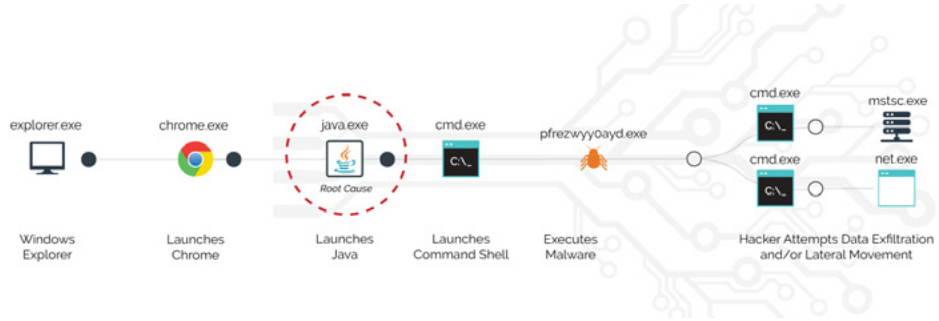
DATA SHEET

Cb Response

Industry-Leading Incident Response & Threat Hunting

ATTACKERS ARE INNOVATING AT A TERRIFYING PACE

With 68% of breaches taking months or longer to discover, many organizations must now accept the very real possibility that intruders have already compromised their systems, regardless of the organization's security posture.[1] Today, compromises are measured in minutes and the speed of response is measured in days. Enterprises the world over are realizing that to close the gap, they need to evolve their security operations from being a largely reactive unit to being proactively on the hunt for new attacks.



But it's impossible to know, and protect against, all bad behavior in advance. Most security operations centers (SOCs) simply do not have the comprehensive visibility necessary to quickly make informed decisions. Other endpoint detection and response products promise speed of search, but have visibility gaps due to the incomplete data they collect.

Cb Response is speciality-built for enterprise SOC and IR teams, delivering unfiltered visibility, rapid analysis, and a remote remediation toolset for intelligent, end-to-end detection and response.

"Carbon Black has decreased the time required to identify and respond to a security incident. Before Cb Response, we required hours or days before we could identify an endpoint compromised by a zero-day in Microsoft Word, for example. Nowadays, we are able to detect and respond even before the user contacts us. To date, we have reduced the IR time from days to hours."

- Senior Security Analyst, Global Satellite/Telecommunications Company

CLOUD-POWERED SECURITY

Cb Response leverages the Cb Predictive Security Cloud (PSC), Carbon Black's converged endpoint protection platform. The PSC is an extensible platform that delivers next-generation endpoint security services using one sensor, one data set, and one cloud-based console.

For Cb Response users, the Cb Predictive Security Cloud delivers crucial threat intelligence and reputation data, allowing security professionals to quickly prioritize potential threats. This empowers organizations with limited resources to focus on the most critical security issues using the latest shared insights from security experts all around the world.

Carbon Black.

BENEFITS

- **Fast, end-to-end response time**
  Provides real-time threat response & remediation
- **Unfiltered endpoint visibility**
  Records endpoint activity to speed up IR & enable proactive threat hunting
- **Unlimited retention & scale**
  Scales to fit even the largest installations, and offers unlimited data retention to meet compliance and dwell time needs
- **Rapid root cause identification**
  See how the attacker got in and what they attempted to do
- **In-depth investigations**
  Create a secure, remote connection to any infected endpoint from anywhere in the world with Live Response
- **Disrupt future attacks**
  Leverage automation to avoid manually hunting for the same threats twice
- **Reduce IT headaches**
  Eliminate unnecessary reimaging and IT tickets

This industry-leading IR and threat hunting solution empowers the SOC with the following capabilities:

UNFILTERED VISIBILITY

- Capture all threat activity with continuous recording
- Access all your data quickly and easily with centralized storage
- Visualize the attack chain to rapidly identify root cause and detect lateral movements to accelerate investigations
- Retain data forever with a full historical review of any attack – no matter how long the dwell time

REAL-TIME RESPONSE

- Radically reduces response time with unlimited endpoint data for investigations
- Stops attacks in progress by isolating infected systems, terminating processes, and banning hashes across the whole enterprise
- Enable remote remediation of infected systems with Live Response
- Take any action, such as collecting advanced forensic data or running custom scripts, from anywhere in the world
- Use knowledge of root cause to close gaps and prevent future attacks

PROACTIVE THREAT HUNTING

- Stop the headline breach and detect advanced attacks faster. Only 30% of 2017 breaches included malware, making threat hunting for fileless attacks critical [2]
- Proactively discover the most advanced threats that may initially appear legitimate
- Leverage open APIs to integrate with the rest of your security stack for advanced attack correlation

PROVEN AT SCALE

- Requires minimal resources and infrastructure investment
- Turnkey integrations and open APIs ensure a seamless fit into even the most complex environments
- Enables prioritized patch management through tight integration with other solutions such as IBM BigFix

1 2018 Verizon Data Breach Incident Report

2 2018 Verizon Data Breach Incident Report

USE CASES

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

SUPPORTED PLATFORMS

"With Cb Response, we've been able to create watchlists and identify viruses that other controls missed."

– Security Analyst at an investment management company

REQUEST A DEMO:

Contact us today to schedule a demonstration.

contact@carbonblack.com

Call us at 617-393-7400

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.

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