DATA SHEET

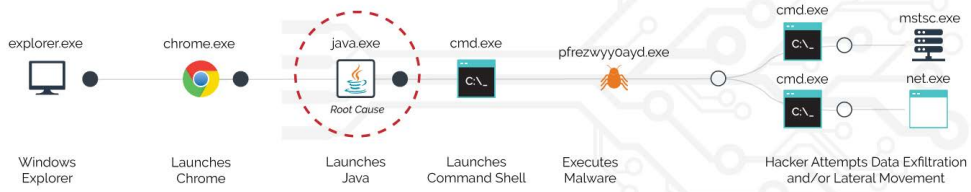
Cb RESPONSE

Detect and Respond Faster

ATTACKERS ARE INNOVATING AT A TERRIFYING PACE.

It's impossible to know, and protect against, all bad behavior in advance. With 93% of breaches taking minutes or less to compromise the system[1], detection and response speed is paramount. Most Security Operations Centers (SOCs) do not have the comprehensive visibility necessary to quickly make informed decisions.

Anything that provides less than 100% visibility is a wasted investment. It results in blind spots that prevent root cause identification and stops IR from preventing future attacks. Other endpoint detection and response products promise speed of search, but have visibility gaps, which means you're searching incomplete data. Only Cb Response provides the complete visibility, fast analysis and remote remediation toolset that enables the fastest possible end-to-end incident response.



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

Cb Response is purpose-built for enterprise SOC and IR teams. Offering a streamlined UI that's built for speed, unlimited historical data retention and unlimited scaling to fit even the largest enterprises, this market-leading IR and threat hunting tool empowers the SOC with the following capabilities:

COMPLETE VISIBILITY WITH CONTINUOUS CENTRALIZED RECORDING:

- Capture all threat activity with 100% continuous recording.
- Centralized storage means the data you need is always at your fingertips.
- Visualize the complete attack kill chain so you always find the root cause and see lateral movements to accelerate investigations.
- Unlimited data retention for full historical review of any attack – no matter how long the dwell time.

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

– Security Analyst at an investment management company

Carbon Black.

BENEFITS

Fastest end-to-end response time
Provides real-time threat response & remediation – cutting average IR time to less than 15 minutes

Complete endpoint visibility
Records 100% of activity to speed 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 requirements

Accelerate investigations
Information you need is always available, never hit a blind spot

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

Optimized for on-premises deployments
Minimal infrastructure requirements – your data is your data

USE CASES

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

REAL-TIME RESPONSE:

- Radically reduces average IR time from 78 hours to less than 15 minutes per incident.[2]
- Stops attacks in progress by isolating infected systems, terminating processes and banning hashes across an enterprise.
- "Live Response" enables complete & remote remediation of infected systems. Take any action, such as collecting advanced forensic data or running custom scripts, from any location.
- Use knowledge of root cause to close gaps and prevent future attacks.

PROACTIVE THREAT HUNTING:

- Stop the headline breach and detect advanced attacks faster. 53% of 2016 breaches did not use malware, making threat hunting critical.[3]
- Proactively discover the most advanced threats that make it past your defenses.
- 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 - 99% of all enterprises can deploy in a single server cluster.
- Turnkey integrations and open APIs ensure a seamless fit in even the most complex environments.
- Enables prioritized patch management through tight integration with IBM BigFix.

TECHNICAL FEATURES

- Scales to the size of any enterprise
- Unlimited historical data retention
- Enables prioritized patch management with IBM BigFix
- 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
- 100% Open APIs for full integration

SUPPORTED PLATFORMS

REQUEST A DEMO

Contact us today to schedule a demonstration.

sales@cybertan.co.za

RANKED #1 IN DETECTION BY FORRESTER

- Perfect score of 5/5 for detection
- Complete visibility that the SOC desperately needs
- A solution that's proven at scale to fit any enterprise
- Empowers proactive threat hunting

The Forrester Wave™: Endpoint Security Suites Report

Cb RESPONSE PROVIDES:

75% faster time to root cause identification

90% reduction in the need to re-image machines

Data from Carbon Black IR partner product usage

[1] *2016 Verizon Data Breach Investigations Report*
[2] *Data from Carbon Black IR partner product usage*
[3] *2016 Verizon Data Breach Investigations Report*

ABOUT CARBON BLACK

Carbon Black is the leading provider of next-generation endpoint security. Carbon Black's Next-Generation Antivirus (NGAV) solution, Cb Defense, leverages breakthrough prevention technology, "Streaming Prevention," to instantly see and stop cyberattacks before they execute. Cb Defense uniquely combines breakthrough prevention with market-leading detection and response into a single, lightweight agent delivered through the cloud. With more than 7 million endpoints under management, Carbon Black has more than 2,500 customers, including 30 of the Fortune 100. These customers use Carbon Black to replace legacy antivirus, lock down critical systems, hunt threats, and protect their endpoints from the most advanced cyberattacks, including non-malware attacks.

Carbon Black.

cyberTAN Information Security

4 Sonop Place Street, Randpark Ext. 5,
Johannesburg, South Africa, 2194
P +27 83 636 0099
www.cybertan.co.za