Carbon Black.

Cb Defense Sensor 2.1 for Windows

Release Notes

June 30, 2017

Carbon Black, Inc.

1100 Winter Street, Waltham, MA 02451 USA

Tel: 617.393.7400 Fax: 617.393.7499

Email: support@carbonblack.com

General Notes

Cb Defense Sensor version 2.1 is a GA (General Availability) release for the Windows operating system only. These notes are *cumulative*, and provide information on all 2.1 releases to date.

New Features

This section lists features introduced in the 2.1 version of Cb Defense Sensor. (For a more thorough description of the new features in this release, see the User's Guide.)

Windows Security Center Integration

Windows Security Center (WSC) requires Windows devices to have an antivirus provider. Cb Defense is now a Microsoft-certified antivirus provider for WSC.

You will now be able integrate Cb Defense with WSC and designate Cb Defense as your antivirus provider on devices that are running Windows 10 or later. You must be using Cb Defense sensor version 2.1.0 or later. When it is enabled, Cb Defense is listed as the antivirus provider in the Security and Maintenance in Control Panel. This option will become available on policy page after July Update of the Cb Defense UI.

For new organizations, WSC integration is enabled by default via a policy group setting in the Standard policy group. You can disable WSC integration; doing so does not disable Cb Defense.

For existing organizations, WSC integration must be enabled through the Cb Defense UI following the July release.

See the User's Guide for details about configuration of these new features.

Enhanced Logging Through Diagnostic Collection on the Sensor

The Cb Defense 2.1.0 Sensor includes enhanced log gathering capabilities to collect additional sensor log files, OS-specific log files, and to obtain OS-specific information that is useful for diagnosing product issues. This newly collected information will greatly improve the ability of our support organization to triage and resolve customer issues.

Issues Resolved in Sensor version 2.1

ID	Description
DSEN-689/CIT-11070	Improved application startup delays.
DSEN-718 EA-8285	Improvements to policy for Windows core processes and expedited reputation queries.
DSEN-864 EA-8331 EA-8513	Fix to prevent applications from freezing while sensor is running.
CIT-10970 EA-7817	Improved script file detection fixes a problem where scripts were unable to run or the sensor misidentified the process being invoked.
CIT-11026	Improvement to support the Untrusted App rule for scripts (Windows).
CIT-10273 CIT-10234	The Sensor User Interface’s log file (RepUx.log) is in the *user’s* temp directory (%TEMP%) rather than the *system* temp directory. Similarly, user-interface “mini-dump” files are written to this same %TEMP% directory.
CIT-11035	Discontinued SHA-1 hashing algorithm as part of our code-signing process.
CIT-11057	Improved detection of Wordpad.exe (.rtf) files resolves issues with zero day detection of Wordpad vulnerabilities
CIT-9777 CIT-11054	Fixed a case in which if Windows Explorer (explorer.exe) was terminated and restarted, the Cb Defense Sensor icon in the Windows system tray would disappear.
CIT-11047 DSEN-302	Blocking events details on the Sensor UI did not have "App Reputation (policy)" - Windows.
CIT-11046 DSEN-738 EA-8064	Local UI says protection is disabled even though it is enabled, because RepUx.exe is being denied access when attempting to ascertain the sensor's protection status.
CIT-11069	Single Instance wildcards are now properly recognized by policy rules.

Known Issues and Caveats

The following section lists known issues in this version of Cb Defense Sensor.

ID	Description
EA-8575 CIT-10882	Duplicate BLOCK or TERMINATE notifications will not be sent to the Sensor UI for a period of 30 minutes.
CIT-11060	The Cb Defense sensor may prevent Windows Defender from removing malware. This is because the sensor is preventing access to the malware file.
EA-9013	Some clients have observed "repmgr" or "Cb Defense" related events getting blocked without bad reputation or related policy rules. These kind of blocking actions are caused by Cb Defense sensor's built-in tamper protection (also known as "self-protection"). In order to provide full protection to your systems, Cb Defense sensors block actions such as access, modify or delete to Cb Defense-related services and processes. Such blocking actions are enforced by design and will present in dashboard as a blocking event with policy action TTPs even though blocking was not actually triggered by a policy action, but by the sensor's self-protection.
EA-8538 EA-8811 EA-8606	The Cb Defense installer has failed in a few cases for clients attempting to upgrade from 2.0.3 to 2.0.4.