VMRAY ANALYZER

For Total Visibility and Defense Against Evasive Malware

In the battle against malware, behavior-based analysis is one of the keys for security teams to detect and mitigate advanced threats. In the controlled environment of a network sandbox, suspect files are detonated and monitored to determine if they're harmful and should be blocked.

Established sandbox solutions have shortcomings that undermine detection and analysis. Some signal their presence, triggering evasion by the malware. Other solutions struggle to scale, or generate needlessly large quantities of data, reducing the speed and accuracy of analysis.

The Power of An Agentless Approach

VMRay Analyzer overcomes these weaknesses with a revolutionary departure from prior methods. Using an agentless, hypervisor-based approach to monitoring, combined with a built-in rapid reputation engine, VMRay Analyzer delivers four traits critical for SOC Analysts and CERTs:

STEALTH
VMRay Analyzer defeats advanced malware evasion techniques

VISIBILITY
Comprehensive dynamic malware analysis enables full insight into malware behavior

SPEED
Bare-metal performance powers rapid threat detection at scale

DEFENSE
Actionable intelligence for even the most evasive malware

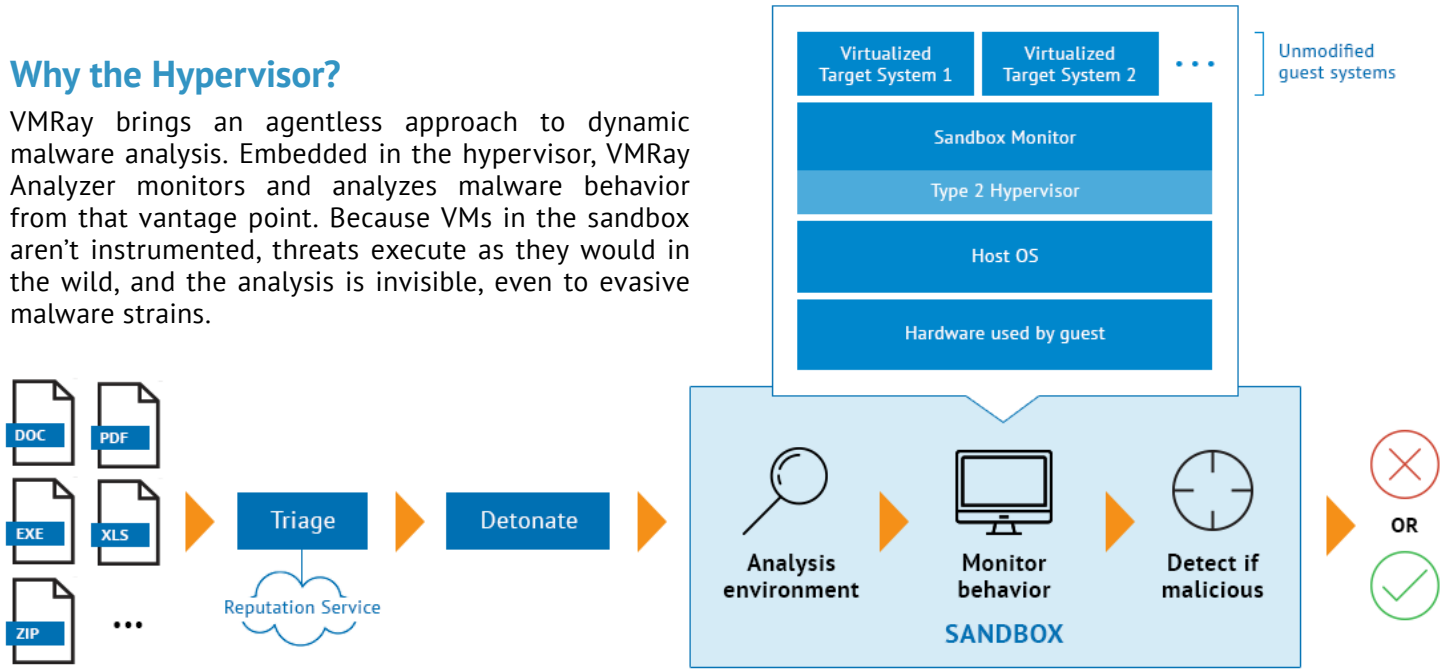
Key Benefits

- Rapid threat detection at scale, with the industry's most comprehensive dynamic threat analysis
- Agentless, hypervisor-based: resistant to detection and evasion by malware
- Reputation engine with severity classification provides fast, automated, actionable intelligence
- Bare metal performance by leveraging CPU hardware virtualization extensions
- Monitors all relevant activity with total visibility into low-level control flow
- Flexible results formats for forensic specialists, IR teams and managers
- Seamless integration with 3rd party security platforms
- Deployed by leading enterprises, security solution providers and OEMs

With VMRay Analyzer digital forensics and incident response (DFIR) specialists can quickly determine whether files are malicious and remedial action needs to be taken. With flexible alerting for SIEM and out-of-the-box connectors for top security platforms, VMRay Analyzer integrates easily into an automated solution for enterprises, solution providers, and OEMs.

Why the Hypervisor?

VMRay brings an agentless approach to dynamic malware analysis. Embedded in the hypervisor, VMRay Analyzer monitors and analyzes malware behavior from that vantage point. Because VMs in the sandbox aren't instrumented, threats execute as they would in the wild, and the analysis is invisible, even to evasive malware strains.



Real-time, High-volume Detection of Known Files

VMRay's reputation engine leverages the industry's most comprehensive source of reputation data on files. It detects known goodware and malware in milliseconds and returns a status —without executing the files.

Comprehensive Network Communication Analysis

VMRay analyzes and captures all network communication, looking for malicious intent. It maps out domains and IP addresses accessed by malware and the protocols used. PCAP files can be opened in a tool like WireShark for deep-packet inspection and analysis. VMRay can run analyses against multiple environments: the combinations of operating system, applications and localization that are of most concern to the IR team.

Actionable Malicious Behavior Scoring

Using threat identifier rules, the system generates a severity score and delivers actionable intelligence to relevant tools: SIEM, EPP, NGFW and others. These tools can automatically block, allow, report, alert, quarantine or remediate.

Carbon Black.

"Our customers are targeted by the most evasive, advanced malware around. When analyzing threats, VMRay Analyzer provides deep analysis and insights that surpass what we've seen from other technologies."

THREAT RESEARCH TEAM

Hindering Analysis by Hiding in Plain View

Malware often incorporates advanced evasion techniques. When a file sees evidence that dynamic analysis is occurring, it mimics harmless files that are typically ignored by threat detection systems. Sandboxing approaches that signal their own presence—for example by instrumenting underlying VMs to intercept malicious function calls—make the analysis environment visible, triggering malware to conceal itself.

Visibility into malware behavior can be compromised in other ways as well. For example, most approaches generate large quantities of data, much of it irrelevant to behavioral analysis. This reduces the visibility, accuracy and speed of the analysis. Furthermore, the extra overhead can mean they can't be easily scaled. Or, while an approach like hooking can scale, it uses shortcuts or simplifications that undermine threat detection.

HOW VMRAY ANALYZER IS USED:

Incident Response by enterprise DFIR teams

Protection that's driven by actionable results

Threat Intelligence that enhances security provider solutions

OEM Integration to embed VMRay in security appliances and cloud solutions

SONICWALL

"SonicWALL Capture Advanced Threat Protection Service incorporates the VMRay third-generation Analyzer threat detection analysis engine, supporting SonicWALL's ability to deliver a first-to-market, adaptive, multi-engine sandboxing approach that enhances organizations' ability to safeguard against today's shape-shifting cyber threats."

DMITRIY AYRAPETOV, EXECUTIVE DIRECTOR
PRODUCT MANAGEMENT

VMRAY ANALYZER FEATURES

Evasion Resistance

Immune to advanced evasion techniques

Survives system reboot and monitors autostart operations

Extensive Coverage

Broad coverage of user- and kernel-level malware types

Complete visibility into low-level control flow

Detailed behavioral analysis and network semantics

Customizable Yet Automated

Built-in Yara ruleset can be customized and extended

Supports custom pre-analysis scripts to tailor the environment for each analysis

Manual interaction with malware using VNC

Easy Deployment and Use

Offered as a cloud service or on premises

Access to all functionality via a user-friendly Web interface or REST APIs

Cost-effective scalability

Seamless Integration

Out-of-the-box support for third-party platforms: Carbon Black, Splunk, ThreatConnect, Ayehu, VirusTotal, MISP, Phantom, and Cisco CloudLock

Flexible REST/JSON API provides seamless integration into other products

Flexible Result Formats

High-level, summary reports for non-security experts and managers

Fine-grained, function-level logs with all input and output parameters

Output formats for automated processing or manual review: HTML, XML, CybOX/STIX, JSON and text files

Get hands-on with VMRay Analyzer

VMRay Analyzer provides DFIR specialists with the high-value capabilities they need to combat advanced threats: evasion resistance, rapid detection, and accuracy in identifying malicious files and behavior.

Available as a cloud service or on-premises solution, VMRay Analyzer has been successfully deployed by leading enterprises, security solution providers and OEMs. To get a sense of its power, accuracy and ease of use, request a demo or start your free, 30-day trial by contacting **sales@vmray.com.**

CONTACT US

VMRay Inc. | www.vmray.com | P: +1 (888) 958-5801