VMRAY

VMRay VMRay FinalVerdict & VMware Carbon Black Cloud Enterprise EDR

Enriched Alert Data with Definitive Malware Verdicts To Speed Incident Response

SOLUTION BRIEF

VMware Carbon Black™

Addressing the SOC Efficiency Challenge

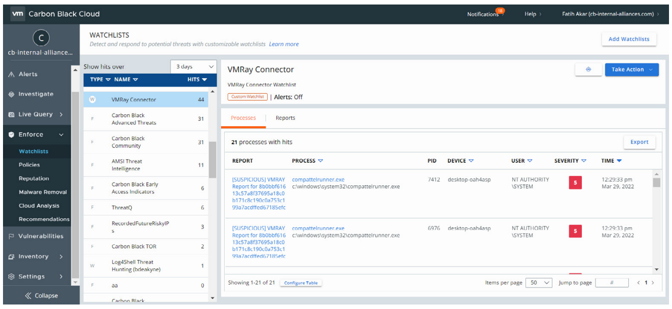
Understanding distinct threats targeting endpoints is vital for modern security teams. When an unknown threat emerges, security teams seek to timely identify, investigate, and respond. However, threat actors are leveraging financial resources and networking channels on the dark web marketplaces to develop new tactics to evade endpoint and perimeter security controls. It's often difficult for enterprise security experts to find the balance between increasing detection sensitivity or potentially increasing the number of alerts, which impacts the overall productivity of the Security Operations Center (SOC) team. Security practitioners ultimately need a way to maintain optimum threat detection capabilities and security operations efficiency while avoiding missed cyber threats.

Joint Solution

VMware Carbon Black Cloud Enterprise EDR is one of **the leading platforms to thwart attacks** by analyzing billions of system events on the endpoints. It helps security teams identify suspicious signals beyond the baseline and adapt their response. Organizations also leverage **VMware Carbon Black Cloud** to **stop current and future ransomware variants**.

VMRay's evasion-resistant hypervisor-based monitoring technology ensures high quality threat detection and alert enrichment with actionable intelligence to organizations of all sizes.

When combined, VMRay's best-in-class malware triage and phishing analysis platform with VMware's next generation behavioral endpoint protection delivers an unmatched capability of identifying zero-day threats, enriched alerts, and enterprise-wide operational cybersecurity benefits.
With the integration, joint customers can maximize the value of their security investments by dramatically reducing Mean Time to Detect (MTTD) and Respond (MTTR).



WATCHLISTS

Detect and respond to potential threats with customizable watchlists Learn more

Show hits over 3 days

TYPE	NAME	HITS
W	VMRay Connector	44
F	Carbon Black Advanced Threats	31
F	Carbon Black Community	31
F	AMSI Threat Intelligence	11
F	Carbon Black Early Access Indicators	6
F	ThreatQ	6
F	RecordedFutureRiskyIPs	3
F	Carbon Black TOR	2
W	Log4Shell Threat Hunting (bdeakyne)	1
F	aa	0
	Carbon Black	

VMRay Connector

VMRay Connector Watchlist

Custom Watchlist | Alerts: Off

21 processes with hits

REPORT	PROCESS	PID	DEVICE	USER	SEVERITY	TIME
[SUSPICIOUS] VMRAY Report for 8b0bbf61613c57a8f37695a18c0b171c8c190c0a753c199a7acdffed67185efc	compattelrunner.exe c:\windows\system32\compattelrunner.exe	7412	desktop-oah4asp	NT AUTHORITY \SYSTEM	5	12:29:33 pm Mar 29, 2022
[SUSPICIOUS] VMRAY Report for 8b0bbf61613c57a8f37695a18c0b171c8c190c0a753c199a7acdffed67185efc	compattelrunner.exe c:\windows\system32\compattelrunner.exe	6976	desktop-oah4asp	NT AUTHORITY \SYSTEM	5	12:29:33 pm Mar 29, 2022

Showing 1-21 of 21 Items per page 50 Jump to page # 1

Products

FinalVerdict

TotalInsight

VMware Carbon Black

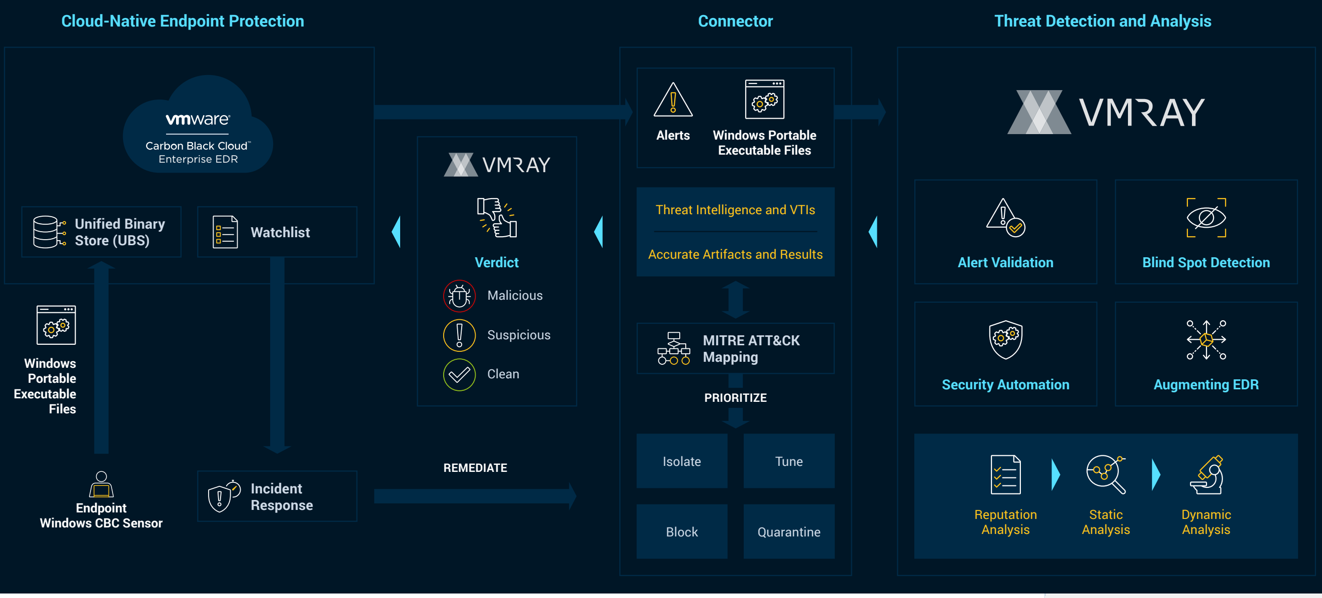
Cloud Enterprise EDR

Highlights

Get proactive against sophisticated, under-the-radar threats.

Uplevel your **SOC efficiency** by combining two critically powerful technologies.

Enable your security analysts **to focus** on what matters most.


Cloud-Native Endpoint Protection
vmware Carbon Black Cloud Enterprise EDR
Unified Binary Store (UBS)
Watchlist
Windows Portable Executable Files
Endpoint Windows CBC Sensor
Incident Response
VMRAY
Verdict
Malicious
Suspicious
Clean
REMEDIATE
Connector
Alerts
Windows Portable Executable Files
Threat Intelligence and VTIs
Accurate Artifacts and Results
MITRE ATT&CK Mapping
PRIORITIZE
Isolate
Tune
Block
Quarantine
Threat Detection and Analysis
VMRAY
Alert Validation
Blind Spot Detection
Security Automation
Augmenting EDR
Reputation Analysis
Static Analysis
Dynamic Analysis

How it works

The connector for VMRay and VMware Carbon Black is built to leverage the core competencies of each other's products. VMRay FinalVerdict or TotalInsight pulls in new binaries and corresponding metadata from Unified Binary Store (UBS) of VMware Carbon Black Cloud for a thorough multilayer analysis to detect malicious behavior. Analyzed threats are assigned a severity score and sent back to Carbon Black Cloud Console along with accurate, detailed threat intelligence.

If the file is malicious, the indicators of compromise (IOCs) and artifacts can be added to the watchlist for future detections and initiate incident response, remediation, or a forensics investigation depending on the predefined workflow. All workflows can be fully automated without any human intervention to quickly mitigate both malware and phishing threats.

> “VMRay's data quality and rich API allowed us to automate our reverse engineering and data extraction tasks in a way no other vendor was able to provide.”
>
> *Threat Intelligence Team, Global Top 10 Technology Company*

FEATURES

- Fully integrated with Watchlists and Unified Binary Store (UBS)
- Automated in-depth malware and phishing analysis
- Enriched alerts with actionable IOC's and Intelligence
- Streamlined with incident response and remediation workflows

KEY BENEFITS

- Seamless automation of threat analysis and malware sandboxing tasks
- Detect blind spots in the form of portable executables
- Increased ROI for endpoint threat detection deployments
- Reduced Mean Time To Detect (MTTD) and Respond (MTTR)
- Increase SOC productivity through rapid malware alert triage and validation

USE CASES

- Security Automation
- Alert Enrichment
- Alert Validation
- Incident Response
- Blind Spot Detection

Getting Started with VMRay

To learn more about how VMRay can augment Carbon Black Cloud EDR or request a free trial: Visit vmray.com

About VMware

VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact.

For more information, please visit vmware.com/company

About VMRay

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

Led by reputable cyber security pioneers, we develop best-in-class technologies to help organizations distinguish genuine threats from the noise and obtain additional context and insights into those threats.

Based on the world's most advanced malware and phishing analysis platform, we enable enterprises, government organizations, and MSSPs to automate **security operations**, accelerate **analysis and response**, and build reliable **threat intelligence**. In times of uncertainty and complexity, we create room for clarity and productivity to help security teams thrive.

Read more about our solutions at vmray.com

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