PSC sensor version 3.4.0.1016 is for Windows only

Notes:

- The 3.4 MSI is signed with a SHA256 signature. Windows 7 predates the SHA256 algorithm and support for SHA256 was provided as part of a Windows 7 patch. If there are Windows 7 machines or Windows Server 2008 R2 machines that do not have this patch, it can be found here: https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2015/3033929. Machines running later operating systems have out of the box support.

- Windows 7 will require SHA256 signing as of July 2019. See https://support.microsoft.com/en-us/help/4474419/sha-2-code-signing-support-update.

- Customers who are upgrading to the 3.4.0.1016 from previous 3.4 sensor versions must ensure that the policy setting **Deny/Terminate Unknown application or process that Runs or is running Deny** should be disabled or not in place. Please see the Knowledge base article: https://community.carbonblack.com/t5/Knowledge-Base/CB-Defense-Sensor-Upgrade-from-3-4-x-x-fails/ta-p/73366. Note that this issue was observed internally, and only fails intermittently. However, Carbon Black recommends that you disable this policy setting to ensure successful upgrades.

New features

Enhanced investigations with CB ThreatHunter

CB ThreatHunter is the next evolution of CB Response on the Predictive Security Cloud, delivering unfiltered endpoint visibility and enhanced search to our cloud platform. To enable a device to return CB ThreatHunter data, your organization must have purchased CB ThreatHunter and must have a 3.4 sensor on the endpoint. The 3.4 sensor supports CB ThreatHunter standalone, as well as any combination of CB Defense, CB LiveOps, and CB ThreatHunter. To read more about CB ThreatHunter, see https://community.carbonblack.com/t5/Cb-ThreatHunter/ct-p/CbThreatHunter

19H1 Compatibility: sensor compatibility with upcoming Microsoft OS update

The 3.4 sensor is compatible with current requirements of the upcoming release of Microsoft's OS update, 19H1. The required features included in the 3.4 sensor are an

Early Launch Anti-Malware (ELAM) driver and running RepMgr.exe as an Anti-Malware Protected Process (AM-PPL). These items fulfill the current compatibility requirements for Carbon Black on the 19H1 OS Update. We recommend that customers upgrade to the 3.4 sensor to prepare for the OS Update. Please also note that it is recommended that the sensor is put in bypass for the OS update due to DSEN-5493 and DSEN-5491.

Reregister device via RepCLI

The `reregister` command is a repCLI command that lets you explicitly mark a machine as a master image just prior to snapshotting, so that upon reboot it is treated as a clone. The command requires authorization: see the following link for the Windows Sensor 3.3 release notes for authenticating users to use the command: https://community.carbonblack.com/t5/Documentation-Downloads/CbDefense-Windows-Sensor-3-3-Release-Notes-November-Update/ta-p/43343

The recommended approach to create a template by using reregister is:

1. Install the OS and any desired applications.
2. Install the CB Defense sensor and wait for background scan to complete and policies to be applied.
3. When you are ready to create your image, run `c:\program files\confer\repcli.exe reregister onrestart`.
4. Shut down the machine.
5. Create your image/VM template.

When the image (either a clone or the original master template) is restarted, the machine re-registers with the backend as a new device.

To make a new template, repeat steps 3-5. To create a live VM snapshot without restarting the machine, issue the `repcli reregister now` command to create a new device post restore as part of the snapshot process.

You can also use the reregister command to update the registered user that is displayed in the console. If you run `repcli.exe reregister now` while online, the sensor will update the backend with the currently logged-in user.

The previous VDI config option still exists and behaves exactly as it did before.

Obfuscation of command line inputs

Endpoint users might input sensitive data into the command line. The obfuscation of command line inputs protects against unauthorized users accessing the data in plain text in the sensor `.log` files and the sensor databases. There are three methods of obfuscating command line inputs:

- Unattended install command line - `HIDE_COMMAND_LINES=1`
- Through RepCLI - `hideCmdLines [0|1]`

- Manually set `HideCommandLines=true` in `cfg.ini`

The setting enables the obfuscation of command line input in sensor `.log` files and databases. The data in the PSC console is not obfuscated.

Performance Improvements

The 3.4 sensor introduces new optimizations that are associated with sensor behavior on files. These optimizations offer the most savings on scenarios where many files are dropped, such as executing an installer. The optimizations include:

1. A reduction in the amount of time the kernel will stall an application waiting for file signature information to be gathered.
2. For customers using CB ThreatHunter only on the PSC, the sensor will no longer stall applications waiting for defense policy to be calculated.
3. An improvement to how the sensor caches network names. The optimization is most strongly associated with cost of open, read, and close operations on files on a network share.

Internal testing showed 30% less performance overhead for CB ThreatHunter customers. Keep in mind that environments vary widely. Optimizations most significantly impact environments that involve many filedrops.

Fixed in this release

Efficacy enhancements and bug fixes

Issue ID	Description
DSEN-3703	This fix resolves an issue where the sensor connected with backend `auth.eu1.apc.avira.com`. This fix closes that connection and makes sure that the sensor only connects with the PSC backend. Please note that endpoints may be experiencing issues connecting to the cloud as noted in DSEN-4873.
DSEN-3014	This fix resolves an issue where the sensor issued an error if trailing or leading whitespace in the registration code input forced an error. The whitespace is now stripped.
DSEN-2107, EA-12455	This fix resolves an issue where the sensor could not update signature packs if an HTTPS URL was provided in the update settings.

DSEN-4121	This fix resolves an issue where forced restarts were always triggered upon reaching a consumption for CPU and memory. The fix enables a customizable threshold for alarming/restarts.
DSEN-4088	Occasionally, the sensor incorrectly identified some files as pre-existing that applied the local_white reputation. With this fix, the sensor better identifies files as pre-existing and therefore applies the correct reputation. This issue was not reported in the field and was found internally.
EA-13152, EA-13334, DSEN-4053	This resolves an issue where the sensor caused applications, such as `ServerManager.exe`, to crash. A workaround was to create an API bypass rule for the application. The API bypass is no longer needed and the user can remove the policy configuration from the prevention policy configurations page.
DSEN-4004	This fix resolves an issue where the service pack version was not reported and surfaced in the UI for endpoints running Windows 7 and Windows Server 2008 R2.
DSEN-3904, EA-12513	This fix resolves an issue where the sensor treated paths identified as glob patterns in the prevention policy configurations page. The sensor appended * to any path that was identified as a glob pattern if it did not already end with *. For example, `**/windows` was translated as `**/windows*`, which would match all filenames starting with windows. The policy configurations are now treated correctly. **Warning**: If you had any policy configurations relying on this behavior, you might need to update them to add the trailing *.
DSEN-3854	This fix resolves an issue in the 3.2.x-3.3.x sensors. Previously, if Windows Security Center integration was enabled in the policy, and a 3.2.x-3.3.x sensor is installed on a Windows Server OS (which does not have Security Center), protection could not be enabled within 1 minute of restarting the CB Defense service.
DSEN-3848	This fix resolves an issue where the attended installer incorrectly issued an error. Previously, if a user were to input an incorrect registration code during an attended install, the user might not have been notified of a failure. The installer UI message in the bottom left corner read "Please wait while CB Defense communicates with the cloud". The UI would have remained responsive and the user could input the correct code and proceed with installation.
DSEN-2877	This fix resolves an issue forcing some sensors into an infinite loop upon system crash. Previously, repmgr consumed nearly 100% of the CPU and disk, and an uninstall/reinstall was required to resolve this issue.

DSEN-2484, DSEN-3047	In Windows 3.3 sensors, when uninstalling the CB Defense sensor, a warning dialog box appeared with the following message: **Warning 1910. Could not remove Shortcut Cb Defense.lnk.** This issue is resolved in 3.4, and the shortcut is automatically removed.
DSEN-3088	This issue fixes an endpoint auto-assignment issue. Previously, when the sensor was removed from an AD domain, the sensor was still reflected as being within that domain on the **Endpoints** page and remained in a sensor group. You no longer have to take the sensor out of auto-assignment to make policy updates to that sensor and endpoint.
DSEN-3716	`RepCli.exe` status command now shows the correct state of slow (standard) or fast (expedited) scan.
UAV-636	This issue caused the sensor to potentially experience a reference counting issue that resulted in a system crash. It has been fixed.
DSEN-2107	This fix enables `RepMgr.exe` to check https certificates for Avira signature pack updates.
DSEN-3610	This fix resolves the issue where `uninstall.exe` could exit almost immediately with error code -1073741510 (0xC000013A) on x86 versions of Windows, but eventually would complete. Previously, it might have appeared that the uninstall failed due to the error code.
DSEN-4265, DSEN-4295	In previous 3.4 releases, the sensor uninstall could hang and can fail after 30 minutes. The sensor uninstall was also observed to fail immediately in some cases. This fix resolves these issues.
DSEN-4424	This fix resolves the issue where the sensor might delete files that are scanned using the local scanner.
DSEN-4520	This fix resolves the issue where files can occasionally not be deleted by taking action through the backend when the endpoint is behind a proxy. Live Query results for endpoints behind a proxy might not populate in the cloud console.
UAV-707, EA-13692	This fix resolves an issue where the sensor repeatedly crashes upon installation due to older CPUs or incompletely virtualized CPUs.
UAV-657	This fix resolves an issue where events were returned with SHA256 hash and not the MD5 hash.
DSEN-2698, EA-12155, EA-13392	This fix resolves an issue where RepMgr experienced a memory leak.

DSEN-4425, DSEN-4501, EA-13578	This fix resolves an issue where customers who had CB ThreatHunter enabled occasionally experienced the inability to open PDF files.
DSEN-4566	This fix resolves an issue with IT Tools where whitelisting DOS paths beginning with the drive letter such as "`c:\users\cb\desktop\cmd2.exe`" or "`c:\users\cb\desktop`" occasionally failed. Wildcard paths "`**\users\cb\desktop\`" function as intended.
DSEN-4366	This fix resolves an issue where the sensor failed to automatically start on machines with 19H1 environments where the Windows Sandbox feature was installed. See https://docs.microsoft.com/en-us/windows-insider/at-home/whats-new-wip-at-home-19h1
DSEN-4614	This fix resolves an issue where process creations blocked via policy did not generate events.
DSEN-2733, DSEN-3818, DSEN-3137	This fix improves general performance including file write, file rename, and file copy. Customers might have previously experienced a slowdown during these operations.
DSEN-3905	Previously, users might have seen failed deletions for files that were queued up for auto-delete. This fix resolves that issue and all files in an auto-delete queue are deleted.
DSEN-4810	This fix resolves the issue where the sensor might not have reported certain events associated with long commands in PowerShell.
DSEN-4826	This fix resolves the issue where the sensor might not report certain events greater than 4096 bytes.
DSEN-4827, DSEN-4828	This fix resolves the issue where the sensor might not report events that are associated with short-lived processes or fileless scripts.
DSEN-4728, EA-13874	CB ThreatHunter customers might have previously experienced increased resource consumption associated with checking signature information on files before they are deleted. This fix resolves that issue.
DEN-3712, EA-13200, EA-13635	This fix resolves the issue where applications running from a network location took several minutes to open. The applications opened in seconds with the sensor in bypass. The applications should now open in a similar timeframe.

UAV-841, UAV-845	This fix resolves crashes reported by customers.The crashes occurred when two driver products simultaneously queried for the same information. The crash was not reproduced consistently.
DSEN-5002	Previously, if a proxy configuration was required to reach the cloud, endpoints might not have been able to connect to the back end. This is due to the libcurl library using WinHTTP rather than OpenSSL. This fix provides a command line install option which resolves the issue. The command line install can only be implemented during a fresh install, so an uninstall is required if there already endpoints running the sensor.
DSEN-5151	This fix resolves an issue that prevented the reverse_shell TTP from appearing in the cloud UI. The fix also resolves an issue that prevented the sensor from reporting on any console-specific API calls such as `cmd.exe` performing a ReadConsole operation.
DSEN-4728, EA-13874	CB ThreatHunter customers might experience increased resource consumption that is associated with checking signature information on files before they are deleted. This can cause latency on the endpoint.
DSEN-3739, EA-14137	Previously, users might have seen terminations on executions of `svchost.exe`, despite there being no additional TTPs and no matching policy configurations to explain the block due to mismatched PIDs. The issue is fixed by DSEN-3739, which improves the handling of PID information and mitigates PID mismatch issues.
EA-14015, DSEN-5052	This fix resolves a breakage in unquarantine functionality. Previously, customers who put their sensor into quarantine might not be able to take them out of quarantine through the PSC console. If the CRL cache in Windows expires, and the device is in quarantine, the CRL check fails, causing backend communication to drop. A sensor uninstall and reinstall was required. This issue impacts the 3.3 sensor and 3.4 versions before 3.4.0.1008.
DSEN-5234, DSEN-5249	Previously, re-enabling the sensor after disabling the sensor via RepCLI `stopcbservices` might have caused the system to hang. This fix resolves this issue.
DSEN-5295	When using Live Response to make edits to the registry (specifically adds and deletes), the edits were previously applied only to the HKLM hive rather than to the specified hive. This fix enables the edits to be made to the specified hive.
DSEN-5272, EA-14241	This fix resolves an issue where one customer observed a crash in the field. The crash was attributed to a race condition with other driver software but had been observed infrequently.

DSEN-5183	This fix resolves an internally found issue in which upgrades from the same minor version (3.4.x) to a later build of that minor version (3.4.x) failed.
DSEN-5309, EA-14195	One customer reported high CPU usage during deployment that was associated with the sensor tracking many short-lived processes. This fix resolves this issue.
DSEN-14291, DSEN-5269	This fix resolves performance issues that one customer reported that were associated with SharePoint. Operations were taking around 20 seconds and should now execute normally.
DSEN-5144	This fix resolves an internally-found issue where the sensor install occasionally failed. The scope of the issue was infrequent, and was observed internally only on 32-bit machines.
DSEN-3866	Previously, Windows Server 2019 devices were shown in the backend UI as Windows Server 2016 devices. There was no compatibility issue; the impact was merely cosmetic. This issue is now resolved.
DSEN-5267, EA-14291, EA-14328	This fix resolves customer-reported performance issues that are associated with Sharepoint and Skype for Business.

Known issues

Issue ID	Description
DSEN-1987	False positive alert when the [application name] attempts to access the raw disk on the file.See https://community.carbonblack.com/docs/DOC-10730.
DSEN-1180, DSEN-3065	When using Live Response, users can terminate the PSC sensor if they terminate `RepMgr.exe`. Terminating this process means that the sensor cannot connect to the back end and the Live Response session ends. The sensor does not recover until after a reboot. Users can also delete certain files within the confer directory. Users are advised to use caution during Live Response sessions.
DSEN-2378	During an attended install, Windows installer shows a blank error dialogue when attempting to install on an unsupported OS.
DSEN-1387	Background Scan remains disabled on devices where VDI=1 was used. See https://community.carbonblack.com/docs/DOC-12001. This issue will be

	resolved in the 3.5 release.
DSEN-3061	Sensor does not whitelist files by certificate if it is signed with multi-byte characters.
DSEN-4216	The 3.4 sensor accumulates deleted files within the sensor cache and does not remove them when the files are removed from disk. This can lead to the sensor reporting that malware is still on disk when it has been removed.
DSEN-4050	If a user executes an unattended install with the flag and argument "`INSTALLFOLDER=<path>`", the sensor will install and be non-functional. Carbon Black does not support non-default install paths.
DSEN-4043	Under high load, the sensor might experience an issue where `repmgr.exe's` handle counts grow very large; this can cause minor performance issues.
DSEN-4143	Users might experience blocks of Microsoft OS upgrades. An admin can workaround this issue by either placing the sensor in bypass or adding the following paths to bypass: 1. `**\windows\servicing\**` 2. `**\$windows.~b\**` Make sure that the policy configuration: "When an unknown application tries to run - deny/terminate" is disabled when you upgrade.
DSEN-3992	Subkeys can be created under the CBDefense key in the Windows registry. This issue will be resolved in 3.5.
DSEN-4054, DSEN-4033	The LiveResponse memdump command can cause crashes. It is disabled by default on Windows sensor 3.3 and above. Instructions on enabling the command can be provided by your support representative. This issue will be fixed in the 3.5 sensor.
DSEN-4375	The sensor has been observed to write 290MB of data to `confer.log` over the course of nine hours. `Confer.log` is expected to be much smaller. This issue will be resolved in the 3.5 sensor release.
DSEN-4591, EA-13682	Arcmap files are corrupted or missing in certain environments.
DSEN-4581, DSEN-4694	You might see a terminate action applied to `wmiprvse.exe`, and an alert in the PSC console during machine start-up. At the time, `wmiprvse` has an unknown reputation and is scraping `lsass.exe`. This commonly happens during Windows updates. `Wmiprvse.exe` should be able to execute after the reputation resolves, and the update should go through.

DSEN-4756, DSER-14090, EA-13906	Customers running CB ThreatHunter as a standalone implementation without CB Defense or CB LiveOps might see Windows Security Center Real Time protection feature disabled. This issue can be resolved by navigating to the **Policies** page, clicking the **Sensor** tab, and unchecking **Use Windows Security Center**.
DSEN-5377	An attended upgrade while the sensor is in Bypass mode and the upgrade is run using a non-Admin CMD prompt can result in an incomplete uninstall during the upgrade process. This can leave the system in a state in which the sensor cannot be re-installed. You might need to use the sensor removal tool prior to a reinstall. This issue will be resolved in the upcoming maintenance release for 3.4.
DSEN-5371	A command line upgrade while the sensor is in Bypass can cause resources to hang on the endpoint after the sensor is taken out of Bypass. This issue can also manifest if the endpoint is taken out of Bypass using the sensor UI on the endpoint. A reboot is required to resolve this. This issue will be resolved in the upcoming maintenance release for 3.4.
DSEN-5480	The team internally observed an issue that results in a failure of the API Bypass feature under the following two joint conditions: 1. Prevention policy to deny running from the path `c:\test\*` 2. A Bypass rule is applied when `c:\test\calc.exe` performs any operation. You can work around this issue by applying Bypass to `c:\test\calc.exe` when it “runs or is running”. This issue will be resolved in the upcoming maintenance release for 3.4.
DSEN-5493, DSEN-5491	During updates to Windows 1H19, the system either blocks the update or potentially crashes during the update. This issue was found internally, and the issue does not reproduce if the sensor is in Bypass mode.
DSEN-5500	Some customers have reported an issue regarding endpoints running on Windows OS Update 19H1 (v1903). Customers can experience a black screen during a login or reboot. Do not upgrade to the 19H1 operating system in the meantime. This issue impacts both 3.3 and 3.4 sensors, and will be resolved in the upcoming maintenance release for 3.4.
DSEN-4924 EA-13414	Some customers have reported interoperability issues with Skype on Windows 7. Other operating systems are unaffected.
EA-14455, DSEN-5699	The install of the sensor has been observed to fail on Windows Server 2019. The issue is observed to fail in the case where there is a missing directory

	value for registry key HKLM\SYSTEM\CurrentControlSet\Control\EarlyLaunch value "BackupPath". The value is typically C:\Windows\ELAMBKUP.
DSEN-5377	Local command line upgrades were observed to fail when run from a non-admin command line.
DSEN-5493, DSEN-5491	During updates to Windows 1H19, the system either blocks the update or potentially crashes during the update. This issue was found internally, and the issue does not reproduce if the sensor is in Bypass mode.
DSEN-4924 EA-13414	Some customers have reported interoperability issues with Skype on Windows 7. Other operating systems are unaffected.
EA-14455, DSEN-5699	The install of the sensor has been observed to fail on Windows Server 2019. in the case where there is a missing directory value for registry key HKLM\SYSTEM\CurrentControlSet\Control\EarlyLaunch value "BackupPath". The value is typically C:\Windows\ELAMBKUP.
DSEN-5105, EA-14012	There have been a few observations of CPU spikes on customer endpoints. These CPU spikes occur when the certificate whitelist is updated. The issue has been infrequent. This fix is targeting the 3.5 sensor release.
DSEN-5626	The sensor no longer prevents copy operations on Known Malware or Blacklisted files that have been quarantined. This fix is targeting the 3.5 sensor release.
DSEN-5995, EA-14707, EA-14723, EA-14729	Customers upgrading from 3.4.0.1016 to 3.4.0.1047 may see that Office applications such as Word and Excel will hang when updating a file on Google File Stream and similar products (Box, Citrix Cloud).
DSEN-5934, EA-14272, EA-14956	Customers may have experienced the inability to open attachments while using applications such as KnowBe4 Second Chance or Digital Guardian's Outlook plug-in.
DSEN-5801, EA-14475	There has been one observed case of CPU increase related to running explorer.exe on a virtual server.
UAV-1160, EA-14700	A small percentage of watchlist hits have been reported as false positives. One customer has reported this issue thus far. This will be fixed in an upcoming maintenance release of 3.4.
DSEN-6322, EA-14880	There have been intermittent reports of short delays when opening various Office files and navigating file systems on Windows 10.

DSEN-6372	If the sensor's background scan goes from **disabled** (either via install args or via cloud policy) directly to **expedited**, it's possible to hit a race condition which puts the background scan to disabled state. This has only been identified internally and has not been observed externally.
DSEN-5163	The sensor does not prohibit downgrades from existing 3.4 versions to older 3.4 versions. The team does not recommend a downgrade between 3.4 builds as it leaves the sensor in a bad state.