Carbon Black.
by Broadcom

Product Brief

Carbon Black® Endpoint Detection and Response

Threat Hunting and Incident Response for Hybrid Deployments

Benefits

- Faster end-to-end response and remediation
- Accelerated Incident Response (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
- Proactive protection against future attacks through automated hunting
- Unmatched scalability and unlimited data retention for large environments
- Reduced IT overhead by minimizing endpoint reimaging and help desk tickets

Key Features

- Out-of-the-box and customizable behavioral detection
- Multiple, customizable threat intelligence feeds
- Automated watchlist query capture
- Process and binary search of centralized data
- Interactive attack chain visualization
- Live response for rapid remediation
- Open APIs and 120+ out-of-the-box integrations

Use Cases

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

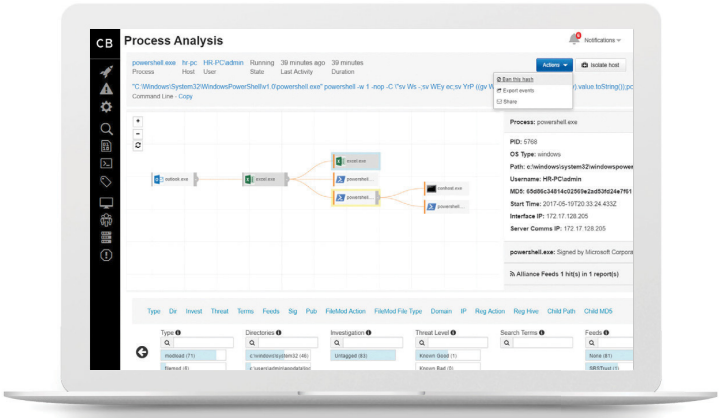
Overview

Security teams often struggle with legacy antivirus tools that lack the visibility needed to counter sophisticated, modern threats. This gap forces analysts into lengthy, manual investigations and creates a reactive security posture driven by high volumes of low-fidelity alerts. An on-premises Endpoint Detection and Response (EDR) solution addresses these challenges by providing the comprehensive endpoint visibility, streamlined workflows, and forensic depth necessary to proactively hunt and remediate threats within strictly controlled environments.

Carbon Black® EDR is an Incident Response (IR) and threat hunting solution designed for Security Operations Center (SOC) teams with offline environments or on-premises requirements. EDR continuously records and stores comprehensive endpoint activity data, allowing security professionals to hunt threats in real time and visualize the complete attack kill chain. The solution leverages Carbon Black Cloud aggregated threat intelligence, applying it to the endpoint activity system of record to detect identified threats and behavioral patterns.

Top SOC teams, IR firms, and Managed Security Service Providers (MSSPs) have adopted EDR as a core component of their detection and response capability stack. Customers that augment or replace legacy antivirus solutions with EDR do so because those legacy solutions lack visibility and context, leaving customers blind to attacks.

Figure 1: Carbon Black EDR Event Telemetry Provides Full Attack Visibility



Platforms

- Windows and Windows Server
- macOS
- Linux:
  - Red Hat Enterprise Linux (RHEL)t
  - CentOS
  - Oracle Linux (RHCK)
  - SUSE Linux
  - Rocky Linux

Deployment Options

- On-Premises
- Virtual Private Cloud (VPC)
- Public Cloud
- Managed Service Provider (MSSP/ Partner-Hosted)

Key Capabilities

Continuous and Centralized Recording

Centralized access to continuously recorded endpoint data gives security professionals the exact telemetry needed to hunt threats in real time and conduct in-depth investigations following a breach.

Live Response for Remote Remediation

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

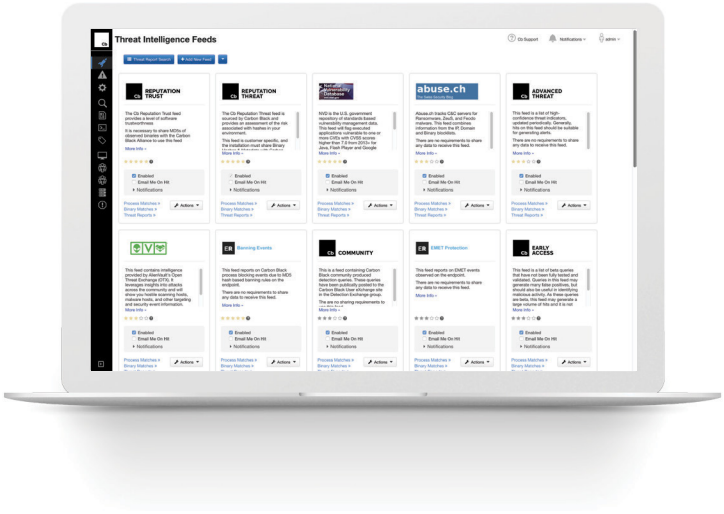
Attack Chain Visualization and Search

EDR provides intuitive attack chain visualization to make root-cause identification fast and simple. Analysts can quickly navigate each stage of an attack to understand attacker behavior and close security gaps—using these new attack insights to prevent repeat incidents.

Automation with Integrations and Open APIs

A robust partner ecosystem and open platform allow security teams to integrate Carbon Black EDR into their existing security stack.

Figure 2: Automated Telemetry Analysis with Carbon Black EDR Threat Intelligence Feeds



BROADCOM®

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

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CB-EDR-PB101 July 23, 2026