Secureworks

Managed Carbon Black Response Cloud Setup and Operations Guide

Last Updated: January / 2018

Document Version: 1.1

Secureworks

Copyright

Secureworks

Table of Contents

Secureworks

Document History

Document Revision #	Date Created:	Comments:
1.0	December 2017	Initial document creation
1.1	January 2017	Added note on data retention for migration clients. Updated the URL for sensor connectivity. Updated the ticket template to associate Secureworks with existing Cb instances. Added the latest link for supported endpoints

Documentation update requests

To request modifications or notify the author of errors in this document, please notify your Secureworks representative. During initial implementation, notify your Provisioning Engineer. After initial implementation, please notify the Secureworks CTOC through a portal ticket.

Secureworks

Introduction

This document provides information on the Cb Response Cloud offering.

What is Cb Response Cloud?

Cb Response sensor software, installed on endpoints, collects data about all executed processes in a central repository. The sensor also stores copies of unknown binaries. Cb Response Cloud indexes this data to make it searchable, and it checks all new data against Threat Indicator feeds.

The Cb Response Cloud management console is hosted in the cloud so there is no need for on-premises hardware.

Secureworks receives a feed of all data sent to the Cb Response Cloud environment prior to processing, and sends this data through Secureworks Advanced Analytics.

Secureworks

Requirements

Perimeter firewall requirements

The vendor recommends allowing endpoints to connect to any HTTPS destination in order to avoid blocking communication. If access needs to be restricted, then allow access to the URLs below. The **clientInstance** will be assigned by Carbon Black.

The best option is to allow access to all of ***.my.carbonblack.io** and ***.carbonblack.io** allowing access to all of the possible client Carbon Black hosts. If this is not possible, then allow access to all of the following:

Source	Destination	Service	Purpose
Cb Response Console Users	Carbon Black Response console URL: **shib.carbonblack.io** **my.carbonblack.io** **carbonblack.io** **<clientInstance>.my.carbonblack.io**	TCP 443	Management console communication
Endpoint Sensor	Carbon Black Response Cloud Minion URLs: **sensors.<clientInstance>.my.carbonblack.io** **sensors.<clientInstance>-00.my.carbonblack.io** **sensors.<clientInstance>-01.my.carbonblack.io** **sensors.<clientInstance>-02.my.carbonblack.io** **sensors.<clientInstance>-03.my.carbonblack.io** **sensors.<clientInstance>-04.my.carbonblack.io** **sensors.<clientInstance>-05.my.carbonblack.io** **sensors.<clientInstance>-06.my.carbonblack.io** **sensors.<clientInstance>-07.my.carbonblack.io** **sensors.<clientInstance>-08.my.carbonblack.io** **sensors.<clientInstance>-09.my.carbonblack.io**	TCP 443	All sensor communication You will not know how many CB destinations will exist until after implementation. After implementation, the full list of node names can be found in "Settings|Server Nodes" in the GUI.

Below is the access required in order to access the Cb Response Cloud console. Access is limited based on source IP, make sure to list any public IPs that require access to the management console via the DCF.

Source	Destination	Service	Purpose
Client Management workstation	Carbon Black Response console URL: **<clientInstance>**.my.carbonblack.io	TCP 443	Console access

Bandwidth requirements

According the Carbon Black's sizing guide, an average endpoint should send about 32MB of data to the Carbon Black Response Cloud per day. Caching is used on the endpoint to limit the impact of network congestion or lack of connectivity

Device Configuration Form (DCF) used for setup

Secureworks has provided you with a Device Configuration Form to aid the installation of the Carbon Black Response service. Fill out this form and return it to your assigned engineer.

All information in the DCF is required to proceed with installation. Providing this data in advance greatly speeds the deployment of the service.

Table 1 - User accounts

You will need at least one user account in order to access the Cb Response Cloud interface. There are two possible roles: Administrator or User.

Table 2 - Instance details

Management source IPs

Access to the cloud management interface is limited to pre-defined IPs. Please specify the IPs you wish to allow access to your cloud management interface. Add as many IPs and subnet ranges as necessary.

This is your public internet IPs, not your internal IPs.

This does not affect sensors, only the management interface.

Purge inactive endpoints

Inactive endpoints will be removed from your instance after the number of days defined. Purging of non-active endpoints is commonly done after 60 days. This only prunes endpoints that have not checked in to the cloud service, and does not affect endpoints that have connected even once within the defined period.

Table 3 - Sensor groups

The service already has a single sensor group named "Default Policy". You do not need additional sensor groups but you can request some additional groups at the time of implementation. The form asks for details of the most common configuration items, but there are many more possible configuration items in the GUI.

Group name

The name should reflect the functional purpose of this group. Multiple sensor groups are not a requirement

Data suppression level

Default is medium. For noisy endpoints, you can create a sensor group with high suppression.

Process banning

This allows you to ban known bad binaries from executing on endpoints, and allows disruption of running processes added to the ban list.

Collect binaries

The default is to enable binary uploads. This is required if you integrate with Lastline.

VDI

Choose "Yes" if the sensor group will support VDI endpoints

Automatic sensor upgrades

The default configuration is "No Automatic Updates".

Choose yes to upgrade sensors as soon as a new version is available. Alternatively, upgrade manually.

A note on migrating from on-premises Carbon Black Response

It is possible to migrate endpoints from an existing on-premises installation to a Cb Response Cloud instance. The data and configuration cannot be migrated, but the sensors can be migrated without the need to reinstall the endpoints.

- If Secureworks already manages your Carbon Black installation, then Secureworks can perform the migration for you.
- If Secureworks does not manage your on-premises console, then you will need to follow the instructions found in this vendor document: https://community.carbonblack.com/docs/DOC-3179
- Data retention in the Cb Response Cloud is limited to 30 days. It is reasonable to keep your current on-premises Carbon Black installation available during the first 30 days so you do not have a gap in your historic logs.

Steps to add Secureworks management to an existing Cb Response Cloud implementation

Add Secureworks as a contact allowed to open tickets with Carbon Black on your behalf, and create a new user account for Secureworks in your cloud instance.

- Create a support case to Cb and state:
  "We have purchased the Secureworks AETD service for our Cb Response Cloud instance. Our instance name is <*>.my.carbonblack.io. Please associate our account with Secureworks so they can submit and work cases on our behalf. Also configure the Cb Event Forwarder to forward all data to the Secureworks S3 bucket. Carbon Black already has all details available in order to configure the Event Forwarder with Secureworks."
- Add a new user account within Cb Response Cloud with an access level of "Administrator" using email address 3rdpartyvendoraccounts@secureworks.com
- Beware that access to the management interface of the cloud instance will be limited to the IPs you define in the DCF. This access limitation is a requirement for the management of this service.
- Notify Secureworks when the steps above have been complete

Secureworks

How to Request Carbon Black Community Portal access

After your access to the Carbon Black Cloud is implemented, you can request access to the Carbon Black community.

Carbon Black directly supports the sensor software. Their community portal provides many self-help tools and documentation.

The Carbon Black Support Portal hosts all of the product documentation for the Carbon Black Security Platforms. If not clearly stated as Cb Response, then information may actually refer to the Cb Protection Platform.

You can request access by doing the following:

1. Email support@carbonblack.com and request that an account needs to be set up. Alternately, open an account at the Carbon Black community site https://community.carbonblack.com
2. Once you receive a username and password go to the following link and log in https://community.carbonblack.com
3. If you have additional questions, please contact support@carbonblack.com or 877-248-9098
4. To access training please click on the training tab at the home screen and email training@carbonblack.com to create a separate account

Note on Live Response

The Live Response feature is disabled before the instance is implemented as a security mechanism. If you need this feature enabled, then open a ticket in the portal and Secureworks will have the feature enabled. Be aware that this feature provides significant access to the endpoints so this is not enabled unless requested.

Additional Information

If you need direct endpoint support, you can contact Carbon Black, Inc. via email at cb-services@CarbonBlack.com or by calling their 24x7 hotline at +1 617.393.7400.

Advanced Endpoint Threat Detection Videos

http://www.secureworks.com/it_security_services/advanced-endpoint-threatdetection/?=hp_us

http://go.secureworks.com/advancedthreats

https://www.brighttalk.com/webcast/11141/108207

Vendor reference documentation

https://community.carbonblack.com/community/resources/product-docs-downloads/content?filterID=contentstatus%5Bpublished%5D~category%5Bcb-response%5D

The vendor also tracks the supported OS list in the following article: https://community.carbonblack.com/docs/DOC-7991

Carbon Black Videos

https://www.carbonblack.com/resources/videos/

https://www.carbonblack.com/resources/webinars/

https://youtu.be/JkB5PSr0csQ

Video training

Cb Response 101 Video #1 - Overview of Capabilities / Key Concepts / Terminology

Cb Response 101 Video #2 - Architecture / Data Flows

Cb Response 101 Video #3 - Threat Intelligence / Alliance Feeds

Cb Response 101 Video #4 - Process Search / Binary Search

Cb Response 101 Video #5 - Process Analysis

Cb Response 101 Video #6 - Watchlists

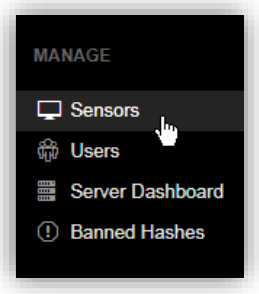
Cb Response 101 Video #7 - Investigations

Secureworks

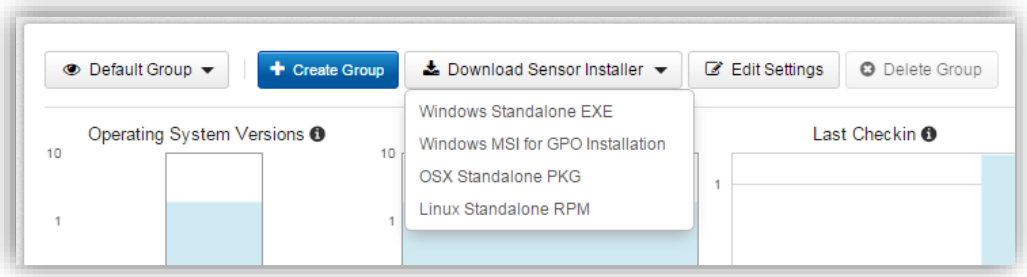
Installing sensor software on the endpoint

Secureworks does not support endpoint installation or management. There are many tools available, and support for endpoint deployment is beyond the scope of our services. The information provided is purely to help clients get started.

Access the sensor software from the GUI via the **Sensors** section of the navigation bar.



If you have more than one sensor group, select the sensor-group before downloading. The sensor software package is tied to that sensor-group:



Windows manual installation

Make sure to extract *all* files from the package to a directory, and then run **CarbonBlackClientSetup** to install the endpoint software. See the readme.txt file for additional command line options.

At the time of this writing, silent installs are documented in the Readme file that is included with the "Windows MSI for GPO installation" package available in the Carbon Black Response GUI.

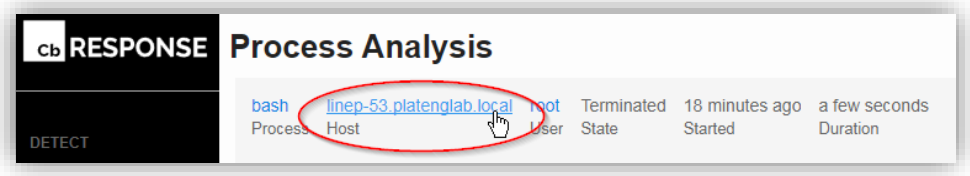
Linux endpoint or Mac OSX installation

Installations instructions for Linux and Mac OSX can be found in the Cb Response User Guide.

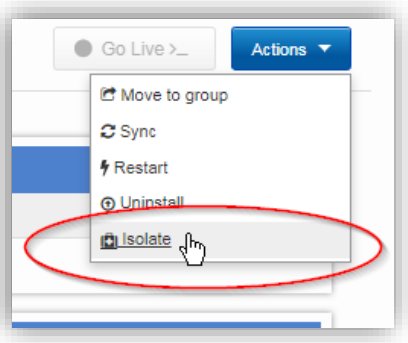
Endpoint Isolation

Carbon Black offers the ability to "Isolate" an endpoint through the Carbon Black Response GUI. This feature renders the endpoint operating system unable to communicate with anything on the network except the Carbon Black Response console.

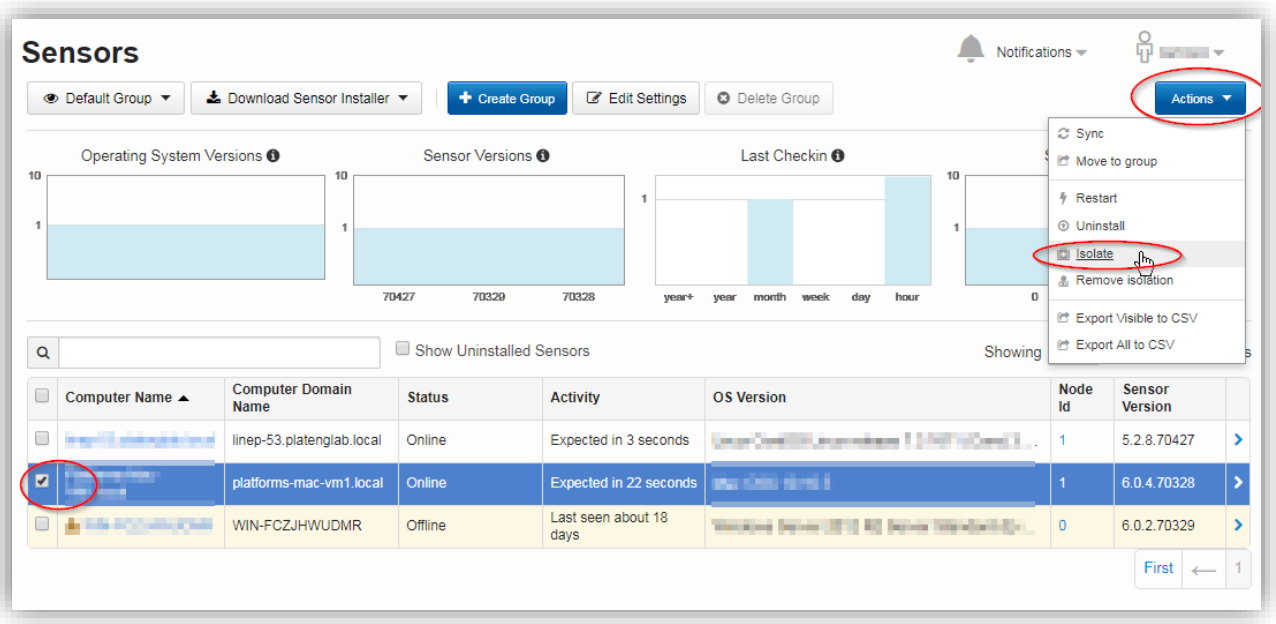
To isolate a host in the GUI when examining a specific event:
On the top of the event window, select the endpoint



In the endpoint window, select **Actions | Isolate**



You can also isolate one or more endpoint from within a sensor group. To do so, open the sensor group, select the endpoints you want to isolate, then select **Actions | Isolate** A warning message will appear, and you will need to approve the isolation before it takes effect.



Sensor health

Below are a list of items to check in order to validate the health of your Sensors.

Sensor end-to-end validation

See the section "Validating the event flow from the sensor" for instructions to trigger an event on a sensor. This validates the entire chain of systems.

Sensor details in the GUI

You can view the sensors that are online or offline in the GUI. Open the "Sensors" menu. An easy way to see all endpoints is in a single pane is to Export All to CSV. If you prefer the GUI, then each "Sensor Group" will need to be selected independently. This only indicates if a sensor can connect to a standalone or cluster Headend. In a cluster, a device will show online even if connectivity to a Minion is blocked.

Viewing the Sensor Queues

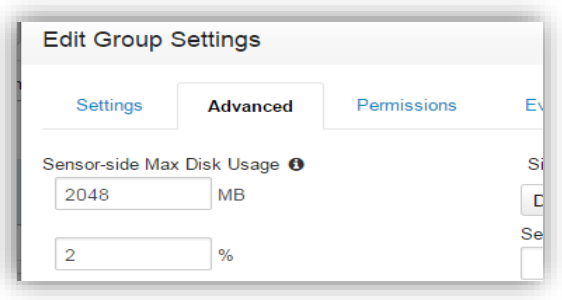
The Aggregate Sensor Queue in the GUI can indicate that many sensors cannot connect to a cluster minion. According to Carbon Black there is no good or bad metric, but a queue that is only increasing could point to something such as a network connectivity issue from the sensor to minions in a cluster. There are two metrics:

Aggregate Sensor Event Queue	Shows the total size of queued events needing to be pushed to the Cb Response server for all online sensors.
Aggregate Sensor Binary Queue	Shows the total size of queued binaries needing to be pushed to the Cb Response server for all online sensors.

Secureworks

Endpoint data caching

Data will be cached by the Sensor software between scheduled check-ins, when the Carbon Black Response Server is not reachable, and when the server throttles communication during periods of high load. By default, 2% of the client hard disk is used for cache, with a max cache of 2GB. This is configurable in the GUI on a per-sensor group basis



Cache storage examples

	Processes per day	Process size in K	Total data per day
Low	1,600	10	16 MB
Medium	3,200	10	32 MB
Highest (uncommon)	6,400	20	240 MB

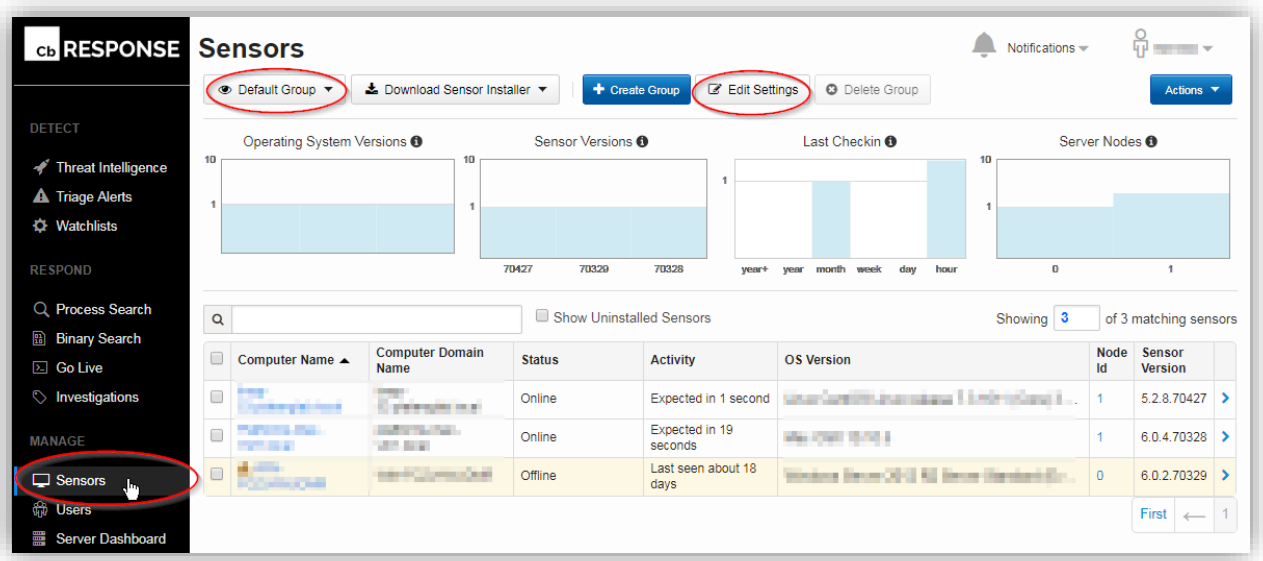
Secureworks

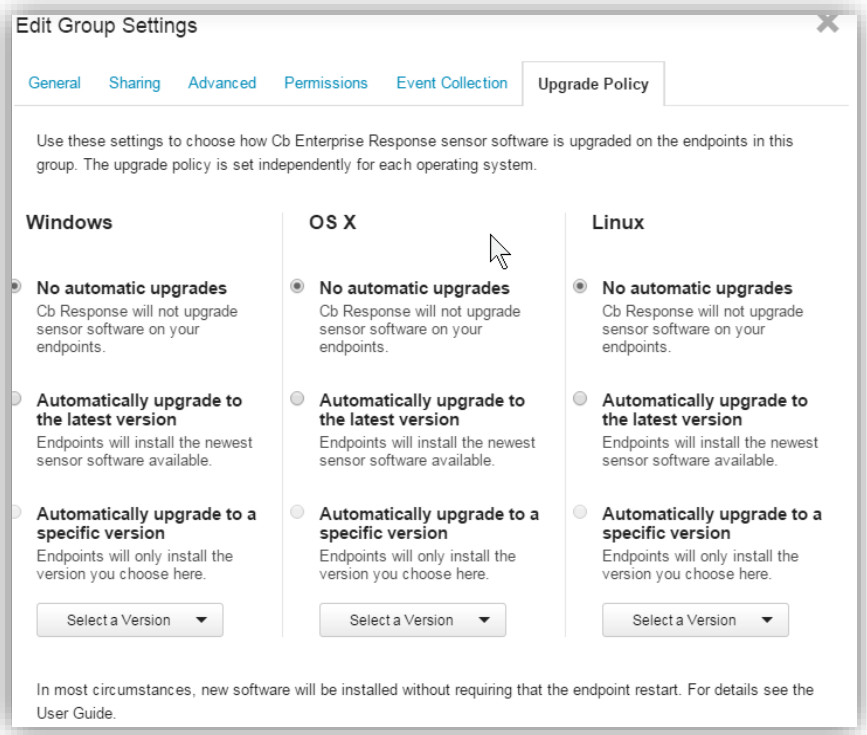
Sensor upgrade policy

You are responsible for updating sensors in your environment. You can manage sensor software on a per-sensor-group basis. You can set this to any of the following:

- Always latest - This will automatically update your endpoints whenever the server is updated
- No automatic updates - Use this when installing the sensor through an external software management solution
- A specific version - Use this if a specific version is needed

To change this setting, log into the GUI, select **Sensors** from the right-hand navigation bar, then select the affected group and edit the settings. See the screenshot below: Once in the settings page, click **Advanced**, and change the **Sensor Upgrade Policy.** Also, please be sure to enable **Tamper Detection**.





Secureworks

Validating the event flow from the sensor (endpoint)

On a Windows host, run the following commands to validate events from both Secureworks Advanced Analytics as well as the Carbon Black built-in feeds:

```
notepad.exe redcloaktest
powershell.exe -enc cwB0AGEAcgB0AC0AcAByAG8AYwBlAHMAcwAgAGMAYQBsAGMA
powershell.exe -enc cwB0AGEAcgB0AC0AcAByAG8AYwBlAHMAcwAgAG4AbwB0AGUAcABhAGQA
wmic process call create
```

After running the commands, it will take time for the Cb Response appliance to send the event to Secureworks and show up on the portal. Expect the elapsed time to be anywhere from 15 minutes to 45 minutes.

Secureworks

FAQ - Frequently Asked Questions

Can the Cb Response sensor be installed in a different directory location?

The Carbon Black Response software can only install into the `%SystemRoot%\CarbonBlack` directory, which is usually the c:\Windows\CarbonBlack directory. This destination cannot be changed.

Is there a best practice for grouping the agents?

Agents should only be separated into different groups if they need to follow a different policy. For example, you would create a new policy if some devices should have a larger event cache or if there is a group of machines that are VDI. See the section on Endpoint Sensor Groups

Are there considerations for Antivirus or HIDS coexisting on the endpoint?

With both Carbon Black Response Sensor and another endpoint product such as antivirus installed on a host, duplicate binary details will be recorded. In some cases, there may also be performance issues without the following rules.

Cause: The Carbon Black Response Sensor writes copies of binaries on the host to the directory:

```
%WINDIR%\CarbonBlack\store
```

Below is taken from the Carbon Black KB article 00000742

Solution Title: Required Antivirus exclusions for Carbon Black

Version: This solution applies to all Carbon Black versions on Windows, Linux, and OSX.

Topic:

The Carbon Black Sensor performs reads and writes to the Carbon Black installation root directories. With Antivirus products continually scanning the directory contents, the below exclusions will help eliminate performance issues and ensure proper coexistence.

Steps:

The directories to exclude in Antivirus products per Sensor platform are:

Windows:

```
%WINDIR%\CarbonBlack\*
```

OSX:

```
/var/lib/cb/*
```

Linux:

```
/var/lib/cb/*
```