mti
A RICOH Company

VMRAY

Der Gold Standard zur Verifizierung und Analyse von Malware. Made-In-Germany

- Hochgradig resistent gegen Sandbox Evasion
- Vollständige Sichtbarkeit des Malware-Verhaltens
- Verkürzung der Verweildauer von Angreifern
- Hochgradig skalierbar, ohne Abstriche an der Analyse-Qualität

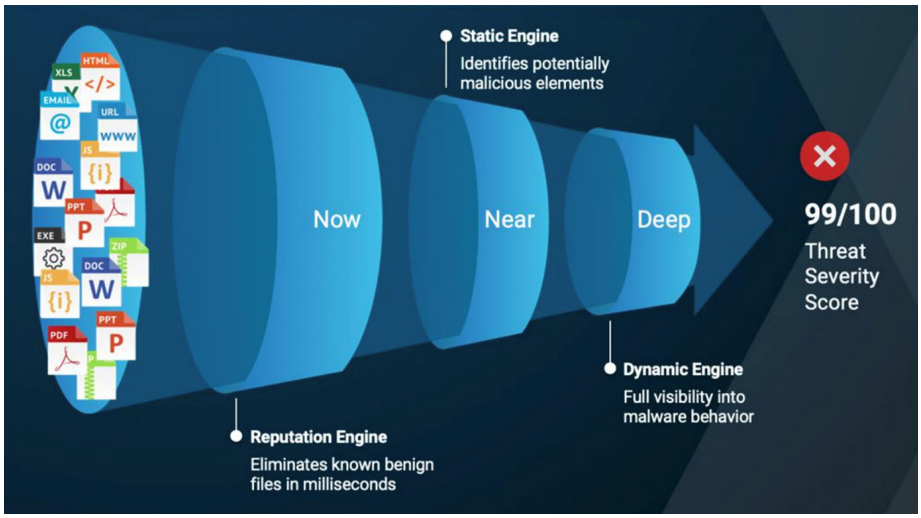
Funktionsüberblick

VMRay ist der führende Anbieter von Sandbox-Technologien zur Verifizierungund Analyse von Cyberbedrohungen.

Eine Sandbox bezeichnet im CyberSecurity-Umfeld einen abgeschotteten sicheren Bereich, in dem potentiell unsichere Aktionen oder Malware von Angreifern ausgeführt und die Auswirkungen der Ausführung analysiert werden können. Durch die Validierung einer potentiell schädlichen Aktion wird gewährleistet, dass IT-Systeme sicher und stabil laufen können und verhindert, dass Angreifer sensitive Unternehmensdaten stehlen oder kritische Systeme sabotieren.

Zur Verifizierung von Schadtprogrammen verwendet VMRay 3 verschiedene Analysemethoden: Repuations-, Statische sowie Dynamische Analyse. Dazu werden verdächtige Dateien aus verschiedenen Quellen gesammelt, analysiert und in detaillierten Reports aufbereitet.

Aus der Masse an forensischen Daten werden zuverlässige IOCs (Indicators of Compromise) extrahiert, während auffälliges, aber harmloses Hintergrundrauschen ebenso zuverlässig herausgefiltert wird - eine Entlastung für die von Alert Fatigue geplagten Security Teams.



NOW-Analysestufe

VMRays schnelle Reputation Engine identifiziert innerhalb von Millisekunden bekannte gutartige, bösartige sowie potenziell gefährliche Dateien.

NEAR-Analysestufe

VMRays statische Analyse-Engine extrahiert und analysiert verdächtige Dateien und URLs, filtert bösartige Elemente heraus und deobfuskiert aktiven Code.

DEEP-Analysestufe

VMRays dynamische Analyse-Engine entdeckt Zero-Day und hochevasive Malware sowie komplexe, zielgerichtete Angriffe.

Produktüberblick

VMRays Lösungsportfolio besteht aus dem VMRay Analyzer, dem VMRay Detector sowie dem VMRay Email Threat Defender.

VMRay Analyzer
VMRay Analyzer ist der Gold Standard für dynamische Malware-Analyse und ermöglicht granularen Einblick in das Verhalten von Zero-Day Angriffen, hochevasiver/amorpher Malware und zielgerichteten, komplexen Attacken. Primär eingesetzt in den Bereichen Digital Forensics & Incident Response sowie SOC.
Zu den Key-Funktionen und Vorteilen gehören: Alert Triage, automatisierte Extraktion von IOCs (Indicators of Compromise), Generierung von Threat Intelligence, Aufdeckung von Angriffsvektoren, Beschleunigung von Incident Investigation und Response. Verfügbar als OnPremises- und Cloud-Lösung für Windows und MacOS.

VMRay Detector
VMRay Detector ist ein Add-On zu VMRay Analyzer (nicht als stand-alone Produkt verfügbar) und dient der Überprüfung großer Mengen potenziell gefährlicher Dateien. Das Ergebnis wird innerhalb als Verdikt zu Art und Schadpotential (Score) der untersuchten Samples zurückgegeben. Granulare Reports mit großer Detailtiefe, so wie bei VMRay Analyzer, werden dabei nicht erstellt. Primär im SOC-Bereich eingesetzt. Zu den primären Funktionen und Vorteilen gehören: Advanced Threat Detection, Alert Triage, hochgradig performant und skalierbar (Verdict innerhalb von Sekunden). VMRay Detector ist als OnPremises- und Cloud-Lösung für Windows und MacOS verfügbar.

VMRay Email Threat Defender
VMRay Email Threat Defender erhöht die Wirksamkeit vorhandener Email-Security-Systeme (z.B. Gateways). Der Schwerpunkt der Lösung liegt auf Advanced Threat Detection, d.h. der Entdeckung von hochentwickelter Malware, die in der Lage ist, herkömmliche Anti-Phishing- und Anti-SPAM-Maßnahmen zu umgehen.
Primär eingesetzt im SOC-Bereich. Die Rückgabe der Analyse-Ergebnisse erfolgt als Verdikt mit Bewertung des Gefahrenpotentials (Score). Zu den Funktionen gehören: Automatisiertes Scannen eingehender Emails, Analyse von Inhalt, Anhängen und eingebetteten URLs, automatisierte Information von betroffenen Nutzern und des Security-Teams. Verfügbar als On-Premises- oder Cloud-Lösung.

Herstellersupport

- Support wird bei aktiver Wartung, d.h. Subscription oder Perpetual-Maintenace, gewährt.
- Support ist per Web https://support.vmray.com oder E-Mail an support@vmray.com verfügbar.
- Supportzeiten: 8x5, während den üblichen Geschäftszeiten

A RICOH Company

VMRay Alleinstellungsmerkmale

VMRAY

International anerkannte Technologie-Experten

Die Gründer von VMRay, Dr. Carsten Willems und Dr. Ralf Hund, sind international anerkannte Pioniere und Experten im Bereich Malware Sandboxing. Sie entstammen der Cybersecurity-Talentschmiede der Ruhr-Universität Bochum und haben ihre Forschungsarbeit in branchenführende Technologien zum Schutz vor hochentwickelten Malware-Bedrohungen umgesetzt.

Exzellente weltweite Reputation bei SOC- und IR-Teams

VMRay hat sich eine exzellente Reputation und Glaubwürdigkeit durch die Zusammenarbeit mit vielen namhaften privaten und öffentlichen Unternehmen sowie Behörden und regierungsnahen Organisationen erarbeitet.

Hochperformante, weltweit einzigartige Technologie

VMRay Lösungen basieren auf einer agentenlosen, hypervisor-basierten Technologie, die für Schadsoftware quasi unsichtbar ist. Da keine Verschleierungsversuche bei der Malware ausgelöst werden, sind VMRay Technologien hochgradig resistent gegen Sandbox Evasion. Diese "Unsichtbarkeit" in Verbindung mit hochperformanter Analyse-Ausführung verschafft Security-Teams detaillierten Einblick in das Verhalten der Malware. VMRay sieht signifikant mehr als herkömmliche Sandboxing-Technologien.

Auswirkung der VMRay Technologie auf Security, Compliance, Prozesse und Skalierbarkeit

Auswirkungen auf Security

Sandboxing-Lösungen sind wichtige Bausteine im Security Stack eines Unternehmens, sie dienen der Erkennung und Analyse moderner Malware. VMRay Produkte können diese Aufgabe auf einzigartige Weise erfüllen. Ihr volles Potential wird jedoch durch die Integration in die vorhandene Security-Landschaft erschlossen, denn VMRay liefert Threat-Informationen, die den Wirkungsgrad der einzelnen Systeme erheblich erhöhen können. Wenn der gesamte Security Stack profitiert, ist das Ergebnis eine deutlich verbesserte Cyber-Resilienz des Unternehmens.

Auswirkungen auf Compliance-Anforderungen

VMRay unterstützt Unternehmen bei der Einhaltung interner, nationaler und internationaler Compliance-Vorgaben. VMRay betreibt Rechenzentren sowohl in Deutschland als auch in den USA, was für Unternehmen mit Vorgaben bei der Datenhaltung ein wichtiges Kriterium darstellt. VMRay besitzt ISO 27001-Zertifizierung, beide Rechenzentren sind DSGVO / GDPR-konform und entsprechen darüber hinaus dem California Data Privacy Act und den Singapore Monetary Authority Guidelines. VMRay Technologien unterstützen Single Sign-On (SAML 2.0 Support) und Multi-Factor Authentifizierung (Time-Based One-Time Password).

Auswirkung auf die Optimierung von IT-Ressourcen

Funktionen wie die automatisierte Erkennung und Analyse verdächtiger Dateien, Reports mit unterschiedlicher Detail-Tiefe und Alert Triage unterstützen IR- und SOC-Teams bei der Bewältigung ihrer zahlreichen Aufgaben und versetzen auch Security-Teams mit dünner Personaldecke in die Lage, skalierbare Prozesse einzuführen. VMRay Technologien sind bekannt dafür, aus der Masse forensischer Daten zuverlässige IOCs zu extrahieren und auffälliges, aber legitimes Hintergrundrauschen herauszufiltern. Das geschieht voll automatisiert und schützt Security-Teams vor der mittlerweile zum Problem gewordenen "Alert Fatigue", der Überlastung und Ermüdung durch Fehlalarme.

Referenzen des Herstellers

Zahlreiche globale Unternehmen haben VMRay bereits zur Erkennung und Analyse von Zero-Day-Bedrohungen sowie komplexer und zielgerichteter Malware gewählt, die meisten wollen aber anonym bleiben. So viel kann jedoch gesagt werden: 3 der 5 FAANG Technologie-Giganten (Facebook, Amazon, Apple, Netflix, Google), 4 der 6 größten Wirtschaftsprüfungsunternehmen, 10 globale Finanzkonzerne sowie 65 nationale und internationale Regierungseinrichtungen gehören zu VMRays zufriedenen Kunden.

Technologiepartnerschaften des Herstellers

VMRay arbeitet eng mit führenden Cybersicherheits- und Infrastrukturanbietern zusammen, um nahtlose, ganzheitliche Lösungen für fortschrittliche Bedrohungserkennung und -analyse zu gewährleisten. Unter anderem wird mit Technologiepartnern aus den Bereichen Endpoint Protection (EPP), Big Data, Gateway Security, SecOps Automation (SOAR) sowie Threat Intelligence Platform (TIP) zusammengearbeitet.

- Anomali (SOAR & TIP)
- Carbon Black (EPP)
- Cybereason (EPP)
- Cybersponse (SOAR & TIP)
- EclecticIQ (SOAR & TIP)
- IBM Resilient (SOAR & TIP)
- InQuest (Big Data)
- MISP (TIP)
- Palo Alto Networks – Demisto (SOAR & TIP)
- Rapid7 (SOAR & TIP)
- SentinelOne (EPP)
- Siemplify (SOAR & TIP)
- Splunk-Phantom (SIEM, SOAR)

Lizenzierung

VMRay Analyzer

- Lizenziert werden ein Kontingent ab 100 eingehenden Malware-Analysen pro Tag, wobei das Ergebnis als detaillierter Report ausgegeben wird.
- Nicht aufgebrauchte Analyse-Kontingente können nicht auf den nächsten Tag übertragen werden.
- VMRay Analyzer ist als Cloud- oder OnPremises-Lösung in Form von Subscription- oder Perpetual-Lizenzen erhältlich.

VMRay Detector

- Eine VMRay Analyzer Lizenz wird vorausgesetzt.
- Lizenziert wird ein Kontingent ab 100 Malware-Analysen pro Tag, wobei das Ergebnis als Verdikt ausgegeben wird (versus detailliertem Report wie bei VMRay Analyzer).
- Nicht aufgebrauchte Analyse-Kontingente können nicht auf den nächsten Tag übertragen werden.
- Die Anzahl der detaillierten Malware-Analyse-Berichte sind auf das zugrundeliegende Kontingent des VMRay Analysers beschränkt.
- VMRay Detector-Addon ist als Cloud- oder OnPremises-Lösung in Form von Subscription- oder Perpetual-Lizenzen erhältlich.

VMRay Email Threat Defender

- Lizenziert wird die Anzahl der vorhandenen Benutzer-Mailboxen.
- VMRay Email Threat Defender ist als Cloud- oder OnPremises-Lösung in Form von Subscription-Lizenzen erhältlich.

Über VMRay

VMRay hat eine klare Mission: Unternehmen zu helfen, sich gegen die wachsende globale Malwarebedrohung zu schützen.

VMRays Technologien zur automatisierten Malwareanalyse und -erkennung helfen Unternehmen weltweit, Geschäftsrisiken zu minimieren, wertvollen Dateninformationen zu schützen und die Reputation nachhaltig zu gewährleisten.

Weitere Informationen: www.vmray.com

Warum Sie mit VMRay zusammenarbeiten sollten:

- Made-in-Germany", ISO 27001-Zertifizierung sowie Rechenzentren wahlweise in Deutschland oder den USA sind starke Verkaufsargumente.
- Der Markt für Detection- sowie DFIR-Technologien bietet zweistellige Wachstumschancen und attraktive Margen.
- Zusammenarbeit mit einem aufstrebenden Unternehmen auf globalem Expansionskurs.
- Partner können mit VMRay überdurchschnittliche Beratungs- und Dienstleistungsumsätze generieren.
- Partner können schnell Beratungsdienstleistungen im MITRE ATT@CK-Umfeld anbieten.
- Partner profitieren vom großen Cross-Selling-Potenzial bei Bestandskunden, da Threat Detection ein Zukunftsmarkt ist.

Zertifizierungen

- GDPR Compliant
- ISO27001

Über MTI Technology GmbH

Als herstellerunabhängiges IT-Systemhaus hat sich MTI seit über 30 Jahren auf Datacenter-Infrastrukturen, Cloud Services und Data-/Cloud-Security und Managed Services spezialisiert. Dabei betreuen wir unsere Kunden über unser eigenes bundesweites Servicenetz.

Mehr als 1.800 Kunden vertrauen auf die Expertise und Lösungen von MTI zur Speicherung, zum Schutz und zur Sicherung von Daten – hersteller-, plattform- als auch applikationsübergreifend.

Mit Erfolg: 98% unserer Kunden würden uns und unsere Services weiterempfehlen.

Weitere Informationen: https://de.mti.com/

Warum Sie mit MTI Technology GmbH zusammenarbeiten sollten:

- starke europäische Präsenz: 8 Standorte, >250 Mitarbeiter
- bundesweites Netz an Vertriebs- und Serviceniederlassungen
- technische Kompetenz mit höchster Zertifizierung
- Service Level Agreements (SLA) nach deutschem Recht
- lokal ansässiger, deutschsprachiger Service mit 24/7 Business-Support

Ansprechpartner

Michael Babylon
Geschäftsführung
T: 06122 995 0
E: mbabylon@mti.com

Jens Racky
Solution Architect
T: 06122 995 272
E: jracky@mti.com

Uli Schunk
Marketing Manager
T: 06122 995 155
E: uschunk@mti.com