ASSURANCE CONTINUITY MAINTENANCE REPORT FOR
VMware Carbon Black App Control v8.10.2

Maintenance Update of VMware Carbon Black App Control v8.8.2

Maintenance Report Number: CCEVS-VR-VID11158-2024

Date of Activity: March 1, 2024

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008.
- VMware Carbon Black App Control v8.10.2 Impact Analysis Report v1.0, February 28,2024[IAR].
- Standard Protection Profile for Enterprise Security Management-Access Control, version 2.1 [AC PP]
- Standard Protection Profile for Enterprise Security Management-Policy Management, version 2.1 [PM PP]

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: VMware Carbon Black App Control v8.8.2 Common Criteria Security Target, Version 1.0, February 27,2022	**Maintained Security Target:** VMware Carbon Black App Control v8.10.2 Common Criteria Security Target version 1.1, Jan 31, 2024 Changes in the maintained ST are: • Identification of the Changed TOE version, and individual component versions • Vendor's name • Security Target dates and versioning • Update of supported SQL Server versions

	• References to Changed TOE guidance documentation • The Technical Decision table • Changes to the functionality that is outside the scope of this evaluation documented in section 2.3.3 of the ST
Common Criteria Guidance Documentation • VMware Carbon Black App Control v8.8.2 Supplemental Administrative Guidance v1.0, dated February 27, 2022 • Server Installation Guide VMware Carbon Black App Control 8.8, dated 8 December 2021 • Operating Environment Requirements VMware Carbon Black App Control 8.8, dated 8 December 2021 • SQL Server Configuration Guide VMware Carbon Black App Control 8.8, dated 8 December 2021 • VMware Carbon Black App Control User Guide Product Version 8.8, Document Version 1.0, dated 6 December 2021	**Maintained Common Criteria Guidance documentation:** • VMware Carbon Black App Control v8.10.2 Supplemental Administrative Guidance v1.1 dated January 31, 2024 • Release Notes – The release notes for each patch between the Validated TOE (version [8.8.2]) and the Changed TOE (version [8.10.2]). • Server Installation Guide VMware Carbon Black App Control 8.10, dated 31 August 2023 • Operating Environment Requirements VMware Carbon Black App Control 8.10.2, dated 31 January 2024 • SQL Server Configuration Guide VMware Carbon Black App Control 8.10.2, dated 31 January 2024 • VMware Carbon Black App Control User Guide Product Version 8.8, Document Version 1.0, dated 31 January 2024

	• VMware Carbon Black App Control Agent Installation Guide dated 25 August 2023 Changes in the maintained Guidance are: • Updated identification of Guidance • Updated identification of References • Updated identification of TOE version • Update of supported SQL Server versions • References to Changed TOE guidance documentation, to include the addition of the Agent Installation Guide which contains information previously contained in the User Guide • All the changes documented in this report corresponding to the updates to the TOE.

Assurance Continuity Maintenance Report:

VMware, submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on February 1,2024. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0. In accordance with those requirements, the IAR describes the changes made to the maintained TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence consists of the Security Target, the CC Configuration Guide, guidance documentation and the Impact Analysis Report (IAR) . The ST and guidance documentation were

updated, the IAR documented the changes from the previously maintained version of the TOE (Version 8.8.2) to the updated TOE(Version 8.10.2).

Changes to TOE:

For this Assurance Continuity, the version number of TOE changed from Version 8.8.2 to Version 8.10.2.

The Changed TOE is VMware Carbon Black App Control v8.10.2 which incorporates several new features and bug fixes into the product. As was the case with the Validated TOE, the Change TOE contains multiple components each having its own software version and the version of the main TOE component (i.e., App Control Server) has been used to identify the overall TOE version. The Changed TOE component versions are:

- The App Control Server and App Control Console are software version 8.10.2.
- The App Control Agent for Windows operating systems is software version 8.9.2.
- The App Control Agent for Linux operating systems is software version 8.7.20.

Software Enhancements

The developer reported the new features/changes to the product located in the table below:

New Feature	Description and Effect	Overall Impact
Content-based Inspection	App Control now supports Content-based Inspection. Content-based Inspection enables administrators to leverage the power of the open source Yara engine to create their own Yara rules to provide more granular control over their security policy. In the 8.9 console, users will see a new tab within Software Rules called Yara. On this tab are existing internal App Control Yara rules and an "Add Yara Rule" button to create rules to use in conjunction with Custom rules. Yara software and Yara rules were in the evaluated product. The product has been updated to allow administrators to make new Yara based rules. This new functionality does not change the rules that were previously evaluated nor the management of those rules. Thus, this change has no impact on the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests.	No Impact

	Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
IPv6-only Support	With the release of the 8.8 Windows agent and the 8.9 Server, customers who want to deploy App Control in an IPv6-only network can now do so. This update makes the product deployable in an IPv6 network. The evaluated product was assessed in an IPv4 network. Thus, the support for IPv6 would be a configuration that was not within the scope of the original evaluation. Thus, this change has no impact on the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Updated Computers and Devices Pages to Leverage API	The Computers and Devices pages within the console did not leverage the API to pull in page content. We have updated them to load data using the API which enables us to load content without reloading the page. Customers should see improved performance as well as the addition of having the ability to save a view on the Devices page. The Computers page provides a table of endpoints and information about them. This is also true of the Devices page, but devices were out of scope for the evaluated product. The Computers page was used to review and navigate to data about an Agent's endpoint. The changes made were to improve the overall performance and real time display of the data collected by the product. No changes to functionality were observed based upon the review of the Console interface as well as execution of regression testing. Thus, this change has no impact on the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP.	No Impact

	Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The Computers Console page was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Active Directory Module Improvement	App Control had leveraged vbscript to manage AD login functionality in the Console. It suffered from performance issues as well as being difficult to debug when customers had issues. The new module is much more robust and allows customers to: • Reduce the domain forest (to improve performance especially when unreachable domains exist) • Login with User Principal Name (UPN) • Select default DNS name of AD environment • Admins can now set a desired level for AD searches, either Global Catalog or LDAP on the System Configuration page The product has been updated to be more robust and provide better error logging when Active Directory is used authenticating administrators to the Console. The use of Active Directory for Administrator authentication was included within the evaluated product. These updates are to address specific scenarios of integration and support of Active Directory. These scenarios were not part of the assessed functionality in the evaluated product. No changes to functionality were observed based upon the review of the Console interface as well as execution of regression testing. Thus, this change has no impact on the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: Active Directory authentication for the Console was used as part	No Impact

	of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Login Page Display Update	Improved the look and feel of the Login page. The Login page has been updated to change colors, fonts, and spatial organization. The function of the Login page has not impacted. The Login page was assessed as part of the evaluated product, but this update has no impact on the assessed functionality as it is a visual only change. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The Console Login page was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Windows XP Installer Update	"ParityHostAgent_sha1.msi" files are now included in policyname.zip files. Windows XP does not support SHA2 certificates and installers for these endpoints needed to use SHA1 signatures instead. The evaluation did not include Windows XP endpoints as part of the evaluated configuration. Only Windows 10 Professional (1903) was used for Windows based endpoints. Thus, this change has no impact on the evaluation.	No Impact

	Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Devices Page Date Field	Added a field on the Devices page to show the date a device was Approved or Banned. The Devices page provides a table of devices and information about them. The change made displays additional information already collected and available on other pages. Devices were out of scope for the evaluated product; thus, this change has no impact on the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Renamed Endpoints GUI Page	"hosts.php" is now called "Computers.php". The GUI page for displaying endpoint information has been changed from hosts.php to Computers.php. This change is not noticeable from the user experience. The page has been updated in this transition to improve the performance to display data to the administrators reviewing the information in the Console. Thus, this change has no impact on the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The Computers Console page was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No	No Impact

	changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Yara Rules Version Displayed	Yara rules version is now on the Computers page. The Yara rules version is now displayed on the Computers page in addition to the other locations it was already displayed. This information has always been tracked by the product and this provides another page to display this data instead of having to navigate to other pages to access it. The display of the Yara rules version does not directly map to any security requirements. Thus, this change has no impact on the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Large Rule Error Handling	Added new event type and alert that is triggered when a user saves a rule that is too large. The product has always allowed administrators to create rules. It was found that when rules were too complex that errors could result when processing the rules. The product has been updated to identify these complex rules to limit the errors from occurring by informing the administrators. The rules created and assessed as part of the evaluation did not and would not produce these errors as they are not complex enough to cause an issue with the product processing them. This type of error handling is not directly related to any security requirements. Thus, this change has no impact on the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP.	No Impact

	Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Devices by Serial Number Page	"Show individual devices" checkbox on the Device Catalog page has been removed, and its data moved to a new tab: "Devices by Serial Number". The Devices page provides a table of devices and information about them. The change made displays additional information through another page versus on the current page. Devices were out of scope for the evaluated product; thus, this change has no impact on the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Platform Filtering	Changed platform filter to a drop-down instead of using checkboxes on the Computers page. In large deployments with many endpoint systems, the ability to filter the systems is needed to easily find data. The evaluated product used checkboxes to filter the endpoints, and this has been updated to use a drop-down list. This change updates content display and selection process for functionality that was present but unused as part of the evaluation because this functionality does not directly relate to a security requirement and the evaluation's deployment was not large enough to need to filter endpoints. Thus, this change does not impact the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact

Improved Events Page Querying	Improved Events Page API Querying to prevent frequent timeouts. The Events page displays audit events for activities within the product. This update improves performance for displaying the data, particularly with larger deployments. This update is purely to address performance and does not change the events collected nor the information displayed. Thus, this change does not impact the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The Events Console page was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Policy Status Filter	The policy status filter on the computers page is now a drop down. In large deployments with many endpoint systems, the ability to filter the systems is needed to easily find data. The evaluated product did not have a method to filter by policy status, and this has been updated to use a drop-down list. This change updates content display and selection process to filter through data more easily. This functionality does not directly relate to a security requirement and the evaluation's deployment was not large enough to need to filter endpoints. Thus, this change does not impact the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP.	No Impact

	Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Autofill Support	Added autofill support for Computer Name "is" filters on the Approval Requests, Computers, and Application console pages. In large deployments with many endpoint systems, the ability to find systems more easily is needed. The evaluated product did not have an autofill function, and this has been added to the product. This change updates content display and selection process to search for data more easily. This functionality does not directly relate to a security requirement. Thus, this change does not impact the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Removing Certificate Trust Update	Administrators can no longer remove the trust of the certificate the server is currently using for agent communication. The product used to allow an administrator to remove the trust of the certificate which is used for the Server and Agents to communicate. Upon doing so, this would cause the product's remote components from communicating and disrupt the operations of the product. This error condition was corrected by including checks which would prevent an administrator from removing trust of this certificate. The evaluation requires the use of certificates by the underlying operating systems for secure communication. However, use of the TOE to remove trust these certificates was not part of the evaluation and would move the product outside of its evaluated configuration. Thus, preventing this error state through this update would not impact the evaluation.	No Impact

	Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Slashes in Active Directory Groups	Active Directory groups with slashes in their names can now be searched for. The product has been updated to be more robust and provide better handling of Active Directory groups for Administrators use in the Console. The use of Active Directory for Administrator authentication was included within the evaluated product. This update is to address a specific naming structure for groups supported by Active Directory. This naming structure scenario was not part of the assessed functionality during the evaluation, as not every permutation of a group name could be tested. This update addresses a specific error for one of these potential permutations. As this does not impact what was claimed, how the product is managed or how the product was tested, this change does not impact the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Improved Performance of Exact Match Queries	Improved database performance on exact match queries. In large deployments with many endpoint systems, the ability to perform searches is needed to easily find data. The evaluated product has always had the ability to search using exact match queries, but the process was slow. The logic has been updated to improve the speed and performance of these queries. This functionality does not directly relate to a security requirement and the evaluation's deployment was not large enough to need to perform these types of searches. Thus, this change does not impact the evaluation.	No Impact

	Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Additional SAML Identity Provide Support	Added support for additional SAML identity providers. This change identifies that the product has been verified to support additional SAML identity providers. In the evaluated configuration, the TOE only operates with Active Directory. As the use of SAML identity providers was not included in the original evaluated configuration and will not be included in this assessment's evaluated configuration, an update to support another operational environment component option does not have an impact on the TOE for the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Server Support for Mac Trusted Publisher	The App Control 8.9.4 Server can now receive publisher certificate information from the latest 8.8.0 Mac agent. This allows server users to approve and ban Apple-based certificates discovered on 8.8.0 Mac agents. This reduces the complexity involved with approving/banning new software and updates from Apple or other third-party vendors. This change identifies that the unevaluated Mac Agent component of the product now provides new data to the Server. The Mac Agent is a separately installed product component that was not included in the evaluated configuration. In the evaluated configuration, only Windows and Linux Agents evaluated. As the Mac Agent is an optional component that was not included in the original evaluated configuration and will not be included in	No Impact

	this assessment's evaluated configuration, features that rely on its use do not have an impact on the TOE for the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Added New Action for Cache Consistency Check	Added a new action on the Computers page to allow users to run cache consistency checks on multiple computers at once. Previously, this could only be performed on the Computer Details page. In addition, a new option to the cache consistency check menu, Re-evaluate publishers, to retrieve publisher certificate information from files on previous Mac agents that did not support Trusted Publishers. The ability to perform a cache consistency check was part of the evaluated product. This update provides the ability to perform this function from an additional Console page (i.e., Computers) and for multiple endpoints simultaneously. The cache consistency check is another mechanism to collect interesting files from an endpoint, but this manual process was not used as part of the evaluation. Instead during the evaluation, the data was initially collected upon Agent install and subsequently through the Agent's policy. Thus, this change does not impact the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Windows Case Sensitive Support	Added 'dircasesensitivityenabled' as an available agent config property in the server to address case insensitive Windows operating systems.	No Impact

	Windows operating system is traditionally case insensitive; however, recent versions of Windows does allow case sensitivity to be enabled. This update allows administrators to manage their Agents to be aware of this difference on how objects needed to be tracked in a case sensitive manner for Windows operating systems where case sensitivity has been enabled. This would have to be specifically enabled for the Windows operating system and the Agent. The evaluation was not tested on a Windows operating system where case sensitivity was enabled. Thus, this change does not impact the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: Although this configuration was not tested as part of the evaluation, regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation on this new configuration. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Computers Page Performance Improvement	Made performance improvements to reduce timeouts and delays while using the Computers page. The Computers page provides a table of endpoints and information about them. This update improves performance for displaying the data, particularly with larger deployments. This update is purely to address performance and does not change the data collected from endpoints nor the information displayed. Thus, this change does not impact the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests.	No Impact

	Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Server UI Refresh	The server has been refreshed with a new visual look and feel. The refreshed server utilizes the same functionality as previous servers, but now has all new colors, shapes, fonts, and logos. All console pages have been updated with a new responsive design allowing them to expand and compress to maximize the space of the browser window a page is being viewed in. In addition, server accessibility has been improved with updates to keyboard-only navigation and screen reader support. With these enhancements, users will benefit from a more pleasurable and accessible user experience on App Control. The Console has been updated to change colors, fonts, and spatial organization. The function of the Console has not been impacted. The Console was assessed as part of the evaluated product, but this update has no impact on the assessed functionality as it is a visual only change. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The Console was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Vulnerability Detection	The server now can identify CVEs (Common Vulnerabilities and Exposures) associated with Windows applications in an environment. The server displays CVEs in the new "CVE Instances" tab, on the Applications page. In this page, the server will display all CVE instances discovered through syncing with the National Vulnerability Database API. From this page, users can search and filter vulnerabilities by their CVE ID, CVSS Score (Common Vulnerability Scoring System), or other criteria of interest. In addition, users can also	No Impact

	identify the specific machines the vulnerabilities are found on. Users can receive alerts about critical CVEs found in their environment as well. With this new feature, users can take additional steps to protect and secure their endpoints using the App Control Server. The collection of CVE data was part of the originally evaluated product, but this functionality was not evaluated as it was not related to any of the SFRs. Thus, an update to now associate the CVE collected data with data collected from endpoint systems, would also not be related to the SFRs. This CVE data functionality is optional and not needed for the TOE's operation. This would also have no impact the installation, configuration, or operation of the TOE. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Countersigned Certificate Approval	The server now allows the approval of countersigned certificates from within the console. A new field has been added to the "File Details" page under "File Properties" that displays the name of a countersigned certificate, if it exists. Clicking on this field directs users to its respective "Certificate Details" page where the certificate's publisher can be found. The user can then approve the countersigned certificate publisher. This avoids the time-consuming process of approving a countersigned certificate manually on an endpoint. This update provides a new method to manage approving certificates which are used for publisher rules. Publisher rules are not a type of rule which were included as part of the evaluation. Thus, providing a new method of administration of functions related to unevaluated functionality would not have an impact on the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target.	No Impact

	Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Communication Key Rotation Visibility and Scheduling	The server now provides users more visibility into the agent/server communication key rotation process. A new section has been added to the "Security" tab on the "System Configuration" page that displays the date the last communication key was generated and the next scheduled rotation. Users can now regenerate keys and reschedule future key rotations to their desired date. In addition, a new console alert has been created that notifies customers 5 days before an upcoming key rotation. This new feature is aimed to help users with air-gapped servers or alternative resource download locations to prepare for communication key rotations and provide flexibility around the process. The evaluated product had the capability to use communication key, but its use was not part of the evaluated configuration. The communication key can be used to secure communications between the Server and Agent when the TLS certificates are expired. As this functionality was not used as part of the evaluated configuration, enhancements to reporting on its status would not impact the evaluated configuration as this functionality would still not be used. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
AD Managed Service Account Support	The server now can be installed and run on an Active Directory (AD) managed service account. AD managed service accounts are a more secure alternative to standard AD accounts. AD managed service accounts utilize more complex passwords not known by any users and are not stored locally. These passwords are also automatically changed every 30 days by default. Support for AD managed	No Impact

	service accounts are for users who desire additional security around server management. This change identifies that the TOE has been verified to support a different type of account on the underlying operating system for the TOE to be installed on. As part of the support process, use of an AD managed service account was fully regression tested for support with the TOE and is continuously regression tested as the TOE is updated. The prior installation procedures describe installing the TOE using an Active Directory administrator account when accessing the underlying operating system. These procedures will remain the same for this assessment and the use of an AD managed service account will be another option that is not within scope of the evaluation. Having this option does not change the currently defined installation procedures. For these reasons, the update to support another operational environment user account does not have an impact on the TOE for the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
SQL Server 2022 Support	Added support for MS SQL Server 2022. This change identifies that the TOE has been verified to support an update to Microsoft SQL Server software. In the evaluated configuration, the TOE is expected to use SQL Server 2014 or higher. Although the use of MS SQL Server 2022 was not included in the original evaluated configuration, this operational environment component option meets the definition of being 2014 or higher. As part of the support process, SQL Server 2022 was fully regression tested for support with the TOE and is continuously regression tested as the TOE is updated. For these reasons, the update to support another operational environment component version option does not have an impact on the TOE for the evaluation.	No Impact

	Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Device by ID Query	Added the ability to get v1/deviceInstance and v1/deviceSerialNumber by ID through the API. The Devices page provides a table of devices and information about them. The change made displays additional information already collected and available on other pages. Devices were out of scope for the evaluated product; thus, this change has no impact on the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Increased Database Storage IDs	Added support for negative anti-body and file name/path names IDs in server database tables which doubles the number of IDs that can be stored. This will help prevent the databases of large deployment users from filling up too quickly. In large deployments with many endpoint systems, a lot of data is collected which needs to be stored in the database. This update increased the numbers of storage IDs be using negative IDs. This does not change the functionality of the evaluated product and only increase the pool of available data identifiers in the database. Thus, this change does not impact the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests.	No Impact

	Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Common Platform Enumeration Change 1	Moved the "Execution sync and matching now" button and date/time of last execution to a more convenient location on the "CPE Applications" page. Common Platform Enumeration (CPE) functionality was part of the originally evaluated product, but this functionality was not evaluated as it was not related to any of the SFRs. Thus, an update to the location of the button and date/time information collected, would also not be related to the SFRs. This CPE functionality is optional and not needed for the TOE's operation. This would also have no impact the installation, configuration, or operation of the TOE. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Common Platform Enumeration Change 2	Added a configuration for an NVD API key for CPE users. Providing an NVD API key allows for faster data sync between the server and the NVD. Common Platform Enumeration (CPE) functionality was part of the originally evaluated product, but this functionality was not evaluated as it was not related to any of the SFRs. Thus, an update to add new configuration options for unevaluated functionality, would also not be related to the SFRs. This CPE functionality is optional and not needed for the TOE's operation. This would also have no impact the installation, configuration, or operation of the TOE. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests.	No Impact

	Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Common Platform Enumeration Change 3	Added the ability to find files in the "File Catalog" by clicking on the magnifying glass icon next to items on the "CPE Applications" page. Common Platform Enumeration (CPE) functionality was part of the originally evaluated product, but this functionality was not evaluated as it was not related to any of the SFRs. Thus, an update to the navigation to information from an unevaluated portion of the Console, would also not be related to the SFRs. This CPE functionality is optional and not needed for the TOE's operation. This would also have no impact the installation, configuration, or operation of the TOE. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Common Platform Enumeration Change 4	CPE applications are now updated whenever the NVD API reports changes. This ensures CVE data is accurate and up-to-date. Common Platform Enumeration (CPE) functionality was part of the originally evaluated product, but this functionality was not evaluated as it was not related to any of the SFRs. Thus, an update to how quickly unevaluated collected information is displayed, would also not be related to the SFRs. This CPE functionality is optional and not needed for the TOE's operation. This would also have no impact the installation, configuration, or operation of the TOE. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests.	No Impact

	Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Common Platform Enumeration Change 5	Transitioned to NVD API 2.0 as the NVD API 1.0 is scheduled to be deprecated later this year. Common Platform Enumeration (CPE) functionality was part of the originally evaluated product, but this functionality was not evaluated as it was not related to any of the SFRs. Thus, an update to improve the version of an unevaluated API, would also not be related to the SFRs. This CPE functionality is optional and not needed for the TOE's operation. This would also have no impact the installation, configuration, or operation of the TOE. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Common Platform Enumeration Change 6	Added a progress bar to show the completion of syncs between the NVD API and the console. Common Platform Enumeration (CPE) functionality was part of the originally evaluated product, but this functionality was not evaluated as it was not related to any of the SFRs. Thus, an update to include a progress bar for unevaluated functionality, would also not be related to the SFRs. This CPE functionality is optional and not needed for the TOE's operation. This would also have no impact the installation, configuration, or operation of the TOE. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact

Common Platform Enumeration Change 7	Made changes to improve the reliability of downloads from the NVD API. Common Platform Enumeration (CPE) functionality was part of the originally evaluated product, but this functionality was not evaluated as it was not related to any of the SFRs. Thus, an update to improve the reliability of an unevaluated API, would also not be related to the SFRs. This CPE functionality is optional and not needed for the TOE's operation. This would also have no impact the installation, configuration, or operation of the TOE. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
User Role Mapping Error Handling	Modified the "User Role Mappings" tab to identify rules with a disabled user role. Removed the ability for users to save a mapping rule with a disabled user role. This update provides error handling when an administrator is assigning users to roles. Previously an administrator could assign a user to a disabled role, this now prevents this from occurring. The evaluation does not have any expectations on disabled roles and only expects the default roles to be unmodified (i.e., not disabled). Since this prevents a role mapping error and is not related to a security function, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Deleted User/Role Mappings	User mappings for deleted user/roles are now deleted to prevent unauthenticated users from accessing the console.	Minor Impact

	This update provides error handling when an administrator is deleting users and/or roles to ensure a security issue with Console access does not occur. Therefore, if a user or role is deleted the mappings related to that user/role are also deleted. The use of user/role mappings is part of the Console's functionality, but the evaluation did not have tests that would have caused this type of scenario to be tested. Once this flaw was discovered, the issue was addressed and is now tested to ensure that the issue does not represent itself. The addressing of this flaw did not change any aspects of how the TOE is described, the management of the TOE, or its testing related to the evaluation. As this was a security flaw that allowed security mechanisms to be bypassed, this enhancement has been labeled as a minor impact. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The Console was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation as well as newly added tests to verify invalid mappings do not exist after a user/role is deleted. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Trusted Filter Changed to Radio Buttons	Changed "trusted" filter to radio buttons on the "Trusted Communication Certificates" table on the Configuration > Security page. The Console continued to have minor enhancements, in this case changing check boxes to radio buttons. The function of the Console has not been impacted. As the evaluated deployment was not large enough to warrant filtering of this content and the ability to filter is not described by a requirement, this ability is not described as part of the evaluation materials. The Console was assessed	No Impact

	as part of the evaluated product, but this update has no impact on the assessed functionality. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The Console was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Column Display Update	Added the ability to double-click column names in "Column Settings" area of table data pages to move them to the left or right. The Console continued to have minor enhancements, in this case adding double click presentation changes. The function of the Console has not been impacted. As the ability adjust the columns of a table is not described by a requirement, this ability is not described as part of the evaluation materials. The Console was assessed as part of the evaluated product, but this update has no impact on the assessed functionality. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The Console was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For	No Impact

	more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Agent Upgrade Wording Clarified	Reworded language to more clearly explain agent upgrade functionality in "Policy Settings" and "System Configuration". The Console continued to have minor enhancements, in this case wording was updated for clarity. The function of the Console has not been impacted. The Console was assessed as part of the evaluated product, but this update has no impact on the assessed functionality as it is a description only change. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Global Dascli Password Validation	Added password validation for Global CLI passwords. Previously, users could enter invalid passwords and they were accepted causing issues authenticating locally with agents. Management of the evaluated product's Agents was performed through the Console interface as part of the evaluation. There is also the ability to manage Agent's locally using the Dascli Command Line Utility. Use of Dascli was not within the scope of the evaluation. This update would require the configuration and use of Dascli. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact

Client Registration Code	App Control now supports the use of client registration codes. These codes prevent other programs from impersonating Carbon Black App Control agents. Added a "Client Registration Code" section to the Security tab on the System Configuration page. This allows users to generate and manage registration codes to be used when agents register with the server. This functionality can be enabled or disabled, and is disabled by default. If enabled, the client registration code must be provided as part of the installation of a new agent that supports this feature. Existing agents that have already connected to the server will remain connected, and will not need the registration code. This feature when enabled results in App Control creating registration codes that are provided through the Agent as part of the installation process and these codes are validated by the Server as part of the registration process. The evaluation's SFRs do not cover this functionality and since this addition is disabled in its default state, it will not impact the installation, configuration, or operation of the TOE. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Removed Support for Windows SQL Server 2012	The Server no longer contains support for Microsoft Windows SQL Server 2012. Microsoft no longer supports This SQL Server version as of July 12th, 2022, which means it will no longer receive security updates, non-security updates, bug fixes, or technical support. Attempting to install the App Control Server on an operating system equipped with SQL Server 2012 will now result in an error message, and the installation fails. This change identifies that the TOE has been updated to no longer support SQL Server 2012 since it is no longer supported by Microsoft. In the original evaluated	Minor Impact

	configuration, the TOE was expected to use SQL Server 2012 or higher. This update limits the available operational environment options due to the security concern that Microsoft is no longer providing updates to the operational environment component. This has no impact on the operation of the TOE. As part of the support process, all supported SQL Server versions are fully regression tested for support with the TOE. The ST and AGD were updated to clarify the current supported versions of SQL Server. Since the ST and AGD were updated, this is a Minor change. Impact to **ST** – Minor – The Security Target was updated to change the supported SQL Server versions from 'SQL Server 2012 or higher' to 'SQL Server 2014 or higher'. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – Minor – The Supplemental Guidance was updated to change the supported SQL Server versions from 'SQL Server 2012 or higher' to 'SQL Server 2014 or higher'.	
Automatic Detection of Expired Server Communication Certificates	Previously the ability to delay the exchange from one agent/server communication certificate to another was added. This was to allow agents adequate time to receive a new certificate without resulting in disconnected agents. However, this default change resulted in some instances where an expired server communication certificate would remain in use due to the "CertificateDelaySwapMinutes" config property being set to a 60-minute interval, preventing a new, valid certificate from being applied. This issue also resulted in agents entering a disconnected state. To resolve this issue, the server now automatically detects an expired communication certificate and will automatically apply a new one once it is or created in the console. Note that when this new process occurs, the console added page may still indicate that a delay occurred before using the new certificate. Refreshing the page will show that the new certificate is in effect. The evaluated product had communication certificates configured for secure communication using TLS. Note that the TLS is handled by the underlying operating systems. Over time the certificates will expire. This update notifies the administrator that certificates have expired and	Minor Impact

	provides mechanisms to rotate the certificates more easily. The evaluation requirements do not have any claims about certificate management. The management that was evaluated was part of the initial installation and configuration of the TOE. However, as the lifetime of certificates is not indefinite, it is important to provide feasible management of them. Although the use of rolled over certificates was not required to be evaluated, testing of this new function for continued support of the evaluated product is necessary. Testing was performed for this new functionality as well as regression testing to ensure that it did not impact the evaluated operation of the product after a certificate rotation occurs. The secure communication which was a security claim of the TOE was determined to still be provided after certificate rollover occurred. Although this does not impact any evaluation claims, previously evaluated management of the product, or the procedures/results of the previously evaluated testing, this change has been marked as Minor due to its relation to a security function included in the evaluated product. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The product's use of certificates for TLS was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance. Note: Although management of the certificates is not related to a specific security requirement, the need for guidance on certificate management when the certificates expire is needed. This guidance can be found under 'Securing Agent-Server Communications' in the VMware Carbon Black App Control User Guide, VMware Carbon Black App Control 8.10.2.	
Additional Communication	There are two new fields when editing a certificate in the console under the System Config -> Security Tab. The first	Minor Impact

Certificate Management Improvements	field is "Agent Certificate Update," and the second is "Update Schedule." Under the "Agent Certificate Update," there are two drop-down options. One option allows users to prevent a newly added or updated communication certificate from being activated until a current active communication certificate expires. The other option will enable users to delay the activation of a communication certificate that has been newly generated or is currently uploading to replace the old one. The "Update Schedule" field allows users to specify a time until the option they choose in the "Agent Certificate Update" drop-down executes. These fields make swapping communication certificates easier for customers with large endpoint counts. The evaluated product had communication certificates configured for secure communication using TLS. Note that the TLS is handled by the underlying operating systems. Over time the certificates will expire. This update provides mechanisms to rotate the certificates more easily. The evaluation requirements do not have any claims about certificate management. The management that was evaluated was part of the initial installation and configuration of the TOE. However, as the lifetime of certificates is not indefinite, it is important to provide feasible management of them. Although the use of rolled over certificates was not required to be evaluated, testing of this new function for continued support of the evaluated product is necessary. Testing was performed for this new functionality as well as regression testing to ensure that it did not impact the evaluated operation of the product after a certificate rotation occurs. The secure communication which was a security claim of the TOE was determined to still be provided after certificate rollover occurred. Although this does not impact any evaluation claims, previously evaluated management of the product, or the procedures/results of the previously evaluated testing, this change has been marked as Minor due to its relation to a security function included in the evaluated product.	

	Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The product's use of certificates for TLS was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance. Note: Although management of the certificates is not related to a specific security requirement, the need for guidance on certificate management when the certificates expire is needed. This guidance can be found under 'Securing Agent-Server Communications' in the VMware Carbon Black App Control User Guide, VMware Carbon Black App Control 8.10.2.	
Alternative Communication Certificates Download Location	Users can enter an alternate download location URL for communication certificates under the System Config -> Advanced Options Tab. Under the "Carbon Black App Control Agent" section, a second URL field (under "Resource Download Location") has been added called "Certificate Download Location." This allows users to reduce IIS resource contention by allowing direct file downloads of communication certificates from the console. The evaluated product had communication certificates configured for secure communication using TLS. Note that the TLS is handled by the underlying operating systems. Over time the certificates will expire. This update provides mechanisms to rotate the certificates more easily by identifying another location for certificate download. The evaluation requirements do not have any claims about certificate management. The management that was evaluated was part of the initial installation and configuration of the TOE. However, as the lifetime of certificates is not indefinite, it is important to provide feasible management of them. Although the use of rolled over certificates was not required to be evaluated, testing of this new function for continued support of the evaluated	Minor Impact

	product is necessary. Testing was performed for this new functionality as well as regression testing to ensure that it did not impact the evaluated operation of the product after a certificate rotation occurs. The secure communication which was a security claim of the TOE was determined to still be provided after certificate rollover occurred. Although this does not impact any evaluation claims, previously evaluated management of the product, or the procedures/results of the previously evaluated testing, this change has been marked as Minor due to its relation to a security function included in the evaluated product. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The product's use of certificates for TLS was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance. Note: Although management of the certificates is not related to a specific security requirement, the need for guidance on certificate management when the certificates expire is needed. This guidance can be found under 'Securing Agent-Server Communications' in the VMware Carbon Black App Control User Guide, VMware Carbon Black App Control 8.10.2.	
NIST NVD API Update	We made changes to restore connectivity to the NIST NVD API and decrease the chances of future service disruptions to CVE/CPE functionality. Common Platform Enumeration (CPE) functionality was part of the originally evaluated product, but this functionality was not evaluated as it was not related to any of the SFRs. Thus, an update to address connectivity issues to the NIST NVD, would also not be related to the SFRs. This CPE functionality is optional and not needed for the TOE's operation. This would also have no impact the installation,	No Impact

	configuration, or operation of the TOE. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Updated Pruning Functions	Improved antibody pruning performance and effectiveness. Includes separating the "DailyPrune" task into three different tasks - DailyAntibodyPruningTask, DailyNamePruningTask and DailyPruneTask, to improve overall performance of the Pruning tasks. The product removes old file data over time with a process called pruning. These updates are performance-based changes to remove data that is no longer needed by the product. Although the pruning function is needed in the product, these changes are unrelated to any security functionality that was evaluated. Thus, there is no impact on the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Installer Issue with Remote Databases	We fixed an installer issue that allowed the selection of "Local System Account" when installing against a remote database. Local system Accounts do not apply to customers doing two-tier server installations. The evaluated product was updated to address an installer issue when using a remote database. The evaluation did not include a remote database configuration as part of the evaluated configuration. Only a database installed on the same system as the Server was part of the evaluated configuration. Thus, this change has no impact on the evaluation.	No Impact

	Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Linux Agent RHEL 8.6 Support	The App Control Linux Agent now supports RHEL 8.6. This change identifies that the TOE has been verified to support an update to the underlying operating system. In the evaluated configuration, the TOE's Linux Agent is running on Red Hat Enterprise Linux 7.6. As the use of Red Hat Enterprise Linux 8.6 was not included in the original evaluated configuration and will not be included in this assessment's evaluated configuration, an update to support another operational environment component option does not have an impact on the TOE for the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Linux Install Verification	The App Control Linux Agent now adds additional security verification for components inside Linux installation packages. The Linux Agent has been updated to perform verification of its installation packages prior to installation. The evaluated configuration required Linux Agent be installed but there were no security requirements within the evaluation related to installation package verification. This additional security feature does not require additional administrative action as the product does the verification without administrative action. As no additional actions are required to manage this new function and its function is not within scope of the evaluation, there is no impact on the evaluation.	No Impact

	Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The Linux Agent was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
RPM with an SHA2-based key	The App Control Linux Agent RPM is now signed with a SHA2-based key. The key used to verify the integrity of the Linux Agent RPM has been updated to now use SHA2. The prior evaluation did not make any security claims on the verification of installation packages. The evaluated configuration required Linux Agent be installed but there were no security requirements within the evaluation related to installation package verification. This additional security feature does not require additional administrative action as the product does the verification without administrative action. As no additional actions are required to manage this new function and its function is not within scope of the evaluation, there is no impact on the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The Linux Agent was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For	No Impact

	more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
RHEL 9 Support	The App Control 8.7.10 Linux agent now supports RHEL 9 (5.14.0). In addition, we now also support Oracle Linux 9, which uses the Red Hat Compatible Kernel (9.0 RHCK). This change identifies that the TOE has been verified to support an update to the underlying operating system. In the evaluated configuration, the TOE's Linux Agent is running on Red Hat Enterprise Linux 7.6. As the use of Red Hat Enterprise Linux 9 and Oracle Linux 9 were not included in the original evaluated configuration and will not be included in this assessment's evaluated configuration, an update to support other operational environment component options does not have an impact on the TOE for the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
RHEL 9.1 and RHEL 8.7 Support	The App Control 8.7.12 Linux agent now supports RHEL 9.1 (5.14.0-162.6.1) and RHEL 8.7 (4.18.0-425.3.1). This change identifies that the TOE has been verified to support an update to the underlying operating system. In the evaluated configuration, the TOE's Linux Agent is running on Red Hat Enterprise Linux 7.6. As the use of Red Hat Enterprise Linux 9.1 and Red Hat Enterprise Linux 8.7 were not included in the original evaluated configuration and will not be included in this assessment's evaluated configuration, an update to support other operational environment component options does not have an impact on the TOE for the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP.	No Impact

	Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Reduced CPU Consumption	The Linux App Control 8.7.12 agent resolves abnormally high CPU consumption issues found in the previous 8.7.10 Linux App Control release. The previous update Linux Agent software update resulted in higher CPU consumption than what was normal. This as analyzed and prior changes were fixed to address this performance issue. This change had no impact on the function of the Linux Agent. Thus, there is no impact on the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The Linux Agent was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
RHEL 8.7 Kernel Update Support	Support for the 4.18.0-425.10.1 RHEL 8.7 maintenance kernel update. This change identifies that the TOE has been verified to support an update to the underlying operating system. In the evaluated configuration, the TOE's Linux Agent is running on Red Hat Enterprise Linux 7.6. As the use of Red Hat Enterprise Linux 8.7 was not included in the original evaluated configuration and will not be included in this assessment's evaluated configuration, an update to support another operational environment component option does not have an impact on the TOE for the evaluation.	No Impact

	Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
RHEL 8.8 Kernel Update Support	Added support for the RHEL 8.8 maintenance kernel update. This change identifies that the TOE has been verified to support an update to the underlying operating system. In the evaluated configuration, the TOE's Linux Agent is running on Red Hat Enterprise Linux 7.6. As the use of Red Hat Enterprise Linux 8.8 was not included in the original evaluated configuration and will not be included in this assessment's evaluated configuration, an update to support another operational environment component option does not have an impact on the TOE for the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
RHEL 9.2 Kernel Update Support	Added support for RHEL 9.2 maintenance kernel update. This change identifies that the TOE has been verified to support an update to the underlying operating system. In the evaluated configuration, the TOE's Linux Agent is running on Red Hat Enterprise Linux 7.6. As the use of Red Hat Enterprise Linux 9.2 was not included in the original evaluated configuration and will not be included in this assessment's evaluated configuration, an update to support another operational environment component option does not have an impact on the TOE for the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target.	No Impact

	Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
ABexclusions and Event Exclusions	Added support for ABexclusions and Event Exclusions. Previously, these server configuration properties could not be configured for Linux agents. These properties allow the suppression of specific Linux file and event reporting users deem unnecessary to improve agent performance. The Linux Agent was updated to add configurable options to limit the collection of data in certain scenarios to improve overall performance of the Linux Agent. These configuration options are disabled by default and would require administrative action to enable. This was to match functionality already present in the Windows Agent, which was disabled in the evaluated configuration. Since this addition is disabled in its default state, it will not impact the installation, configuration, or operation of the TOE. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The Linux Agent was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Added Support for read-only VMware App Volumes (AppStacks)	An AppStack is a read-only volume containing any number of Windows applications, files, folders, registry settings, and more. An administrator assigns applications to an AppStack that they want to run in their environment for specific people or groups. In order to improve the user's experience, App Control can now detect if an application	No Impact

	resides within an AppStack and automatically approve that file to run. Additionally, interesting files within the AppStack are not scanned when the new volume appears thus improving performance. Support for management of objects (i.e., AppStacks) provided by another VMware product has been added for Windows environment. The evaluation did not make any claims regarding the management of these objects, the evaluated configuration did not specify the inclusion of this separate VMware product, and the addition of support for a separate product's objects does not change the functionality for the objects which were claimed in the evaluation. Therefore, AppStacks are outside the scope of the evaluation and this update has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Offloaded Data Transfer (ODX) Support	Windows Server 2012 added ODX to enable file transfers between storage devices without traversing the host operating system. This improves transfer speeds and reduces resource consumption on the host OS. The App Control Windows agent now supports this transfer method. This change identifies that the TOE has been verified to support an update to the underlying operating system's ability to transfer data in a new method. In the evaluated configuration, the TOE's Windows Agent is running on Windows 10 Professional (1903). This update is applicable to Windows Server 2012 which was not included in the original evaluated configuration and will not be included in this assessment's evaluated configuration, an update to support another operational environment component option does not have an impact on the TOE for the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target.	No Impact

	Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
UPX Installers Now Detected	With the release of the 1.18 Rules package, the agent can now support detecting UPX file installers and correctly "promote" them so that once approved their child files will also be approved on write. This change identifies that the TOE has been verified to support another type of file installer called UPX. Management of any installers and their child files through the "promote" operation was not claimed in the evaluation. The addition of support for a new type of object/operation does not change the functionality for the objects and operations which were claimed in the evaluation. Therefore, promoting UPX file installers is outside the scope of the evaluation and this update has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Process Hollowing Detection	In conjunction with the Rules Installer 1.20 release, the Windows App Control agent can now detect if a process is being hollowed out and hijacked to execute malicious code. This expands upon App Control's excellent file-based attack prevention by adding protection for this widely recognized fileless attack. The evaluated product had the capability to create rules which would detect operations which would be considered attacking objects on the endpoint. This functionality was not claimed in the evaluation. This update provides detection of another attack operation to the product's capabilities. The addition of support for a new type of object/operation does not change the functionality for the objects and operations which were claimed in the	No Impact

	evaluation. Therefore, detecting the hollowing out of processes is outside the scope of the evaluation and this update has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Large File Processing Exclusions	The 8.9.0 Windows Agent now allows customers to specify a limit for maximum size of the files that are scanned on endpoints. This will improve performance for customers who have endpoints that constantly produce large files and scripts that the agent must analyze. This feature can be enabled by using the new agent config property "max_analysis_size_mb." The Windows Agent was updated to add configurable options to limit the collection of data involving large files to improve overall performance of the Windows Agent. This configuration option is disabled by default and would require administrative action to enable. Since this addition is disabled in its default state, it will not impact the installation, configuration, or operation of the TOE. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The Windows Agent was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact

Rule Expanding Update	Made changes to rule processing to only expand rules for newly discovered users while evaluating user logon events. This prevents rules from being unnecessarily expanded for user-specific rules. The evaluated product would expand rules every time a user logged onto the endpoint to identify user-specific rules. However, expanding rules to acquire the user-specific rules only needs to occur the first time the user is discovered by the product on an endpoint (i.e., the user's first log on event). Therefore, it was determined that performance was being impacted by performing this for every log on event with no change in what was actually being identified. The update now determines if it is the first logon event and the expanding of rules in needed, or if this is the subsequent logon event and the user-specific rules have already been identified. This is a performance change and does not impact any of the security mechanisms evaluated. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The Windows Agent was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Automatic DFS Mapping	Several changes have been made to improve the user experience for customers enforcing rules on a distributed file system (DFS). To do this, we've added the ability for the agent to automatically detect referral server paths for DFS folders. This prevents customers from having to manually specify physical server paths for the agent to recognize as DFS server paths. This manual process is time-consuming and does not scale well, especially for customers managing large numbers of DFS Servers.	No Impact

	The evaluated product had the capability to enforce rules on a DFS. This functionality was not claimed in the evaluation. This update provides enhancements to the processing rules for DFS. Since processing rules for DFS configuration was outside the scope of the evaluation, updates to the processing of those rules would also be outside the scope of the evaluation. Thus, this update has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Specify Minimum Key Size Values For RSA and ECC Certificates	The "minimum_alg_cert_key_size" adds flexibility to the minimum key size that it can accept on publisher certificates. Formerly, there was a fixed minimum size allowed for certificates. This is a problem for customers who approve publishers using ECC certificates. The value for this property is a list of key-value pairs consisting of algorithm and minimum key size, e.g., RSA:512,ECC:256. This would set the minimum key size for RSA algorithm certificates to 512 bytes, and certificates using Elliptic Curve Cryptography to 256. The evaluated product had the capability to create rules based upon the publisher of an installable and these rules operate based upon certificates. This update allows the product to support certificates of different sizes. Publisher rules were not included as part of the evaluation. Since processing of publisher rules was outside the scope of the evaluation, updates to the processing of those rules would also be outside the scope of the evaluation. Thus, this update has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP.	No Impact

	Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Rules Expansion Exclusions	The "rule_expansion_exclusions" config prop allows customers to prevent rule expansion for a specific USER SID. This can reduce wait times for users logging into a physical or virtual machine with a large number of rules that need to be processed. The value for this property consists of one or more SIDs, e.g., SID1*, SID2*. By default, the list contains following exclusions: rule_expansion_exclusions=S-1-5-90*,S-1-5-96* Accounts beginning with S-1-5-90-0 (account names DWM-x) are generated on the fly by the Desktop Window Manager component for its system services. Accounts beginning with S-1-5-96-0 (account names UMFD-x) are generated on the fly by the User Mode Driver Framework component for its system services. The evaluated product needs to expand rules every time a new user logs onto an endpoint to identify user-specific rules. However, there are certain scenarios where the product may need to be configured to not perform this for a specific user. This update provides the ability to configure the product to exclude this from occurring for specific users. This must be configured by an administrator to specify any users. In the evaluated configuration this would not be configured to be consistent with the original evaluation. Note that Microsoft – system level accounts are included in here by default. Since these accounts are not intended to be managed by the evaluated product, their inclusion in the default list is not inconsistent with the evaluated configuration. Since this addition is disabled in its default state, it will not impact the installation, configuration, or operation of the TOE. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The Windows Agent was used as part of the Common Criteria	No Impact

	evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Dascli Command Line Utility Changes	We have made a couple of changes to our dascli command line utility to aid customers in performing actions at the endpoint. Dascli previously did not have the ability to re-evaluate publisher information for a file. We have extended the parameter "analyzenow" to retrieve the publisher information for the specified file. We have also extended dascli with a new parameter called "register." Calling "dascli register code [server.id]" registers the agent with the server specified. Management of the evaluated product's Agents was performed through the Console interface as part of the evaluation. There is also the ability to manage Agent's locally using the Dascli Command Line Utility. Use of Dascli was not within the scope of the evaluation. This update would require the configuration and use of Dascli. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Repeated Blue Screen of Death (BSOD) Prevention	We have added the ability to detect repeated BSOD's caused by policy enforcement on agents. This prevention can aid in the event of a critical MS process being blocked due to rules being incorrectly written. When a specific number of BSOD's are detected the agent will automatically move to a visibility policy preventing any further occurrences. By default this function is disabled.	No Impact

	The product was updated to detect BSOD's caused by rules which accidently block critical MS operating system functions. The product was also updated to provide a configuration to alleviate this issue by placing the Windows Agent in visibility mode while the rules are being fixed. This configuration is disabled by default and would require administrative action to enable. Since this addition is disabled in its default state, it will not impact the installation, configuration, or operation of the TOE. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Driver Support Fix	Some applications incorrectly attach to the App Control process at launch which can cause App Control to hang. We have made changes to detect if a process is running and account for when a third-party driver behaves poorly. The Windows Agent could hang due to the kernel drivers on the underlying operating system not processing as expected, causing the Windows Agent to hang. This update addresses inoperability with these drivers. This is a performance issue for drivers that were not on the system during the product evaluation, and would also not be on the system as part of this assessment. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact
Server.id File Updates	Diagnostic capture files now includes the server.id file in an unencrypted form so that customers and our Support team can aid in diagnosing customer issues.	No Impact

	The Windows Agent has a server.id file that was originally unencrypted but has been updated to be encrypted to secure data from being easily accessed. This update is purely to increase security of the product but is not related to any specific security function evaluated. Additionally, diagnostic data needs to be sent from the Windows Agents to the Server and this data must include information from the server.id file. The sending of diagnostic data is also not related to any specific security function. Therefore, this has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Note: The Windows Agent was used as part of the Common Criteria evaluation, and regression testing was performed as part of this enhancement. This included performing tests that were specific to the Common Criteria evaluation. No changes in functionality nor procedure were identified with the Changed TOE when compared to the Validated TOE. For more information on the Regression Testing, refer to Section 6 of this document. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Uninstall Registry Clean-up	Updated AgentUninstallUtility to more effectively clean out registry entries. The uninstall utility for the Windows Agent has been updated to remove registry entries that were not previously removed upon the product's uninstall. The evaluation did not have any claims regarding the uninstallation process of the evaluated product as there are no security requirements related to this process. Thus, this update has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests.	No Impact

	Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	
Reduce Assertion Violation Events	Made changes to reduce unhelpful assertion violation events in the console. The evaluated product has the capability to provide notices on the Console for assertion violation events. This functionality is not related to any security functions included in the evaluation. It was also determined that many of these events were not helpful, so the product was updated to reduce the events that were considered unhelpful. Since generating assertion violation events was outside the scope of the evaluation, updates to reduce these events would also be outside the scope of the evaluation. Thus, this update has no impact to the evaluation. Impact to **ST** – None – This feature has no impact to the Security Target. Impact to **ADV** – None – This feature has no impact to the FSP. Impact to **ATE** – None – This feature has no impact to the Test Procedures or the outcome of the tests. Impact to **AGD** – None – This feature has no impact to the Supplemental Guidance.	No Impact

Bug Fixes

There were several bug fixes that were addressed as part of various release version through release 8.10.2. None of the bug fixes resulted in changes to the ST or the Common Criteria Evaluated Configuration Guide. Also, the changes made to the TOE as part of the bug fixes did not have any effect on the result of any Assurance Activities. Regression testing was also performed to verify that the bug fixes did not impact other functionality of the product and to confirm that there were no negative impacts and no documentation needed to be updated. Therefore, it was concluded that these bug fixes did not change how the TSF performed, and the TOE continues to implement the TSF in a manner that is consistent what is defined in the Security Target.
The details of the bug fixes are documented in the proprietary IAR provided to the validation team.

Regression Testing:

In addition to the vendor performing vulnerability analysis, functional regression testing was also performed against the updated TOE to ensure the TOE functionality is maintained and that the source code is fit for use. This functional testing included verification that any newly introduced

feature does not affect the security functionality previously tested and verified. This testing ensured that the functionality claimed within the Security Target has not been impacted by any software changes made to the product between releases.

For instances when security related bugs or general defects were identified, the vendor performed specific testing on the updates to ensure that the identified behavior is no longer present within the TOE and the TOE operates as expected. Details of vendor's regression testing are detailed as below :

VMware performs continuous testing on VMware Carbon Black App Control's code with regular testing cycles to ensure that each piece of updated code is tested several times before a new image is released. VMware's development and quality assurance process performs unit testing as the code is developed and operational testing to verify the functionality of the entire product. The unit tests and operational tests that comprise the Quality Assurance System are maintained by VMware's developers and Quality Assurance team to ensure that tests are updated to test the latest code/product.

Any time a bug is fixed, or a new feature is implemented, the new code is unit tested to ensure that the code operates correctly. The new code will then be merged with the VMware Carbon Black App Control base code and VMware's Quality Assurance team will perform a suite of operational tests to verify that the code changes were properly implemented and do not affect any of VMware Carbon Black App Control's other functionalities. The suite of operational tests is a combination of automated and manual testing. The automated testing is executed both nightly and weekly for different aspects of the product. All automated testing assigned to a testing cycle (i.e., nightly, weekly) is performed during its testing cycle. VMware's Quality Assurance team will analysis each change within the code to identify what manual tests need to be performed due to the changes made in the code. Based upon the analysis, VMware's Quality Assurance team will select manual tests to perform that are related to the change and/or could have been impacted by the change. Included in these manual tests are the test cases that were performed during the Common Criteria certification of VMware Carbon Black App Control v8.8.2. Once a new software image for VMware Carbon Black App Control is ready for release, VMware will create a build of the software for release. The release candidate is also tested using VMware's Quality Assurance System before being provided to end customers.

VMware's regression testing on VMware Carbon Black App Control v8.10.2 demonstrated that the behavior of the TSF remained consistent with the testing results obtained during the original evaluation.

Vulnerability Analysis:

A public search for new vulnerabilities that might affect the TOE since the evaluation was completed was performed.The vulnerability search was performed on the VMWare Carbon Black App Control product that is posted on the NIAP Product Compliant List web pages.

- CCEVS-VR-VID11158-2022 - VMware Carbon Black App Control v8.8.2 .
  Certificate Date: 2022.03.03

The original search terms for the evaluation listed above have been provided below as well as the results of a new search performed on 01/30/2024.

Databases used for the searches:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php
- US-CERT: http://www.kb.cert.org/vuls/html/search
- Tenable Network Security http://nessus.org/plugins/index.php?view=search
- Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities]

These search criteria were applied as follows:

Keyword	Description
Carbon Black	This is a vendor specific term for searching for known vulnerabilities produced by the company, overall. *The term VMware is too broad and returns over 1300 findings. The term was refined to VMware Carbon Black which returned the same results as just Carbon Black.
Carbon Black App Control (8.10.2)	This is a vendor specific term for searching for known vulnerabilities for the specific product. This covers server and agents.
VMware App Control (8.10.2)	This is a vendor specific term for searching for known vulnerabilities for the specific product. This covers server and agents.

Host Based Access Control	This is a generic technology term for searching for known vulnerabilities for the specific technology.
Server/Console Libraries The following terms are libraries contained in the TOE's Server/Console.	
7-zip-23.01	nghttp2-1.57.0
AjaxControlToolkit-19.1.0.0	nlog.targets.syslog-6.0.1
AWSSDK.SQS-2.0.0.4	NLog-4.7.3
AWSSDK-2.0.0.4	OMAC-28-01-2004
Boost C++ Libraries - boost-1.74	OpenSSL-3.2.0
Bootstrap -4.5.0	Parsifal-1.0.7
curl-8.5.0	pcre2-10.42-1
entityframework-6.4.4	pear-1.10.12
Font Awesome -6.2.1	php-8.1.24
gsoap-2.8.122	prototype.js-1.7
JQuery.localscroll.js -1.2.7	raleway -3.001
JQuery.scrollTo -2.1.2	Roboto-2.138
JQuery.selectbox -3.2.0	script.aculo.us -1.9.0
JQuery.tablesorter.js-2.1.7.8	SD.LLBLGen.Pro.DQE.SqlServer 3.5.12.0317
jquery-3.6.4	SimpleSAMLphp -2.1.0
jquery-cron-0.1.4.1	smarty-4.3.1
jquery-hoverintent-r7	sqlite3-3.44.2
jquery-ui-dist-1.13.2	Superfish Menu -1.7.4
libsodium-1.0.17	System.Runtime.InteropServices.RuntimeInformation -4.3.0
libssh2-1.9.0	Telerik Ajax RadControls for ASP.NET 2020.2.617.45
Microsoft.Csharp 4.8.4084	TinyXML2 -9.0.0
Microsoft Drivers for PHP for SQL Server -5.11.1	visual_studio_runtime 14.00.24210.0
minizip-1.1	Web Services Enhancements (WSE) for Microsoft .NET 3
mochikit-1.4.2	yara-4.2.2
Newtonsoft.Json-13.0.3	zlib-1.3
Linux Agent Libraries The following terms are libraries contained in the TOE's Linux Agent.	**Windows Agent Libraries** The following terms are libraries contained in the TOE's Windows Agent.
boost-1.69	boost-1.59.0
minizip-1.1	boost-1.81.0
sqlite3-3.43.1	lzma-19.0
tinyxml2 3.0.0	minizip-ng-3.0.6
wxwidgets-3.1.5	rapidjson-v1.1.0
golang-runtime-1.20.5	sqlite3-3.38.1
7zip-9.20	tinyxml2-9.0.0

	unshield-0.5
	xxhash-0.8.1
	yara-4.0.2
	zlib-1.1.4
	zlib-1.2.12
	zlib-1.2.13

There were no open or unpatched known vulnerabilities to the TOE or the libraries used by the TOE as a result of the public search. Therefore, there are currently no publicly known vulnerability issues that could affect the security posture of a deployed TOE.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found them all to be minor. No functionality, as defined in the SFRs, was impacted, and none of the software updates affected the security functionality or the SFRs identified in the Security Target. Therefore, CCEVS agrees that the original assurance is maintained for the product.

However, the validation team would like to emphasize that any enhancements or inclusions made to the features that were considered outside the scope of the original evaluation were considered to have no impact to the TSF. The functionality evaluated as part of this assurance maintenance is scoped exclusively to the security functional requirements specified in the Security Target and other functionality included in the product was not assessed as part of this effort. All other functionality provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness as stated in the original validation report.