

Cb RESPONSE

Market-leading incident response and threat hunting



Cb Response is the most precise IR and threat hunting solution, allowing you to get the answers you need faster than any other tool. Capture all threat activity so you can hunt threats in real time, visualize the complete attack kill chain, and then respond and remediate, quickly.

Available: On-premises, in the cloud or through one of our many partners.

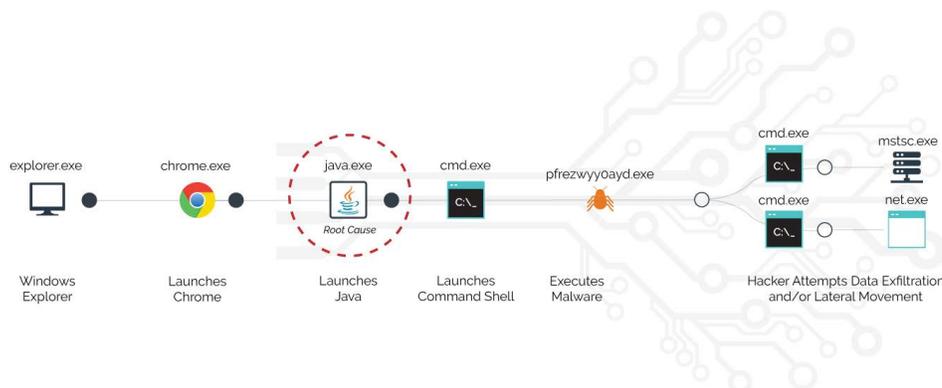
SEE EVERY THREAT AND CAPTURE ALL THREAT ACTIVITY

Modern attacks are getting more complex and harder to predict. Attackers are innovating in new ways to get past defenses. It's impossible to know 'bad' in advance of an attack. The only solution is to capture all threat activity so you can see and respond to attacks, even if they are initially undetected. If new malware self-deletes as part of an attack, you need to know it was there and what it did to your endpoints.

Cb Response is the only solution that continuously records all endpoint activity and then centralizes everything for fast access at all times. The result is zero-gap endpoint visibility. Investigations are accelerated because information you need is always available. You always have a conclusive answers to your questions. It streamlines alert validation and triage because the details of what caused an alert are always at your fingertips.

VISUALIZE THE ATTACK KILL CHAIN

When you capture all threat activity, you will also visualize the complete attack kill chain, making it easier to understand every detail of how you're being attacked. You can see everywhere the attacker went, what they did, and what needs to be fixed. You have a better idea of how to defend your environment because you know exactly how attackers are targeting you. With zero-gap endpoint visibility, you always know root cause, so you can close gaps to stop future attacks.



Visualize the attack kill chain so you always know root cause and the scope of the attack.

BENEFITS

Reduce alert fatigue

Triage more alerts, faster

Accelerate investigations

The information you need is always available, never hit a dead end

Conclusive understanding of the attack

See where the attacker went and what they did

Find threats missed by defenses

Reduce dwell time and damage done

Disrupt future attacks

Know root cause then address gaps and blind spots

Reduce IT involvement

Eliminate unnecessary reimaging and tickets

Require less security expertise

Improve productivity of security team

Deploy the way you want

Available on-premises or as a SaaS offering through Carbon Black or an MSSP

USE CASES

- Breach preparation
- Attack detection
- Alert validation and triage
- Incident response
- Attack isolation
- Threat hunting
- Remediation
- Threat banning

“Carbon Black [Cb Response] gives me visibility that I desperately need.”

— Customer, Financial Services

HUNT THREATS IN REAL TIME

Zero-gap endpoint visibility allows you to hunt threats in real time. Use your knowledge of your environment to proactively seek and discover advanced threats that made it past your defenses and slipped past your detection. Threat hunting allows you to find threats and anomalous behavior before anything bad happens — reducing dwell time and damage done to your organization.

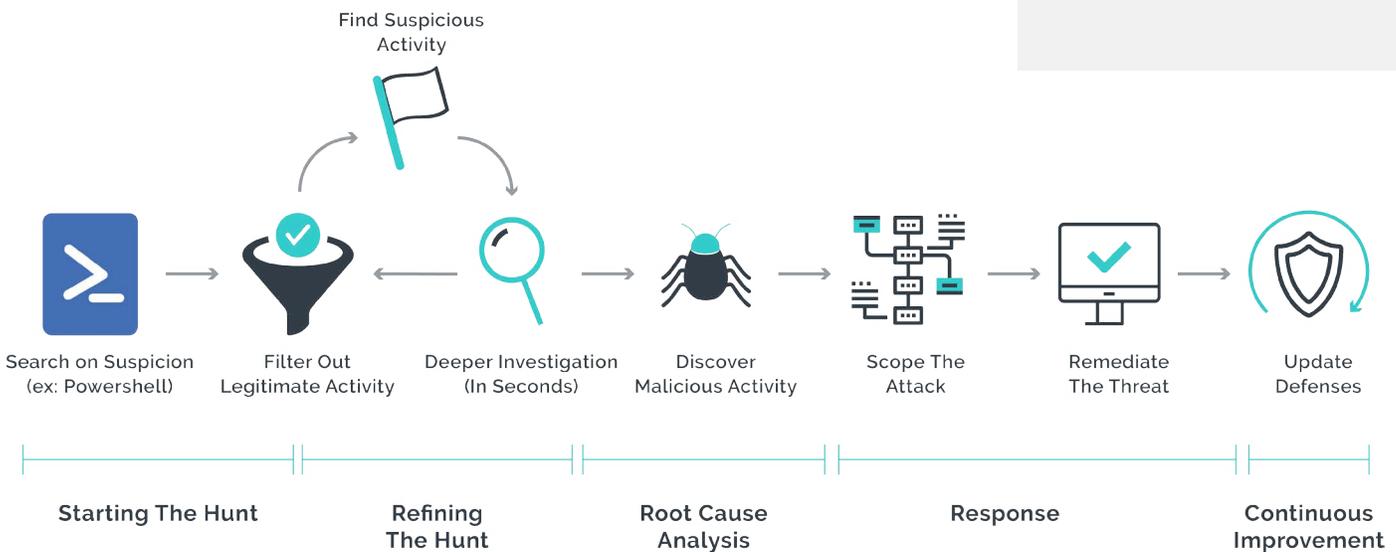
RESPOND AND REMEDIATE

Cb Response is a single console for all incident response and threat hunting activities, including remediation. Once a threat is detected you can isolate the attack, then remotely investigate and clean up any endpoint, from anywhere. With detailed root cause and full scope you can be more precise in remediation, fixing only what needs to be fixed. This allows you to eliminate unnecessary machine reimaging and avoid unnecessary IT involvement.

TECHNICAL FEATURES

- CPU usage less than 1%
- RAM usage less than 20MB
- Network bandwidth 50 bytes per second on average
- Man-in-the-middle protection through bidirectional SSL authentication with server
- Centralized management, storage, and control — available on-premises or in the cloud (SaaS)

SUPPORTED PLATFORMS



The Carbon Black Hunt Chain: The process that users of Cb Response can employ to effectively hunt out evasive threats in their environment.

REQUEST A DEMO:

Contact us today to schedule a demonstration.

contact@carbonblack.com

ABOUT CARBON BLACK

Carbon Black has designed the most complete next-gen endpoint security platform, enabling organizations to stop the most attacks, see every threat, close security gaps, and evolve their defenses. The Cb Endpoint Security Platform helps organizations of all sizes replace legacy antivirus technology, lock down systems, and arm incident response teams with advanced tools to proactively hunt down threats. Today, Carbon Black has approximately 2,000 worldwide customers, including 25 of the Fortune 100 and more than 600 employees. Carbon Black was voted Best Endpoint Protection by security professionals in the SANS Institute's Best of 2015 Awards.

2016 © Carbon Black is a registered trademark of Carbon Black, Inc. All other company or product names may be the trademarks of their respective owners. 20160715 JPS

**CARBON
BLACK**
ARM YOUR ENDPOINTS

1100 Winter Street, Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499

www.carbonblack.com