DATASHEET

Malware, Meet Your Match:

The Most Advanced Deep Threat Analysis Solution

DeepResponse

Stay ahead of emerging threats with the most advanced malware and phishing analysis solution.

Malware and phishing attacks can have severe consequences for organizations, including data breaches, loss of sensitive information, financial loss, and damage to reputation. **Effective malware and phishing analysis** are therefore important for organizations as it helps them to identify, mitigate threats and minimize harm.

Many vendors make broad claims about their analysis and detection capabilities. Still, when one looks at the underlying architecture, it becomes clear these vendors have been forced to accept painful tradeoffs, attempting to bridge the divide between **achieving a high rate of speed and providing deep visibility into malware behavior**. Because of the unique architecture of VMRay DeepResponse, the dynamic analysis engine sees every interaction between malware and the target system. The product logs and analyzes everything from simplistic, easily defeated attacks to advanced threats that good enough sandboxes aren't good enough to catch. This deep insight provides precise, actionable results that guide security measures across the enterprise.

VMRay DeepResponse helps organizations overcome their challenges in responding to and mitigating file and URL-based threats. With a focus on speed and efficiency, our malware and phishing analysis sandbox is designed to help you reduce incident response times, minimize threat dwell times, improve the ROI of your threat-hunting efforts as well as enable you to start your detection engineering journey efficiently. Comprehensive and in-depth analysis reporting of DeepResponse, strengthened by threat classification, malware configuration extraction, and IOC scoring, provides you with the **insights you need to fully understand the threats you face**.

DeepResponse also has functionality and volume level separation in the pricing plans, which can help organizations to select the features and capabilities that best meet their needs while also providing the flexibility to scale their use of the product as their needs change.

Benefits

Reduce time spent analyzing malware by 90%

Complete visibility into every malicious behavior

Lower the barrier for classifying malware families with configuration extractors

Structure hunting workflows with laser-sharp IOCs and IOBs

Enhance detection rules with unique and intriguing artifacts

Classification	Threat name	C&C	Processes
Banking Trojan	Qbot	Extracted	

90% less manual analysis

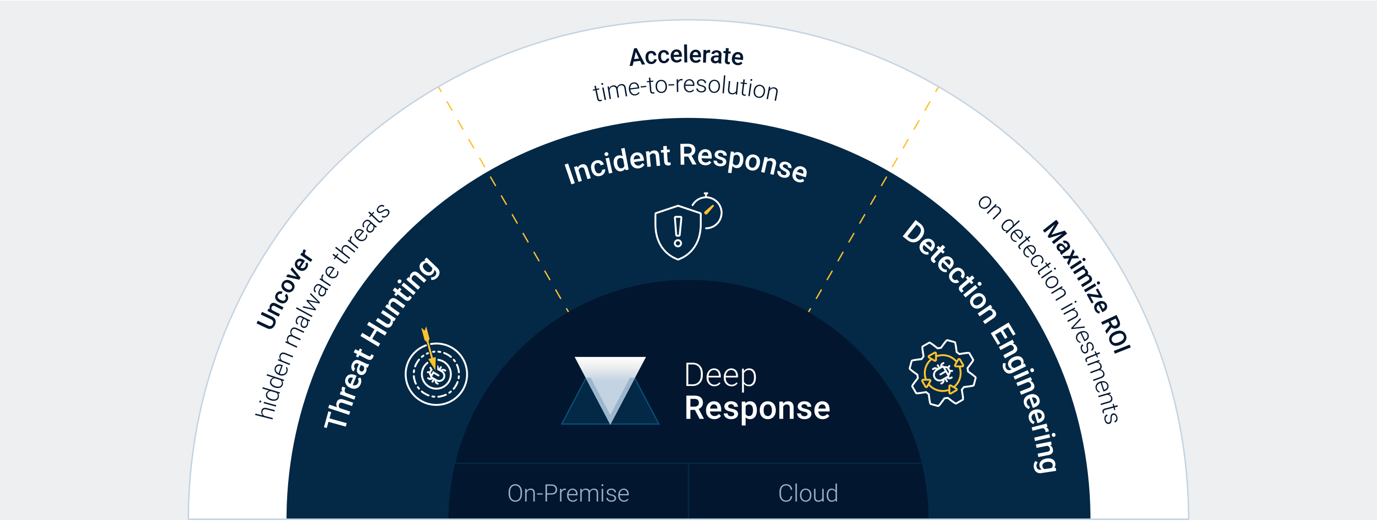


Figure 1. VMRay DeepResponse at a glance

Use cases

Incident Response

Incident response teams are often tasked with investigating confirmed incidents involving malware, phishing emails, malicious download links, or phishing URLs. This process can be **time-consuming and require manual analysis** to gain visibility into the malicious behavior. Modern threats are often highly evasive, making it difficult to uncover even the most sophisticated ones.

VMRay DeepResponse is designed to enhance and automate file and link analysis for incident response workflows. Thus, **saving analysts' time and enabling faster response** to incidents. The product also reduces skillset barriers in SOCs and CERTs by automating much of the analysis process.

Save precious time for incident response.

Threat Hunting

Threat hunting can be demanding, requiring a continuous analysis of recent threats in the wild and the extraction of indicators of compromise (IOCs) and behavior (IOBs) to pivot hunting operations on.

Built on VMRay Platform, DeepResponse is designed to enhance threat hunting capabilities for malware and phishing threats, giving security teams **deeper visibility** into the operations of real-world threats and thus enhancing the ability to assess the effectiveness of defenses against them. DeepResponse provides a wealth of data for threat hunters to enhance their processes, including classifying malware families, MITRE's ATT&CK mapping, and laser-sharp IOCs scored by relevance. On top of that, DeepResponse provides extensive behavioral information in its analysis reports, including a forensic super-timeline of every behavior.

Detect threats **more effectively**.

Detection Engineering

Security teams are often tasked with analyzing the most recent malware and phishing threats in the wild and manually creating detection rules for them using YARA and SIGMA. However, this can be challenging due to the large number of new threats appearing every day and the need for specialized expertise to analyze them.

VMRay DeepResponse is designed to help security teams quickly receive categorized indicators of compromise (IOCs) of outstanding merit and incorporate the information into their detection operations. By using DeepResponse, teams can **boost their productivity, maximize their return on investment** in analysis and detection, and **reduce the risk** of advanced tactics, techniques, and procedures (TTPs) going undetected.

Maximized ROI on detection investments.

See DeepResponse in Action

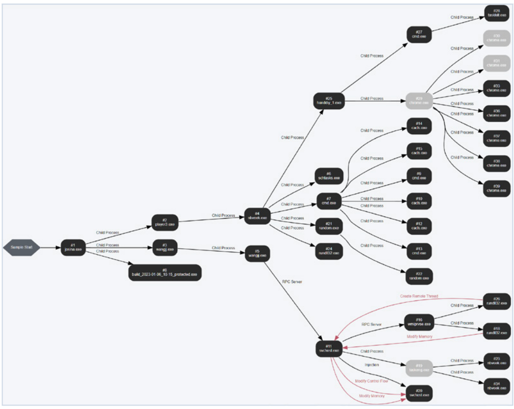
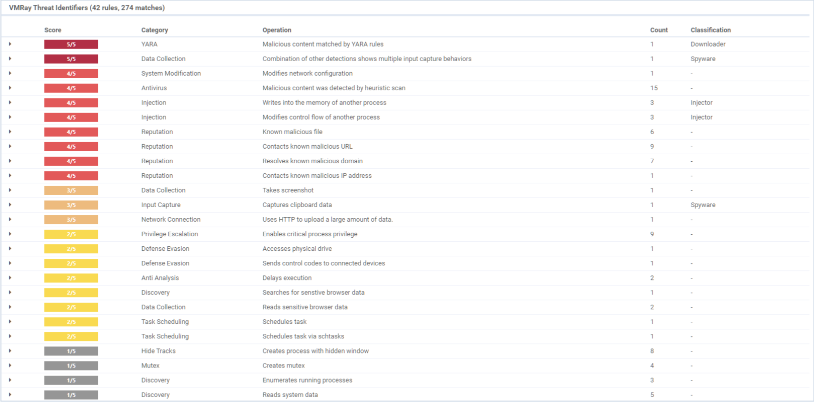


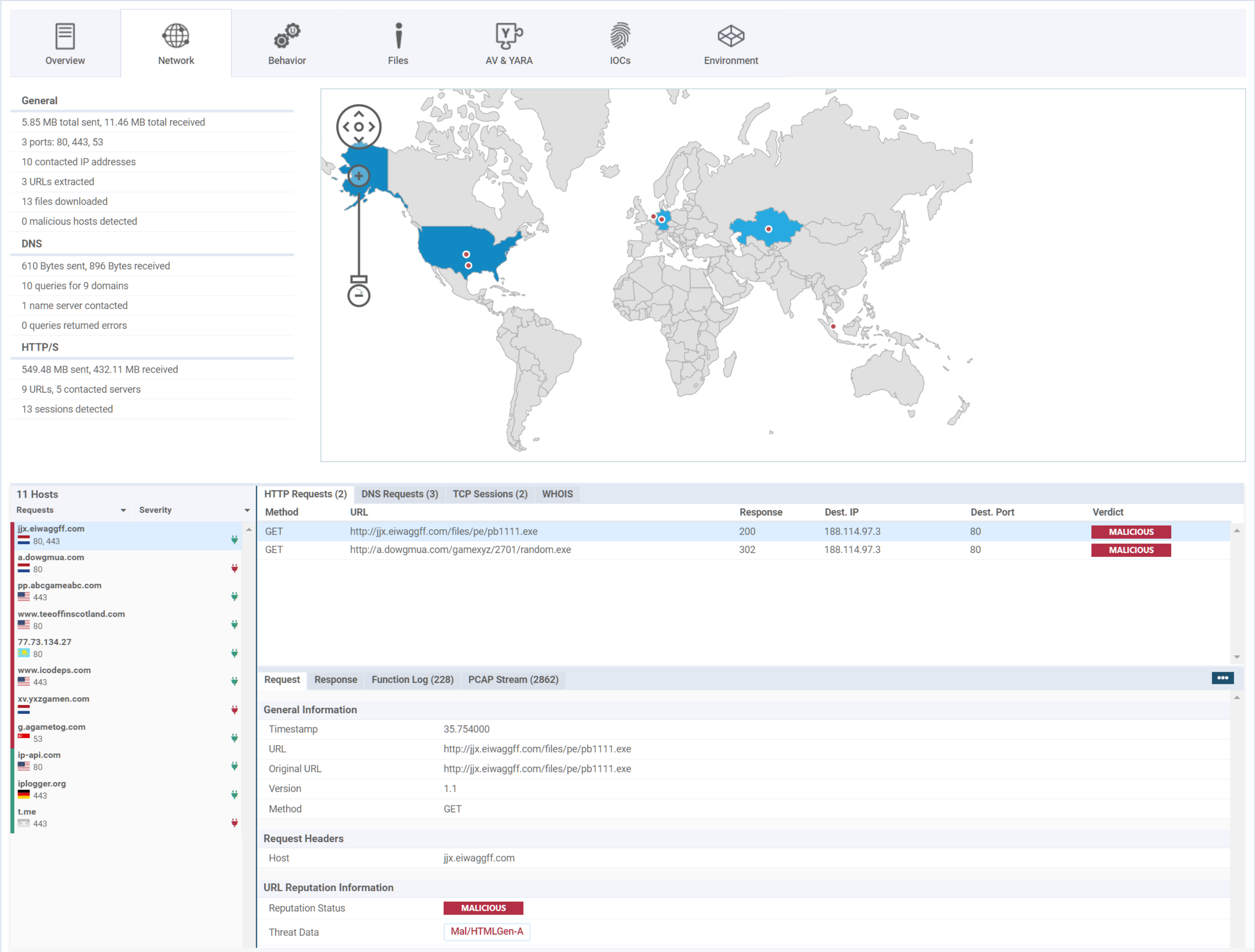
Figure 2. Monitored Processes



VMRay Threat Identifiers (42 rules, 274 matches)

	Score	Category	Operation	Count	Classification
▸	5/5	YARA	Malicious content matched by YARA rules	1	Downloader
▸	5/5	Data Collection	Combination of other detections shows multiple input capture behaviors	1	Spyware
▸	4/5	System Modification	Modifies network configuration	1	-
▸	4/5	Antivirus	Malicious content was detected by heuristic scan	15	-
▸	4/5	Injection	Writes into the memory of another process	3	Injector
▸	4/5	Injection	Modifies control flow of another process	3	Injector
▸	4/5	Reputation	Known malicious file	6	-
▸	4/5	Reputation	Contacts known malicious URL	9	-
▸	4/5	Reputation	Resolves known malicious domain	7	-
▸	4/5	Reputation	Contacts known malicious IP address	1	-
▸	3/5	Data Collection	Takes screenshot	1	-
▸	3/5	Input Capture	Captures clipboard data	1	Spyware
▸	3/5	Network Connection	Uses HTTP to upload a large amount of data.	1	-
▸	2/5	Privilege Escalation	Enables critical process privilege	9	-
▸	2/5	Defense Evasion	Accesses physical drive	1	-
▸	2/5	Defense Evasion	Sends control codes to connected devices	1	-
▸	2/5	Anti Analysis	Delays execution	2	-
▸	2/5	Discovery	Searches for senstive browser data	1	-
▸	2/5	Data Collection	Reads sensitive browser data	2	-
▸	2/5	Task Scheduling	Schedules task	1	-
▸	2/5	Task Scheduling	Schedules task via schtasks	1	-
▸	1/5	Hide Tracks	Creates process with hidden window	8	-
▸	1/5	Mutex	Creates mutex	4	-
▸	1/5	Discovery	Enumerates running processes	3	-
▸	1/5	Discovery	Reads system data	5	-

Figure3. Unique VMRay Threat Identifiers (VTIs)



General

5.85 MB total sent, 11.46 MB total received

3 ports: 80, 443, 53

10 contacted IP addresses

3 URLs extracted

13 files downloaded

0 malicious hosts detected

DNS

610 Bytes sent, 896 Bytes received

10 queries for 9 domains

1 name server contacted

0 queries returned errors

HTTP/S

549.48 MB sent, 432.11 MB received

9 URLs, 5 contacted servers

13 sessions detected

11 Hosts

Requests	Severity
jjx.eiwaggff.com 80, 443	
a.dowgmua.com 80	
pp.abcgameabc.com 443	
www.teeoffinscotland.com 80	
77.73.134.27 80	
www.icodeps.com 443	
xv.yxzgamen.com	
g.agametog.com 53	
ip-api.com 80	
iplogger.org 443	
t.me 443	

HTTP Requests (2) | DNS Requests (3) | TCP Sessions (2) | WHOIS

Method	URL	Response	Dest. IP	Dest. Port	Verdict
GET	http://jjx.eiwaggff.com/files/pe/pb1111.exe	200	188.114.97.3	80	MALICIOUS
GET	http://a.dowgmua.com/gamexyz/2701/random.exe	302	188.114.97.3	80	MALICIOUS

Request | Response | Function Log (228) | PCAP Stream (2862)

General Information

Timestamp	35.754000
URL	http://jjx.eiwaggff.com/files/pe/pb1111.exe
Original URL	http://jjx.eiwaggff.com/files/pe/pb1111.exe
Version	1.1
Method	GET

Request Headers

Host	jjx.eiwaggff.com

URL Reputation Information

Reputation Status	MALICIOUS
Threat Data	Mal/HTMLGen-A

Figure 4. Malicious Network Behavior and IOCs

Features

VM Introspection

API hooking is a technique used by most sandboxes to monitor behavior by redirecting and logging certain API calls. While this approach is relatively simple and quick to implement, it can cause performance and visibility issues as API hooking monitors only a limited number of functions. Additionally, it cannot distinguish between calls made by the sample being analyzed and those made by the operating system, leading to incomplete and noisy monitoring. VMRay DeepResponse, on the other hand, operates at the hypervisor layer and monitors all API calls, including their string parameters, for a more complete analysis. The logged API calls and strings can be used for malware detection, classification, and running custom YARA rules. They can also be downloaded in human-readable and machine-parsable formats.

Get a **more complete analysis** that also covers API calls thanks to **hypervisor based sandboxes**.

Machine Learning for Phishing

VMRay DeepResponse analyzes samples using cutting-edge advanced detection technologies that observe and report the “actual” behavior of malicious samples and generate accurate and noise-free outputs. This is why VMRay DeepResponse is trusted by leading private and public organizations to cover the blind spots and validate the alerts and false positives of their existing security products. DeepResponse’s Machine Learning model works as a module of this strong platform and gets the highest quality input directly from the dynamic analysis: reliable, relevant, and wide range of data.

Malware Configuration Extraction

VMRay DeepResponse can automatically extract and parse malware configurations for certain malware families including Qakbot, GuLoader, RedLine, AgentTesla and Remcos. Malware configurations contain detailed information about the malware’s behavior, including C2 addresses and indicators such as registry keys, mutexes, and filenames. Extracted malware configurations can be used for threat hunting and blocking. They can also be used to reveal connections among different malware samples and provide insight into the development of a malware family.

Detect **connections between different malware samples** and receive detailed information about their families and behavior.

Report and VTIs

The VTI scoring system is a clear and intuitive report which can be integrated into other security products and enterprise’s security ecosystem. Its clarity and simplicity are an advantage where some scoring systems are either incomprehensible or opaque. This clarity is especially important when responding to incidents because time is of the essence. The VTI scoring system accelerates the response process by providing clear answers to analysts. The full analysis report helps SOC teams to reduce attacker dwell time and take prompt remediation steps to prevent future attacks.

Automated IOCs Classification

IOCs (Indicators of Compromise) are a subset of artifacts, which are pieces of forensic data observed during analysis. It can be difficult for organizations to evaluate the effectiveness of IOCs generated by a malware sandbox, as misclassifying an artifact as an IOC can lead to false alerts and negative impacts on the organization's network. VMRay DeepResponse automates the process of extracting IOCs from analysis artifacts by flagging relevant artifacts as IOCs with VTIs to bridge the IOCs and IOBs. The VTIs are also used to assign a severity level to the IOC, which is presented in the Analysis Report IOCs tab along with a list of related VTIs.

MITRE ATT&CK Mapping

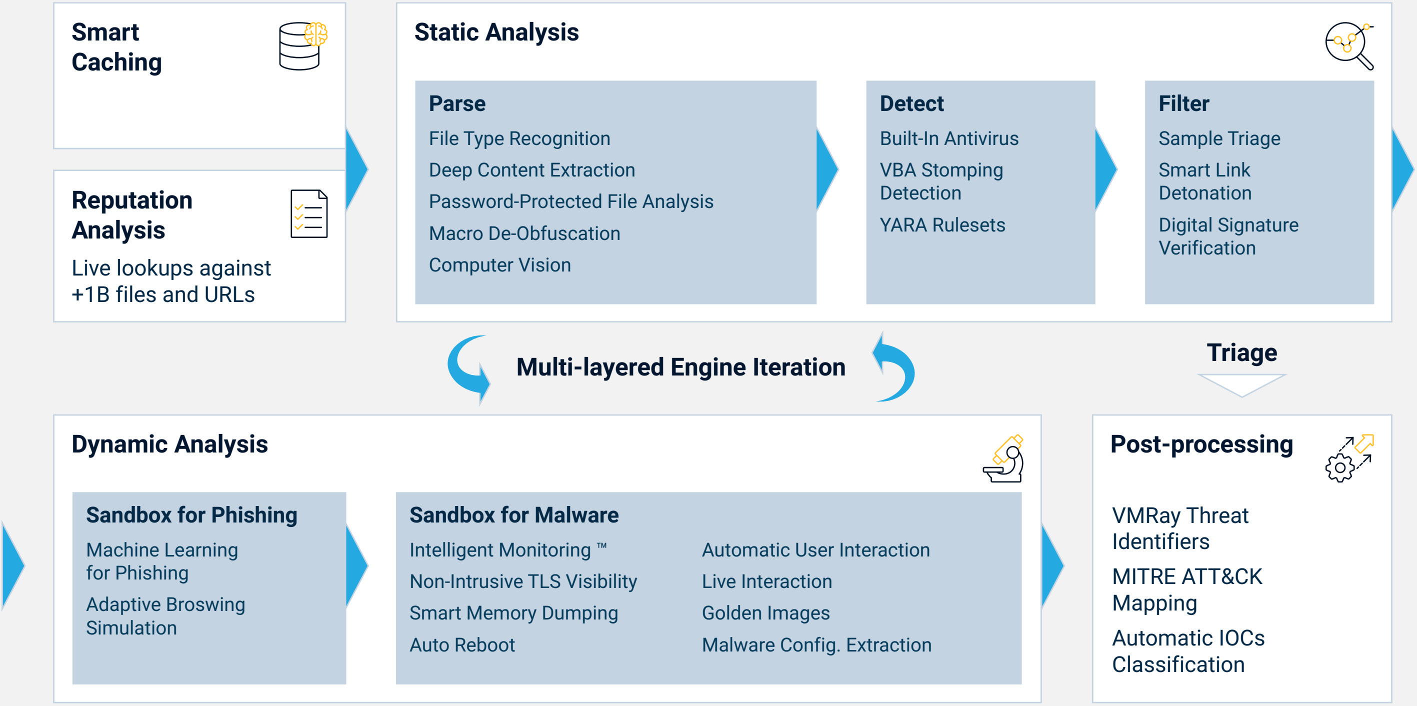
ATT&CK is the industry-standard framework and knowledge base of adversary tactics and techniques, threat groups, and related software and tools. Security teams can leverage the mapping of VMRay DeepResponse's analysis results to the MITRE ATT&CK framework for more effective incident response. The entire VMRay Threat Identifier (VTI) rules are mapped to the MITRE ATT&CK framework. This allows security teams to understand the scale and impact of an incident fast, leading to actionable mitigation measures.

Reduce false alarms caused by misclassification through VMRay DeepResponse's automated IOC extraction processes.

VMRay Platform Technologies

Built on VMRay Platform, DeepResponse utilizes the right technology at the right time for immediate detection of unknown threats.

The smart combination of 30+ technologies allows our customers to effectively defend against the latest threats.



Smart Caching

Reputation Analysis
Live lookups against +1B files and URLs

Static Analysis

Parse
File Type Recognition
Deep Content Extraction
Password-Protected File Analysis
Macro De-Obfuscation
Computer Vision

Detect
Built-In Antivirus
VBA Stomping Detection
YARA Rulesets

Filter
Sample Triage
Smart Link Detonation
Digital Signature Verification

Multi-layered Engine Iteration

Triage

Dynamic Analysis

Sandbox for Phishing
Machine Learning for Phishing
Adaptive Broswing Simulation

Sandbox for Malware
Intelligent Monitoring ™
Non-Intrusive TLS Visibility
Smart Memory Dumping
Auto Reboot
Automatic User Interaction
Live Interaction
Golden Images
Malware Config. Extraction

Post-processing
VMRay Threat Identifiers
MITRE ATT&CK Mapping
Automatic IOCs Classification

> What our team loves about VMRay is the **ability to quickly triage a lot of malicious samples** by providing a wide variety of targets, configurations and applications out of the box.
>
> We get a good sense of all the behavior, whether it uses an Office document or malicious PDF, and because VMRay foils many sandbox-evasion techniques and allows more malware to run. We also appreciate the little time-savers that VMRay has provided: quick access to PCAPs and function logs, sample tagging, and YARA rule tests against submitted samples.
>
> **Fortune 500 Company** | Cybersecurity & IT

Ready for the next step?

VMRay Public Threat Feed

Explore 1M+ analysis reports

https://threatfeed.vmray.com/

See DeepResponse in action

Request free trial

https://www.vmray.com/try-vmray-products/

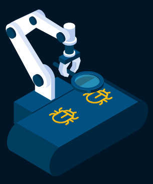
Portfolio

Our portfolio of products (DeepResponse, FinalVerdict, and TotalInsight) offers the ultimate solution for organizations looking to overcome their challenges in detecting and responding to malware and phishing threats.

Whether you need to automate alert processing, share industry-specific threat intelligence or build a comprehensive threat repository, our portfolio has you covered.

Deep**Response**

Final**Verdict**



Total**Insight**

VMRay Professional Services

At VMRay, our purpose is to liberate the world from **undetectable digital threats**.

Led by reputable cyber security pioneers, we develop best-of-breed technologies to detect unknown threats that others miss. Thus, we empower organizations to **augment and automate** security operations by providing the world's best threat detection and analysis platform.

We help organizations build and grow their products, services, operations, and relationships on secure ground that allows them to focus on what matters with ultimate peace of mind. This, for us, is the foundation stone of digital transformation.

Contact Us

Email: sales@vmray.com
Phone: +1 888 958-5801

VMRay GmbH

Suttner-Nobel-Allee 7
44803 Bochum • Germany

VMRay Inc.

75 State Street, Ste 100
Boston, MA 02109 • USA