Carbon Black Enterprise Response 5.1.1 Patch 3 Release Notes

Version 5.1.1.160623.1033

23 June 2016

Carbon Black, Inc.

1100 Winter Street, Waltham, MA 02451 USA

Tel: 617.393.7400 Fax: 617.393.7499

E-mail: support@carbonblack.com

Web: http://www.carbonblack.com

Introduction

The *Carbon Black Enterprise Response v5.1.1 Patch 3 Release Notes* document provides information for users upgrading from previous versions as well as users new to the product. It consists of the following major sections:

- **Preparing for server installation or upgrade**: This section describes preparations you should make before beginning the installation process for Carbon Black Enterprise Response server.
- **New and modified features**: This section provides a quick reference to the new and modified features introduced with this version.
- **Upgrading the Carbon Black Enterprise Response server**: This section provides information and instructions specific to server upgrades.
- **Corrective content:** This section describes issues resolved by this release as well as more general improvements in performance or behavior.
- **Known issues and limitations:** This section describes known issues or anomalies in this version that you should be aware of.
- **Contacting Carbon Black support:** This section describes ways to contact Carbon Black Technical Support, and it details what information to have ready so that the technical support team can troubleshoot your problem.

This document is a supplement to the main Carbon Black Enterprise Response product documentation.

Purpose of this release

Carbon Black Enterprise Response v5.1.1 Patch 3 release contains *quality and performance* improvements, and security fixes.

Documentation

The standard user documentation for Carbon Black Enterprise Response product includes:

- **Carbon Black Enterprise Response User Guide:** Describes Carbon Black Enterprise Response feature functionality in detail, plus administrative functions, including installing the Carbon Black Enterprise Response server and sensors.
- **Carbon Black Enterprise Response - Enterprise Server Sizing Guide:** Provides details on infrastructure sizing for Carbon Black Enterprise Response server.

- **Carbon Black Enterprise Response API**: Documentation for the Carbon Black Enterprise Response API is located at https://github.com/carbonblack/cbapi.

Additional documentation for special tasks and situations is available on the Carbon Black User eXchange.

Preparing for server installation or upgrade

This section describes requirements to meet and key information needed before beginning the installation process for the Carbon Black Enterprise Response server. All users, whether upgrading or installing a new server should review this section before proceeding. Once you have reviewed this document, see the following for specific installation instructions:

- **To install a new Carbon Black Enterprise Response server**, see "Installing the Carbon Black Enterprise Response Server" section in the *Carbon Black Enterprise Response User Guide* for version 5.1.1
- **To upgrade a Carbon Black Enterprise Response server**, see Upgrading the Carbon Black Enterprise Response Server below in this document.

System requirements

Operating system support for the server and sensors is listed here for your convenience. The document *Carbon Black Enterprise Response - Enterprise Server Sizing Guide* describes the full hardware and software platform requirements for the Carbon Black Enterprise Response server and provides the current requirements for systems running the sensor. Both are available on the Carbon Black User eXchange.

Both upgrade and new customers should be sure to meet all of the requirements specified here and in the Server Sizing Guide before proceeding.

Server / Console Operating Systems

- CentOS 6.4-6.8 (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.4-6.8 (64-bit)

Installation and testing is done on default installs using the 'minimal' distribution and the distribution's official package repositories. Customized Linux installations must be individually evaluated.

Sensor Operating Systems (for endpoints and servers)

- **Windows**: XP SP3 - 10 / Server 2003 - 2012R2, x86 and x64
    - Windows embedded OSes are individually evaluated

- **Mac**: OS X 10.7 through 10.11.4, x64 on Intel
- Linux: RHEL & CentOS 6.4-6.8, 7.0-7.2 x64 – standard kernel versions (2.6.32-358.el6, 2.6.32-431.el6, 2.6.32-504.el6, 2.6.32-573.el6, 2.6.32-642.el6, and 3.10.0-123.el7, 3.10.0-229.el7, 3.10.0-327.el7) and the standard minor/ maintenance releases. Non RHEL/CentOS distributions or Modified RHEL/CentOS environments (those built on the RHEL platform) are not supported.

YUM URL

Please use caution when pointing to the YUM repository. Different versions of the product are available on different branches as shown below:

- The current 5.1.1 Patch 3 version is available on Carbon Black YUM, pointed to by the following base URL: baseurl=https://yum.carbonblack.com/enterprise/stable/x86_64/
- The current 5.1 Patch 3 version is available on Carbon Black YUM, pointed to by the following base URL: baseurl=https://yum.carbonblack.com/enterprise/release/x86_64/

Note: Carbon Black Enterprise Response Server software packages are maintained at the Carbon Black YUM repository (yum.carbonblack.com). Communication with this repository is over HTTPS and requires the presence of appropriate SSL keys and certificates. During the Carbon Black Enterprise Response server install or upgrade process, other core CentOS packages may be installed to meet various dependencies. The standard mode of operation for the YUM package manager in CentOS is to first retrieve a list of available mirror servers from http://mirror.centos.org:80 and then select one of those mirrors to download the actual dependency packages. If your Carbon Black Enterprise Response server is installed behind a firewall that blocks access to the outside, it is up to the local network and system administrators to ensure that the host machine is able to communicate with standard CentOS YUM repositories.

Technical support

Carbon Black Enterprise Response server and sensor installation and support is covered under the Customer Maintenance Agreement. Carbon Black recommends contacting Technical Support prior to performing an upgrade for further details on the upgrade process and the latest information that supplements the information contained in this document. Technical Support is available to assist with the installation or upgrade process and ensure a smooth and efficient installation.

Upgrading the Carbon Black Enterprise Response Server

Supported upgrade paths

Server upgrades to v5.1.1 Patch 3 are supported from the following previous versions:

- All 4.2.x versions
- All 5.0 versions, including earlier patch releases
- All 5.1.x versions, including earlier patch releases

For more detailed instructions for installing or upgrading the server, please refer to the *Carbon Black Enterprise Response User Guide*. It is available on the Carbon Black User eXchange. For upgrading from 4.1.x and earlier versions, please call or e-mail Carbon Black Technical Support.

Configure sensor updates before upgrading server

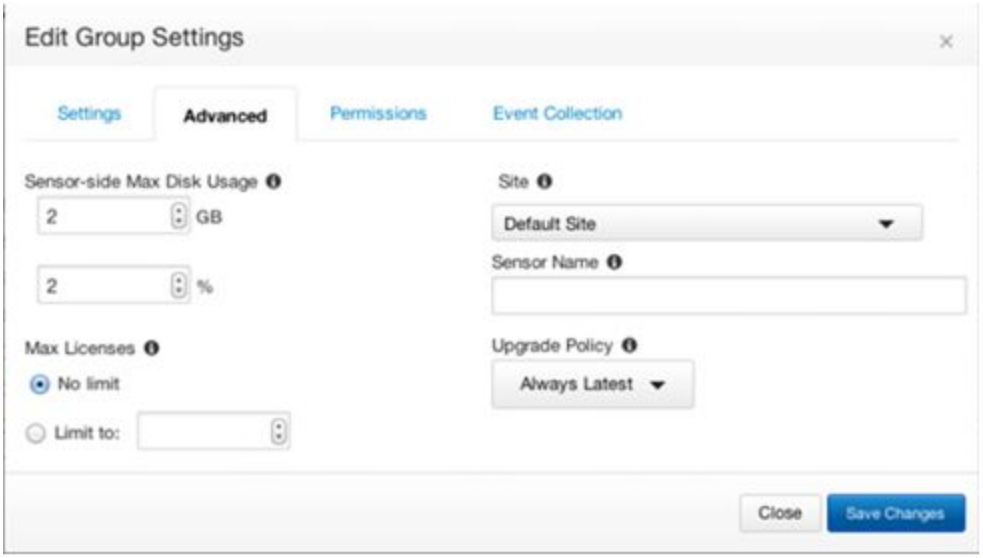
Carbon Black Enterprise Response v5.1.1 Patch 3 comes with updated sensor versions. If you are upgrading your server, you should determine if you would like to upgrade to the new *sensor* versions *before* you run the server upgrade program. Servers and sensors can be upgraded independently, and sensors can be upgraded by sensor groups, rather than all at once.

Decide if you would like the new sensor to be deployed immediately to existing sensor installations, or if you want to install only the server updates first. Carbon Black recommends a gradual upgrade of sensors to avoid any unacceptable impact on network and server performance.

Note: There is no expected degradation to sensor performance with Carbon Black Enterprise Response v5.1.1 Patch 3.

To configure deployment of new sensors via the Carbon Black Enterprise Response web UI:

1. Log in to the console, navigate to the Sensors page, and edit the group settings for each active Sensor Group:



2. Under the Advanced tab, find the Upgrade Policy setting. If this is set to **Always Latest**, the server will automatically upgrade sensors in this group to the latest sensor version.
   a. To keep the sensors at a specific version, select that version number from the dropdown prior to upgrade.
   b. To continue using whatever sensor versions are already installed, regardless of version, select **Manual**.

Note: Automatic upgrade settings for Sensor Groups apply to Windows sensors only. To change OS X and Linux sensor upgrade settings please see the “Installing Sensors” chapter of the *Carbon Black Enterprise Response User Guide*.

Updating Carbon Black Enterprise Response server

If you are upgrading the server, please follow the steps in this section. These steps require SSH or console access to the server and minions with root privileges.

To upgrade a standalone server:

1. On the server, stop the Carbon Black services: `service cb-enterprise stop`.
2. Update the Carbon Black services: `yum update cb-enterprise`.
3. Restart the Carbon Black services: `service cb-enterprise start`.

To upgrade a clustered server:

1. On the Master server, navigate to the cb install directory (defaults to /usr/share/cb) and stop the Carbon Black services: `./cbcluster stop`.
2. Update the Carbon Black services on each node: `yum update cb-enterprise`.
3. Restart the Carbon Black services: `./cbcluster start`.

Note: Improvements of Carbon Black Enterprise Response server will occasionally require using a utility called 'cbupgrade' (after `yum install/update cb-enterprise`) to migrate the database schema or alliance feed data. Upgrading from a previous stable version of Carbon Black Enterprise Response server to the current release does not require this step. However, running the utility is required when there are local changes to configuration files that have to be manually consolidated with the newer versions distributed by this release. The operator will be notified of this requirement when attempting to start the cb-enterprise services. In a clustered server configuration, this utility will need to be run on all nodes before restarting the cluster. *When running this utility in a clustered environment, be sure to answer 'NO' when asked to start server services; the administrator will need to use 'cbcluster' to start the clustered server.*

Installations Using Single Sign On

Customers upgrading to 5.1.1 Patch 3 from earlier releases may need to edit their SSO configuration file to ensure proper operation after upgrading. The following steps should be taken:

1. Verify the name of the current sso configuration file being used. This is defined in /etc/cb/cb.conf with the SSOConfig parameter, e.g.:
   `SSOConfig=/etc/cb/sso/sso.conf`
2. In the sso configuration file, find the entry for the assertion_consumer_service. It will look similar to the following:

```
"endpoints": {
          "assertion_consumer_service": [
            [
              "https://<IP Address>/api/saml/assertion",
             "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            ]
          ]
  },
```

3. If the assertion_consumer_service is defined using square-bracket syntax as in the example above, change it to use curly-brace and replace the comma to a colon in its syntax, as follows:

```
        "endpoints": {
        "assertion_consumer_service": {
              "https://<IP Address>/api/saml/assertion":
             "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
        }
    },
```

Using boolean OR with negated query terms

Carbon Black Enterprise Response server query language relies on the query syntax of the underlying database architecture that uses SOLR/Lucene. This query syntax has limitations when dealing with negated terms in queries that contains boolean OR, e.g. A OR -B.

In such cases, negated term is OR'ed with the result set of the terms that are not negated, instead of being applied first over the entire document set and then OR'ed with the result set of the other terms. This may return confusing search results, e.g.

```
netconn_count:[20 TO *] OR -process_name:chrome.exe
```

This query is expected to return processes that have more than 20 network connections OR processes not named *chrome.exe*, regardless of their network connection count. However, the results set will be a set of processes that are not named *chrome.exe* in the set of processes that have more than 20 network connections.

In order to workaround this shortcoming, the logical OR could be translated into a logial AND by using the equivalent negated version of the entire query, e.g. A OR -B → -(-A AND B)

```
-(-netconn_count:[20 TO *] AND process_name:chrome.exe)
```

Alternatively, the negated term can be replaced with a term that includes logical AND to a term that would match all documents, e.g.

```
netconn_count:[20 TO *] OR (process_id:* AND
        -process_name:chrome.exe)
```

A comprehensive fix to this limitation will be included in the upcoming releases.

Tracking and isolation of network connections the existed before OS X sensor was installed

In OS X sensor version included in 5.1.1 Patch 2, we have made a design change to improve sensor interoperability with a number of other endpoint applications, for example Symantec

Endpoint Protection agent and LittleSnitch. This resulted in a modified behavior in tracking and isolation of network connections. In 5.1.1 Patch 2, network connections and sockets that are established *before* the sensor is installed will not be tracked for monitoring and isolation. If the machine is rebooted after installation, sensor will continue to monitor and successfully isolate all network connections.

New and modified features

This section lists new and modified features in this version of Carbon Black Enterprise Response. If you are upgrading from version 5.1.0, you only need to read the "Carbon Black Enterprise Response 5.1.1" section immediately below. If you are upgrading from a release prior to 5.1.0, you should also read the "Carbon Black Enterprise Response 5.1.0 feature changes" section.

Carbon Black Enterprise Response 5.1.1 feature changes

The following sections provide a quick reference to the new and modified features introduced in version 5.1.1.

Endpoint isolation for Linux and OS X

The support for this feature, which was previously introduced in version 5.0.0 for Windows endpoints, has now been extended to include OS X and Linux endpoints. Requires 5.1.1 OS X and Linux sensor.

Responders can now instantly disrupt active intrusions by quarantining one or multiple endpoints from the network while still maintaining an active connection with the Carbon Black Enterprise Response server. This enables IR (Incident Response) teams to perform more conclusive and surgical investigations, while limiting the damage from the attack.

Carbon Black live response for Linux and OS X

The support for this feature, which was previously introduced in version 5.0.0 for Windows endpoints, has now been extended to include OS X and Linux endpoints. Requires 5.1.1 OS X and Linux sensor.

Responders can now perform remote live investigations, intervene with ongoing attacks, and instantly remediate endpoint threats. This enables incident responders to "look at" and "touch" endpoints to take immediate action during an investigation—even while the endpoint remains isolated from the rest of the network. For example, by getting a real time file directory or killing a process running currently.

Custom endpoint threat banning for Linux and OS X

The support for this feature, which was previously introduced in version 5.1.0 for Windows endpoints, has now been extended to include OS X and Linux endpoints. Requires 5.1.1 OS X and Linux sensor.

With endpoint threat banning in Carbon Black Enterprise Response, responders can now instantly stop, contain and disrupt advanced threats as well as block the future execution of similar attacks by banning binaries from being able to execute. This expands Carbon Black's ability to drive additional corrective action on impacted endpoints as a part of incident response efforts.

Note: *OS X and Linux sensors do not support excluding certain hashes from being banned via restrictions.conf. This feature is only supported for Windows platform.*

Cb Enterprise Response *Unified View*

Through a separate install package, the Carbon Black Unified View Server can be used to tie several clustered Carbon Black Enterprise Response deployments together with a unified user console. This capability allows for searching across multiple clusters with a unified result set.

Please refer to *Carbon Black Unified View Server User Guide* for more details on acquiring, deploying and maintaining Cb Unified View.

Splunk Integration

Carbon Black integration with Splunk is now available through the use of the Carbon Black Event Forwarder, which is located at the Carbon Black Github site. This connector takes feed and watchlist hits plus raw event data directly from Carbon Black Enterprise Response server, converts the data into JSON format, and allows the results to either be written out to a file or sent to a configurable destination. Combining the JSON output with the Carbon Black Technology Add-On provided by Splunk allows users to ingest Carbon Black Enterprise Response data into Splunk in a way that is compliant with Splunk's Common Information Model (CIM).

Please visit https://github.com/carbonblack/cb-event-forwarder for more details on the event forwarder and https://splunkbase.splunk.com/app/2790/ for information on the Carbon Black Technology Add-On.

Carbon Black Enterprise Server 5.1.0 feature changes

The following sections provide a quick reference to new and modified features introduced in 5.1.0.

Instant attack disruption & threat recovery with endpoint threat banning

With endpoint threat banning in Carbon Black Enterprise Response, responders can now instantly stop, contain and disrupt advanced threats. In addition, they can block the future execution of similar attacks by banning binaries from being able to execute. This expands Carbon Black's ability to drive additional corrective action on impacted endpoints as a part of incident response efforts.

Improved threat detection & kill chain analysis with Microsoft Enhanced Mitigation Experience Toolkit (EMET) integration

Carbon Black Enterprise Response 5.1.0 integrates with Microsoft's Enhanced Mitigation Experience Toolkit (EMET). This enables responders to correlate blocked exploitation attempts—from Microsoft EMET—with Carbon Black's collective intelligence to show key aspects of the attack both before and after the event. This empowers responders to optimize and improve their detection, investigation and patch management efforts by understanding the full kill chain of every exploitation attempt at the moment of compromise. SOC Personnel and incident responders can also have visibility into EMET configurations across an enterprise via this integration. This capability aids them in their investigations and allows them to properly determine the appropriate response.

Searchable threat intelligence reports

Providing new visibility and control into the threat intelligence feeds, Searchable Threat Reports allows visibility into the intelligence feeds. The visibility provided by the searchable reports includes insight into all indicators and queries contained within a feed. In addition, users can now suppress individual reports from triggering alerts to reduce false positive alerts for a feed.

Enriched threat intelligence with Damballa integration, domain reputation, geolocation & icon matching

Carbon Black Enterprise Response now leverages enhancements made to the Carbon Black Threat Intelligence Cloud's services: Attack Classification, Reputation and Threat Indicator Services.

- **Attack Classification:** The Threat Intelligence Cloud's Attack Classification Service provides comprehensive attack context and attribution by integrating with a robust list of industry-leading third-party sources to assist enterprises in identifying the type of malware and threat actor group behind an attack. The Threat Intelligence Cloud now delivers unmatched network-to-endpoint attack classification through its integration with Damballa's leading threat intelligence on malicious destinations, advanced threat actor groups and command-and-control communications.

- **Reputation:** To optimize trust-based endpoint threat detection and response techniques, the Threat Intelligence Cloud now extends reputation to the network layer by delivering domain reputation—an excellent addition to its already unmatched reputation regarding known-good, known-bad and unproven software.
- **Threat Indicators:** To identify spear phishing campaigns that actively deceive end users by masking malicious activities under the appearance of trusted applications, the Threat Intelligence Cloud now provides icon matching to help detect social engineering attacks:
    - The Threat Intelligence Cloud also now provides geolocation look-ups of inbound and outbound network connections.
    - In previous releases, Carbon Black Enterprise Response tracked the destination port (the local port for inbound connections) and the remote IP address for network connections. In version 5.1.0, Carbon Black Enterprise Response tracks Local IP for both ends of the connection. (Note that search functionality is limited to destination port and remote IP addresses.)

Note: Access to these enhanced threat intelligence features requires data sharing with Carbon Black Threat Intelligence Cloud (TIC).

Enhanced threat inspection, analysis & correlation with Cyphort integration

Carbon Black Enterprise Response now integrates with Cyphort for inspection, analysis and correlation of suspicious binaries discovered at the endpoint. Now Carbon Black can submit unknown or suspicious binaries to Cyphort Core—a secure threat analysis engine, which leverages Cyphort's multi-method behavioral detection technology and threat intelligence—to deliver threat scores used in Carbon Black Enterprise Response to enhance detection, response and remediation efforts.

Resolving alerts as false positive and ignoring future events

In version 5.1.0, you have the option to resolve Alerts as false positives and go one step further by preventing the feed from alerting you to the same conditions in the future.

Automatic pruning of inactive sensors

In version 5.1.0 Patch 1, we have added configuration logic to prune out sensors that are dormant or inactive. This would include systems that are offline, uninstalled or otherwise not communicating with the Carbon Black Enterprise Response server for a given number of days. The following configuration has been added to the cb.conf file to control pruning of such inactive sensors:

```
DeleteInactiveSensors=True
DeleteInactiveSensorsDays=10
```

By default the value is set to *False*.

In 5.1.1 Patch 1, we modified the configuration to filter out sensors that are dormant or inactive, rather than pruning them from the database to preserve the historical context of process activity stored by the server. The configuration option in cb.conf has also been modified to reflect the change in implementation:

```
SensorLookupInactiveFilterDays
```

If this value is unset (default), all sensors are returned. When SensorLookupInactiveFilterDays set to > 0, only sensors that checked in the past SensorLookupInactiveFilterDays days will be returned.

Important Note:

Users upgrading to 5.1.1 Patch 1, Patch 2 or Patch 3 from earlier releases may need to update their cb.conf file to reflect this change. ***The new setting supersedes both previous settings and the legacy settings are ignored by the system****.*

Corrective Content

The following section provides the corrective content changes made for each release.

Carbon Black Enterprise Server 5.1.1 Patch 3

Console and Server

1. Changed requests from datastore to use POST method rather than GEt when querying for feed reports so that long report ids can be accommodated without hitting URL limits. (CB-9635)
2. Improve ingress matching for domain name based IOCs to matching on subdomains in addition to the FQDNs, e.g. an IOC domain *example.com* would now match both a network connection to *a.example.com* and *b.example.com.* (CB-7478)
3. UI now correctly honors use_proxy and validate_server_cert options correctly when adding a custom feed. (CB-9649)
4. Server now uniquely identifies alerts generated on ingress feed hits (e.g. from feed hit events feed.hit.ingress.process and feed.hit.ingress.binary) from alerts generated by the feed_searcher cron job nightly runs. While the former alerts only on new process executions or binary reports that match a given feed report, the latter also creates an alert when there is a change in the feed report content or score since the last time a process or binary was tagged. Alerts generated from feed_searcher cron job now have specific alert type that refers to “feedsearch” in name and are displayed in Triage Alerts page with yellow exclamation marks instead of red for easy visual differentiation (CB-9393)
5. UI now asynchronously requests facet data on all search requests instead of only when visiting a search page the first time, reducing the time it takes to load them. (CB-9797)

Windows Sensor (5.1.1.160603.1529)

1. Fixed an issue where sensor service’s attempt to access files on network shares as SYSTEM was causing problems with various DFS shares, ranging from corrupted file writes to disconnected share drives. (CB-7764)
2. Corrected a potential issue where sensor service caused divide-by-zero exception. (CB-6839)

3. Corrected an issue where legacy TDI filter driver was accessing pointers without checking if they are valid. (CB-7718)
4. Corrected a slow memory leak that occurred when sensor service is under heavy load. (CB-7065)
5. Corrected a rare bugcheck that occurred in the cbk7.sys sensor driver. (CB-9328)

OS X Sensor (5.1.1.160603.1506)

1. Child process terminated events now correctly report the timestamp of end event, rather than the start event. (CB-9357)
2. Improved DNS parsing code to avoid high CPU usage. (CB-8394)
3. Sensor service no longer reports itself and its child processes to the server. (CB-7534)
4. Fixed an issue that caused sensor service crash in DNS parsing library. (CB-8798)
5. Corrected an issue where remote commands executed via Cb Live Response left behind zombie processes. (CB-9193)
6. Corrected an issue where force umount on a directory currently being used casued a kernel panic. (CB-9244)
7. Sensor now correctly reports CNAMEs in network connection events. (CB-9549)

Linux Sensor (5.1.1.160603.1515)

1. Corrected an issue where sensor service failed to start on reboot following an upgrade. (CB-8864)
2. Netconn events now contain process path as part of the protobuf message headers like in Windows platform. This is useful when parsing raw events on enterprise message bus for 3rd party analysis. (CB-9045)
3. Corrected a slow memory leak that caused elevated memory usage over long periods of time. (CB-9134)
4. Corrected an issue where remote commands executed via Cb Live Response left behind zombie processes. (CB-9236)
5. Added support for RHEL/CentOS 6.8 version on the endpoint. (CB-9253)

Carbon Black Enterprise Server 5.1.1 Patch 2

Console and Server

1. Corrected an issue where binary file store synchronization cron job was inserting incorrect MD5 hash values into PostgreSQL and therefore was never synchronizing correctly with files stored on disk. (CB-8750)
2. Added ability to broadcast raw sensor eventlogs to api.rawsensordata RabbitMQ exchange. (CB-7330)
3. Incoming network connection events that are tagged as feed hits now correctly shows up as feed hits in the Process Analysis page. (CB-7513)
4. CB Tamper feed hits are now correctly shown in Process Analysis page. (CB-8826)
5. Corrected an issue where Alliance feed hit tags were not correctly copied over when SOLR documents for long-lived processes split into multiple segments causing hit information to be lost. (CB-8346)

Windows Sensor (5.1.1.160415.1734)

1. Corrected an issue where eventlogs were sent to the wrong minion in clustered environment when a CB Live Response session was initiated. (CB-8486)
2. Corrected an issue where last eventlogs were not written to disk upon power off of endpoint causing some events occurring right before shutdown event to be lost. (CB-8420)
3. Fixed an issue that caused core driver to bugcheck in error path during initialization. (CB-8903)

OS X Sensor (5.1.1.160415.1724)

1. Fixed a memory corruption in network connection tracking that caused a crash. (CB-8785)
2. Fixed a memory leak in sensor user space service code. (CB-8740)
3. Fixed a memory leak in sensor kernel extension code. (CB-8802)
4. Fixed a sensor crash due to a failure to map a file to memory. (CB-8410)

5. Added process path and process MD5 to the header of network connection eventlogs uploaded by sensor. This is useful if raw sensor events are broadcast on RabbitMQ bus for archiving or further analysis. (CB-8924)

6. Fixed a spelling mistake in sensor uninstaller output. (CB-8720)

Linux Sensor (5.1.1.160415.1732)

1. Addressed memory leak in cbdaemon on RHEL 7.1/CentOS 6.7 (CB-8444)

2. Added process path and process MD5 to the header of network connection eventlogs uploaded by sensor. This is useful if raw sensor events are broadcast on RabbitMQ bus for archiving or further analysis. (CB-8924)

3. Added event timestamp to the header of process start eventlogs uploaded by sensor. This is useful if raw sensor events are broadcast on RabbitMQ bus for archiving or further analysis. (CB-8551)

4. Fixed an issue that resulted sensor driver to fail after install. (CB-8313)

5. Fixed a kernel panic that was result of a NULL pointer being dereferenced in kernel space. (CB-8754)

Carbon Black Enterprise Server 5.1.1 Patch 1

Console and Server

1. Corrected an issue where query of feed reports into memory for ingress matching could take a long time and cause data ingest to stop due to small default database paging size of 100. Paging size is now configurable via cb.conf (CB-7487, CB-8287)

2. Corrected an issue with cbinit script failing to create “cb” service user when it is ran as a non-root user. (CB-7545)

3. Corrected an issue with cbinit script failing to locate iptables if it is not in the running user’s PATH variable. (CB-7622)

4. Corrected an issue where cb-enterprise daemon does not successfully re-connect to RabbitMQ message bus if RabbitMQ socket temporarily goes down. (CB-8216)

5. cb-solr service throws UnknownHostException on feed hits if server hostname can’t be resolved causing feed hits to not to be reported. (CB-8218)

6. Corrected an issue where failure to download a file using the command line utility cbget causes Carbon Black Alliance Server communication status to show failure, even though server communication is intact. (CB-8423)
7. If a non-root user has been added to cluster.conf during *cbcluster add-node*, changes to this user in cluster.conf are not reflected in subsequent ssh communication with minions causing other *cbcluster* commands to fail. (CB--7571)
8. Corrected sensorsettings.ini file values for eventlog disk quota percentage and absolute size which were inadvertently reversed. (CB-8387)
9. Corrected an issue with CB API usage where passing an empty string as a sort parameter into a query API caused search to fail. (CB-7351)
10. Corrected an issue with *binary metadata* index purge script command line parsing that caused -g option to not to be honored when in dry-run mode. (CB-4578)
11. Corrected an issue with CBLR execfg command incorrectly parsing its arguments. (CB-7779)
12. Corrected an issue with UI dialog for ignoring future alerts from a feed not appearing when alerts are resolved as false positive. (CB-7640)
13. Corrected tooltips that were not correctly escaped for binary hashes banned from the UI. (CB-8380)
14. Corrected incorrect sizing of process icons in process search page. (CB-7768)
15. Corrected incorrect reference to documentation in VDI sensor group settings. (CB-7547)
16. Modified the feature to filter out sensors that are dormant or inactive. Instead of pruning them from the database, they are now filter at the API level to preserve the historical context of process activity stored by the server. The configuration option in cb.conf has also been modified to reflect the change in implementation (see section under server upgrade topic.) (CB-4096)

Windows Sensor (5.1.1.160314.0129)

1. Fixed an issue with sensor service frequency computation that caused intermittent “divide-by-zero” errors that resulted in system crash. (CB-8533)
2. Corrected a memory leak in core driver that only occurred if all event collections were disabled. (CB-6969)

3. Corrected an issue in sensor TDI driver (for Windows XP and Windows server 2003) that caused a bug check by accessing pointers without checking if they were valid. (CB-8520)
4. Corrected an issue in sensor TDI driver that caused a bug check due to incorrect handling of chained receive buffers. (CB-8521)
5. Corrected an issue where sensor missed process events generated close to endpoint shutdown due to a missing flush to disk in shutdown path. (CB-8524)
6. Corrected an issue where sensor uninstall from the UI failed when service name has been changed for obfuscation. (CB-8519)

OS X Sensor (5.1.1.160314.0122)

1. Fixed an issue with excessive memory usage on CbOsxSensorService due to incorrect tracking of some processes where sensor did not see the process start (e.g. because service was restarted after). (CB-8230)
2. Fixed an issue with excessive debug messages printed to /var/log/system.log by the sensor. (OS-8227)
3. Fixed a kernel panic under 10.11.2 due to changes to underlying OS kernel structures. (CB-7408)
4. Fixed an issue where some of the child process terminate messages were not reported to the server. (OS-8487)

Linux Sensor (5.1.1.160314.0136)

1. Fixed an issue with excessive memory usage on cbdaemon due to incorrect tracking of some processes where sensor did not see the process start (e.g. because service was restarted after). (CB-8314)
2. Corrected an issue where cbdaemon stopped working after some time and a status check on it returned “cbdaemon is dead but subsys locked”. (CB-8371)
3. Fixed an incorrect reference to a directory path during cbdaemon initialization script. (CB-8386)
4. Fixed an issue that caused sensor to post CBLR commands incorrectly. (CB-7510)
5. Corrected an issue that caused sensor to hang under heavy system load. (CB-6650)

Carbon Black Enterprise Server 5.1.1

Console and Server

1. Improved logging in feed synchronizer background task. (CB-3932)
2. Corrected an issue with sensor uninstall from the UI when user does not have global administrator privileges. (CB-4006)
3. Resolved a race condition between SQL purge maintenance task and Alliance Server binary uploads. (CB-4008)
4. Updated nginx cb-multihome.conf.example to match the nginx cb.conf that is shipping in 5.1. (CB-4012)
5. Fixed incorrect time stamps on sensor communication failures. (CB-4014)
6. Corrected misleading cb.conf content. (CB-4016)
7. Resolved emails not being sent for host-based Tamper Detection events issue. (CB-4020)
8. Fixed failures in moduleinfo_insert statements because of an integer overflow in primary 'id' sequence on the SQL table. (CB-4028)
9. Fixed an issue with bulk resolve of alerts due to a logic error in API calls. (CB-4035)
10. Fixed an issue with alerts from OSX/Linux 4.x sensors that resulted in invalid process links. (CB-4037)
11. Fixed an issue with redundant syslog events from feed searcher job every time a MD5 matches a feed. (CB-4045)
12. Corrected invalid report id errors from watchlist searcher. (CB-4048)
13. Fixed an issue persistence of global feed alert settings on the UI across multiple users. (CB-4058)
14. Corrected an issue with total blocks counter not being updated for banned hashes. (CB-4059)
15. Corrected an issue with ignore status on feed report being nullified on feed full-sync. (CB-4062)
16. Corrected an issue with cbcluster start hangs while CbTools continues to run. (CB-4065)

17. Corrected an issue with disabling "Process user context" event collection not being reflected in the systemsettings.ini file. (CB-4066)
18. Removed sensor purge functionality in favor of filtering sensor detail page results in the API. (CB-4069)
19. Added parent_unique_id field to the results returned by the rest API search() endpoint. (CB-4074)
20. Fixed an issue with feed facets on the Process Analysis page. (CBUI-1036)
21. Corrected a discrepancy in sensor queue values reported by UI versus the rest API. (CBUI-1130)
22. Corrected “Email Me” option not being persisted after watchlist creation issue. (CBUI-1532)
23. Corrected an issue with "Export All to CSV" action on sensor page failing to export all sensors. (CBUI-1575)
24. Improved how drag and drop on "team settings" UI page works. (CBUI-1576)
25. Binary search page now correctly displays "ago" in the first-seen field on result rows. (CBUI-1578)
26. Corrected an issue with incorrect search being performed when clicking on “Publisher” field in process analysis page. (CBUI-1582)
27. Corrected an issue on selection of a facet for process analysis. (CBUI-1600)
28. Corrected an issue with “sensor filter by node” facet, which resulted in incorrect selections on sensor list page. (CBUI-1601)
29. Fixed an issue with hyperlinks on UI notifications drop down. (CBUI-1602)
30. Improved sensor "yield" tooltip messaging when the issue is health score related. (CBUI-1612)
31. Corrected an issue with custom threat feed dialog not correctly disappearing after adding a feed url manually. (CBUI-1686)

Windows Sensor (5.1.1.151030.0948)

1. Fixed an issue with kernelSocketConnect in cbk7.sys that resulted in system crash in some machines. (WIN-306)

2. Fixed a potential memory leak in cbtdiflt close completion handling. (WIN-340)
3. Fixed an issue with sensors not honoring "collect binaries" checkbox in sensor group settings. (WIN-349)
4. Fixed an issue with sensor dropping network connections on Win 2K3 endpoints. (WIN-352)
5. Resolved an issue that resulted in sensors not communicating to server on isolate. (WIN-360)
6. Resolved a potential deadlock due to holding FAST_MUTEX while calling ZwSetValueKey(). (WIN-362)

OS X Sensor (5.1.1.151217.0244)

1. Sensor now correctly rotates/expunges log files so that /var partition is not filled. (OSX-251)
2. Reduced excess error events in system.log with OS X 10.11. (OSX-281)

Linux Sensor (5.1.1.151215.1153)

1. Sensors now correctly rotate/expunge log files so that /var partition is not filled. (LNX-194)
2. Sensor now correctly honors Binary/Eventlog collection limits (1GB or 2% each) with small partitions. (LNX-196)
3. Fixed a kernel panic on systems running *named* linux service. (LNX-206)

Carbon Black Enterprise Response 5.1.0 Patch 3

Console and Server

1. Fix file permissions for /etc/cb/cb_ssh so that it is not readable except by root user. (CB-3645)
2. Updated /api/user/<name>/permissions API call to check requester’s team membership before returning permissions information for users. (CB-3692)

3. Fixed e-mail actions so that notifications are sent for host-based tamper detection events. (CB-4020)
4. Corrected an issue with negation of Alliance-based feed fields in process searches. (CB-4033)
5. Corrected an issue with IP address searches with CIDR ranges broader than /8. (CB-4044)
6. Fixed an issue where a previously *ignored* feed report's status is nullified after feed-sync action. (CB-4062)
7. Disabled caching of HTTPS responses by browser clients. (CB-4655)
8. Corrected an issue where deleting all watchlists caused watchlists page to fail. (CB-4995)
9. Corrected an issue where resolving an alert failed if alert name contained ">" character. (CB-5026)
10. Corrected an issue in behavior of *sensor -n* command in CB Live Response session. (CB-5176)
11. Corrected an issue where some complex queries failed due to improperly encoded POST request by the API. (CB-7241)
12. Corrected an issue where escaping a colon in text-based queries resulted in a failed request. (CB-7252)
13. Corrected an issue where a watchlist search link failed if the query terms included forward slashes. (CB-7275)

Windows Sensor (5.1.0.151215.1242)

1. Fixed an issue where turning off all event collections resulted in memory leak and instability in the core Carbon Black driver. (CB-6969)

Linux Sensor (4.2.9.151215.0933)

1. Added support for RHEL/CentOS 7.2. (CB-7376)

Carbon Black Enterprise Response 5.1.0 Patch 2

Console and Server

1. Corrected a behavior where throttle_calc task in cb-enterprise uses progressively more CPU. (E-4698)
2. Fixed an issue with OS process document count in alliance statistics are broken in clustered deployments. (E-4688)
3. Updated nginx cb-multihome.conf to match nginx cb.conf in the product shipping with 5.1. (E-4669)
4. Corrected an issue with feed_searcher sending to syslog every time a md5 matches a feed to include VirustTotal. (E-4652)
5. Added logic to rate-limit number of binary hash check HTTP calls to prevent self-inflicted denial of service on the cb-datastore. (E-4697)
6. Corrected an issue with cbdiag --post failing when post size is “too large” in some customer environments. (E-4668)
7. Corrected an issue with watchlist searcher throwing “Invalid Report ID” error causing current job to fail. (E-4677)
8. Fixed the system hang due to CbTools background task is running in the system cbcluster. (E-4646)

Windows Sensor (5.1.0.150911.0926)

1. Fixed an issue with CB 5.1.0 sensor upgrades failing if service is renamed (obfuscation) but core driver is not. (WIN-346)
2. Fixed a potential memory leak in cbtdiflt “connection close/completion” handling. (WIN-340)
3. Fixed a system crash issue when doing a live migration of a VM host. (WIN-329)

Linux Sensor (4.2.8.150908.0431)

1. Corrected a kernel panic in systems running Linux named service. (LNX-206)

Linux Sensor (4.2.9.151002.1507)

This is sensor adds support for Linux 6.7. It is not generally available. Please contact Bit9 + Carbon Black Technical Support team to get access.

Carbon Black Enterprise Response 5.1.0 Patch 1

Console and Server

1. CentOS 6.7 fails requesting to upgrade python-urllib3 library. This issue has been addressed in this release. (E-4612)
2. Addressed a failure when cb-enterprise services are started, due to cb-redis service no longer being able to create its own PID file. This is because SELinux policy in CentOS 6.7 has changes that restrict Redis process to where it is allowed to write PID and log files. (E-4653).
3. Several changes were made to increase the security of Carbon Black. (CBUI-1216)
4. Tagged processes could lose their highlighting in the console when they were later shown in search results. This issue has been fixed in the patch. (CBUI-1224)
5. URLs that directly referenced a console page would first open the login page and then display the Welcome Page instead of the page referenced in the URL. In this release, the user is directed to the correct page after authentication. (CBUI-1386)
6. Process or binary search boxes now accept a comma-separated list of query fields. (CBUI-1502)
7. Fixed an issue where the UI would occasionally display 504 errors, timeout errors or the license graph not being displayed after an upgrade from earlier releases to version 5.1.0. (E-4094)
8. Addressed an issue where the watchlist page was blank if a proxy was configured for the server. (E-4334)
9. Inactive sensors are now removed after 10 days of inactivity. (ENT-4409)
10. Corrected an issue where the EventPurgeEarliestTime date in cb_settings is being set in the future. This prevented deletion of files that should have been purged, which caused unnecessary disk usage. (E-4457)
11. Addressed performance issues, especially with backlog processing. (E-4506)
12. Corrected an issue where the binary downloads failed in clusters using a non-standard API port. (E-4508)

Windows Sensor (5.1.0.150805.0434)

1. Fixed an issue where Chkdsk would not run on reboot when Carbon Black sensor was installed on certain Windows operating systems. (WIN-314)

Carbon Black Enterprise Response 5.1.0

Console and Server

1. Administration/Sensors page takes a long time to load on Servers with large number of sensors. (CBUI-1236)
2. Addressed some non-functioning CBLR Commands on FireFox. (CBUI-1285)
3. UI does not allow non-global-admin administrator of a group to edit group settings, the issue has been addressed in this release. (CBUI-1307)
4. Fixed the Binary Preview hyperlink search it was not returning any results. (CBUI-1385)
5. If you click on the notification boxes in a threat intelligence feed (the available boxes are "create alert" and "log to syslog"), the boxes will remain checked for the user who checked them, but they will not appear checked for other users. This issue has been addressed. (CBUI-1437)
6. Fixed the Watchlist Email Me option as when changed by 1 user, it affected other users. (CBUI-1448)
7. When performing a process search by date, CB 5.0 will return search results for the prior day's data. The issue has been addressed. (CBUI-1402)
8. Address the issue where the server was reaching maximum number of DB connection in a clustered environments. (E-3835)
9. After an alert has been resolved from the alerts page's default query, and the page is reloaded the alert shows unresolved again. This issue has been fixed. (E-3838)
10. Server dashboard does not display on occasion due to a product issue. The displayed error was: "unable to add db connection back to pool". This issue has been fixed. (E-3852)
11. The cbcluster startup performance issue has been addressed for this release. This issue appears after upgrading to 5.0.0 Patch 2. (E-4002)
12. Server scripts are displaying the following error <gevent.dns.DNSError'>: [Errno 67] request timed out. (E-4190)
13. If an exception is thrown during a full feed sync via the command line, all work appears to stop. The issue has been fixed. (E-4200)
14. Observing constant stream of HTTP 500 errors in the NGINX. The issue has been addressed by the server having a background health check task that monitors activity and log any time there is a SQL transaction that runs for a long time. (E-4210)

15. The purge process is not processing all appropriate files, which causing excessive disk usage. This issue has been addressed. (E-4235)
16. Triage alert is getting triggered repeatedly for the same file from the same endpoint even after it was acknowledge. The issue has been addressed in this release. (E-4290)
17. CSV generation from the process analyze view results in empty filemods.csv and regmods.csv. This is even if the result on the console shows entries for filemods and regmods events. The issue has been addressed in this release. (E-4382)
18. SSO setting is not redirecting with the specified port. (E-4388)

Windows Sensor (5.1.0.150618.0432)

1. CB Live Response “kill” command now works correctly on Windows 8+ machines when attempting to kill a process not running in the same session as cb.exe (typically session 0). (WIN-304)
2. Upgrade failure messages are now correctly sent to the server when upgrades failed. (WIN-144)
3. Improved accuracy of binary storefile backlog reporting. (WIN-199)
4. Modload event collection now can be correctly disabled. (WIN-235)
5. Fixed an issue with false positive tamper events sent related to sensor’s own activity on startup and shutdown. (WIN-300)
6. Fixed a race condition where persisted events may have been lost if another application on the system happened to have the file open when the sensor tried to send the events. (WIN-297)
7. Fixed an issue with operation of CB Live Response that prevented it to start after clean install of sensor. (WIN-296)
8. Reduced the likelihood of CB sensor’s hashing and binary inspection to cause sharing violations with other applications’ binaries. (WIN-290)
9. Fixed an issue with sensor uninstaller not removing the “HKLM\software\wow6432node\carbonblack” registry key on 64-bit systems. (WIN-297)
10. Improved reporting of delayed writes that occurred after a process has exited. (WIN-279)
11. Fixed an issue on Windows 7+ machines that led to cb.exe to have high CPU utilization. (WIN-277)
12. Improved agents debouncing logic to avoid sending duplicate module info events to the server. (WIN-276)
13. Corrected reporting of cross-process events on Windows XP and 2003 systems when one process successfully performed a CreateRemoteThread operation. (WIN-274)

14. Fixed a small race condition on driver unload that could lead to memory leak or in rare cases a system crash. (WIN-265)
15. Fixed an issue with very long registry paths causing system to crash. (WIN-264)
16. Improved accuracy of byte counts of outstanding uploads that is reported to the server. (WIN-262)
17. Fixed an issue that causes events that were in queue to be lost when the sensor service was stopped. (WIN-259)
18. Fixed an issue that caused sensor to report multiple ntoskrnl.exe (SYSTEM) processes for the same boot session with slightly different process creation times. (WIN-250)
19. Fixed an issue that caused binary information of running processes to not be collected If binary info collection is disabled and then re-enabled. (WIN-248)

OS X Sensor (4.2.7.150624.0430)

1. A race condition in the daemon would occasionally cause it to crash. This has been corrected. (OSX-209).

Linux Sensor (4.2.7.150624.1613)

1. The Linux sensor now gracefully handles DNS timeouts. (LNX-98).
2. An issue was fixed involving RPM name collision of the Linux sensor installer package installed on the cb-enterprise server. (LNX-137).
3. Support for Redhat/Centos 7.1 has been added. (LNX-144).
4. The Linux sensor will now ignore its own operations. (LNX-152).
5. The subsystem start/shutdown sequence was adjusted to avoid a potential race.

Known Issues and Limitations

1. OS X and Linux sensors do not support excluding certain hashes from being banned via restrictions.conf. This feature is only supported for Windows platform.
2. Version 5.1.0 implementation of sensor purging has a known issue. If a sensor has been purged prior to its process data being purged, the Process Analysis page will return a 404 error for that sensors processes. All searching capabilities and process events are still present, searchable, and will be alerted. To reduce the chances of this scenario if you choose to enable DeleteInactiveSensors, we recommend setting your DeleteInactiveSensorsDays equal to or greater than your desired storage retention period. *This issue has been addressed in 5.1.1 Patch 1*

3. Negated terms in queries with boolean OR logic have some limitations (see section under upgrading the server). (CB-4068)
4. Right after installation or upgrade of the sensor Tamper events are not reported to the server. Restarting the cb service and driver seems to fix the issue. (CB-6857)
5. In order for sensor upgrades to work properly, McAfee EPO may need to be configured to exclude c:\windows\carbonblack\cb.exe from its "Prevent creation of new executable files in the Windows folder" option. (CB-7061)
6. On endpoints running the Windows 8.1 32-bit platform, banning may fail when processes are executed using gitbash (sh.exe). (CB-6975)
7. The power state of a Linux sensor is not displayed correctly on the Host Details page. When a Linux sensor is powered off, the icon next to the Computer Name does not change to the correct state. (CB-6671)
8. Some outbound UDP network connections are not reported on Linux platforms. (CB-6630)
9. ICMP traffic is allowed when sensor is isolated on Linux and OS X platforms. (CB-6483/CB-6623)
10. Non-binary file write event collection can not be disabled on Linux and OS X platforms. (CB-6686/CB-6491)
11. Some network connections events do not report Local IP and Local Port on Linux and OS X platform. (CB-6410/CB-6714)
12. On OS X platforms, the UI setting to turn all “event collections” off is not honored. (CB-6389)
13. Binary execution of a file can still be banned if the file reuses the same inode on Linux and OS X platforms. (CB-6647/CB-6402)
14. If a sensor’s system clock is wrong and in the future, the start time for processes from that sensor are not displayed correctly in the Carbon Black console. (CB-6257)
15. On the Carbon Black server, when a sensor is moved out of a group with a user on a team that has only "Viewer" access to that particular group, results for that group are still searchable for the time period it was in that group, but the process details page links get 405 errors. If the sensor is put back into the group, the 405 errors for those processes go away. (CB-3704)
16. The Reshard tool can fail with “File Not Found” exception, in turn causing a corrupt index. If a re-shard is necessary please contact support for a potential work around. (CB-3743)
17. The Linux sensor crashes sporadically sending Health to 75: Driver failure. The sensor checks into the server, but no new events are received. (CB-6700)

18. The Linux sensor sometimes misses or incorrectly reports events associated with a forked process. Reporting of forked POSIX processes will be improved in 5.2 release. (CB-6626/CB-6810)
19. The Linux sensor fails to properly cache observed events after the disk quota is reached and connection to the server is lost. (CB-6722)
20. The Linux sensor may fail to generate an MD5 and collect a binary image of file on a network share or user-space file system. (CB-6749)
21. CbEP enforcement fails after the Linux Sensor is uninstalled. A restart of CbEP is required to restore enforcement. (CB-7674)
22. The Linux sensor only reports the connection to a web proxy, but not the connection through the proxy. (CB-6669)

Contacting Carbon Black Support

For your convenience, Carbon Black Technical Support offers several channels for resolving support questions:

Technical Support Contact Options
Web: www.carbonblack.com
E-mail: support@carbonblack.com
Phone: 877.248.9098 (877.**BIT9**.098)
Fax: 617.393.7499
Hours: 8 a.m. to 8 p.m. EST

Reporting Problems

When you call or e-mail Carbon Black Technical Support, please provide the following information to the support representative:

Required Information	Description
Contact	Your name, company name, telephone number, and e-mail address
Product version	Product name (Carbon Black Enterprise Response server and sensor version)
Hardware configuration	Hardware configuration of the Carbon Black Enterprise Response server (processor, memory, and RAM)
Document version	For documentation issues, specify the version of the manual you are using. The date and version of the document appear after the copyright section of each manual.
Problem	Action causing the problem, error message returned, and event log output (as appropriate)
Problem severity	Critical, serious, minor, or enhancement