VMware Carbon Black

Endpoint Detection and Response (EDR)

Threat Hunting & Incident Response for Hybrid Deployments

USE CASES

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

BENEFITS

- Faster end-to-end response and remediation
- Accelerated IR and threat hunting with continuous endpoint visibility
- Rapid identification of attacker activities and root cause
- Secure remote access to infected endpoints for in-depth investigation
- Better protection from future attacks through automated hunting
- Unlimited retention and scale for the largest installations
- Reduced IT headaches from reimaging and helpdesk tickets

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

Carbon Black EDR is an incident response and threat hunting solution designed for security operations center (SOC) teams with offline environments or on-premises requirements. Carbon Black EDR continuously records and stores comprehensive endpoint activity data, so that security professionals can hunt threats in real time and visualize the complete attack kill chain. It leverages the VMware Carbon Black Cloud's aggregated threat intelligence, which is applied to the endpoint activity system of record for evidence and detection of these identified threats and patterns of behavior.

Top SOC teams, IR firms and MSSPs have adopted Carbon Black EDR as a core component of their detection and response capability stack. Customers that augment or replace legacy antivirus solutions with Carbon Black EDR do so because those legacy solutions lack visibility and context, leaving customers blind to attacks. Carbon Black EDR is available via MSSP or directly via on- premises deployment, virtual private cloud or software as a service.
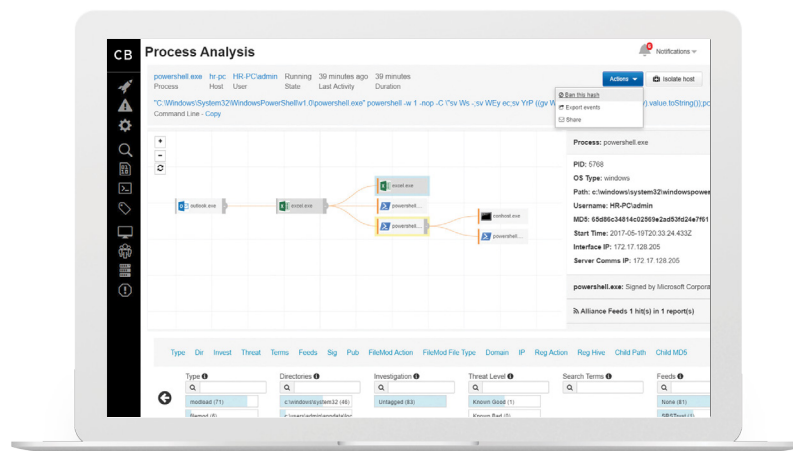

FIGURE 1: Carbon Black EDR captures comprehensive information about endpoint events, giving incident responders a clear understanding of what happened.

vmware® Carbon Black

FEATURES

- Out-of-the-box and customizable behavioral detection
- Multiple, customizable threat intel feeds
- Automated watchlists capture queries
- Process and binary search of centralized data
- Interactive attack chain visualization
- Live Response for rapid remediation
- Open API sand 120+ out-of-the-box integrations
- On-prem, virtual private cloud, SaaS, or MSSP

PLATFORMS

Sensor Support:
- Windows & Windows Server
- MacOS
- Red Hat
- CentOS
- Oracle RHCK
- SuSE

Deployment Options:
- Clouds or On-Premise

LEARN MORE

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

"Using Carbon Black EDR increases our confidence in investigations because it produces richer findings than traditional AV can. This includes detecting advanced malware and malicious behavior like rootkits while allowing for host isolations, hash banning, execution chaining, and more."

MEHAN KASINATH, ENTERPRISE SR. DIRECTOR OF INFORMATION SECURITY AT IAC

Key Capabilities

Continuous and Centralized Recording

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

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.

Attack Chain Visualization and Search

Carbon Black 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.

Automation via Integrations and Open APIs

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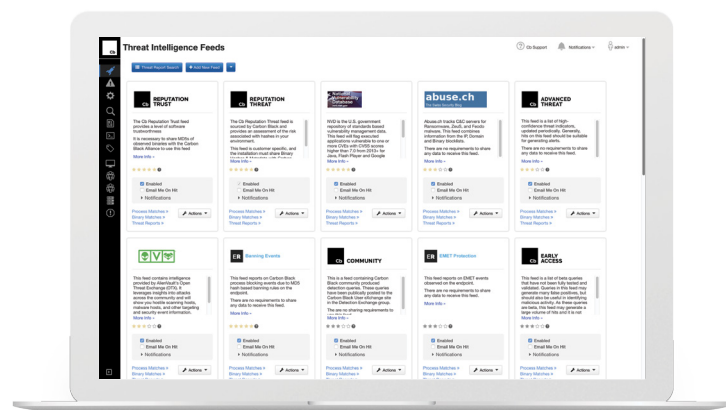

FIGURE 2: Carbon Black EDR leverages the VMware Carbon Black Cloud's aggregated threat intelligence, which is applied to all endpoint activity data to detect patterns of malicious behavior.