Carbon Black.

Cb

Cb Defense Sensor 3.0 for Windows

Release Notes

September 13th, 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 3.0 is a release for the Windows operating system only.

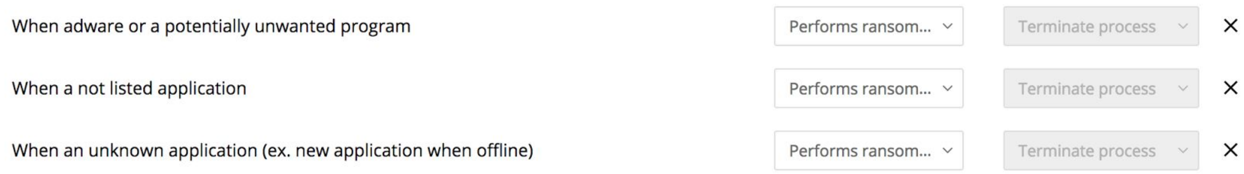
New Features

This section lists features introduced in the 3.0 version of Cb Defense Sensor. (For a more thorough description of the new features in this release, see the User's Guide.)

Ransomware Prevention Improvements

The 3.0 Cb Defense sensor introduces multiple enhancements that improve prevention efficacy against Ransomware TTPs. To take advantage of these enhancements, you can now set a policy rule to handle ransomware-like behavior. When a ransomware policy rule is applied on an endpoint, the sensor UI displays a message that notifies the user that potential ransomware was terminated.

New customers will receive updated policies out of the box enabling ransomware improvements. Current customers may add the following 3 rules to their policies to get started with ransomware defenses in the same way:



When adware or a potentially unwanted program	Performs ransom...	Terminate process	×
When a not listed application	Performs ransom...	Terminate process	×
When an unknown application (ex. new application when offline)	Performs ransom...	Terminate process	×

We encourage customers to start with these policies as they provide defense against a wide range of ransomware and have a low risk of false positives.

To read more about these improvements and how to implement ransomware policies, please see the User's Guide.

Live Response

This release introduces Live Response to Cb Defense. Live Response offers authorized administrators remote access to enabled endpoints. This allows them to inspect systems during investigations, eradicate threats, and return hosts to normal operations after an incident. A new administrative role, "Live Response Admin", and a new policy option, Enable Live Response, control access to the feature.

The Live Response Admin role supersedes the Admin role. This privilege can only be granted by another administrator who has Live Response Admin rights. For current

customers, all users that have Admin privilege at the time of release will be promoted to the Live Response Admin role. We encourage customers to audit their administrators prior to upgrading to the 3.0 sensors and demote any administrators who should not have Live Response access.

To help prevent abuse, Live Response includes a kill switch to disable remote access to any endpoint. After enabling the kill switch on a host, Live Response cannot access the host regardless of policy settings or the administrator's role. To re-enable Live Response for that endpoint, the Cb Defense sensor must be reinstalled on the endpoint.

You can monitor Live Response use through the Cb Defense Audit Log. Live Response-related messages include the token, "LiveResponse", making it easy to use the Audit Log's search function to show Live Response related messages only. By default, the Audit Log displays connection attempts and error messages. Turn Verbose logging ON to additionally display each command that is issued during Live Response sessions.

To read more about this feature and how to enable/disable this new role, please see the User's Guide.

Elongated Activation Code

To improve deployments and better enable scalability on the sensor, this release increases the length of the activation code. Users must update any software deployment tools or any existing installation scripts (such as those used to deploy sensors via tools like SCCM or GPO) that utilize the previous 8 digit codes.

Issues Resolved in 3.0

ID	Description
EA-9507	Resolved an issue where Lync/Skype for Business was being terminated, even when whitelisted.
DSEN-945	Fixed issues with Microsoft Office on Whitelist by configuring string match rules for each office app (Winword, Powerpoint, Excel, etc.) and for each operation type (execute from memory, network, etc.).
EA-9231	Resolved an issue where Outlook was being blocked even though it was whitelisted.
EA-9608	Resolved an issue with Outlook plugin iManage that could potentially cause a Blue Screen.

Known Issues and Caveats

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

ID	Description
N/A	Upgrade issues have been observed when upgrading from sensor 2.0.3 to any newer version. Please contact Carbon Black Support if you encounter an issue upgrading from an earlier sensor version.
EA-8575 CIT-10882	Duplicate BLOCK or TERMINATE notifications are not sent to the Sensor UI for a period of 30 minutes.
CIT-11060	The Cb Defense sensor can 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"). To provide full protection to your systems, Cb Defense sensors block actions such as access to, modify, or delete Cb Defense-related services and processes. Such blocking actions are enforced by design and present in dashboard as a blocking event with policy action TTPs, even though blocking was not actually triggered by a policy action.
DSEN-1180	When using Live Response, users can kill the PID for repmgr32, and the Live Response UI session ends; however, the sensor does not recover until after a reboot.
DSEN-1293	When trying to delete a registry key (that contains subkeys) using Live Response, keys will not be deleted; however, no error message displays.