Carbon Black Cloud

Release Notes

Linux 2.5.0

Carbon Black Cloud Linux Sensor version 2.5.0 release supports **CB ThreatHunter Event Collection and Linux Group Support**. Click the following link to view the Supported Linux Distributions.

New features

This section lists features that are introduced in the Linux 2.5.0 sensor.

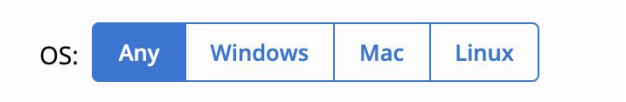
- Enhanced Investigations with CB ThreatHunter
- Linux Group Support

Enhanced Investigations with CB ThreatHunter

Carbon Black ThreatHunter is the next evolution of CB Response on the Carbon Black Cloud. It delivers comprehensive endpoint visibility and enhanced search capabilities. To enable a device to return CB ThreatHunter data, your organization must have CB ThreatHunter enabled and have a 2.5.0 Linux sensor on the endpoint. The 2.5.0 sensor supports CB ThreatHunter standalone, and any combination of CB LiveOps and CB ThreatHunter. To read more about CB ThreatHunter, see https://community.carbonblack.com/t5/Cb-ThreatHunter/ct-p/CbThreatHunter

Linux Group Support

You can now add Linux v2.5.0 sensors to sensor groups by device name and subnet. Use the **Any** operating system option as the Linux option is not currently functional.



Attended and Command Line Installation

For direct end user installs, an `install.sh` script is provided to input the company code. Command Line Installation is also supported via the use of the native RPM installer (assuming prerequisite steps are taken). See the PSC Sensor Installation Guide for instructions. Please note that `install.sh` should not be used to upgrade sensors.

Known differences between Linux and other operating systems

The **User** field on the **Endpoints** page is typically populated with the email address of the user who installed the sensor on the endpoint. We've intentionally left this field blank for Linux

sensors because there can be multiple logged-in users and multiple simultaneous desktop users.

Fixed in this Release

Issue ID	Description
PSCLNX-4547	Given a low bandwidth connection, an upload of information to the backend could fail. This is resolved in v2.5.0.

Known issues and Limitations

Issue ID	Description
PSCLNX-2710	The sensor does not support uninstall from the Carbon Black Cloud. To uninstall, issue the following commands: For CentOS, RHEL, SUSE or Amazon Linux: `rpm -e cb-psc-sensor` For Ubuntu: `dpkg --purge cb-psc-sensor` **Note**: The agent will still be listed in the **Registered Devices** list on the backend after running the command unless you choose **Take Action > Uninstall**
PSCLNX-455	The sensor only supports unauthenticated proxies.
PSCLNX-106	CB Live Response **Go Live** icon always shows for Linux sensors. A policy must be assigned to each sensor to use Live Response.
PSCLNX-4121 PSCLNX-4086 PSCLNX-4085	Incorrect local and remote addresses are sometimes reported for UDP netconn events. Outgoing TCP netconn events can be duplicated in the console.
PSCLNX-3874	When the agent restarts successfully Error[00000002 (00000002)] is reported.
PSCLNX-4464	Empty paths can be reported with events data.
N/A	Deploying the Carbon Black Cloud Linux sensor and the CB Response Linux sensor to the same endpoint is not recommended. There are no known interoperability issues when running both sensors; however, there will be higher performance utilization if both sensors are running on an endpoint.