Carbon Black.

Cb Response

Industry-Leading Incident Response and Threat Hunting

Cb Response is an industry-leading incident response and threat hunting solution designed for security operations center (SOC) teams. Cb Response continuously records and captures unfiltered endpoint data, so that security professionals can hunt threats in real time and visualize the complete attack kill chain. It leverages the Cb Predictive Security Cloud's aggregated threat intelligence, continuously comparing intel to current and historical endpoint activity, exposing undetected threats.

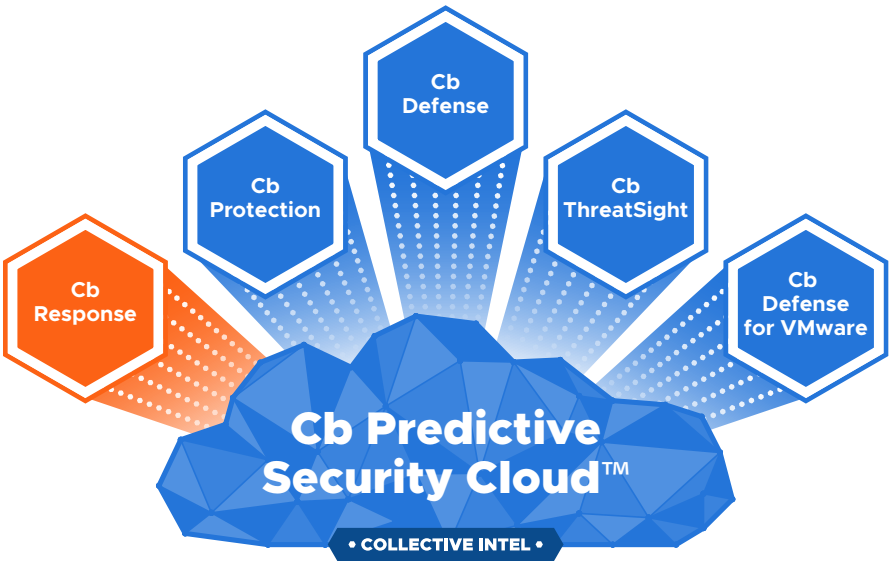
Cb Response provides advanced tools enabling SOC teams to understand the current state of an endpoint, perform remote live investigations, intervene with ongoing attacks and promptly remediate endpoint threats. As new patterns and indicators emerge, they are assessed against historical endpoint data to identify previously unknown attacks.

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

> "Carbon Black is able to give us a great deal of context such as the process that reached out to a domain, parent processes, command line at launch and so forth. The details surrounding an event are extremely valuable."

— DAN BANKER, CYBER DEFENSE ANALYST, MOTOROLA

MOTOROLA



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 unfiltered 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
- Scale to 100's of thousands of endpoints
- Reduced IT headaches from reimaging and helpdesk tickets
- 24x7 support
- Clearer view of security trends to help guide policy

Cb Response and the PSC

- Cloud threat intelligence enriches endpoint data with attack context
- Robust reputation data allows users to quickly prioritize severe threats
- Watchlists shared across customers and threat researchers speed detection of new threats

Carbon Black.

Key Capabilities

Continuous and Centralized Recording

Centralized access to unfiltered 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

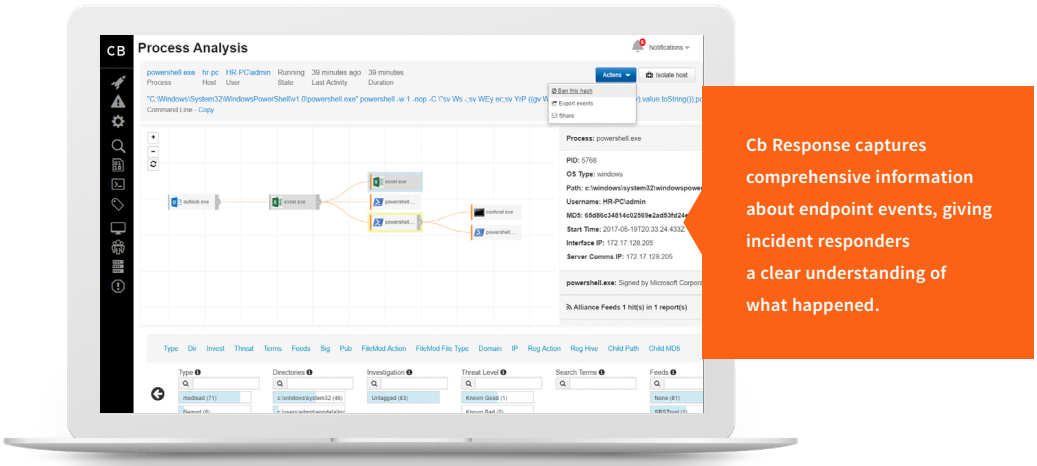
With Live Response, incident responders can create a secure connection to infected hosts to pull or push files, kill processes, perform memory dumps, and quickly remediate from anywhere in the world.

Attack Chain Visualization and Search

Cb Response 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 Cb Response into their existing security stack.



Cb Response captures comprehensive information about endpoint events, giving incident responders a clear understanding of what happened.

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 APIs and 120+ out-of-the-box integrations
- On-prem, virtual private cloud, SaaS, or MSSP

Platforms

Sensor Support:

Deployment Options:

- Cloud or On-Premise

About Carbon Black

Carbon Black is a leading provider of next-generation endpoint security. Carbon Black serves more than 3,700 customers globally, including 33 of the Fortune 100. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV). Leveraging its newly introduced big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black solutions enable customers to defend against the most advanced cyber threats, including malware, ransomware, and non-malware attacks. Deployed via the cloud, on premise, or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus. For more information, please visit www.carbonblack.com or follow us on Twitter at @CarbonBlack_Inc.

Carbon Black.