role in day-to-day security operations.

OPSWAT.
Trust no file. Trust no device.

For further information
https://www.opswat.com/solutions/malware-analysis