VMRay Analyzer

AGENTLESS THREAT DETECTION

"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."

SONICWALL™

Patrick Sweeney, Vice President, Product Management and Marketing, SonicWALL

Key Features

- Evasion Resistant: Embedded in hypervisor for unique agentless monitoring
- Built-in reputation engine and severity classification
- 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)

Why VMRay Analyzer

VMRay Analyzer combines rapid reputation scoring of files with a unique agentless hypervisor-based monitoring approach for deep analysis. With this combination VMRay Analyzer delivers rapid threat detection at scale coupled with the most comprehensive dynamic threat analysis in the industry.

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, Syslog/CEF alerting for SIEMs and a range of out-of-the-box connectors for products like the Splunk® Enterprise Platform, VMRay Analyzer can integrate seamlessly as part of an automated security solution.

Revolutionary Hypervisor-based Approach

VMRay Analyzer is a revolutionary departure from traditional virtualization-based malware analysis. Since it is directly integrated into the hypervisor, nothing is modified inside the virtual machine (VM). As a result, the analysis process is invisible to malware and cannot be evaded.

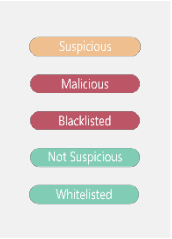
By leveraging unique hardware virtualization extensions, malware runs on bare-metal and executes with near-native performance. Hundreds of VMs can run in parallel to analyze 100,000's of samples daily. Each VM can be customized, or existing gold images used.

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.

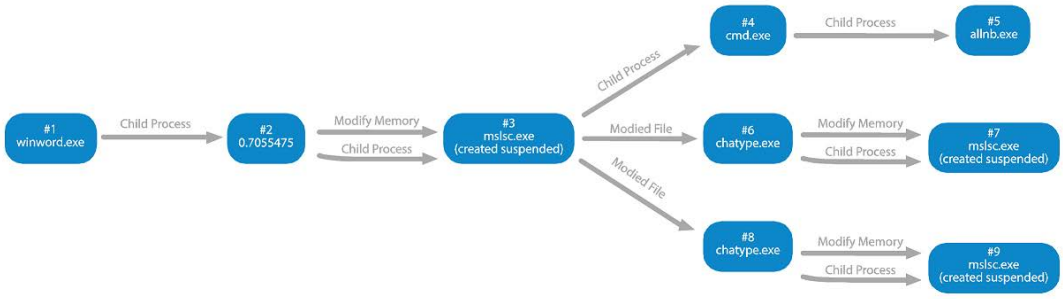
Built-in Reputation Engine and Severity Classification

- Detects known benign or known malicious files in milliseconds
- Provides real-time, high volume malware detection
- Triage mode queries reputation engine and runs malware analysis only if reputation status is unknown
- Provides actionable severity classification



Extensive Coverage of Malware and Full Insight into Behavior

- Analysis of user and kernel-level malware: apps, drivers, documents (PDF, Word, Excel, etc.) and URLs
- Complete visibility into low-level control flow (APIs, COM methods, system calls, interrupts, APCs, DPCs)
- Detailed behavioral analysis and network semantics (filesystem, registry, network interaction etc.)



Evasion Resistant

- Survives system reboot and monitors autostart operations
- Immune to evasion techniques (like direct system calls, skipping function prologs and more)
- Operation in ring “-1” provides full control and allows 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

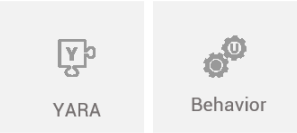
- Flexible REST/JSON API for seamless system integration into other security products
- Out-of-the-box connectors for 3rd party platforms: Splunk, CarbonBlack, ThreatConnect, Metadefender

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

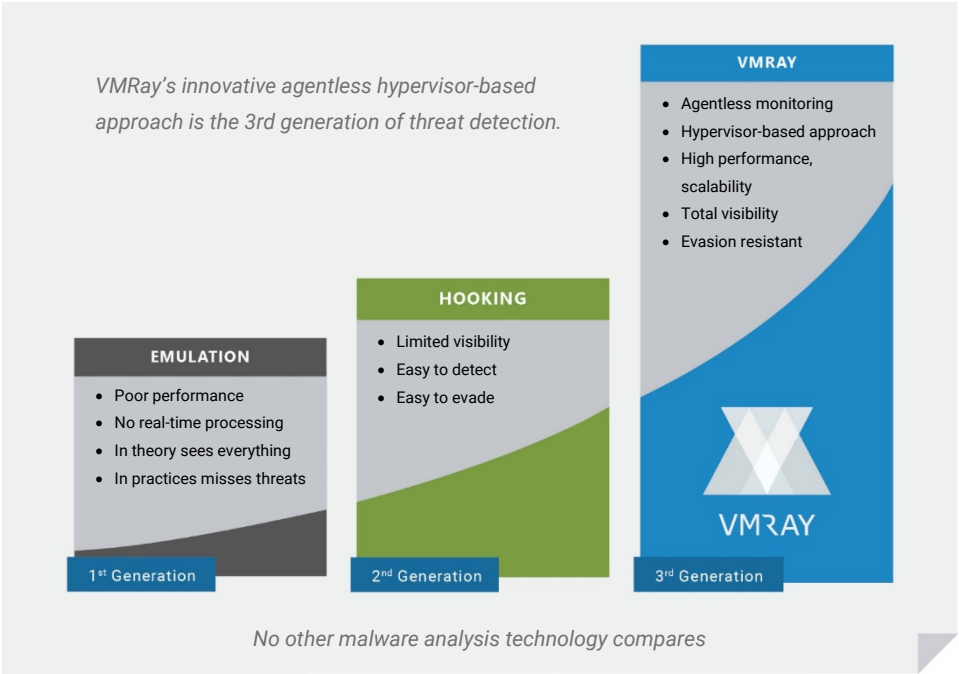
Highly Customizable Yet Automated

- Supports custom YARA rules
- Custom pre-analysis scripts to individually configure the system environment for each analysis
- Interact manually with the malware by using VNC



Easy Installation and usage

- Debian packages for easy installation and updates
- Easy access to all functionality via user-friendly Web UI
- 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***.

"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 sandbox technologies. Like Carbon Black, VMRay strikes a balance between being easy-to-use while providing a powerful, rich, feature-set."

Carbon Black Threat Research Team

CARBON BLACK