VMware Carbon Black Cloud

Enterprise EDR

Threat Hunting & Incident Response

USE CASES

- Threat hunting
- Incident response
- Alert validation and triage
- Root cause analysis
- Forensic investigations
- Host isolation
- Remote remediation

BENEFITS

- Reduced complexity for more efficient endpoint security
- Easy deployment,automated updates, and elastic scalability
- Accelerated investigations with continuous endpoint visibility
- Complete understanding of root cause to close existing gaps
- Secure remote access for investigations
- Greatly reduced dwell time and average time to resolution

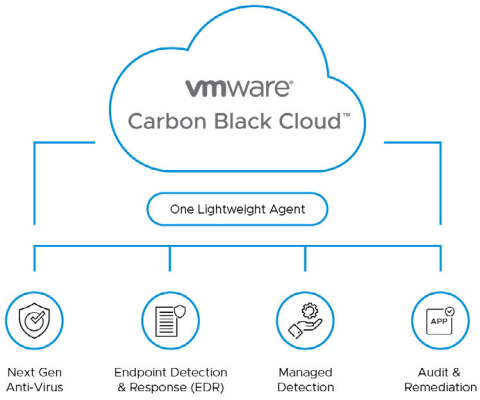
Enterprise security teams struggle to get their hands on the endpoint data they need to investigate and proactively hunt for abnormal behavior. Security and IT professionals currently lack the ability to see beyond suspicious activity and need a way to dive deeper into the data to make their own judgments.

VMware Carbon Black Enterprise EDR is an advanced threat hunting and incident response solution delivering continuous visibility for top security operations centers (SOCs) and incident response (IR) teams. Enterprise EDR is delivered through the VMware Carbon Black Cloud, a next-generation endpoint protection platform that consolidates security in the cloud using a single agent, console and dataset.

Using data continuously collected and sent to the VMware Carbon Black Cloud, Enterprise EDR provides immediate access to the most complete picture of an attack at all times, reducing lengthy investigations from days to minutes. This empowers teams to proactively hunt for threats, uncover suspicious behavior, disrupt active attacks and address gaps in defenses before attackers can.

Along with continuous visibility, Enterprise EDR gives you the power to respond and remediate in real time, stopping active attacks and repairing damage quickly.

Cloud-Native Endpoint Protection Program



"Enterprise EDR has simplified incident response by allowing quick discovery of both simple and advanced threats. Its simplicity and responsiveness are amazing, especially when you are running an investigation where every minute matters... Endpoint security used to be difficult."

DENIS XHEPA, IT SYSTEMS SECURITY ENGINEER OF MIDCAP FINANCIAL SERVICES

FEATURES

- Lightweight sensor deployed and managed from the cloud
- Process and binary search of centralized, unfiltered data
- Out-of-the-box and customizable behavioral detection
- Proprietary and third-party threat intel feeds
- Automated watchlist store-run queries
- Interactive and expandable attack chain visualization
- Secure remote shell for rapid remediation
- Open APIs

PLATFORMS

- Windows
- macOS
- Red Hat
- CentOS

LEARN MORE

To set up a personalized demo or try it free in your organization, visit *CarbonBlack/trial*

For more information or to purchase VMware Carbon Black Products please call: (855) 525-2489 in the US, (44) 118 908 2374 in EMEA

For more information, email *Contact@CarbonBlack.com* or visit *CarbonBlack.com/epp-cloud*

Key Capabilities

Complete Endpoint Protection Platform

Built on the VMware Carbon Black Cloud, Enterprise EDR provides advanced threat hunting and incident response functionality from the same agent and console as our NGAV, EDR and real-time query solutions, allowing your team to consolidate multiple point products with a converged platform.

Continuous & Centralized Recording

Centralized access to continuously collected data means that security professionals have all the information they need to hunt threats in real time as well as conduct in-depth investigations after a breach has occurred.

Attack Chain Visualization & Search

Enterprise EDR provides intuitive attack chain visualization to make identifying root cause fast and easy. Analysts can quickly jump through each stage of an attack to gain insight into the attacker's behavior, close security gaps, and learn from every new attack technique to avoid falling victim to the same attack twice.

Live Response for Remote Remediation

With Live Response, incident responders can create a secure connection to infected hosts to pull or push files, kill processes, perform memory dumps and quickly remediate from anywhere in the world.

Automation via Integrations & Open APIs

Carbon Black boasts a robust partner ecosystem and open platform that allows security teams to integrate products like Enterprise EDR into their existing security stack.

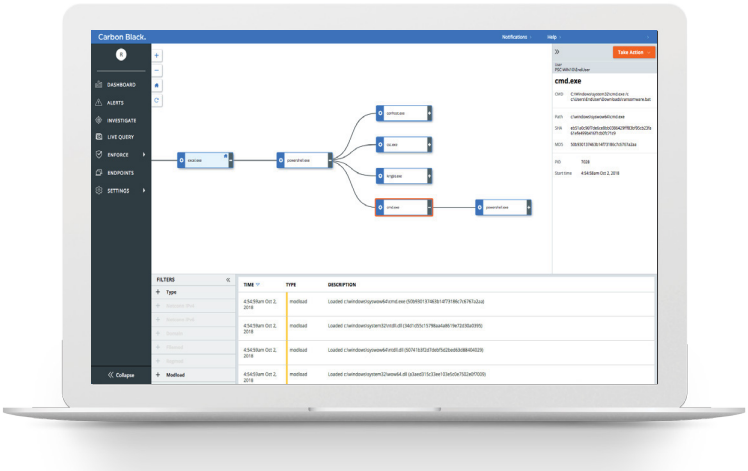


FIGURE 1: Enterprise EDR leverages continuously collected endpoint activity data to provide extensive attack chain visualization and a clear understanding of what happened at every stage of the attack.

vmware Carbon Black