

VMRay Analyzer & VMware Carbon Black Cloud Enterprise EDR

Automate the analysis of sophisticated threats



VMware Carbon Black™

Addressing the SOC Efficiency Challenge

Understanding distinct threats targeting endpoints is vital for modern security teams. When an unknown threat knocks the door, the 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 detection.

It's often tricky for enterprise security leaders to find the sweet spot between tightening the detection configurations, so ramping up the number of alerts and the overall productivity of the Security Operations Center (SOC) team. They need a way to gain solid threat detection capabilities and increase 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 spot the abnormal fluctuations and adapt prevention in response. Organizations also leverage **VMware Carbon Black Cloud** to **stop current and future ransomware** variants. Evasion-resistant hypervisor based monitoring technology of VMRay Analyzer ensures high quality threat detection to organizations of all sizes.

Combining VMRay's best-of-breed threat analysis platform with VMware's next generation behavioral endpoint protection technology delivers unmatched capability of surfacing zero day threats as well as 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).

Products

VMRay Analyzer Cloud

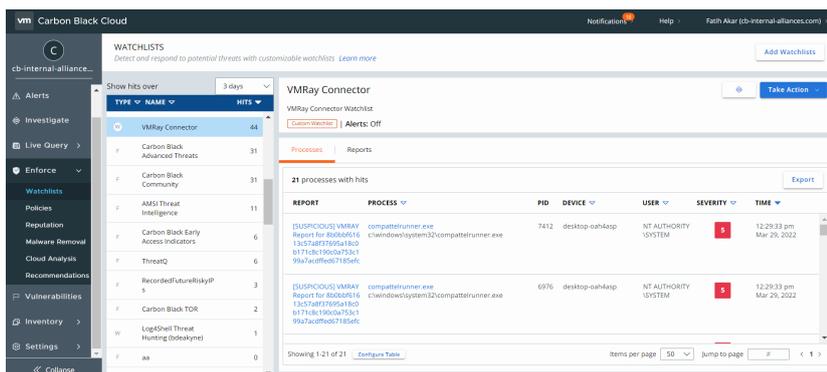
VMware Carbon Black Cloud Enterprise EDR

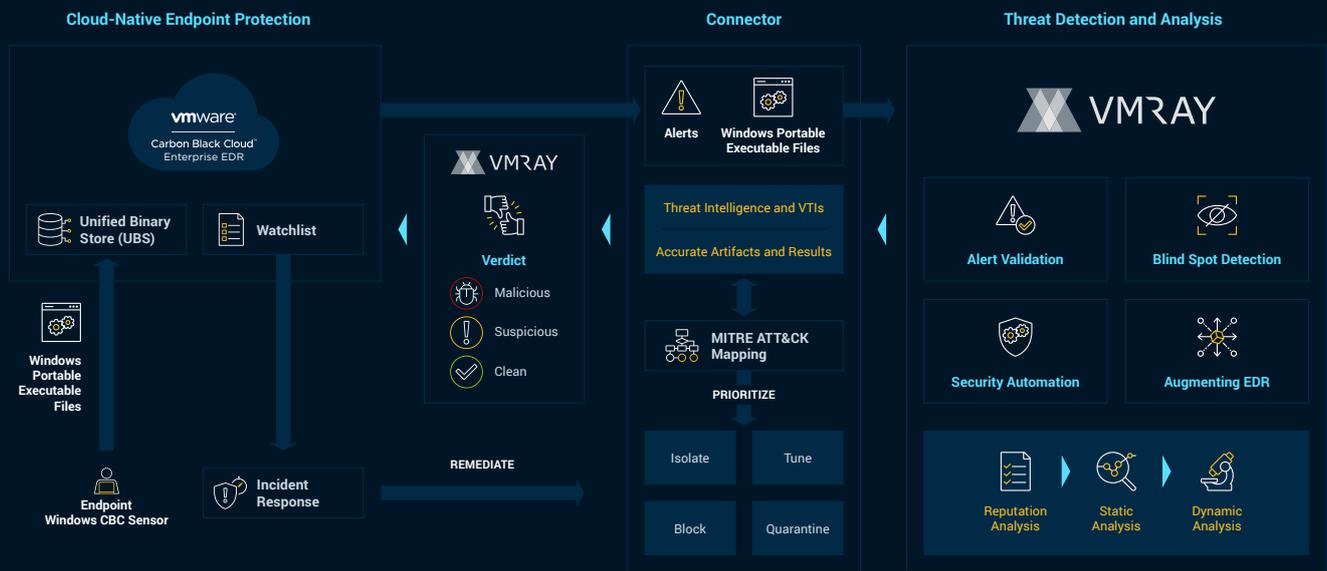
Highlights

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.





How it works

The connector for VMRay and VMware Carbon Black is built to leverage the core competencies of each other's products. The VMRay Analyzer 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 detail-rich threat intelligence.

If the file is malicious, the indicators and artifacts can be added to the watchlist for future detections and initiate incident response, remediation or forensics investigation depending on the preconfigured workflow. All this process is lightning-fast and fully automated.

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 threat analysis
- ♦ Actionable threat intelligence delivered within seconds
- ♦ Streamlined with incident response and remediation workflows



KEY BENEFITS

- ♦ Reduced MTTD and MTTR
- ♦ Ramped up ROI for endpoint threat detection deployments
- ♦ Seamless automation of threat analysis and malware sandboxing tasks
- ♦ Detect blind spots in the form of portable executables
- ♦ Empower your SOC productivity through rapid security alert triage and validation



USE CASES

- ♦ Security Automation
- ♦ 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-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.

Read more about our solutions at vmray.com

vmware®

Contact Us

Email: sales@vmray.com

Phone: +1 888 958-5801

VMRay GmbH

Universitätsstraße 142
44799 Bochum • Germany

VMRay Inc.

22 Boston Wharf Road, 7th Floor
Boston, MA 02210 • USA

