Carbon Black.

Reducing the Cost of Incident Response

Introduction

Cb Response is the most complete endpoint detection and response solution available to security teams who want a single platform for hunting threats, disrupting adversary behavior and changing the economics of security operations. Only Cb Enterprise Response continuously records all endpoint activity, centralizes and correlates that data with unified intelligence sources, and reveals a complete kill chain that pinpoints attack root cause to power live threat containment, banning and remediation activities. Built entirely on open APIs, Cb Enterprise Response pushes and pulls data through the security infrastructure to automate and enhance adaptive threat response processes, helping to make it the #1 EDR solution among global enterprises and 70+ of the world's leading IR and MSSP firms.

Cb Enterprise Response reduces the cost, complexity and time of traditional incident response by replacing reactive "after-the-fact" manual data acquisition with proactive continuous monitoring and recording of all activity on endpoints and servers—dramatically decreasing the dwell time of targeted attacks. By combining Cb Enterprise Response's continuous endpoint recording with comprehensive cloud-delivered threat intelligence—supplied from Carbon Black Threat Intel—responders can customize their detection and optimize their response. To disrupt the further spread of an attack, Cb Enterprise Response can instantly ban the execution of malicious files across an enterprise's endpoints for instant attack recovery. Cb Enterprise Response also integrates with Microsoft's Enhanced Mitigation Experience Toolkit (EMET)—which protects against exploit-based attacks for select, critical applications—to correlate events generated from EMET with Cb Enterprise Response's continuous endpoint recording for enhanced detection and rapid response.

As sophisticated attackers now target company-specific data or intellectual property, the target is not the network—it's the endpoints where that data resides. Therefore, the new threat landscape requires solutions that can prepare an organization's endpoints for constant attack and the inevitability of compromise. Cb Enterprise Response makes advanced threats easier to see and faster to recover from by empowering SOC and IR teams to arm their endpoints against the most advanced and targeted attacks.

Efficiencies of using Cb Response - Incident Response

The table below represents data gathered from Carbon Black Partners actively involved in providing incident response services, and data from our own Carbon Black SOC.

	In-House FTE	Conventional 3rd party	Carbon Black Enterprise Response
Endpoint located	2 hours	2 hours	<1 minute
Forensic resource applied to endpoint	1 hour	12 hours	n/a
Endpoint imaged	6 hours	4 hours	n/a
Endpoint analyzed	70 hours	40 hours	10 minutes
	78 hours **(per endpoint)**	**58 hours** **(per endpoint)**	**<15 minutes** **(per endpoint)**

Table Definitions:

Endpoint located:

Time from initial indication to properly identify the exact endpoint based upon IP address of suspected endpoint.

- Top 3 initial indicators for conventional IR solutions are: SIEM alerts, 3rd party notifications, or anomalous network traffic. - *SANS Race to Detection Report 2015*
- Continuous recording feature of Cb Enterprise Response provides immediate visibility of any endpoint based solely on IP address, and offers expanded initial indicators based upon Patterns of Compromise versus a single indicator of compromise, like an IP address.

Forensic resource applied to endpoint:

Time from identification of endpoint resource to get security personnel access to the end system.

- Conventional 3rd party assumes resource is not sitting on the bench and must be dispatched to the customer location.
- Cb Enterprise Response continuous recording eliminates the need to deploy personnel to retrieve data.

Endpoint imaged:

Time to capture data from the endpoint.

- Conventional methods rely on complex scan based solutions or full HDD image captures from the endpoint.
- Cb Enterprise Response continuously records endpoint activity eliminating the need for complex forensic activity merely to identify the threat.

Endpoint analyzed:

Time involved to sift through all the data collected, tie together events and processes, create timeline maps of the suspected activity, research different findings against known threats, compare data against threat information sources, and create a report of findings.

Efficiencies of using Cb Response - Managed Operations

Security Operation Center (SOC) table is displaying data gathered from clients using Conventional Solutions that must query the endpoint for status and correlate the gathered data across multiple tools, and data gathered from clients using Cb Response integrated solutions with continuous recording and instant visibility across the enterprise.

	Conventional	Cb Response
Number of alerts per day	Numerous (too high to accurately gauge)	High fidelity alerts due to "Patterns of Compromise" methodology
Alerts personnel were able to respond	10%-20%	80%-90%
Time to root cause identification	20 hours	<10 minutes
Analyst time on console	8 hours	1 hour
Track binary across enterprise	2 days	<1 minutes

Alerts per day:
Conventional solutions generate a high number of false positive due to limited visibility across endpoints and limited integration with other source of detection within the enterprise.

Root Cause:
Conventional solutions follow the same timetables listed in the response tables previously. Root Cause can only be ascertained through direct access to the machine which occurs through HDD cloning or dispatched personnel to the affected machine.

Binary tracking:
Conventional solutions must gather data from endpoints either through scripted or scheduled job-based mechanisms. Cb Enterprise Response continuous recording allows for immediate identification of executed binary status.

Response rates:
Cb Enterprise Response filters alerts allowing for higher response rates due to the limited numbers and quick filtering of false positives due to visibility. Conventional solutions lead to "top 10" methodologies and risk measurements to segment the high number of alerts to manageable sums resulting in unanswered alerts that are not investigated.

Time on console:
An indirect FTE requirement metric. Running scheduled queries, interpreting results, or responding to high false positive rates consumes analyst time resulting in full shift "on console" tasking.

FTE requirement:
Direct results of alerts, required data gathering, and analysis of collected data to make proper determination of cause. Cb Enterprise Response's streamlined solution allows for minimal staffing compared to conventional SOC endpoint solutions.

Example of Cb Response Efficiencies in Incident Response

We asked a Carbon Black Partner to give us a real world example of how Cb Response better enables them to perform incident response activities. Following is their summary of a single engagement where another non-Carbon Black partner started the investigation, and after significant delays the Carbon Black partner was asked to assist.

- Conventional Responder engaged two weeks before Carbon Black Partner
- Conventional Responder used command line tools to manually collect artifacts
- Conventional Responder had only 50% of the 500 server network completed after 2 weeks!
- Conventional Responder reviewed firewall logs for anomalous network traffic and found a "bad" IP address. Recommendation to client was to begin imaging hard drives of devices that communicated with "bad" IP.
- Carbon Black Partner was engaged at the 2-week mark, and within 24 hours were monitoring every process, binary, and IP address. (Note – all this was done remotely. No travel costs to client. No on-site personnel. Better utilization of resources.)

Within minutes identified the "bad" IP connection, the endpoint making the connection, the binary making the connection, and the geolocation of the IP along with threat actor information known to be associated with the site.

Example of Cb Response Efficiencies in Managed Operations

During a quarterly update with a client, Cb Enterprise Response alerted to the presence of known attacker using a new attack vector. While still in the meeting, the partner was able to provide the following data points from the Cb Enterprise Response console, and everything below was accomplished in <10 minutes. Not a single machine was imaged!

- Methods attacker was using
- machine under attack
- Identified the malware connecting to the C&C server, AND identified the directory on the affected endpoint where the malware was staging
- Identified other endpoints in the network where the same malware was staging (even though the malware wasn't beaconing out at the time)
- All IP addresses associated with the malware
- All commands used in conjunction with the attack
- Reconnaissance activities of the attacker and what accounts the attacker was trying to access

Whitepaper

Summary

For incident response teams, half the battle is just collecting the data to do your job. Reactively collecting data using antiquated forensic tools and outdated antivirus products delivers very little visibility into the full context of an incident and continues to prove laborious and inefficient. Collecting data after detection is a backwards approach and makes it nearly impossible to understand lateral movement or the root cause of advanced attacks.

Cb Response reduces the cost and complexity of traditional incident response by replacing reactive "after-the-fact" manual data acquisition with proactive continuous monitoring and recording of all activity on endpoints and servers. Responders can dramatically reduce the cost of incident response while also decreasing the dwell time of targeted threats with instant attack intervention and remediation of advanced threats.

Cb Response is the most complete endpoint detection and response solution available to security teams who want a single platform for hunting threats, disrupting adversary behavior and changing the economics of security operations. Only Cb Enterprise Response is the #1 EDR solution among global enterprises and 70+ of the world's leading IR and MSSP firms.

Carbon Black.

Carbon Black is the leading provider of a next-generation endpoint-security platform designed to enable 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 650 employees. Carbon Black was voted Best Endpoint Protection by security professionals in the SANS Institute's Best of 2015 Awards.

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