VMRay Analyzer

"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

- Evasion Resistant: Unique agentless monitoring approach with hypervisor integration
- Near-native performance using hardware virtualization extensions
- User and kernel-level malware analysis: Apps, drivers, documents and URLs
- Detects zero day threats and targeted attacks
- REST/JSON API for seamless integration into automated security solutions
- YARA rule support
- Browser based VNC access for manual VM interaction
- Automated document interaction such as auto-detonation of links in documents, mouse clicks etc.
- Out of the box connectors for 3rd party security platforms
- VMRay Threat Identifier (VTI) engine provides actionable, customizable severity score

Why VMRay Analyzer

VMRay Analyzer uses a unique agentless hypervisor-based monitoring approach to detect malware. Unlike other virtualization based approaches VMRay Analyzer cannot be evaded because of its unique monitoring 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 be easily used by forensic specialists, IR teams and managers.

With its flexible, scalable REST/JSON API and Syslog/CEF support for SIEMs, VMRay Analyzer can be integrated seamlessly into automated security solutions.

Revolutionary Hypervisor-based Approach

VMRay's approach is a revolutionary departure from traditional virtualization based malware analysis systems. Since it is directly integrated into the hypervisor, nothing is modified inside the VM. As a result, the analysis process is invisible to malware and cannot be evaded.

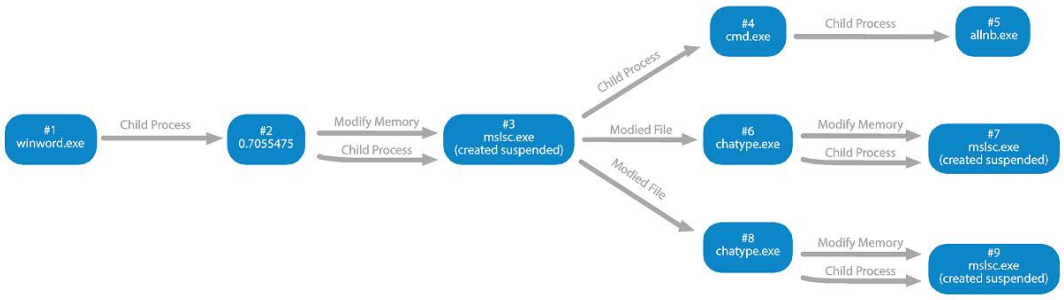
By leveraging unique hardware virtualization extensions, malware runs on bare-metal and executes with near-native performance. Hundreds of virtual machines (VMs) can run in parallel to analyze 100,000's of samples daily. Each VM can be customized, or existing gold images used.

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

VMRay's approach is a revolutionary departure from simply analyzing malware within a VM.

Extensive coverage of malware and full insight into behavior

- User and kernel-level malware: apps, drivers, documents (PDF, Word, Excel, etc.) and URLs
- Low-level control flow (API functions, COM methods, system calls, interrupts, APCs, DPCs, etc.)
- High-level and network semantics (filesystem, registry, network, etc.



Evasion resistant

- Survives system reboot and monitors autostart operations
- Immune to evasion techniques (like direct system calls, skipping function prologs and more)
- Operates from ring "-1": full control and monitoring of even high-privileged kernel malware

Unparalleled performance

- Leverages unique hardware virtualization extensions, executes with near-native performance
- Hundreds of virtual machines (VMs) can run in parallel

Seamless Integration

- Flexible REST/JSON API for seamless system integration into other security products
- Out-of-the-box connectors for 3rd party platforms: Splunk, CarbonBlack, ThreatConnect, Metadefender

Flexible Result Formats

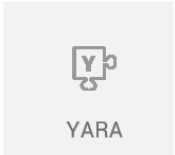
- Summary high-level reports for non-security experts and managers
- Fine-grained function level logs with all input and output parameter
- Output formats for manual review or automated processing: HTML, XML, CybOX/STIX, JSON, and text files

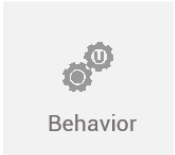
Severity Classification: VMRay Threat Identifier (VTI)

- Severity is automatically determined to assess maliciousness
- Enables automated mitigation of zero day threats and targeted attacks
- Summary of malicious artifacts for risk estimation at a glance
- Easy identification of vulnerable applications

Highly Customizable Yet Automated

- Support for creation of Yara rulesets
- Custom pre-analysis scripts to individually configure the system environment for each analysis
- Interact manually with the malware by using VNC



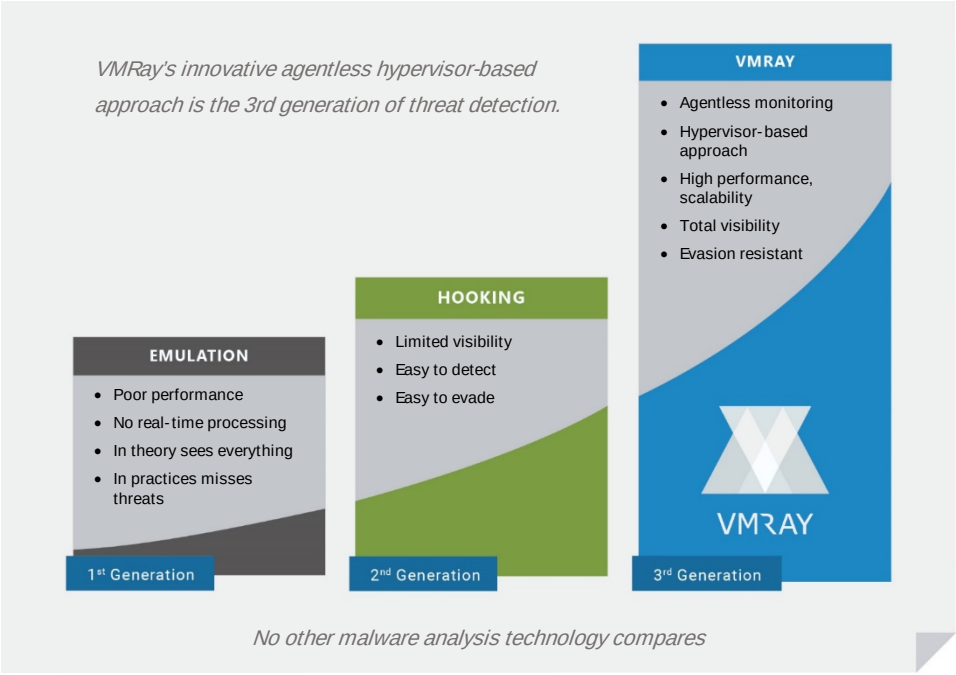


Easy Installation, Usage and Integration

- Debian packages for easy installation and updates
- Easy access to all functionality via user-friendly Web UI
- Flexible REST/JSON 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.



START NOW

Start your **free 30-day trial** today by contacting us at ***sales@vmray.com***.