Carbon Black.

CB RESPONSE

Industry-Leading Incident Response and Threat Hunting

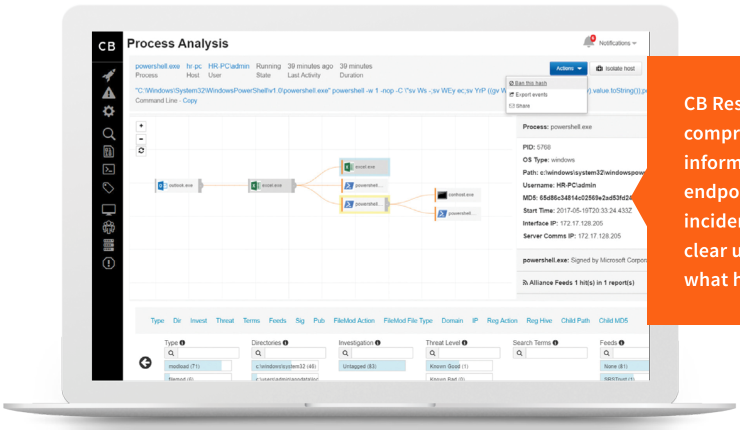
Enterprise security teams struggle to get their hands on the endpoint data they need to properly investigate and proactively hunt for abnormal behavior. Security and IT professionals lack the ability to see beyond suspicious activity and need a way to dive deeper into the data to make their own judgments.

CB Response is an industry-leading incident response and threat hunting solution designed for security operations center (SOC) teams. CB Response continuously records and stores 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, 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 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-premises deployment, virtual private cloud or software as a service

> **"Using CB Response 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**

IAC



Process Analysis

powershell.exe Process | hr-pc Host | HR-PC\admin User | Running State | 39 minutes ago Last Activity | 39 minutes Duration

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" powershell -w 1 -nop -C \"sv Ws -;sv WEy ec;sv YrP ((gv W

).value.toString());p

Command Line - Copy

Process: powershell.exe

PID: 5768

OS Type: windows

Path: c:\windows\system32\windowspow

Username: HR-PC\admin

MD5: 65d86c34814c02569e2ad53fd24

Start Time: 2017-05-19T20:33:24.433Z

Interface IP: 172.17.128.205

Server Comms IP: 172.17.128.205

powershell.exe: Signed by Microsoft Corpor

Alliance Feeds 1 hit(s) in 1 report(s)

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

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
- Unlimited retention and scale for the largest installations
- Reduced IT headaches from reimaging and helpdesk tickets

THREAT HUNTING ON THE PSC

All the threat hunting and incident response capabilities of CB Response are now available in CB ThreatHunter, our new offering on the CB Predictive Security Cloud!

Learn more at **carbonblack.com/products/CB-threathunter**

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

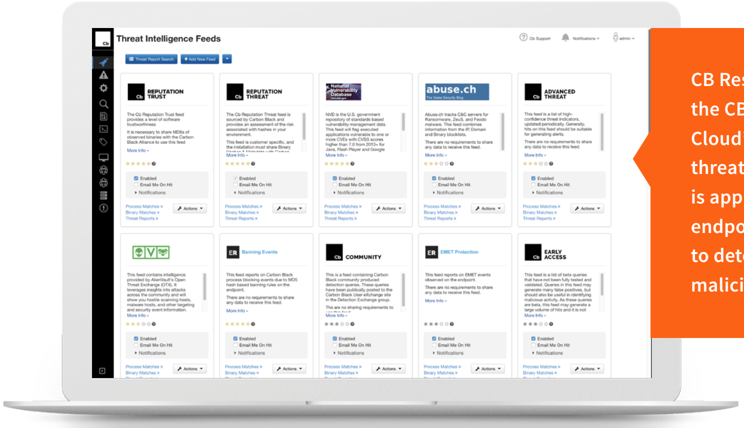
With Live Response, incident responders can create a secure connection to infected hosts to pull or push files, kill processes, perform memory dumps and quickly remediate from anywhere in the world.

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.



The Cb Reputation Trust feed provides a level of software trustworthiness

It is necessary to share MD5s of observed binaries with the Carbon Black Alliance to use this feed

The Cb Reputation Threat feed is sourced by Carbon Black and provides an assessment of the risk associated with hashes in your environment.

This feed is customer specific, and the installation must share Binary

NVD is the U.S. government repository of standards based vulnerability management data. This feed will flag executed applications vulnerable to one or more CVEs with CVSS scores higher than 7.0 from 2013+ for Java, Flash Player and Google

Abuse.ch tracks C&C servers for Ransomware, ZeuS, and Feodo malware. This feed combines information from the IP, Domain and Binary blocklists.

There are no requirements to share any data to receive this feed.

This feed is a list of high-confidence threat indicators, updated periodically. Generally, hits on this feed should be suitable for generating alerts.

There are no requirements to share any data to receive this feed.

This feed contains intelligence provided by AlienVault's Open Threat Exchange (OTX). It leverages insights into attacks across the community and will show you hostile scanning hosts, malware hosts, and other targeting and security event information.

This feed reports on Carbon Black process blocking events due to MD5 hash based banning rules on the endpoint.

There are no requirements to share any data to receive this feed.

This is a feed containing Carbon Black community produced detection queries. These queries have been publically posted to the Carbon Black User eXchange site in the Detection Exchange group.

The are no sharing requirements to

This feed reports on EMET events observed on the endpoint.

There are no requirements to share any data to receive this feed.

This feed is a list of beta queries that have not been fully tested and validated. Queries in this feed may generate many false positives, but should also be useful in identifying malicious activity. As these queries are beta, this feed may generate a large volume of hits and it is not

CB Response leverages the CB Predictive Security Cloud's aggregated threat intelligence, which is applied to all endpoint activity data to detect patterns of malicious behavior.

ABOUT CARBON BLACK

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security delivered via the cloud. Leveraging its big data and analytics cloud platform – the CB Predictive Security Cloud – Carbon Black consolidates prevention, detection, response, threat hunting and managed services into a single platform with a single agent and single console, making it easier for organizations to consolidate security stacks and achieve better protection. 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) enabling customers to defend against the most advanced threats. More than 4,300 global customers, including 35 of the Fortune 100, trust Carbon Black to keep their organizations safe.

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:

- Windows
- MacOS
- Red Hat Linux
- CentOS (Linux)
- Oracle RHCK

Deployment Options:

- Clouds or On-Premise

REQUEST A DEMO

Contact us today to schedule a demonstration.

CONTACT@CARBONBLACK.COM

617.393.7400

Carbon Black.

1100 Winter Street
Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499
www.CarbonBlack.com