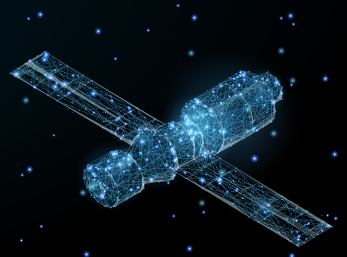
VMRAY ANALYZER

X-Ray Vision for Malware

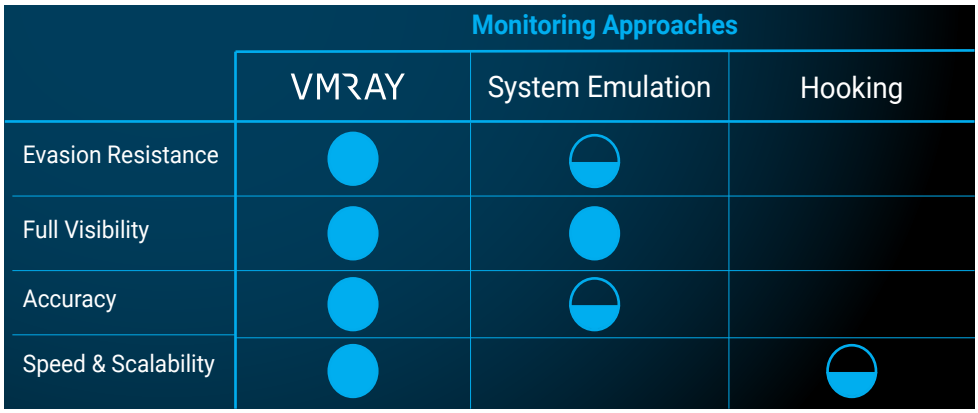


Datasheet

Our customers see VMRay Analyzer as a disruptive technology, one that solves the toughest challenges that SOC and DFIR teams face.

Trust the Gold Standard for Dynamic Malware Analysis

VMRay Analyzer is a breakthrough solution for dynamic analysis of advanced threats, including zero day and targeted attacks. By surmounting inherent flaws that plague other products, VMRay Analyzer has become the gold standard for malware sandboxing among leading DFIR teams worldwide.



With X-Ray Vision, Catch Threats Others Miss

The core of VMRay Analyzer is an agentless, hypervisor-based sandbox, which is unique in combining near-total evasion resistance with full visibility into malware behavior: a trait we call X-Ray Vision.

Because nothing touches or modifies the analysis environment, monitoring is invisible, and even the most evasive malware strains fully execute in the sandbox. By monitoring every interaction between malware and the target system, VMRay captures a complete and accurate record of threat behavior – data that enriches detection, incident response, digital forensics, and threat intelligence.

VMRay Intelligent Monitoring excels over other solutions in distinguishing between malicious behavior and legitimate activity. As a result, VMRay Analyzer delivers precise, noise-free output that reduces false positive rates to near zero. This shortens investigations, enhances efficiency and prevents legitimate traffic from being blocked.

Where Others Fall Short

Here's why competitors can't keep up with VMRay Analyzer:

Static Analysis solutions are only effective at analyzing and detecting known malware. In-depth static analysis does not scale.

System Emulation promises full visibility into malware activity. In practice, this approach is slow and costly to scale. So vendors make trade-offs, compromising security to boost performance.

Hooking-Based Monitoring places instrumentation in the analysis environment, which is easily detected and evaded by advanced threats, leaving gaps in visibility.

The Best Choose VMRay

3 of the FAANG
4 of the Big 6 accounting firms
10 Global financial organizations
63 Government customers

VMRAY

VMRAY ANALYZER

Automation: Set It and Forget It

All VMRay Analyzer features and functions are mapped to our REST API; key threat indicators are mapped to the MITRE ATT&CK™ framework. Our flexible REST/JSON interface enables security teams to automate the submission of suspicious files and URLs, easily extract actionable threat intelligence, and integrate VMRay Analyzer with other security tools across heterogeneous environments.

Core Capabilities and Advanced Features

Fully Automated Analysis shortens DFIR investigations with hands-free features such as simulated user interaction and automatic reboot to trigger malicious behavior.

Manual Analysis lets team members interact with suspicious malware in near real time to identify IOCs and fully reveal harmful behavior that automated methods occasionally miss.

Automated IOC Extraction captures threat details (files, URLs, network traffic, registry activity) to enhance incident response, threat intelligence and support threat hunting.

Golden Images and Cloud Localization support lets you replicate the users' production environment to optimize detection of targeted malware.

Smart Memory Dumping supports deep-dive investigations by capturing "just the right information at just the right time," without noise or visibility gaps.

Phishing Detection identifies credential-harvesting and drive-by download sites.

Key Facts

Platforms: Windows, macOS

Coverage: Full range of file types and URLs

Deployment: Cloud or On-Premises

Integration: 25+ built-in connectors for web, email, SOAR, EPP/EDR and other tools

Compliance: GDPR-compliant, ISO-27001 certified

IDA Plugin: Enrich IDA Pro static analysis with behavioral-based data

Support for Industry Standards: MITRE ATT&CK™ Framework, YARA rules, STIX™ and others

Tailored Environments: Golden images and cloud localization for optimizing detection of targeted malware

Let's Talk...

Contact us at sales@vmray.com
or call 1+ 888-958-5801 (N. America)

Carbon Black.

"What our team loves about VMRay is the ability to quickly triage a lot of malicious samples by providing a wide variety of targets, configurations and applications out of the box. We get a good sense of all the behavior, whether it uses an Office document or malicious PDF. And because VMRay foils many sandbox-evasion techniques [it] allows more malware to run."

VMRAY