VMware Carbon Black Cloud Console Release Notes - 2022 Archive

VMware Carbon Black Cloud

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Introduction

1

This document contains the release notes for Carbon Black Cloud for the year 2022.

Known Issues as of 31 December, 2022 2

The following issues are known to affect the software. Each lists the date when the issue was first reported. Issues are removed after they are resolved.

This chapter includes the following topics:

- All
- Endpoint Standard
- Enterprise EDR
- Container Essentials
- Workloads

All

- **CWP-10433: Export for large data sets under Vulnerabilities (where the exported file size > 5 GB) times out (first listed: 17 December 2021)**

  Workaround is to export a reduced number of records by applying filters to the affected table.

- **CBC-8443: Actions taken by VMware users are not visible in customer's audit logs (first listed: 1 December 2021)**

  Work around: Logs are available upon request with a support ticket.

- **DSER-36314: Data Forwarder filtering throws an error for the process_path field when the : character is not escaped, but not if \ or / characters are not escaped (first listed: 8 November 2021)**

- **DSER-36023: Linux VDI parent/child hierarchy may be reported incorrectly in environments where an appliance is installed (first listed: 27 October 2021)**

  There is no known workaround for this issue, but it will be resolved in a future sensor release.

- **DSER-33682: When viewing the Process Analysis page, the wrong file path for the process can be displayed (first listed: 26 August 2021)**

- **DSER-33621: The Alerts detail panel does not show notes for grouped alerts even though the Alert status displays “Notes Added” (first listed: 26 August 2021)**

  You can still view the Alert notes when searching for the corresponding Threat ID.

- **DSER-33425: Audit Log export to CSV is timing out after 60 seconds without any error or message in the user interface to notify the user (first listed: 16 July 2021)**

- **DSER-32435: Sensor groups configured to include devices based on minor OS names can include devices that match the major OS name (first listed: 25 June 2021)**

  For example, a group configured to include Windows 7 x64 devices can include other Windows 7 devices. This issue affects Windows, macOS, and Linux devices.

- **DSER-32398: Some alerts display blank nodes on the Alert Triage page process graph (first listed: 25 June 2021)**

- **DSER-32381: The Alert Triage process tree does not include the processes listed in the alert, although these process events are displayed when searched in the console (first listed: 25 June 2021)**

- **DSER-32293: When viewing the Investigate page, the Effective Reputation displays two dashes ("--") instead of a valid reputation (first listed: 27 May 2021)**

- **DSER-32209: When exporting to CSV from the Investigate page, the resultant CSV can have missing fields (first listed: 27 May 2021)**

- **DSER-32012: The Sensor group “Processing” message can continue to display if the job has not completed successfully (first listed: 27 May 2021)**

- **DSER-31444: The Uninstall Sensor action does not apply to all sensors matching the current search on the Endpoints page (first listed: 26 April 2021)**

- **DSER-30497: Enabling the Auto Ban feature at any threshold changes the default action of the Application on the company banned list rule from Terminate if Runs or is Running to Terminate when Communicates over the network (first listed: 26 April 2021)**

  This change is applied to any policies that have the banned list rule enabled.

- **DSER-29646: Sensors might not be assigned to the expected sensor group when subnet rules are configured (first listed: 18 March 2021)**

- **DSER-29898: Case sensitive-email checks on SAML login flow (first listed: 2 March 2021)**

- **DSER-28814: The process tree on the Alerts Triage page might include blank entries (first listed: 16 December 2020)**

- **DSER-27969: The Process Analysis graph might display a process as both parent and child of the same process (first listed: 11 November 2020)**

- **DSER-25397: Watchlist report does not port to the Investigate query page (first listed: 17 August 2020)**

- **DSER-23471: Exporting individual widgets sometimes times out in dashboard Export (first listed: 3 August 2020)**

- **DSER-25329: Facet searches can report as completed before the search completes (first listed: 16 July 2020)**

- **DSER-25244: Watchlist deletion is not tracked in the audit log (first listed: 16 July 2020)**

- **DSER-25244: If an org removes Enterprise EDR, Watchlist alerts can still occur (first listed: 16 July 2020)**

- **DSER-24196: API search might return different results based on field filtering order (first listed: 16 July 2020)**

- **DSER-4390: Devices only show the status of Eligible for Upgrade if the sensor version is lower than any versions that are available in the Endpoints > Download Sensor Kits window (first listed: 18 September 2019)**

Endpoint Standard

- **DSER-40635: Minor versions for MAC OS are not specifiable in Sensor Groups (first listed: 14 July 2022)**

- **DSER-40671: Endpoints UI Asynchronous Export not linked in console (first listed: 14 July 2022)**

  Asynchronous export/download feature is not linked in the console. Currently the userinterface is using the synchronous download. This can fail for larger environments.

- **DSER-38742: LiveResponse cannot manage commands that contain special characters (first listed: 14 July 2022)**

  - LiveResponse: Unable to change directories when their name include extended characters

  - Non-ASCII characters are garbled by using *exec msg* command on Live Response

- **DSER-30385: When viewing the Alerts page, the user value can show the user that installed the sensor instead of the user logged in at the time of the Alert (first listed: 18 March 2021)**

Enterprise EDR

- **DSER-25536: The Process Analysis button on the Investigate page does not work when Investigate is opened from the Watchlists page (first listed: 03 August 2020)**

- **DSER-25981: Search API facet requests do not process range parameters (first listed: 17 August 2020)**

- **DSER-25929: Link from Watchlist Alert to Investigate does not show all relevant metadata (first listed: 17 August 2020)**

- **DSER-26185: When using arrow keys to select a suggested query term or value, the search bar on some pages replaced the existing search bar contents instead of inserting (first listed: 21 August 2020)**

- **DSER-26035: The /tree Search API endpoint returns "resource does not exist" for known process_guid (first listed: 21 August 2020)**

- **TPLAT-9183: Signature status is UNKNOWN for valid signatures (first listed: 31 August 2020)**

Container Essentials

- **CBC-6388: Exceptions tab on a CVE modal window (first listed: 29 April 2021)**

  In the exceptions tab on a CVE's modal window, there is a slight delay between when an exception is deleted and when the exceptions table reflects the updated status. As a result, the table can show stale or invalid exception data for up to a second after the deletion.

  Refreshing the table resolves this issue.

- **CBC-6468: Numbers for images and vulnerabilities under the All filter do not reflect the correct status (first listed: 29 April 2021)**

  On the container image vulnerabilities page, the numbers for images and vulnerabilities under the **All** filter do not reflect the status of the **Running in Kubernetes** filter in the table.

- **CBC-6540: On the Kubernetes images page, the number of workloads displayed can occasionally fall out of sync with the most recent value (first listed: 29 April 2021)**

  On the Kubernetes images page, the number of workloads displayed can occasionally fall out of sync with the most recent value. The corresponding Workloads window displays up-to-date information.

- **GRC-320: When updating a template, rules search fields are disabled and rules cannot be searched (first listed: 22 December 2020)**

- **GRC-328: Searching Kubernetes resources using a MAPL rule with no conditions returns no results (first listed: 22 December 2020)**

- **GRC-345: Some violations appear under the unknown resource group (first listed: 22 December 2020)**

- **GRC-418: On data-planes running Kubernetes version 1.15 or lower, the workload name might be empty (first listed: 22 December 2020)**

- **GRC-2222: CLI-created API keys are not deleted after the CLI instance is deleted (first listed: 14 April 2022)**

- **KRS-606: Network map shows no activity on GKE v2 dataplane cluster (first listed: 27 October 2021)**

- **KRS-902: Clicking on a policy's side panel and opening another policy's alerts modal (while the first one is still in focus) disrupts rules (first listed: 28 February 2022)**

- **KRS-903: Workload summary Runtime tab fails to load the workload baseline when opened in a modal mode through the Alerts page (first listed: 28 February 2022)**

- **KRS-904: RuntimePolicyModal fetches twice the policy data (first listed: 28 February 2022)**

- **KRS-919: RuntimePoliciesTableSidePanel closes on policies change. This should happen on delete only (first listed: 28 February 2022)**

- **KRS-975: SimpleSelect does not support disabled options (first listed: 28 February 2022)**

- **N/A: Searching for literal strings containing regular expression modifiers may yield unexpected search results (first listed: 29 April 2021)**

All search boxes for container image search tables support regular expression queries; searching for literal strings containing regular expression modifiers may yield unexpected search results. Characters such as “+” and “*” must be prefixed with a “\” (the regular expression escape character) to search for those actual characters.

Workloads

- **CBC-19264: Inaccurate error message displays if timeout occurs when downloading public key**

  While installing a sensor using automation scripts (user data, ansible,chef,puppet), the script downloads the VMware public key and validates the public key once downloaded.

  If the download fails due to a timeout, a public key validation error displays:

  ```
  VMware public key seems to be tampered. Exiting...
  ```

  This error message is not accurate. The correct error message should refer to a key download error.

  Workaround: Retry after waiting a few minutes.

- **DSER-28998: Audit & Remediation queries are still running after Audit & Remediation is disabled**

  Although Audit & Remediation is disabled, previously scheduled live queries continue as per their schedule. It is expected that if the feature is no longer available, the query runs should stop.

- **DSER-39330: CBC Recommendations Page: "Unknown" values display for all signatureCA fields**

What's New - 15 December 2022

3

Build 1.9

To see changes made in previous releases, see Chapter 33 Archive of 2023 Improvements and Resolved Issues

This release includes:

- **Console updates to accommodate the 3.9 Windows sensor**

Resolved Issues - 15 December 2022

4

- **DSER-40298: The Device API documentation has been updated with all fields in snake_case**

  Previously, there were inconsistencies in field names where the request specified camelCase and the response used snake_case.

- **DSER-43560: LiveQuery now displays REG__BINARY values as a hexadecimal string to match registry table format**

  When querying the registry table, the data for REG_BINARY values are reported in osquery as a hexadecimal string. Users expect that same format when viewing results in the Query Results page. However, there were cases where the data was presented as a floating point number using scientific notation. Information was lost due to this conversion.

What's New - 23 November 2022

5

Build 1.8

- **Vulnerability Management**

  VMware Carbon Black Cloud Vulnerability Management now provides a new capability to dismiss and undismiss vulnerabilities from the CBC UI.

  Dismissed vulnerabilities no longer appear in the standard vulnerability views, but will instead be accessible under the dismissed view in the CBC UI. Users can provide the reason for dismissing the vulnerability as well as any associated notes. Once dismissed, these vulnerabilities can be restored to the standard vulnerabilities views at any time.

- **Containers - Support for ephemeral containers**

  Ephemeral containers is a new Kubernetes feature introduced in 1.25. It is useful for interactive troubleshooting when `kubectl exec` is insufficient because a container has crashed or a container image does not include debugging utilities. You can limit ephemeral containers permissions by selectively applying policy rules on ephemeral containers. Ephemeral container enforcement is applied by default.

Resolved Issues - 23 November 2022

6

This chapter includes the following topics:

- All
- Containers

All

- **DSER-33450: Watchlist - Carbon Black known IOCs feed hits now include events that the feed IOC details**

- **DSER-36748: Export Devices CSV v6 API are now encapsulating name fields in double quotes, thereby fixing the previous parsing error**

Containers

- **CNS-113: An image already scanned by the cbct gets results from the backend without generating the SBOM**

- **CNS-991: Syft version is updated to 0.60**

- **CNS-1229: Fixed Wrong scanned tags count under image repos tab**

- **CNS-1200: Fixed export CVS not working when filters were not applied in image summary Vulnerabilities tab**

- **CNS-341: Fixed cbctl image packages command get error**

- **CNS-354: Improved cluster refresh state mechanism**

- **CNS-1098: Added Node counts to clusters page**

- **CNS-1102: Fixed annotation to detect Internal load balancer on GKE**

What's New - 13 October 2022

7

Build 1.7

- **Containers - Image File Reputation and Malware Detection**

  Image File Reputation and Malware detection - Image Layers Data

  Customers now can use the Carbon Black Cloud console to view the list of all individual layers comprising a particular container image, the unique identifier of a layer, and the available packages per layer.

  After container images are deployed and available in the Carbon Black Cloud console, customers can use the filters to only receive packages and vulnerabilities of interest.

- **Audit Log**

  Audit Log now includes actions taken by authorized VMware employees

  All actions taken in a Carbon Black Cloud organization are now reported in the organization's Audit Log, whether those actions are taken by users or by authorized VMware employees. Previously, VMware employee activity was only available by Support request. This change not only reports those actions that were already logged when performed by users (such as Customer Support enrolling a new user login, generating new company registration codes, and more), but also shows previously-invisible logs for such actions as disabling SAML/2FA or requesting sensor logs. In cases where an audit log entry reports on VMware employee activity, the specific email and IP addresses are obfuscated for privacy. To quickly find those audit log entries, you can search for **VMware employee** in the Audit Log page. This change has been applied retroactively to make all such past actions visible in your Audit Log.

Resolved Issues - 13 October 2022

8

This chapter includes the following topics:

All

- **DSER-42211: Fixed error causing the AV signature pack download option to be missing in the Carbon Black Cloud Console**

- **DSER-41413: Fixed an error in the sensor kit deployment to avoid publishing the same sensor kit more than once**

- **DSER-31444: Added the option to uninstall sensors from the inventory pages on all devices matching a search**

- **DSER-39241: Added Device IDs for Audit Log entry for Sensor Uninstall**

Containers

- **CNS-806: Fixed missing virtual workload UI indication in Alerts and Events pages**

What's New - 19 September 2022

9

Build 1.6

- **Virtual Workloads**

  We've added the ability to group together pods that aren't spawned through native Kubernetes controllers.

  These pods group are addressed as **Virtual Workloads**. The grouping logic is applied automatically and without any user action. Users can identify Virtual Workloads on all relevant Kubernetes pages. The same Kubernetes scope and policy are applied to all pods that are matched under the same Virtual Workload.

- **RBAC Permissions**

  The names of two RBAC permission roles have been changed. **Manage Sensor Groups** is changed to **Manage Groups**, and **View Devices and Sensor Groups** is changed to **View Devices and Groups**.

Resolved Issues - 19 September 2022

10

- **CNS-781: Container images scan log tab, changing the chart text from “No vulnerabilities” to “No new vulnerabilities”**

- **CNS-780: Vulnerabilities tab - The table columns were not aligned properly**

- **CNS-791: Container images overview dashboard**

  On Firefox, the vulnerability timeline graph was not showing formatted dates correctly (Invalid date instead of actual date).

- **DSER-41475: CSV file upload**

  When uploading a CSV file of reputation overrides, the upload could stall in a RECEIVED state. This caused all further uploads to fail because the current system only allows one upload to be processed at a time.

- **DSER-28360: Policy rule changes**

  You could not save policy rule changes in the Carbon Black Console unless the action was toggled. These are policy rule operations (Deny operation / Terminate process) for each reputation listed under the **Blocking and Isolation** section in the Policies page.

What's New - 18 August 2022

11

To see changes made in previous releases, see Chapter 33 Archive of 2023 Improvements and Resolved Issues.

- **Audit and Remediation**

  Recommended Query Refresh

  The VMware Carbon Black team has completed a review of the Recommended Query collection. Queries were reviewed for effectiveness, quality, and timeliness. As a result, some queries have been updated and new queries have been added.

  • Several existing queries are updated to increase effectiveness and specificity. These updates will be added in the form of new queries to avoid affecting current customer workflows.

  • New queries are added from the Query Exchange. These queries are vetted by the VMware Carbon Black team.

  See the Carbon Black User Exchange for details.

Resolved Issues - 18 August 2022

12

This chapter includes the following topics:

- All
- Workloads

All

- **DSER-38582: Sensor Update Services -> MSSP user could not create upgrade job in child organization**

  Updated Sensor Update Service APIs to properly check users permissions against the target organization for a create Upgrade job operation. This resolves issues preventing MSSP users from creating an upgrade job in a child organization.

- **DSER-36900: Updated Update Senor bulk API to properly set Sensor Update status**

  Updated Update Senor bulk API to properly set Sensor Update status information to reflect accurate update state, time, and so forth. This resolves reported issues where sensors showed as **Pending Update** state even when updated.

- **DSER-41180: Org Reputation Override Service consistently timed out (504), preventing customer from adding hashes to the approved list**

- **DSER-39404: Updated Policy Change bulk API to properly generate an audit log entry with device information**

  This allows customers to track down changes for specific devices.

Workloads

- **CBC-15559: CB Cloud Workload customers need an option both at an org level and policy level to de-register VM Workloads**

CB Cloud Workload customers need an option both at an org level and policy level to de-register VM Workloads that have been inactive for a certain period. Options for the period are: 1 hour, 3 hours, 24 hours, 3 days, 1 week, 30 days.

What's New - 4 August 2022

13

To see changes made in previous releases, see Chapter 33 Archive of 2023 Improvements and Resolved Issues.

VMware Carbon Black Cloud Workload for Public Cloud

14

The VMware Carbon Black Cloud Workload for Public Cloud is now available. It provides the ability to secure AWS workloads while simplifying the overhead of AWS account management.

Core capabilities include:

- single and multiple AWS account management
- auto-generated CI-CD agent installation packages
- enhanced visibility into inventory of protected and unprotected workloads

Prior to the Carbon Black Cloud Workload for Public Cloud, Amazon EC2 instances were treated as Endpoints. We recommend updating the Carbon Black sensor to the latest sensor version prior to enabling the Carbon Black Cloud Workload for Public Cloud. These sensors can also be upgraded after the Carbon Black Cloud Workload for Public Cloud is enabled.

Features include:

- **Known Issues specific to Public Cloud**

  There are no new resolved issues with this release.

  There is only one new Known Issue: List item..

- **Vulnerability Assessment**

  VMware Carbon Black Cloud Workload provides InfoSec and AWS admins with a list of OS and Application vulnerabilities across protected Amazon EC2 instances.

  This solution is scan-less and risk-prioritized to reduce operational overhead and to provide the most critical data to you in an easy-to-consume format.

- **Inventory**

  Infosec admin and AWS admin can view the inventory of the Amazon EC2 instances using the Carbon Black Cloud Console. They can:

  - learn about its protection status and assigned policies.
  - view summarized and actionable metrics of the inventory to understand the security posture and the key information about their AWS footprint.

  - get access to a richer data set about EC2 instances including but not limited to AWS tags, their vulnerabilities, and trigger various management actions.
  - Use auto-deregistering of EC2 instances after termination to enhance the management of ephemeral EC2 instances out of the box.

- **Sensor Deployment**

  Infosec admins can easily download auto-generated sensor install packages to incorporate into their existing CI-CD workflows. Popular tools like Chef, Puppet, Ansible and AWS User Data scripts are supported.

- **AWS Account Management**

  Infosec admin and AWS admin can easily manage their AWS accounts and regions. They can:

  - add a single account.
  - leverage bulk import of accounts to facilitate quick onboarding of existing AWS accounts.
  - search and export onboarded AWS accounts and regions into an easy-to-consume format.

What's New - 19 July 2022

15

Note: To see changes made in previous releases, see Archive of 2022 Improvements and Resolved Issues.

- **Audit and Remediation: Differential Analysis API**

  Live Query provides the ability to run snapshot queries that provide point-in-time results. With the addition of the Differential Analysis API, these point-in-time queries can be compared to see when something has changed, what was changed, and the current and previous values. This feature allows users to monitor artifacts with a low change probability, and know that differential results mean something has changed and should be investigated.

  Differential Analysis can be used to monitor files, folders, and registry keys to detect:

  - Persistence
  - Tampering
  - Infiltration
  - Lateral Movement
  - Boot Time Changes
  - Security Posture Changes
  - Browser Extension Modifications

  This release is API only.

  More details are available at the VMware Carbon Black Tech Zone and the VMware Carbon Black Developer Network.

- **Carbon Black Cloud Apps for ServiceNow**

  The VMware Carbon Black Cloud apps for ServiceNow are now available in the ServiceNow Store. These integrations provide joint customers with access to pre-built ticketing and incident response workflows powered by Carbon Black Cloud data and response actions.

  Joint customers of ServiceNow and VMware Carbon Black can now get more value out of their existing security investments by automating workflows that span both products and by leveraging their Carbon Black Cloud data to enrich the insights available in their ServiceNow console.

Resources:

- ServiceNow App Store Listings:
  - Carbon Black Cloud App for ServiceNow
  - Carbon Black Cloud App for ServiceNow IT Service Management
  - Carbon Black Cloud App for ServiceNow Security Operations
- Developer Documentation
- Announcement Blog

Resolved Issues - 19 July 2022

16

- CBCUI-1056: The training link on the top navigation was previously going to a dead link
- CBCUI-1187: Top Alerted Devices were Showing Numeric IDs Instead of Device Names

What's New - 23 June 2022

17

Note: To see changes made in previous releases, see Archive of 2022 Improvements and Resolved Issues.

- **Container Essentials**

  Enforce Compliance without Compromising Security

  The Auto Enforce feature was created to help with misconfigurations of Kubernetes Workloads and Containers. SecOps teams can audit workload vulnerabilities and misconfigurations and use VMware Carbon Black Container to mutate the workload to the desired state. The tool uses automation to mitigate and enforce policy management across environments at the cluster layer.

  This feature allows users to:

  - Enforce compliance without compromising security
  - Regain control of K8s
  - Quickly remediate misconfigurations and deviations from compliance standards

  Reducing Friction for DevOps Teams

  Carbon Black is releasing two new features to help reduce friction for DevOps teams regarding deployments.

  - **Cbctl**: - cbctl is now available as a container. With the newly released container, you can easily integrate Carbon Black image scanning to your CI of choice. This includes Tanzu Application Platform.
  - **Helm Chart**: The Carbon Black agent is now available as Helm chart and allows the DevOps team to keep the Carbon Black installation process on par with all other infrastructure tools and processes.

Resolved Issues - 23 June 2022

18

This chapter includes the following topics:

- Container Essentials
- Workloads

Container Essentials

- **GRC-1171: Changed imagePullPolicy for DP services to IfNotPresent**

- **GRC-1599: Changed the operator so it does not use its own ClusterRole for the deployed agent components**

  Created a dedicated role for the agent components that has only the needed permissions.

- **GRC-1996: Added ability to deploy dataplane using Helm chart**

- **GRC-2083: cbctl publicly available as docker image**

- **GRC-2140: Implemented label-based exceptions**

  Changes include:

  - Support label exception in the exception/policy API for adding/removing/editing exception
  - Support the exception in the agent and policy engine
  - Support calculating violations by taking the new exception into account (for the Policy violations modal where violations are shown)

- **GRC-2144: Implemented presets management in guardrails-apis**

  This includes:

  - API changes to navigate the client, which rules support enforce action, and what are their "preset" configs
  - CRUD APIs for the presets themselves

  - Policy APIs changes to validate enforce rules and the selected presets

- **GRC-2169: Added support for alternative ways for configuration via cbctl: via global CLI parameters and environment variables**

- **GRC-2395: Upgraded Operator SDK**

  Follow the operator SDK upgrade documentation to fix vulnerabilities found by Github.

Workloads

- **CBCUI-959: Users can now create and edit a data forwarder without having to set a filter**

- **DSER-40966: Fixed misaligned bullets when viewing permissions on the Roles page, due to a recent Chrome browser update**

What's New - 8 June 2022

19

The 8 June 2022 release includes:

- Allow users to export CSV from Endpoints - Sensor Update Status for in-progress jobs
- No longer creates duplicate Alerts through historical evaluation on selected Watchlist when adding new Query to existing Watchlist

Resolved Issues - 8 June 2022

20

This chapter includes the following topics:

Endpoint Standard

- **DSER-29616: Allows clients to download CSV of processing jobs and allows export of logs while sensor update is processing**

Enterprise EDR

- **DSER-39270: Adding IOC query to existing Watchlist**

  Adding IOC query to existing Watchlist is evaluating on all existing data. Fixes an issue where a user selection can be erroneously retained when updating a watchlist, thereby resulting in the watchlist being evaluated on all existing data.

What's New - 26 April 2022

21

Note: To see changes made in previous releases, see Archive of 2022 Improvements and Resolved Issues.

The 26 April 2022 release includes bug fixes and enhancements.

- **New Policy Service API Release**

  You can now use the new Policy Service API to manage your Policies for endpoints and workloads with a single CUSTOM API key. This allows more granular permission controls when creating API keys to manage Policies. This iteration of the Policies API also aligns many field names with those used elsewhere in the product. Policy Service API will serve as the primary API to manage policies in the Carbon Black Cloud going forward and will be updated with additional features as we work to simplify the Policy experience.

  For more information, please visit the Policy Service API documentation on the Developer Network.

- **Data Forwarder Improvements**

  There are two improvements to the Data Forwarder:

  - Simplified Policies
  - Data Forwarder-compatible KMS encryption of an AWS S3 bucket

  Simplified Policies:

  We have simplified the Data Forwarder to require fewer permissions. The following actions are no longer required in the bucket policy:

  - “s3:AbortMultipartUpload”
  - “s3:GetObjectAcl”
  - “s3:ListMultipartUploadParts”

  Data Forwarder-compatible KMS encryption of an AWS S3 bucket

  You can now enable KMS encryption on any AWS S3 bucket used to store data sent from the Carbon Black Cloud Data Forwarder. For detailed instructions, see:

  - User Guide: Encrypt Your S3 Buckets Using AWS KMS

  - Developer's Network: KMS Encryption and Simplified Bucket Policies for the S3 Carbon Black Cloud Data Forwarder

- **Improved testing LR for invalid device session**

Resolved Issues - 26 April 2022

22

- CBCUI-668: Test LR for invalid device session
- CBCUI-743: User with non-admin role grant cannot change role

What's New - 14 April 2022

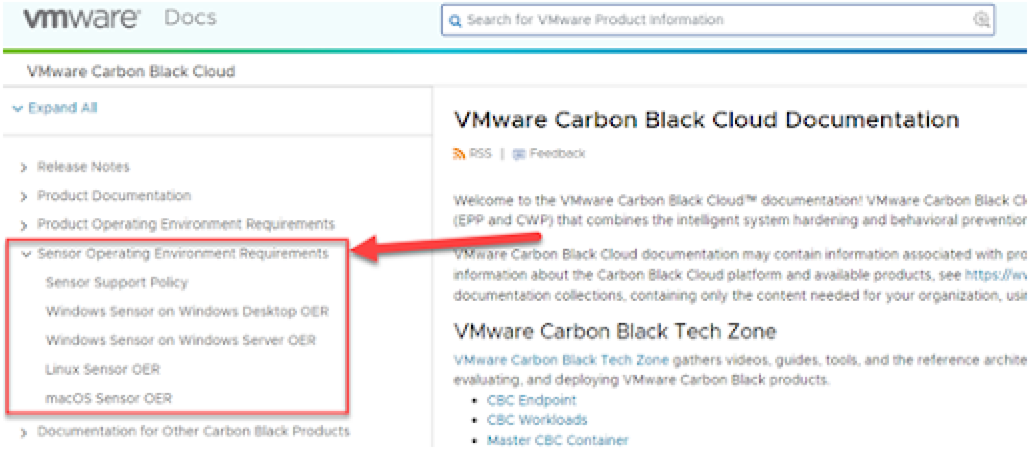
23

The 14 April 2022 release includes bug fixes and enhancements.

- **Major Documentation Update: Sensor-Specific OERs**

  As part of our continuing effort to consolidate key content onto VMware Docs, we have moved and consolidated sensor-specific information from the Carbon Black User Exchange (UEX) to VMware Docs. Each Carbon Black Cloud sensor now has a unique Operating Environment Requirements (OER) document. Specifics regarding the new content:

  - Created the following new documents:
    - Windows Sensor on Windows Desktop OER
    - Windows Sensor or Windows Sensor OER
    - Linux Sensor OER
    - macOS Sensor OER
    - Sensor Support Policy
  - Created user-friendly architecture specific to the delivery method.

    
    vmware Docs
Search for VMware Product Information
VMware Carbon Black Cloud
Expand All
Release Notes
Product Documentation
Product Operating Environment Requirements
Sensor Operating Environment Requirements
Sensor Support Policy
Windows Sensor on Windows Desktop OER
Windows Sensor on Windows Server OER
Linux Sensor OER
macOS Sensor OER
Documentation for Other Carbon Black Products
RSS | Feedback

    VMware Carbon Black Cloud Documentation

    Welcome to the VMware Carbon Black Cloud™ documentation! VMware Carbon Black Cl (EPP and CWP) that combines the intelligent system hardening and behavioral preventio

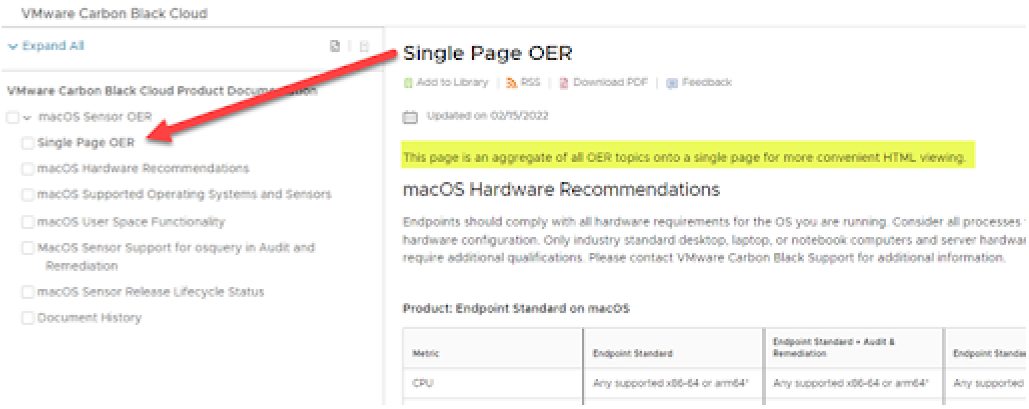
    VMware Carbon Black Cloud documentation may contain information associated with pro information about the Carbon Black Cloud platform and available products, see https://w documentation collections, containing only the content needed for your organization, usi

    VMware Carbon Black Tech Zone

    VMware Carbon Black Tech Zone gathers videos, guides, tools, and the reference archite evaluating, and deploying VMware Carbon Black products.

    - CBC Endpoint
    - CBC Workloads
    - Master CBC Container

    - In HTML, created a single-page OER to improve readability


VMware Carbon Black Cloud
Expand All
VMware Carbon Black Cloud Product Documentation
macOS Sensor OER
Single Page OER
macOS Hardware Recommendations
macOS Supported Operating Systems and Sensors
macOS User Space Functionality
MacOS Sensor Support for osquery in Audit and Remediation
macOS Sensor Release Lifecycle Status
Document History
Add to Library
RSS
Download PDF
Feedback

Single Page OER

Updated on 02/15/2022

This page is an aggregate of all OER topics onto a single page for more convenient HTML viewing.

macOS Hardware Recommendations

Endpoints should comply with all hardware requirements for the OS you are running. Consider all processes
hardware configuration. Only industry standard desktop, laptop, or notebook computers and server hardwa
require additional qualifications. Please contact VMware Carbon Black Support for additional information.

Product: Endpoint Standard on macOS

Metric	Endpoint Standard	Endpoint Standard + Audit & Remediation	Endpoint Standa
CPU	Any supported x86-64 or arm64*	Any supported x86-64 or arm64*	Any supported

        - In HTML, improved search engine optimization (SEO)
        - In PDF, improved the title page and table of contents
    - Updated product OERs with consistent architecture.
        - UEX Redirects:
            - On April 14th, redirects will be added to each affected UEX page.
            - On May 13th, content in respective UEX pages will be deleted. Only redirects will remain.

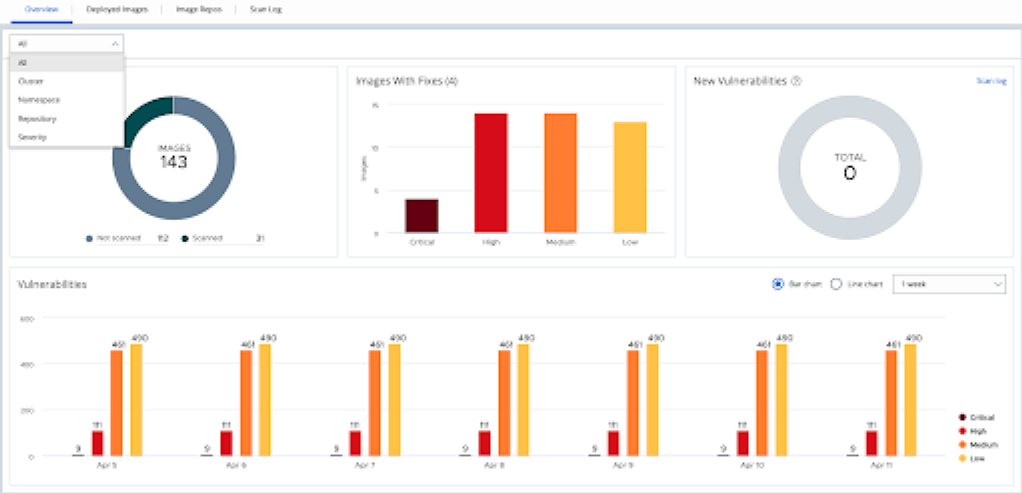
- **Under the Console Help menu, added a link to the Carbon Black Tech Zone (CB TechZone)**

- **Container Essentials: Image Vulnerability Dashboard**

  The dynamic nature of Vulnerability management in cloud-native environments can make it difficult to control the state of different areas or applications, and can require pulling data from multiple sources. With the new image vulnerability, the active dashboard is improved. The new dashboard helps you continuously analyze the vulnerability state of your environment based on scan status, severity, and it highlights fixes. With the new Vulnerability widget, you can easily detect new vulnerabilities introduced in the last 24 hours to ensure nothing slips. Combined with the Kubernetes-driven filters, where you can focus your view on the important areas like clusters, namespaces, or different repositories, your vulnerability management is now easier.

  See **Container images -> Overview** tab.

Figure 23-1.



For a video regarding recent changes to VMware Carbon Black Cloud Container, see What's New with Vulnerability Dashboard, Backend Version 0.77.

Resolved Issues - 14 April 2022

24

The following issues were fixed in this version of the software.

Note: To see issues resolved in previous releases, see Archive of 2022 Improvements and Resolved Issues.

This chapter includes the following topics:

- All
- Endpoint Standard
- Container Essentials

All

- **DSER-39468: Fixed Grouping Result search issue**
- **CBCUI-637: While signing In, Sign-in button gets disabled with loading icon**
- **CBCUI-633: Adjusted the Sensor release link (Endpoints->Download kits)**
- **CBCUI-508: Sidepanel process card displays IOCs using TTP components**
- **CBCUI-573: Fixed selection of Policy on new Live Query and its scheduling**
- **CBCUI-669: Reduced footprint of momentJS date-time library**
- **CBCUI-649: Fixed log error from GET_LIVE_QUERY_DEVICES_SUMMARY_SUCCESS**
- **CBCUI-663: Fixed log exception: Cannot read properties of undefined (reading 'get'):**
- **DSER-38810: Assigned policy modal defaults to Automatic assignment selection instead of showing current selection**

- **DSER-38817: Added more sensor state/bypass descriptions to side panel**

- **DSER-34381: Alert Triage Process Tree Blank Processes**

Endpoint Standard

- **N/A - Efficacy Improvement - Added a new detection related to Jupyter Infostealer**

- **EA-20637: Efficacy Improvement - Windows code injection monitored detections**

  Changed some Windows code injection monitored detections to no longer alert, but still tag events with relevant TTPs to reduce unwanted alerts.

- **DETECT-2643: Efficacy Improvement - low severity score macOS and Linux monitored detections**

  Changed some low severity score macOS and Linux monitored detections to not alert, but tag events with relevant TTPs to reduce unwanted alerts.

Container Essentials

- **KRS-1068: Reset policy learning period upon enabling the policy**

- **KRS-1054: Rules started learning even when saved as draft**

- **GRC-2022: Fixed counter mismatches in the facet in the K8s clusters page**

- **GRC-2003: Workloads violation details did not show disabled policy violations**

- **GRC-1884: Improvements in scope selection in the policy creation flow**

What's New - 17 March 2022

25

Note: To see changes made in previous releases, see Archive of 2022 Improvements and Resolved Issues.

The 17 March 2022 release includes bug fixes and enhancements.

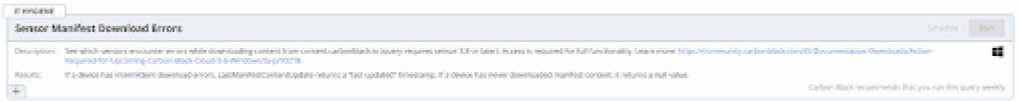
- **Audit and Remediation**

  Two new Recommended Queries have been added to the New Query page.

  Sensor Manifest Download Errors

  This query locates sensors that encounter errors while downloading content from content.carbonblack.io. This query requires Windows sensor version 3.8 and higher.

  Figure 25-1.



Sensor Manifest Download Errors

Description: See which sensors encounter errors while downloading content from content.carbonblack.io (query requires sensor 3.8 or later). Access is required for full functionality. Learn more: https://community.carbonblack.com/t5/Documentation-Downloads/Action-Required-for-Upcoming-Carbon-Black-Cloud-3-6-Windows/ta-p/93218

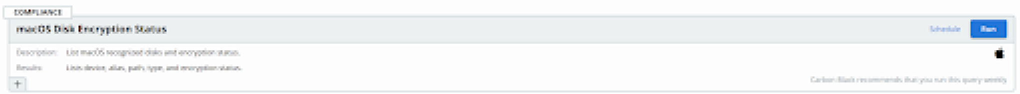
Results: If a device has intermittent download errors, LastManifestContentUpdate returns a "last updated" timestamp. If a device has never downloaded manifest content, it returns a null value.

Carbon Black recommends that you run this query weekly

  macOS Disk Encryption Status

  The query will list macOS disk devices and their current encryption status.

  Figure 25-2.



macOS Disk Encryption Status

Description: List macOS recognized disks and encryption status.

Results: Lists device, alias, path, type, and encryption status.

Carbon Black recommends that you run this query weekly

Resolved Issues - 17 March 2022

26

The following issues were fixed in this version of the software.

Note: To see issues resolved in previous releases, see Archive of 2022 Improvements and Resolved Issues.

This chapter includes the following topics:

- All
- Endpoint Standard
- Audit and Remediation

All

- **DSER-38259: Enhanced bulk device policy change to properly report operation status using Notifications for Success and Failure**

- **DSER-34842: Improved clarity in the Policy section of the Endpoints page's filter panel when an endpoint has been deregistered and its policy has been deleted**

- **DSER-38481: Endpoints UI Export: blank email column**

- **DSER-38481: Fixed CSV exported from Endpoints page to contain proper User Information in the loginUserName column**

- **DSER-35501: Fixed sensor logs data retention to meet the GDPR requirements**

- **DSER-39177: Endpoints UI Export: not exporting "deploymentType": "AWS"**

- **DSER-39177: Fixed AWS Instances not appearing in Export CSV results in Endpoints**

Endpoint Standard

- **DETECT-2612: Efficacy improvement - Endpoint Standard cloud detections now set MITRE ATT&CK v10 TTPs**

- **DETECT-2640: Efficacy improvement - Raised the threshold on when to create alerts for scanning behavior**

  Raised the threshold on when to create alerts for scanning behavior. This should reduce the volume of alerts while still tagging the events with relevant TTPs.

- **EA-20809: Efficacy improvement - Fileless behavior**

  Adjusted the severity scores for monitored Fileless behavior to account for the expanded definition of fileless on the Windows 3.8 sensor.

Audit and Remediation

- **DSER-37931: Free Disk Space on Linux/macOS**

  The recommended query for "Free Disk Space on Linux/macOS" sometimes returned inaccurate numbers. The query now shows accurate numbers. Used and remaining space values are returned as a percentage.

What's New - 28 February 2022

27

- **Bypass mode**

  Additional bypass reasons have been added to the user interface. For a complete list, see https://community.carbonblack.com/t5/Knowledge-Base/Carbon-Black-Cloud-What-are-the-Sensor-Bypass-Reasons-and/ta-p/111310.

- **MITRE TTPs**

  The latest release of Carbon Black Cloud introduces new MITRE TTPs, both new techniques and sub techniques, throughout the platform as specified in MITRE ATT&CK v10. **Starting in early March 2022**, Carbon Black Cloud will begin to emit the successor MITRE TTPs whenever we set their corresponding deprecated MITRE TTPs.

  On March 6th, 2023, we will remove the deprecated MITRE TTPs from our products completely. Deprecated MITRE TTPs will no longer be emitted from the Carbon Black Cloud and will no longer be selectable when creating or editing a notification from Settings > Notifications page in Carbon Black Cloud. For more information see our full update.

- **Container Essentials**

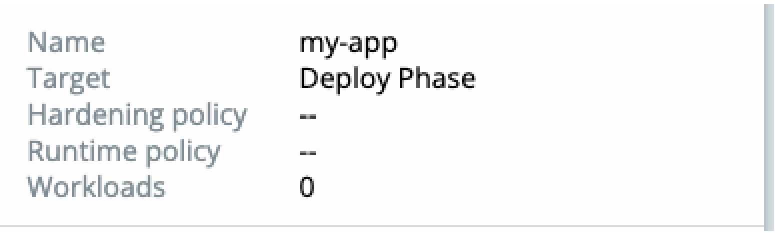
  We are announcing the general availability of Container Runtime Security for VMware Carbon Black Container. This release includes many new features and capabilities, which are available with the Container Advanced bundle. With this new release, you can quickly identify any network anomaly that happens in the cluster and get alerts on a consolidated alert page. The primary detected anomalies are Egress, Internal, and Ingress in a workload level, and Egress connections with IP reputation in a cluster and scope level. In addition, you can detect malicious activity such as internal or external port scanning.

New Container Advanced security capabilities include:

- **Kubernetes Visibility Mapping:** Allows DevOps and security teams to quickly understand the architecture of an application that was set pre-deployment to better identify egress destination connections, potential workload policy violations, and vulnerable images.
- **Anomaly Detection:** Leverages artificial intelligence to standardize networking modules and alert SecOps teams on any deviation from that module, which is critical when setting up new workloads.
- **Egress and Ingress Security:** Provides security teams with added visibility into the external source that is reaching out to the Kubernetes service and easier detection of malicious egress connectivity based on the IP address and the behavioral data.
- **Threat Detection:** Allows customers to scan open ports to check for vulnerabilities and quickly see if there is a lateral attack in progress. If an attacker tries to exploit a vulnerability to find the next lateral move, the internal port scan and egress port scan will raise an alert.
- **Integrated Alerts Dashboard:** Provides a single pane of glass for security teams to view events and address anomalies in their runtime environment.

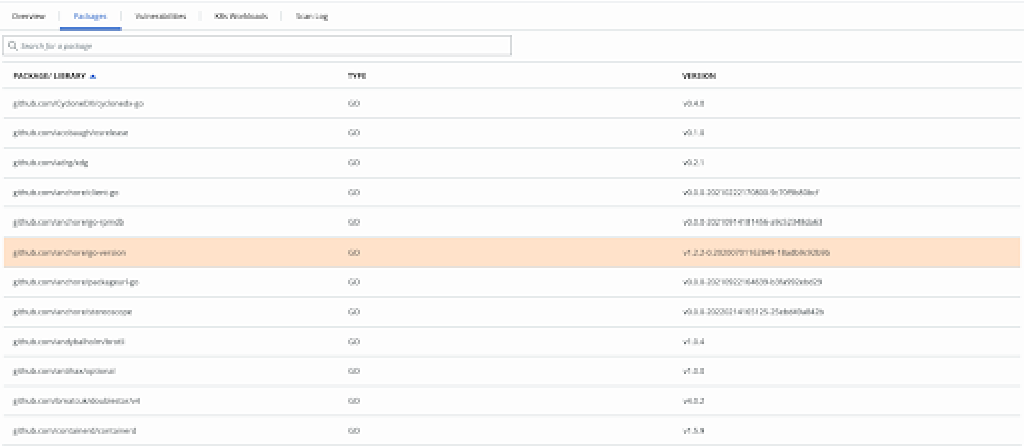
New Container Essentials capabilities include:

- **Runtime Cluster Image Scanning:** To ensure that your container image doesn't contain any vulnerabilities, images must be scanned throughout the entire application lifecycle. Our new image scanning feature is not just limited to CI/CD scanning but also allows you to scan images in production. The ability to scan through the runtime layer gives security and DevOps teams visibility to vulnerable images in images that were not previously scanned, and images deployed from any third-party registries.
- **Workload Deployment Controls Policy:** Kubernetes is the de facto developer platform that helps delegate many of the responsibilities previously owned by operation teams that empower developers to deliver in their own cadence. But how can you make sure this power is not abused by adversaries? The addition to the workload deployment control rules allows you to deny deployment of new resources to sensitive areas such as kube-systems or default namespace to follow best practices. This feature is at **Kubernetes Policies > Hardening Policies** in the console.
- **User Exception Policy:** The new user exception rule allows for the admin to create exceptions for a specific user based on their account username. This feature will help teams mitigate alerts coming from ClusterRoleBinding in GKE.
- **PowerShell Script for the Operator Installation:** A sensor installation script is now available with PowerShell to enable sensor configuration from a Windows-based OS.
- **Workload Count for Scope Cards:** Scopes are dynamically selected groups of workloads used for policies and filtering. The dynamic nature of the allocation of these scopes can be confusing or even misleading. The newly added scope card is designed to provide more information about the different policy allocation and workload to bring all the relevant information to you exactly when you need it. This feature can be accessed by going to **Inventory > Kubernetes > Scopes.**



Name	my-app
Target	Deploy Phase
Hardening policy	--
Runtime policy	--
Workloads	0

- **Sensor Component Additions:** The introduction of Kubernetes DaemonSet highlights the need to fine-tune the agent's pod scheduling across the different nodes in the environment. With the ability to add tolerations, affinity, and the nodeSelector to your sensor components, you can easily configure the agent to fit your needs. You can read more details on GitHub here.
- **Export Vulnerability information by PDF/CSV:** To increase visibility and improve operational efficiency, you can now export vulnerability information into a PDF or CSV file directly in the console.
- **Runtime Cluster Image Scanning:** To ensure that your container image doesn't contain any vulnerabilities, images must be scanned throughout the entire application lifecycle. Our new image scanning feature is not just limited to CI/CD scanning but also allows you to scan images in production. The ability to scan through the cluster layer gives security and DevOps teams visibility to vulnerable images in images that were not previously scanned, and images deployed from any third-party registries.
- **List go modules and find their vulnerabilities:**Not only does our image scanning feature now include runtime cluster image scanning capabilities, but also includes the ability to list and identify go module vulnerabilities.



PACKAGE/ LIBRARY ▲	TYPE	VERSION
github.com/CycloneDX/cyclonedx-go	GO	v0.4.0
github.com/acobaugh/osrelease	GO	v0.1.0
github.com/adrg/xdg	GO	v0.2.1
github.com/anchore/client-go	GO	v0.0.0-20210222170800-9c70f9b80bcf
github.com/anchore/go-rpmdb	GO	v0.0.0-20210914181456-a9c52348da63
github.com/anchore/go-version	GO	v1.2.2-0.20200701162849-18adb9c92b9b
github.com/anchore/packageurl-go	GO	v0.0.0-20210922164639-b3fa992ebd29
github.com/anchore/stereoscope	GO	v0.0.0-20220214165125-25ebd49a842b
github.com/andybalholm/brotli	GO	v1.0.4
github.com/antihax/optional	GO	v1.0.0
github.com/bmatcuk/doublestar/v4	GO	v4.0.2
github.com/containerd/containerd	GO	v1.5.9

Cbctl

The cbctl command-line tool, based on the open source syft, is now up to date to the latest version with the following noticeable enhancements:

- Add Pipenv support (Pipfile.lock) #242
- Enhance CPE generation to improve downstream matching in grype #471
- Allow syft to populate distro data for all types #499

  - Updated the distro package to include SLES #489
  - Modify CPE vendor candidate generation approach #484
  - Catalog Go modules used in Go binaries #434
  - Capture additional go package data #540
  - Stabilize package identifier based on contents #363
  - Support for PHP/composer installed.json files #642
  - Adding AlmaLinux OS Support #652
  - pip should support vcs url #679
  - support .par for java ecosystems #727
  - Add support for searching for jars within archives #734
  - Add lpkg as java package format #682
  - Add additional PHP metadata #753
  - Remove strong distro type #342
  - Support more java artifact extensions #728
  - Add distro information to package URLs for OS packages #754
  - Encode upstream qualifier on OS package pURLs #769

- **Managed Detection**

  VMware Carbon Black Cloud Managed Detection and **Managed Detection and Response** customers can now subscribe to a daily report through email. The report outlines all Endpoint Standard or Workload Advanced alerts within the service level objective (SLO) for Managed Detection.

  Alerts are classified into 4 categories:

  - **Likely Threats** - A likely true threat in your environment that may require your remediation.
  - **Unlikely Threats** - An unlikely threat in your environment. Alerts in this category are often trusted applications that operate similarly to malicious actors (such as vulnerability scanners).
  - **Not Reviewed** - Alerts within the SLO that were not reviewed by Managed Detection and may require your remediation.
  - **No Threat** - Does not represent a true threat within your environment. Alerts in this category are grouped. Search for the Threat ID on the Alerts page in the Carbon Black Cloud to return all alerts within the group. Action can be taken to refine policy or reputation configurations to reduce future instances of these alerts.

To configure the report, enable the **Daily Summary** for recipients on the **Settings > Managed Detection** page.

Resolved Issues - 28 February 2022

28

The following issues were fixed in this version of the software.

- **GRC-1994: Container Essentials - Compress SBOM to scan large images**
- **GRC-1719: Container Essentials - Digested images could not be scanned with runtime cluster-scanner**
- **GRC-1899: Container Essentials - Fixed a bug in policy rule enforcement of workloads with an owner**
- **GRC-1876: Container Essentials - Fixed errors when editing notification hooks (Settings > Notifications > Kubernetes tab)**
- **GRC-1748: Container Essentials - User data was missing from violation details (Harden > K8s Violations)**
- **CWP-9462: Workloads - Not Enabled Tab Facet filter selection no longer marks other values as 0**
- **DSER-35390: Endpoint Standard - Brought the Windows sensor and Cloud detections into alignment to improve fileless behavior detection**
- **DSER-35514: Export DeviceId on Endpoints page was not working**
- **DSER-32435: Inconsistent OS Criteria in Sensor Group Rules**

  Sensor groups including endpoints did not match the group criteria when the OS limit was more specific than Windows/macOS/Linux.
- **DSER-34605: Could not edit users without a grant**

Prior to this change, if a user was missing a grant, they would not be able to log in or be edited by another user. This would result in the user having to be deleted. Now the user can be edited to assign a role and create a grant upon save.

- **DSER-36029: Audit log entries for removal of Reputation Trust overrides on the Reputation user interface lacked sufficient detail to review the action**

- **DSER-33425: Audit log entries for removal of Reputation Trust overrides on the Reputation user interface lacked sufficient detail to review the action**

What's New - 24 January 2022

29

The 24 January 2022 console release includes various bug fixes.

Resolved Issues - 24 January 2022 30

The following issues were fixed in this version of the software.

- **DSER-37462: "Equality" type IOCs for certain fields (for example, process hash, netconn_ipv6, etc.) are combined for optimized evaluation**

  Before this fix, only one IOC would trigger a hit, even if there were more IOCs for the same field with the same value. After the fix, all IOCs for the same field with the same normalized value will produce a hit, regardless of whether the IOCs are in different reports or the same report.

- **DSER-35926: Modified email notifications to include an Alert Type selector, which includes a new container runtime option**

- **DSER-38285: Dashboard to Vulnerability filters were not showing properly**

What's New - 13 January 2022

31

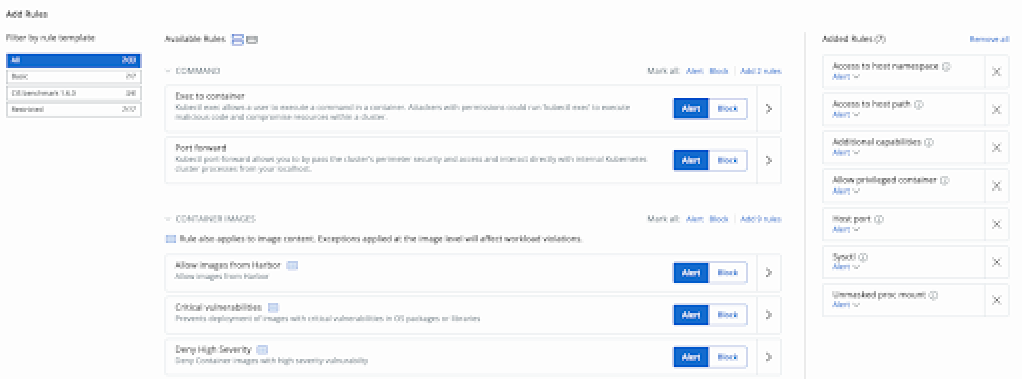
- **Container Essentials**

  New Policy and Scope Experience

  Policy Rule Selector

  To address the continuing growing number of policy rules, we are introducing an enhanced rule selection experience. With the new design, you can easily browse through all available rules using filters, and organize and manage the selected rules to better understand policy impact. Check it out in **Enforce -> K8s policies**.

  Figure 31-1. K8 Policies

  Add Rules

  Filter by rule template

  - All
  - Basic
  - CIS benchmark 1.6.0
  - Restricted

  Available Rules

  COMMAND — Mark all: Alert Block | Add 2 rules

  Exec to container
  Kubectl exec allows a user to execute a command in a container. Attackers with permissions could run 'kubectl exec' to execute malicious code and compromise resources within a cluster.

  Port forward
  Kubectl port-forward allows you to by pass the cluster's perimeter security and access and interact directly with internal Kubernetes cluster processes from your localhost.

  CONTAINER IMAGES — Mark all: Alert Block | Add 9 rules

  Rule also applies to image content. Exceptions applied at the image level will affect workload violations.

  Allow images from Harbor
  Allow images from Harbor

  Critical vulnerabilities
  Prevents deployment of images with critical vulnerabilities in OS packages or libraries

  Deny High Severity
  Deny Container images with high severity vulnerability

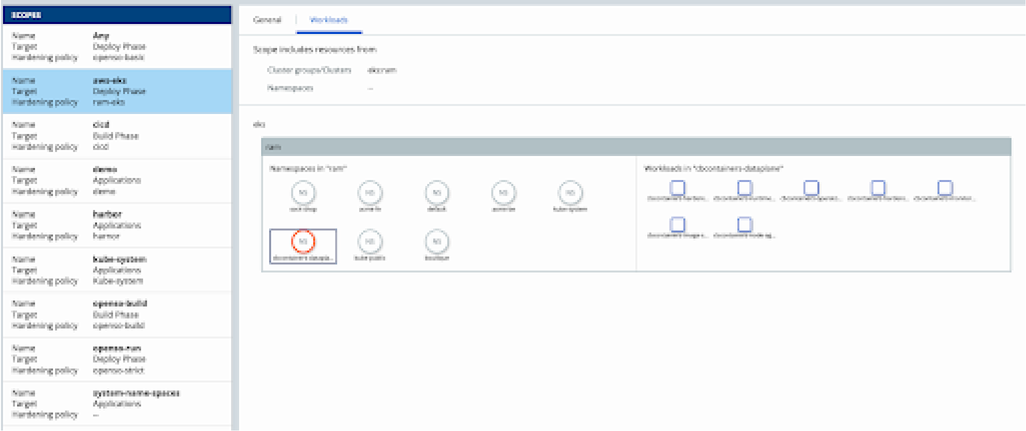
  Added Rules (7) — Remove all

  - Access to host namespace — Alert
  - Access to host path — Alert
  - Additional capabilities — Alert
  - Allow privileged container — Alert
  - Host port — Alert
  - Sysctl — Alert
  - Unmasked proc mount — Alert

  Scope Page

  What is the workload scope type? How many namespaces are included in the scope and which workloads? What is the policy assigned to the scope? These are questions we often get when trying to manage the scope. With the newly designed page, we addressed it all! With a new modern look, you can easily identify the scope by its type, the assigned policy, and even the clusters, namespaces, and workloads assigned to it. Check it out at **Inventory-> Kubernetes-> Scope**.

Figure 31-2. Scope



- **Endpoint Standard**

  API decommissioning - v3 Alerts, Events and Process APIs

  After 31 January 2022, the v3 Alerts, Events and Process APIs will be decommissioned. After this date, they will return an HTTP Response of "410 GONE" and will no longer return previously available data.

  For more information, see this October 2021 announcement on the Carbon Black User Exchange: https://community.carbonblack.com/t5/Developer-Relations/Upcoming-API-shutdowns-Carbon-Black-Cloud-v3-Events-Alerts-and/td-p/107722

  Efficacy Improvements

  Endpoint Standard customers will see an increase in default prevention value. TAU provides improved detections and fixes for AMSI Threat Intelligence, Privilege Escalation, CarbonBlack Threat Intelligence, and Credential Theft.

  - AMSI Detection - Inhibit System Recovery behaviors – Filebacked
  - AMSI Detection - Inhibit System Recovery behaviors – Fileless
  - Detect Suspect SAM Credential Access – Filebacked
  - Detect Suspect SAM Credential Access – Fileless
  - Detect Suspect Browser Credential Access
  - Detect bitsadmin file transfer
  - Detect bitsadmin execution
  - Detect Suspect Startup Modifications
  - Detect parent process identifier (PPID) spoofing
  - Detect suspect registry changes

- **VMware Carbon Black Cloud**

The Dashboard now supports modeless editing. There is no longer a need to click **Edit** before moving and resizing widgets; it can be done without entering an edit mode.

Resolved Issues - 13 January 2022

32

The following issues were fixed in this version of the software.

- **DSER-36396: Clicking on the Basic button twice toggled the Filter Data section between Basic and Custom Query**

- **DSER-37701: Endpoints page crashed when updating all sensors without a proper searchDef**

- **DSER-37956: Data Forwarder user interface inaccurately reported connection test was successful**