VMRay Analyzer

www.vmray.com

"VMRay Analyzer rapidly analyzes zero day threats, targeted attacks, 64-bit rootkits and other malware that evades existing virtual machine detonation technologies in the market today."

Dmitri Alperovitch, Co-Founder and CTO of CrowdStrike

Key Features

- Analyzes everything, including 64-bit rootkits and other malware that evades other solutions
- Detects zero day threats and targeted attacks
- Evasion resistant
- 3rd generation technology: hypervisor integration & unique monitoring method
- Provides full insight into malware activities at different abstraction levels
- Delivers unparalleled performance providing the fastest possible threat analysis & detection
- Easy installation and usage. No special expertise necessary
- Customizable and flexible API for seamless integration
- Intuitive high-level management reports
- Ability to zoom in to fine-grained behavior descriptions at system level

Why VMRay Analyzer

VMRay Analyzer quickly and reliably analyzes any piece of malware, including the most dangerous threats like 64-bit rootkits. Unlike traditional analysis systems VMRay Analyzer cannot be evaded by malware because of its unique hypervisor-based approach.

Sophisticated analyses are generated at multiple abstraction levels, ranging from high-level severity classification down to fine-grained system level behavior. The results can easily be utilized by forensic specialists, non-security experts and managers.

With its flexible scalable API, VMRay Analyzer can be integrated seamlessly into high-throughput automated security solutions.

Revolutionary Hypervisor-based Approach

With its innovative 3rd generation design, VMRay Analyzer provides the fastest dynamic threat detection in the market today. By instrumenting unique hardware virtualization extensions, examined malware runs on bare-metal and executes with near-native performance. It can be run on hundreds of machines in parallel to analyze 100,000's of samples per day.

VMRay's approach is a revolutionary departure from simply analyzing a virtual machine (VM) inside a hypervisor. VMRay is directly integrated into the hypervisor. Because ***nothing*** is modified inside the VM the analysis process is invisible and cannot be evaded.

By leveraging new CPU features with a unique monitoring method, VMRay provides a level of analysis detail and amount of information surpassing traditional analysis systems. VMRay monitors all interaction between the analyzed software and the operating system and installed applications.

START NOW

Start your **free 30 day trial** today

To explore the capabilities of VMRay Analyzer, we offer a **free 30-day trial** of VMRay Cloud service. To start your free trial period, contact us at ***sales@vmray.com***.

Covers all types of Malware and behavior:

- ✓ User and kernel-level malware: apps, drivers, Office documents (PDF, DOC, etc.) and URLs
- ✓ Low-level control flow (API function calls, system calls, interrupts, APCs, DPCs, etc.)
- ✓ High-level semantics (file system, registry, network, user/group administration, etc.)
- ✓ Identifies and parses Layer7 protocols (HTTP, FTP, IRC, SMTP, DNS, etc.)

Evasion resistant

- ✓ Detects master boot record (MBR) tampering
- ✓ Survives system reboot and monitors autostart operations
- ✓ Immune to evasion techniques (like system calls, skipping function prologs and more)

Comprehensive Rootkit Analysis

- ✓ Operates from ring "-1": full control and monitoring of even high privileged kernel malware
- ✓ Monitors the complete system if kernel code execution is detected
- ✓ User-friendly visualization of malicious kernel code blocks and their interdependence



Adaptable Results

- ✓ Summary high-level reports for non-security experts and managers
- ✓ Fine-grained function level logs with all input and output parameters
- ✓ Output formats for human and machine processing: HTML, XML, and text files

Automated Severity Classification

- ✓ Severity of each analyzed file is automatically determined to assess its maliciousness
- ✓ Allows automated mitigation of zero day threats and targeted attacks
- ✓ Summary of malicious artifacts allows risk estimation at a glance

Highly Customizable

- ✓ Fully customizable configuration: install the security patches and applications you want
- ✓ Custom pre-analysis scripts to individually configure the system environment for each analysis
- ✓ Interact manually with the malware by using VNC



Easy Installation, Usage and Integration

- ✓ Debian packages for easy installation and updates
- ✓ Easy access to all functionality via user-friendly Web UI
- ✓ Flexible API for seamless system integration into other security products

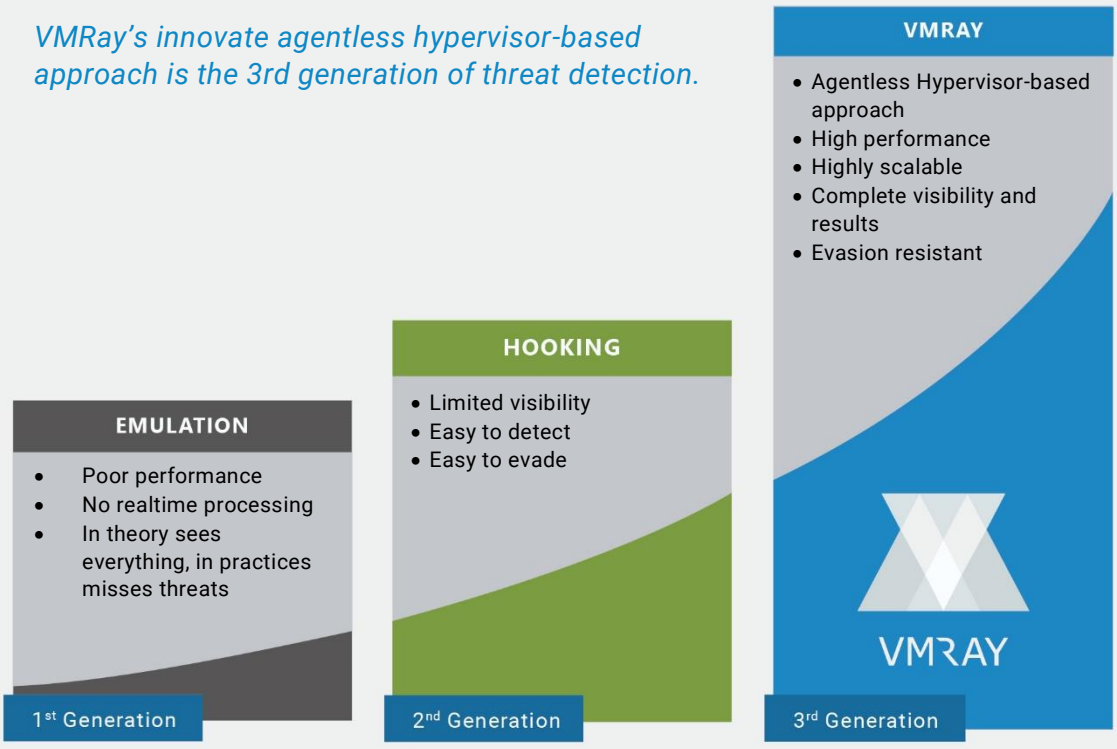
On-Premise or Cloud

VMRay Analyzer can be installed on premise or used as a cloud service.

The on premise solution does not require special hardware yet still allows full customization of the virtual analysis environments. Multiple customized VMs can be operated in parallel, each one with a different patch level or different set of installed target applications. For instance, VMRay analyzes PDF documents in dozens of different reader applications and versions very quickly and at the same time.

VMRay's cloud solution gives you the benefit of not having to worry about software installation, hardware maintenance, or providing a reliable network infrastructure. Immediately start analyzing suspicious files, either directly by the easy to use web interface or by utilizing the flexible API. All generated analyses can be comfortably displayed and navigated interactively via your browser, and can also be downloaded for (later) off-site usage.

VMRay's innovate agentless hypervisor-based approach is the 3rd generation of threat detection.



No other malware analysis technology compares

START NOW

Start your **free 30 day trial** today

To explore the capabilities of VMRay Analyzer, we offer a **free 30-day trial** of VMRay Cloud service. To start your free trial period, contact us at ***sales@vmray.com***.