VMRAY

MALWARE ALERT TRIAGE

for Microsoft Defender for Endpoint

VMRay FinalVerdict : Automate and Enrich EDR Alerts with Actionable Threat Intelligence

Microsoft Defender for Endpoint provides the critical signals needed to identify the early stages of a malware attack, but often requires further manual investigation to identify the root cause of the alert.

VMRay FinalVerdict complements Microsoft Defender EDR/XDR solutions with best-in-class automated malware alert triage and analysis of Zero Day threats by enriching alerts with dynamic threat intelligence in the form of IOCs, artifacts, and threat actor attribution. VMRay's alert enrichment ensures accelerated investigations, definitive verdicts of malicious or benign, and significantly reduces Tier 1 Analyst workloads.

Integrated via API, VMRay's hypervisor-based, automated sandbox technology works in high-volume alert environments using both static and dynamic analysis to significantly reduce the window of malware and phishing vulnerability.

Strengthen Your Endpoint Detection and Response with VMRay and Microsoft

Detect advanced threats
Identify advanced, highly evasive Zero-Day malware and phishing threats and enriching suspicious EDR alerts with dynamic threat analysis.

Supplement your security
Quickly enrich suspicious EDR alerts with detailed, actionable threat intelligence. Reduce alert fatigue with clear analysis, definitive verdicts, and IOCs to facilitate automated responses.

Integrate your essential tools
Deploy VMRay FinalVerdict in the cloud and enjoy a quick and frictionless integration with Microsoft Defender for Endpoint through the built in API.

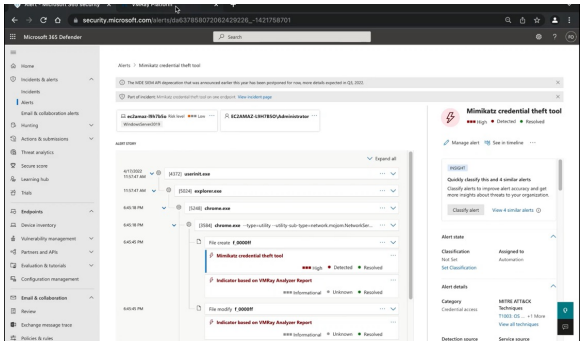
Eliminate alert fatigue
Consolidate threat intelligence into Microsoft Defender Security Center or Microsoft 365 Defender. Reduce the Mean Time to Detect (MTTD) and Respond (MTTR) in the SOC.

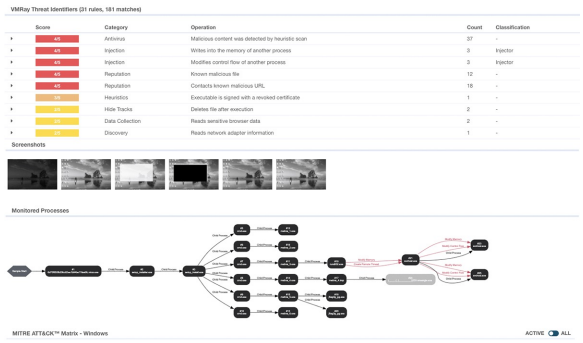
VMRAY

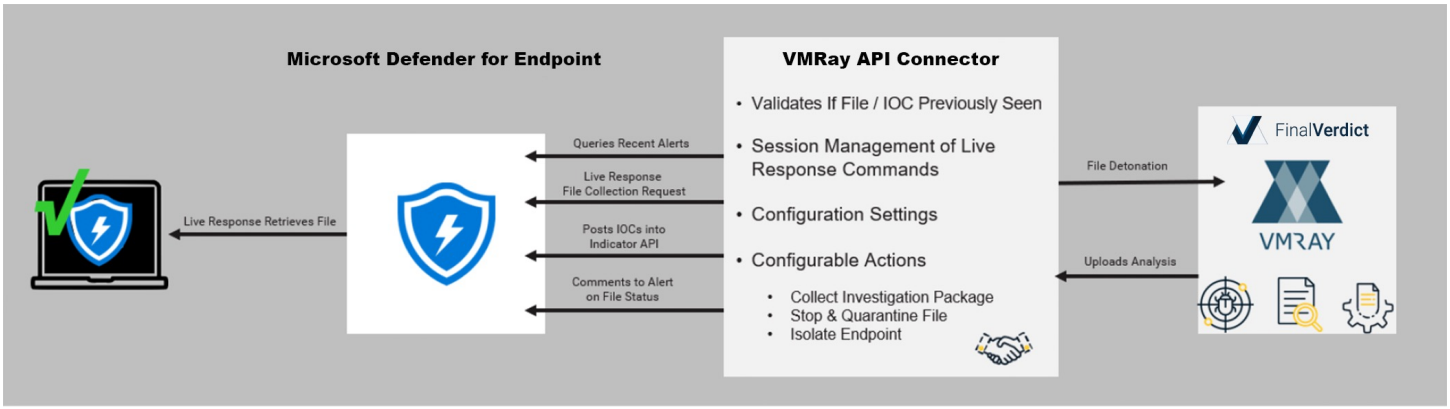
> “VMRay provided the **fully automated detection** capabilities that were crucial to speed up our incident response process and shorten investigation.”
>
> Cyber Threat Analyst | Global Top 5 Telecom company

Best-in-Class Malware Detection and Analysis

- Reduce the time to detect, triage and respond to unknown, advanced malware and phishing threats
- Creates operational threat intelligence to mitigate active threats, delivered within seconds
- Analyze files, password-protected attachments, nested files, scripts, and phishing emails.
- Automated IOC and artifact extraction and classification
- Concise and focused reporting and analysis
- Integrates with Microsoft Defender Security Center or Microsoft 365 Defender for streamlined incident response and remediation workflows
- Maximizes Threat Analysts' productivity and skillset
- Increases security operations efficiency and improves return on Investment (ROI) of EDR deployments







VMRAY

Learn more at VMRay - Cyber Security Threat Detection & Analysis Platform

Contact us at sales@vmray.com