Carbon Black.

Understanding Data Retention in Cb Response Cloud

Cb Response Cloud deployments assume a rate of 3,200 processes per day per endpoint. If your endpoints produce a higher amount of process executions, the amount of data retained can be affected.

To understand data retention for your organization, estimate the effective endpoint count based on your mix of operating systems.

Effective endpoint count calculates process executions per actual endpoint:

Actual endpoint count X normalization factor = effective endpoint count

The normalization factor assumes a certain level of activity, based on the average number of process executions observed per endpoint per day.

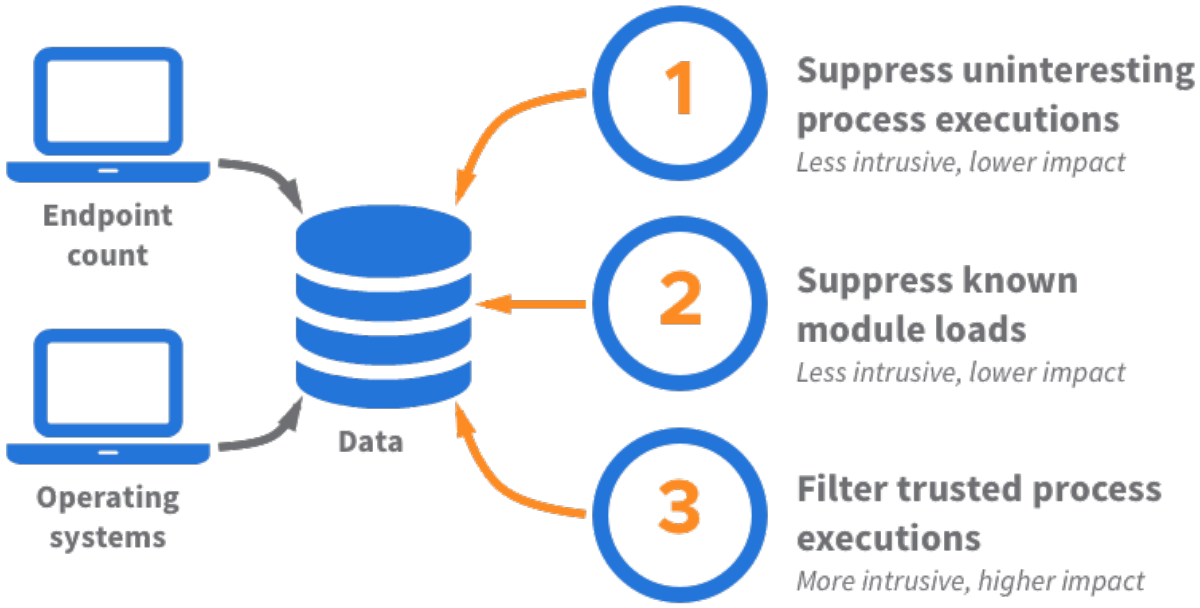
The biggest impact on the normalization factor is the operating system type.

OS	Processes per day per endpoint	Normalization factor
Windows	2,500	0.8
Mac OS X	15,000	4.7
Linux	25,000	7.8

Once you analyze your endpoint activity, there are three ways to manage your data retention in Cb Response Cloud. You can consider any or all of these choices, depending on the needs of your organization.

Key Points

+ Endpoint OS and activity affects data retention
+ Analyze your operating system mix
+ Calculate your effective endpoints
+ Choose options to manage retention for your organization



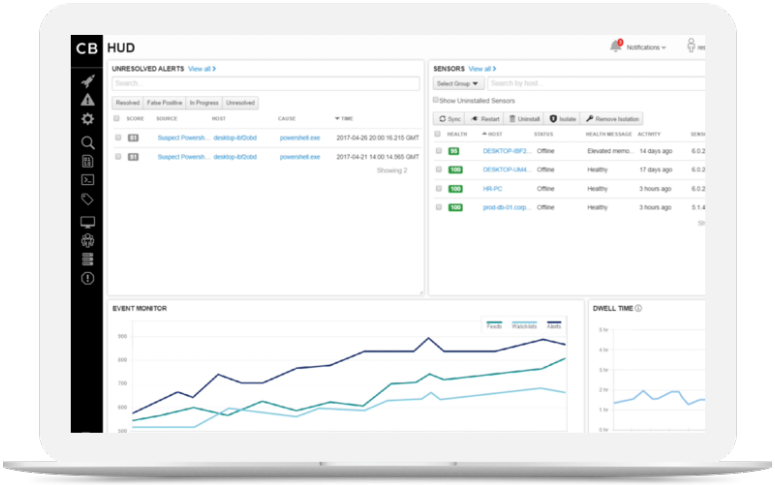
1

Suppress uninteresting process executions

You can change the suppression level in the advanced settings for sensor groups.

- **Medium**: Only performs module loads and no other events, typically a full enterprise deployment including a smaller number of MacOS and Linux endpoints.
- **High**: Module loads and any cross-process activity such as file modifications or network connections, and/or a higher number of MacOS and Linux endpoints.

☑ **Default**: Cb Response Cloud suppresses medium uninteresting process executions



2

Suppress known module loads

You can change the filtering of known modloads in the advanced settings for sensor groups.

Known modules, or modloads, are good shared libraries inherent to the respective operating system. Many processes load these known modules at each execution, increasing the total number of events reported by the endpoint.

☑ **Default**: Cb Response Cloud includes known module loads

3

Filter trusted process executions

Carbon Black Support can assist you with implementing ingress filters for your organization.

If your organization can select specific, trusted process executions, adding ingress filters reduces or eliminates that data. A process can be filtered by either an absolute path or by its MD5 cryptographic hash. In addition to ignoring a process itself, a filter can be configured to ignore a process's children, or the entire process tree.

This type of filtering is the best choice when a high amount of data is produced from a few processes that are common across many endpoints.

☑ **Default**: Cb Response Cloud includes all process executions

Carbon Black can help you make the best decisions for your organization

Carbon Black.

Carbon Black is a leading provider of next-generation endpoint security. Carbon Black serves more than 3,700 customers globally, including 30 of the Fortune 100. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV). Leveraging its newly introduced big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black solutions enable customers to defend against the most advanced cyber threats, including malware, ransomware, and non-malware attacks. Deployed via the cloud, on premise, or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus. For more information, please visit www.carbonblack.com or follow us on Twitter at @CarbonBlack_Inc. Carbon Black and Predictive Security Cloud are registered trademarks or trademarks of Carbon Black, Inc. in the United States and other jurisdictions.

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