Carbon Black.

CB THREATHUNTER

Advanced Threat Hunting & IR in the Cloud

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.

CB ThreatHunter is an advanced threat hunting and incident response solution delivering unfiltered visibility for top security operations centers (SOCs) and incident response (IR) teams.CB ThreatHunter is delivered through the CB Predictive Security Cloud (PSC), a next-generation endpoint protection platform that consolidates security in the cloud using a single agent, console and dataset.

By leveraging the unfiltered data collected by the PSC, CB ThreatHunter provides immediate access to the most complete picture of an attack at all times, 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 unfiltered visibility, CB ThreatHunter gives you the power to respond and remediate in real time, stopping active attacks and repairing damage quickly.

> "CB ThreatHunter has simplified incident response by allowing quick discovery of both simple and advanced threats. Its simplicity and responsiveness are amazing, especially when you are running an investigation where every minute matters... Endpoint security *used to be* difficult."
>
> **— DENIS XHEPA, IT SYSTEMS SECURITY ENGINEER OF MIDCAP FINANCIAL SERVICES**

USE CASES

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

BENEFITS

- Reduced complexity for more efficient endpoint security
- Easy deployment, automated updates, and unlimited scalability
- Accelerated investigations with unfiltered endpoint visibility
- Complete understanding of root cause to close existing gaps
- Secure remote access to infected endpoints for in-depth investigation
- Greatly reduced dwell time and average time to resolution

CB THREATHUNTER AND THE PSC

- Best-of-breed threat hunting delivered from a cloud platform
- One consolidated agent, one unified console
- Access to unfiltered data gathered from all protected endpoints
- Cloud threat intelligence enriches endpoint data with attack context
- Watchlists shared across customers and threat researchers speed detection of new threats

Carbon Black.

Key Capabilities

Complete Endpoint Protection Platform

Built on the CB Predictive Security Cloud, CB ThreatHunter provides advanced threat hunting and incident response functionality from the same agent and console as our NGAV, EDR and real-time query solutions, allowing your team to consolidate multiple point products with a converged platform.

Continuous & Centralized Recording

Centralized access to unfiltered endpoint 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 & Search

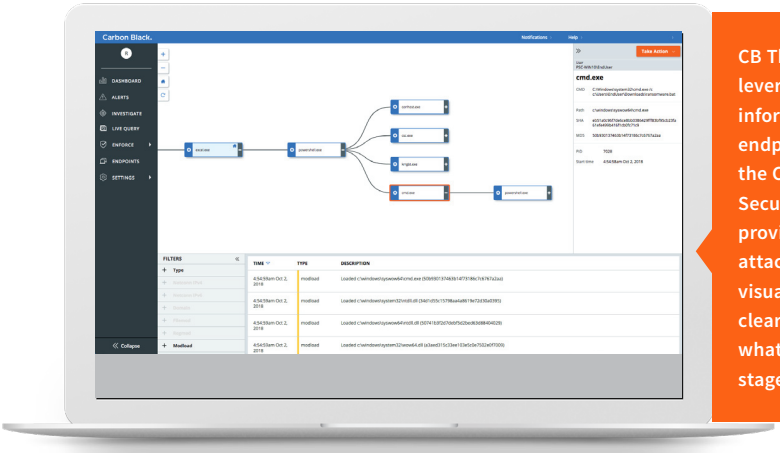
CB ThreatHunter provides intuitive attack chain visualization to make identifying root cause fast and easy. Analysts can quickly jump through each stage of an attack to gain insight into the attacker's behavior, close security gaps, and learn from every new attack technique to avoid falling victim to 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.

Automation via Integrations & Open APIs

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



CB ThreatHunter leverages unfiltered information about endpoint events from the CB Predictive Security Cloud providing extensive attack chain visualization to get a clear understanding of what happened at every stage of the attack.

FEATURES

- Lightweight sensor deployed and managed from the cloud
- Process and binary search of centralized, unfiltered data
- Out-of-the-box and customizable behavioral detection
- Proprietary and third-party threat intel feeds
- Automated watchlists to re-run queries
- Interactive and expandable attack chain visualization
- Secure remote shell for rapid remediation
- Open APIs

PLATFORMS

- Sensor Support - Windows

REQUEST A DEMO

Contact us today to schedule a demonstration.

CONTACT@CARBONBLACK.COM

617.393.7400

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.

Carbon Black.

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