DATA SHEET

VMRAY | Secez services

VMRAY ANALYZER

A Smarter, Stealthier Malware Sandbox

Today's advanced malware attacks execute in minutes and may persist for weeks or months, causing damage all the while. That's why rapid detection and fast, effective incident response are so essential.

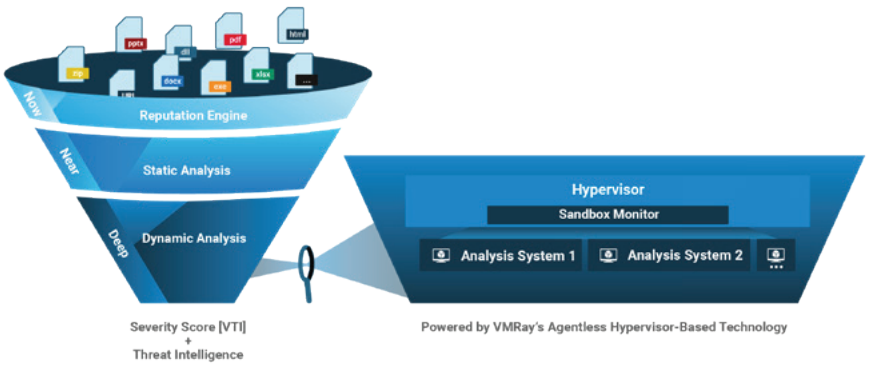
For under-staffed SOC and IR teams, traditional security solutions—which rely on signature-based reputation services and static analysis—are no match for today's zero day malware. Sandboxes based on dynamic analysis are more effective, but most have significant limitations.

Those shortcomings include:

- **Vulnerability to evasive measures:** Traditional sandboxes can't reliably detect malware evasion techniques, exposing organizations to attacks by these evasive threats.
- **Limited visibility into malware behavior:** Underlying technology limitations mean that most sandboxes have limited visibility into malware behavior, thus missing critical information
- **Noisy analysis results:** Most sandboxes generate analysis results packed with unrelated system activity or noise, which slows down incident response.

UNMATCHED PROTECTION AGAINST ADVANCED THREATS

VMRay's groundbreaking solution for malware analysis and detection addresses all these shortcomings. The core of VMRay Analyzer is an agentless, hypervisor-based dynamic analysis engine that detects even the most evasive malware variants. Combined with the strengths of a built-in rapid reputation service and VMRay-developed static analysis, our industry leading platform provides complete, uninterrupted visibility into malware behavior.



EMPOWER YOUR TEAM

- Address the challenges that stem from skills shortages and lack of automated tools.
- Analysts can quickly evaluate and triage incoming threats, getting immediate insights into suspicious files and links.
- Enabling SOC and IR teams to do a rapid "deep dive", gaining a complete understanding of a threat's behavior.

> *Carbon Black's customers are targeted by some of the most evasive and advanced malware around. Our team uses VMRay Analyzer to provide deep analysis and insights that surpass what we've seen from other sandboxing technologies.*

Carbon Black.
Threat Research Team

As a result, security teams can quickly analyze, detect and respond to advanced threats, including those that other technologies miss. VMRay's combination of evasion resistance, noise-free output, scalability, and low TCO is unparalleled—and impossible to achieve with traditional sandbox technologies.

WHAT SETS VMRAY APART

EVASION RESISTANCE

VMRay Analyzer runs solely in the hypervisor. Unlike other sandboxes, it remains completely invisible to malware and defeats the evasive measures built into today's advanced threats. As a result, VMRay Analyzer analyzes and detects malware that other sandboxes miss.

FULL VISIBILITY

Based on groundbreaking technology, VMRay Analyzer transparently monitors every interaction between the malware and the operating system. Security teams have complete, uninterrupted visibility into malware behavior, so they don't miss any critical information.

PRECISE, NOISE-FREE OUTPUT

VMRay's Intelligent Monitoring engine works like the auto-zoom lens on a camera. It self-adjusts to the optimal level of monitoring detail, based on malware behavior. The system also distinguishes between malware-related activity and noise created by the sandbox or other sources. Only precise, relevant and actionable threat intelligence is presented to security personnel. As a result, team members don't waste time and effort sifting through extraneous information, and they're better equipped to make sound and timely decisions about incident response.

SCALABILITY AND LOW TCO

With VMRay's virtualized architecture organizations can affordably scale malware protection in response to changing business needs and ever-growing malware threats.

CHOOSE THE VERSION THAT FITS YOUR BUDGET & NEEDS

Cloud

On-Premises

Investigator

KEY FEATURES

- **Centralized analysis solution** for multiple sources and use cases, including email monitoring and direct submissions by SOC and IR teams.
- **Full automation and integration** with other security tools, using a flexible REST/JSON API interface.
- **Gold images** can be deployed to support real-world analysis environments for detection of targeted malware.
- **Versatile real-time interaction** allows analysts to interact directly with malware that is looking for specific inputs.
- **Generates threat intelligence** in machine-readable formats.
- **Role-specific reports** give tailored insights for every member of the security team.
- **Operating Systems Supported**: Windows & Mac

THERE'S NO TIME LIKE THE PRESENT

Get an up-close look and a hands-on feel for how VMRay Analyzer can help strengthen your organization's malware defenses. Sign up today for a 30-day free trial.

CONTACT US

Email: enquiry@secez.com
Tell: +91-120-2423448