Our April 24, 2019 release of the PSC includes:

CB Defense

- Filter updates to improve performance
- Known issues

CB Defense changes are live in all production environments as of April 24, 2019.

CB LiveOps

- Recommended queries
- Delete a query
- Search query history and results
- Device view
- Osquery updates

Reference the URL that appears in your browser when logging into the CB Predictive Security Cloud console to determine when you can expect to see the CB LiveOps changes in your console.

Login URL	ETA
https://dashboard.confer.net/	Complete
https://defense.conferdeploy.net	Complete
https://defense-prod05.conferdeploy.net	April 25
https://defense-eu.conferdeploy.net	April 24
https://defense-prodnrt.conferdeploy.net/	April 24

Carbon Black.

CB Defense

Filter updates to improve performance

We've made a few updates to the filters on the **Investigate** page to improve page performance.

- Before devices populate in the **Devices** filter, you must now either enter a query in the search bar or select a time-frame that is less than or equal to one day.
- We are no longer saving **All Time** as a persistent choice for the time frame default as this caused performance impacts when searching for alerts. Previously, when you selected a search time frame on the **Investigate** page, the PSC maintained this setting and used that as the default time frame during subsequent sessions.
- When navigating to the **Investigate** page from elsewhere in the console (e.g., clicking on a device on the **Endpoints** page), your current time filter will be respected, rather than forcibly changing the time frame to **All Time**.
- The event timeline on the **Investigate** page's **Events** tab is now collapsed by default. Additionally, if you collapse the timeline visualisation, this setting persists and the timeline visualisation remains collapsed in future sessions. Similarly, if you expand the event timeline, this choice will persist across sessions.

Known issues

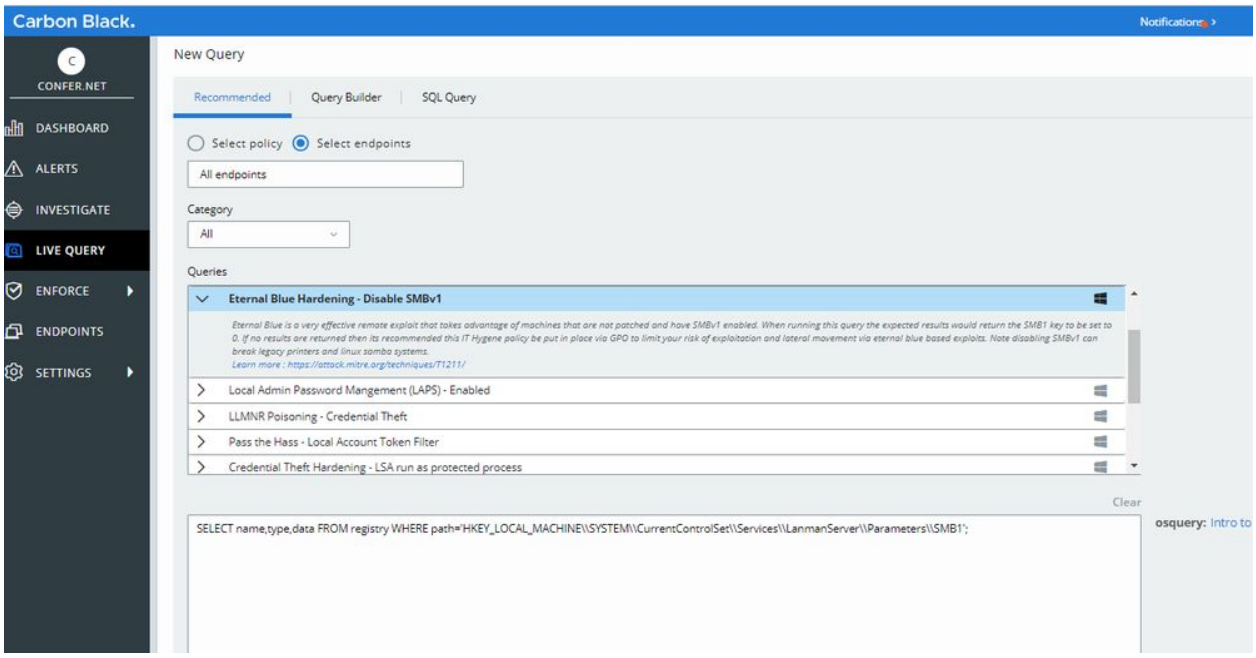
ID	Description
DSER-4390	Some sensors that should be **Eligible for Upgrade** are not marked as such.
DSER-5437	Additional markup is added to events forwarded via the event forwarder.
DSER-9664	Occasionally, clicking the link in an email alert notification results in a mis-rendered **Alert Triage** page.
DSER-9670	Searching for "Threat Category: Malware" on the **Alerts** page returns results that are non-malware.

DSER-10342 / DSEN-2894	Selecting **Take Action > Uninstall** from the **Endpoints** page fails to uninstall sensors in some cases. This leaves the sensor installed on an endpoint, but unable to communicate with the cloud.
DSER-10468	When **Sensor UI: Detail Message** is left blank on the **Policy** page, the sensor UI displays “false” in some situations. Adding a space to the **Sensor UI: Detail Message** resolves this issue.
DSER-10667	When an application's reputation is first determined to be NOT_LISTED and is then whitelisted, events shows WHITE_LISTED on the **Investigate** page. The application still shows as NOT_LISTED in the **Applications** tab.
DSER-10714	An incorrect API URL is listed on **Settings > Connectors > Download**. See this KB for the proper URLs: https://community.carbonblack.com/t5/Knowledge-Base/CB-Defense-What-URLs-are-used-to-access-the-API/ta-p/67346.
DSER-10961	Older macOS sensor versions allow deletion of sensor files from the backend. This can occur on macOS sensor versions 3.1 and below. This only occurs if an org admin manually triggers the deletion.
DSER-11370	If an alert dismissal reason is selected when dismissing an alert, the alert does not dismiss properly.
DSER-12676	A notification for an alert can be sent when dismissing an alert, causing duplicate notifications to appear.
DSER-12728	In rare situations, navigating to some pages in the UI causes the page to render as gray. Refresh the page to render the page as expected.
DSER-13914	Auto-delete of deregistered devices is not functioning properly. Manual deregistration is working as expected.
DSER-14906	When using the “all devices” export API, the results include devices that have been deleted.
DSER-15073	In some cases, resetting two factor for another admin causes the user performing the action’s two factor code to be reset.

CB LiveOps

Recommended queries

We've added a new feature to the **Live Query** page: **Recommended queries**.



To use this feature, go to the **Live Query** page. In the **New Query** section, the **Recommended** tab is now the default. This tab provides a catalog of pre-built, recommended queries for both Windows and macOS endpoints.

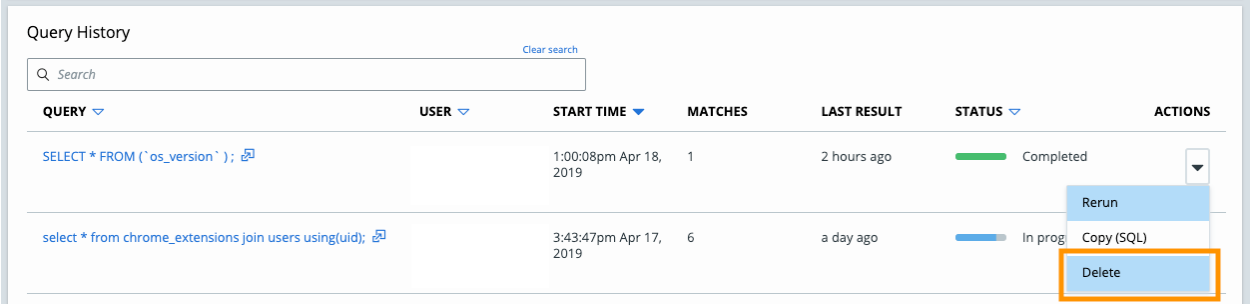
Select specific endpoints to be queried, or choose a policy to select the endpoints it contains. Scroll through the query options, or filter the recommended queries by category (Compliance, IT Hygiene, Vulnerability Management, Threat Hunting). When you select a recommended query, the text box auto-fills with the SQL command, allowing you to review and edit the query before running it against your endpoints.

These queries are created, categorized, and tested by the Carbon Black threat research team so that you can quickly run high-value queries. Each recommended query includes a short description that explains the value of the query, or what anticipated results will look like.

Delete a query

You can now delete query results. Eliminate clutter and reduce concerns about sensitive query results being available longer than they are needed.

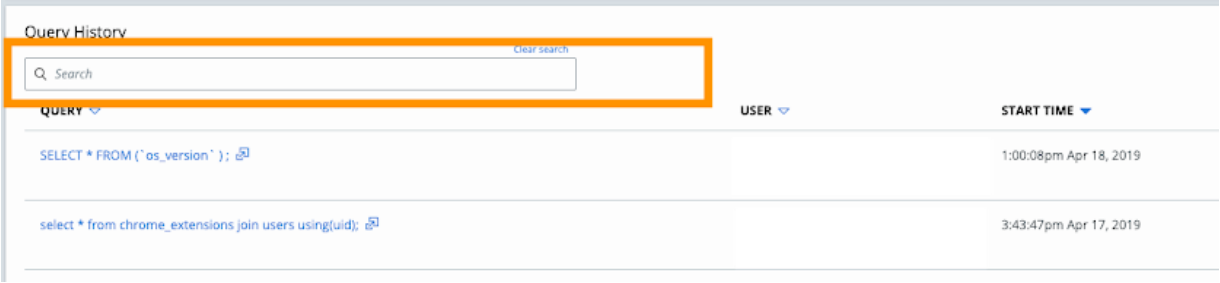
Go to the **Query History** table, find a query you no longer need, click the dropdown arrow under **Actions**, and click **Delete**.



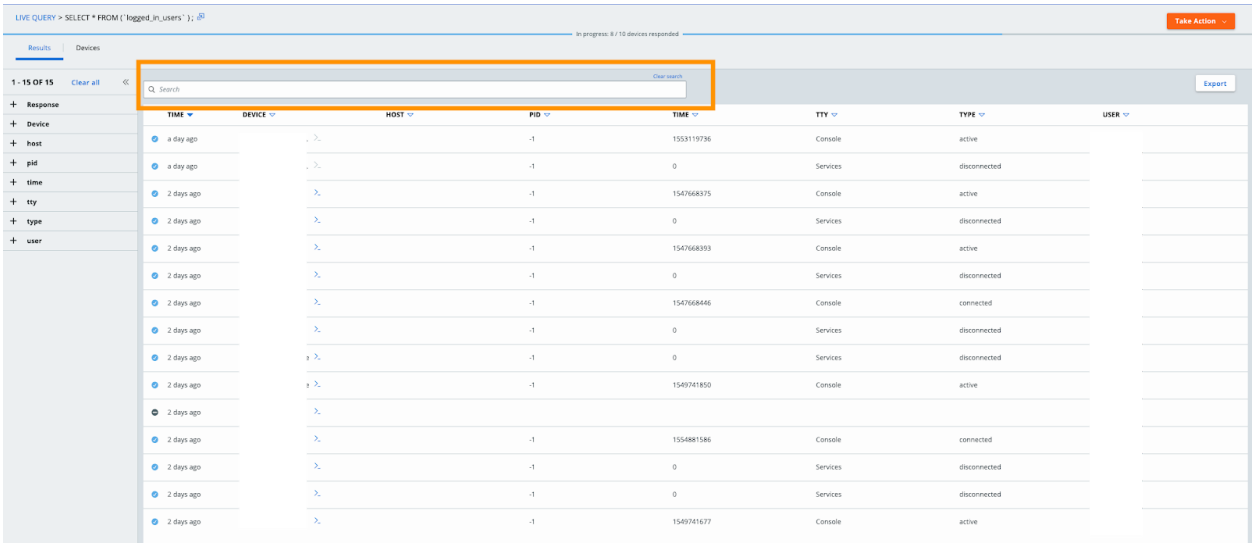
You can only delete queries that have completed or stopped via the Query Results page. Deleted queries cannot be restored.

Search Query History and results

We've added a search bar to the **Query History** table so you can easily find results from past queries.

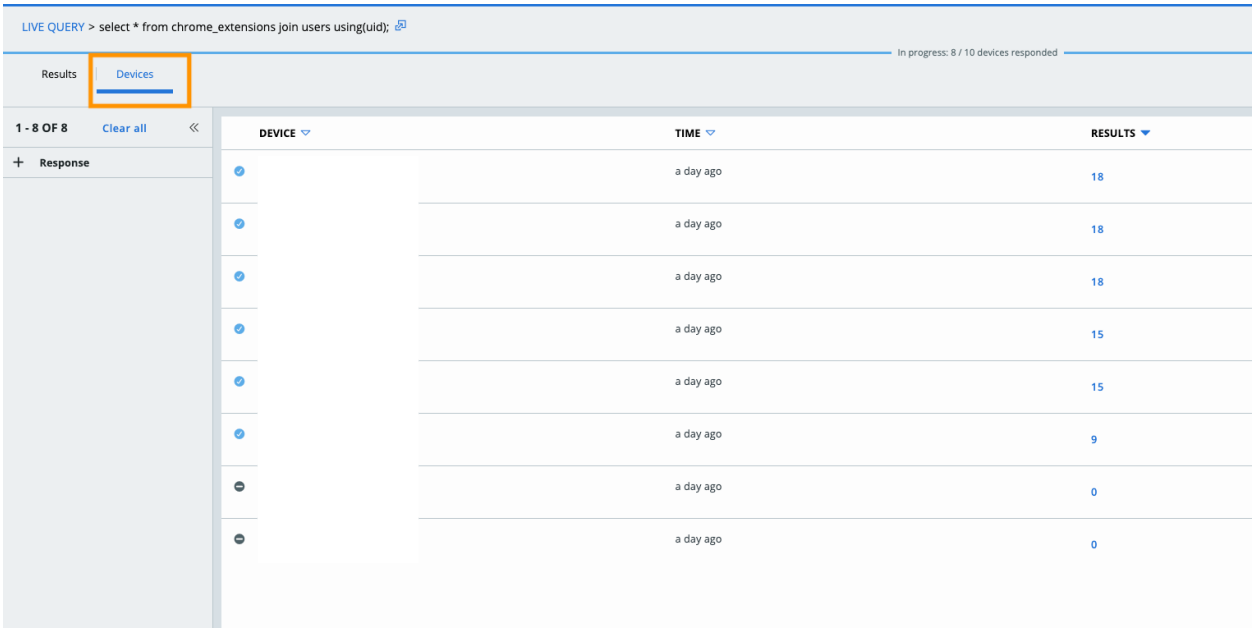


You can also click a specific query and search through the results of that query. Note that you must use a full text string to search on Live Query pages.



Device view

We've added an additional tab to the **Results** page called **Devices**. This view will make it easier to see the results of a query from a device-centric perspective which is particularly helpful for queries that return multiple results from each device that is being queried.



This new view provides information about the status of a query, including: which devices have already responded; which devices matched the query criteria; metrics on memory and CPU usage for each device; and the response time for each device.

For devices that have multiple results, you can click the number in the **Results** column to see details about all results that come from that specific endpoint. Pivot between the **Results** tab and the **Device** tab to find the specific details that are most important to you at any given time.

Osquery updates

The **chrome_extensions** table has been removed from the **Query Builder**. In order for the table to work properly, it must be JOINed with another table to target a specific user, something which is not currently supported by the **Query Builder** in the console. The table can still run using the **SQL Query** builder**.**

Additionally, there is a known osquery bug with the **chrome_extensions** table that results in inconsistent behavior when returning results. We have filed a bug ticket and are working with the community to get this resolved.