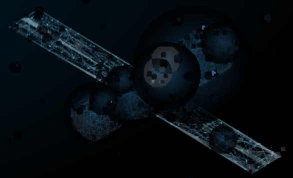
VMRAY DETECTOR

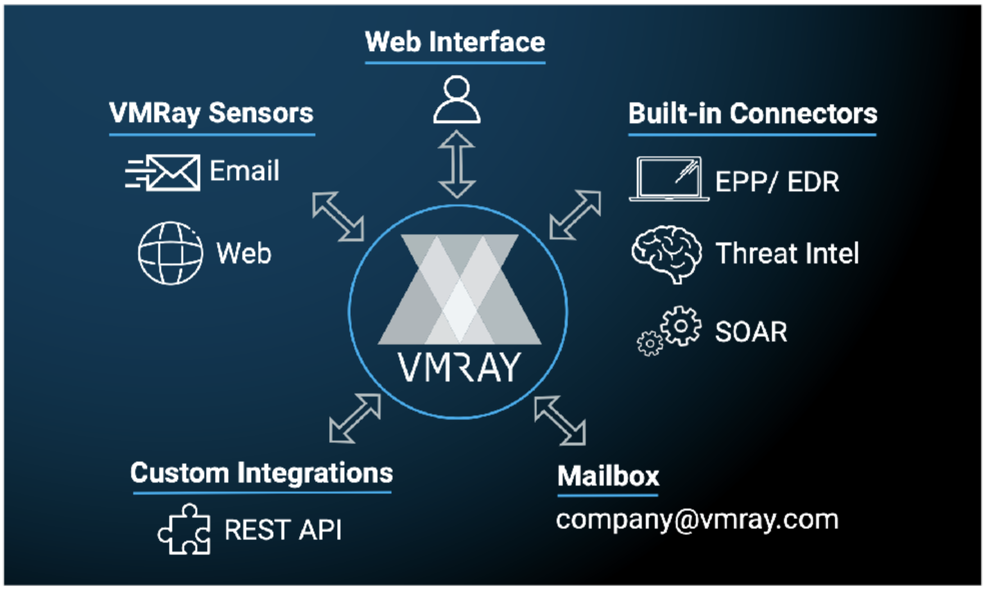
High-Precision Threat Detection at Scale



Data Sheet

Scalable, Accurate Threat Detection at the Core of Your Security Infrastructure

SOC teams struggle to contain the deluge of advanced malware threats that flood the security ecosystem every day from all directions. Now they can turn the tide with VMRay Detector, a high-volume, fully automated solution for fast, accurate malware detection.



VMRay integrates with the security ecosystem via web and email gateways, built-in connectors, VMRay sensors and our REST API.

Integrated with other security tools and platforms, VMRay Detector can ingest the massive volume of potential threats that are seen by email and web gateways, endpoint detection systems, security operations systems, and so on. VMRay Detector subjects all this data to a multi-stage, fully automated detection process. Applying the appropriate detection technologiy at just the right time, the system quickly winnows out benign files and URLs while submitting suspicious or unknown samples to increasing levels of scrutiny. High level detection results can be used by other security tools to automate block/allow decisions and other protection measures. Where it's warranted, detection results are available to the CERT team for deeper investigation and incident response.

VMRay Detector is based on our groundbreaking sandboxing technology and Now, Near, Deep architecture for malware analysis and detection. Because VMRay's hypervisor-based sandbox is invisible to malware, it detects even highly evasive strains that other solutions miss.

Key Benefits

- Groundbreaking technology detects highly evasive malware that other platforms miss.
- Accurate detection, without human intervention, reduces false positives that divert SOC staff from more critical tasks.
- Solution scales to support increased email volumes without hurting performance or TCO.
- Complements anti-spam and anti-phishing solutions.
- Can be deployed in the cloud or on-premises.

See Everything, Detect All

- Empowers SOC teams to master a deluge of threat information from many sources.
  Fully automated threat detection, with no human intervention needed.
- Leverages a REST API and the integration capabilities of VMRay Analyzer.
- Scales to support the growing volume of threat data, without compromise.

VMRAY DETECTOR

VMRay’s Now, Near, Deep Architecture

VMRay Detector automates the malware detection process and quickly distinguishes between malicious and benign files: dismissing the latter so system resources can be focused on the former. Because of VMRay’s high accuracy and low noise, detection is automatic, with no human intervention required. The solution architecture integrates three core components:

Now: Rapid Reputation Lookup of Potential Threats

In milliseconds, a quick lookup identifies and dismisses known benign files while submitting malicious files and URLs and unknown but potential threats for further scrutiny. The rapid reputation engine leverages threat intelligence from leading security providers.

Near: Static Analysis of Active Elements

In seconds, VMRay’s proprietary static analysis looks at embedded scripts, macros and other active components that could indicate a multistage threat. Clean files are dismissed, while those with higher severity scores are passed along for dynamic analysis.

Deep: Dynamic Analysis to Enhance Accuracy

Isolated in VMRay’s malware sandbox, known or suspected malware is allowed to execute without interruption so malicious files can be identified with a high degree of certainty. High-level detection data can be automatically shared with other vendor’s integrated security tools to drive block/allow decisions and inform the incident response process.

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, endpoint and other tools

Compliance: GDPR-compliant and ISO-27001 certified

Support for industry standards: MITRE ATT&CK™: Framework, YARA rules, STIX™ and others

Let’s Talk

Contact us at sales@vmray.com
or call +49 234 973 55 40 0

CyberInt is detecting a growing amount of threats both in volume and sophistication that successfully recognize and evade sandbox environments. Our cyber analysts leverage VMRay’s multi-layered analysis engine to rapidly detect evasive threat variants

Adi Peretz, Head of Threat Research Cyberint

VMRAY