Carbon Black.
by Broadcom

PRODUCT BRIEF

Carbon Black® Enterprise EDR

Threat Hunting and Incident Response

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

KEY FEATURES

- Lightweight sensor deployed and managed from the cloud
- Search through unfiltered process, binary, and authentication data
- Interactive and expandable attack chain visualization
- Identity intelligence
- Out-of-the-box and customizable detections
- Proprietary and third-party threat intel feeds
- Quarantine endpoints from the network
- Secure remote shell for rapid remediation
- Software reputation determinations
- Open APIs

APPLICATIONS

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

Overview

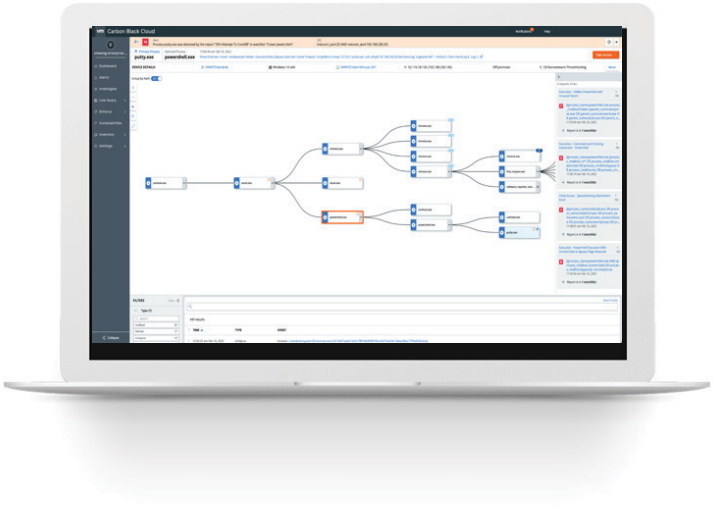
Enterprise security teams struggle to get their hands on the endpoint data they need to investigate and proactively hunt for abnormal behavior. Security and IT professionals currently lack the ability to see beyond suspicious activity and need a way to dive deeper into the data to make their own judgments. Endpoint detection and response (EDR) systems are the chosen tool for security professionals and incident responders to get the visibility required to see and stop attacks.

Carbon Black® Enterprise EDR is an advanced threat hunting and incident response solution delivering continuous visibility for security teams. Enterprise EDR is delivered through the 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 Carbon Black Cloud, Enterprise EDR always provides immediate access to the most complete picture of an attack, 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.

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.



PLATFORMS

- Windows
- macOS
- Linux

Key Capabilities

Continuous and 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 and 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.

Identity Intelligence for User-Centric Visibility

Collect identity intelligence, such as user authentication events, to improve context and identify additional types of anomalies and threats. Analysts gain increased visibility into endpoint activity, correlation of authentication and process events, and gain greater insight into identity behavior, such as brute force attacks, use of stolen credentials, and more.

Automation via Integrations and Open APIs

A robust partner ecosystem and open platform allows security teams to integrate products like Enterprise EDR into their existing security stack.

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

CB-EnterpriseEDR-PB100 December 17, 2024