# VMware Carbon Black Cloud on VMware Cloud Services Platform Release Notes - 2023 Archive

VMware Carbon Black Cloud on VMware Cloud Services Platform

**vmware®**
by **Broadcom**

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

https://docs.vmware.com/

# Contents

# Introduction

<div style="text-align: right; color: #ccc; font-size: 3em;">1</div>

VMware Carbon Black Cloud on VMware Cloud Services Platform | 03 JAN 2024

Check for additions and updates to these release notes.

# Archive of 2023 Improvements and Resolved Issues

# 2

This section contains the information regarding all 2023 releases prior to this release.

**Note**  To view the changes made in 2022, see: VMware Carbon Black Cloud on VMware Cloud Services Platform Release Notes - 2022 Archive.

# What's New - 14 December 2023

# 3

**Build 1.21**

To see changes made in previous releases, see VMware Carbon Black Cloud on VMware Cloud Services Platform Release Notes - 2022 Archive.

This release includes:

Read the following topics next:

- API Keys
- Alerts
- Data Forwarder
- Endpoint Standard
- Facet Field Customizations
- Workloads

## API Keys

- **Custom API Keys now support Authorized IP Addresses**

    You can configure 'Custom' access level API keys to specify IP addresses that are authorized to send requests. This allows you to restrict the use of an API key to specific IP addresses or IP address ranges.

- **Inventory Export**

    There is a new API request to export devices. See the developer network discussion here for details. This API request deprecates Legacy Export Devices (CSV).

    Changes to the CSV output are the following:

    a   Additional device related data.

    b   Use the snake case naming convention for column names instead of camel case.

    c   Reordering of columns.

Additional device data includes columns that correlate with the recent release of Asset Groups. Temporarily, the names of the Asset Groups columns are **groups_id**, **groups_name**, and **groups_membership_type**. However, in preparation for referencing Asset Groups in other pages within the Carbon Black Console, these names are transitioning to **asset_group_id**, **asset_group_name**, and **asset_group_membership_type**.

Most of the changes in naming convention are minor, including:

- **deviceId** is now **device_id**

- **osVersion** is now **os_version**

There are some changes to align with the **_search** API response:

- **deviceType** is now **os**

- **targetValue** is now **target_priority**

- **vcenterHostName** is now **vcenter_name**

# Alerts

- **Enhancements to Alert Email Notifications**

  To align email notifications with the new alert experience and fields available in the V7 Alerts API, Carbon Black is excited to announce that enhancements to alert email notifications are rolling out over the next few weeks to all email notification rules. Carbon Black is introducing additional fields such as parent and child process information, process username, MITRE ATT&CK information, and other highly requested pieces of alert metadata. These new fields provide a greater alert context directly from the email notification and help reduce initial triage time prior to entering the console. In addition to these initial field updates, please be aware that there are additional email notification enhancements and field updates planned for a later date. These updates might result in additional fields becoming visible in the email notification.

- **Export to PDF Option for Individual Alerts**

  You can now export alert details to PDF for long-term record keeping.

  From the Alerts page, select an alert to open the alert details pane. In the upper left of the pane, click **Export**. After 5 - 10 seconds, the PDF displays in your browser downloads.

  - The file name format is *Alert_Report_{alert_id}_{date}.pdf*

  - The PDF contains a page break between each alert details section

  - You can only export a single pdf at one time

# Data Forwarder

- **Data Forwarder Now Supports Forwarding XDR Events**

As an XDR customer, you now have the option to upgrade or add an Endpoint Events Data Forwarder to send XDR-enhanced events data out of the Carbon Black Cloud. This enhancement also enables all Endpoint Event Forwarder users to opt-in for automatic upgrades of their Forwarder to future additions to the Endpoint Event data schema, and control the types of upgrades they are willing to automatically adopt (and which types of upgrades they will perform manually).
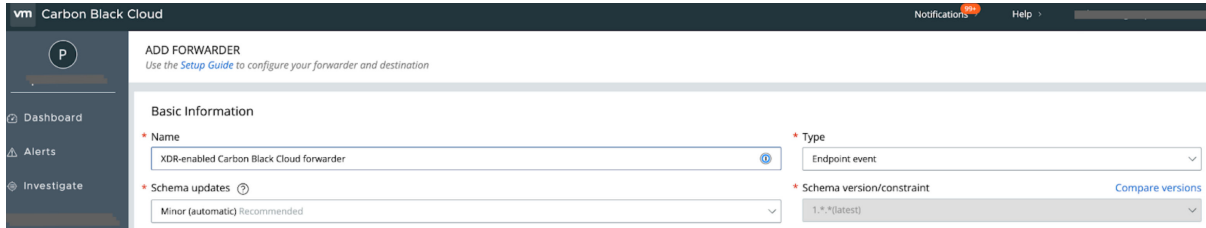


- You can find further information on what this new Endpoint Event Forwarder option means to existing and new Data Forwarder here.

- The complete v1.1.0 Endpoint Event schema is documented here.

- The Carbon Black Cloud Data Forwarder commitment to support Semantic Versioning is outlined here.

# Endpoint Standard

- **Device Control - Separation of Read, Write, and Execute Controls**

  Carbon Black Cloud gives visibility and control over USB mass storage devices detected in your environment with the ability to block untrusted devices and approve trusted devices. The pre-existing implementation of Device Control blocks all operations on any external device. This enhancement allows users to separate read, write, and execute permissions for approved devices on Windows endpoints. You can determine whether a device must be approved for *read-only*, *read + write*, *read + execute*, or *read + write + execute*.

# Facet Field Customizations

- **Asset Groups**

  Organizations using Asset Groups can customize what filters are shown on the Endpoints, VDI Clones, VM Workloads and Public Cloud pages.
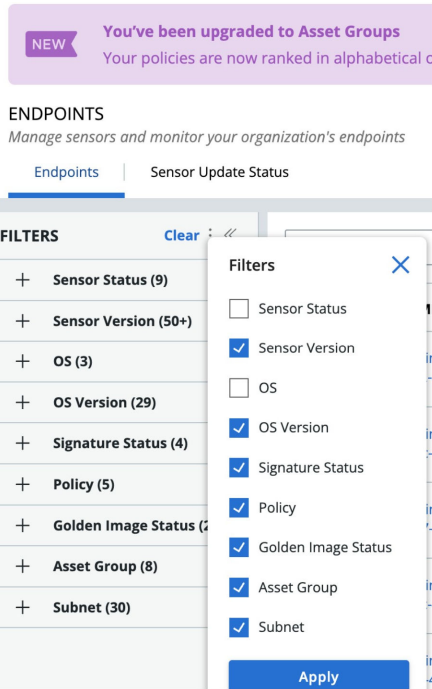
# Workloads

- **CIS Benchmarking for GCP and AZURE Cloud Assets are supported from this release**

  The CIS Benchmarks now support Google Cloud Platform (GCP) and Azure Instances having Windows sensor version 4.0.0.1292. This feature currently supports the following Windows Servers: Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, and Windows Server 2022. This feature is accessible to all Workload customers.

  The CIS Benchmarks recommendations tab now allows users to select whether to view All Assets, VM Workloads, AWS Instances, GCP Instances, or Azure Instances. On the left navigation pane, you can choose from All Assets, VM Workloads, AWS Instances, GCP Instances, or Azure Instances in the asset type drop-down menu. After selecting the asset type, the compliance values reflect the selection, and all tabs display the chosen asset type.
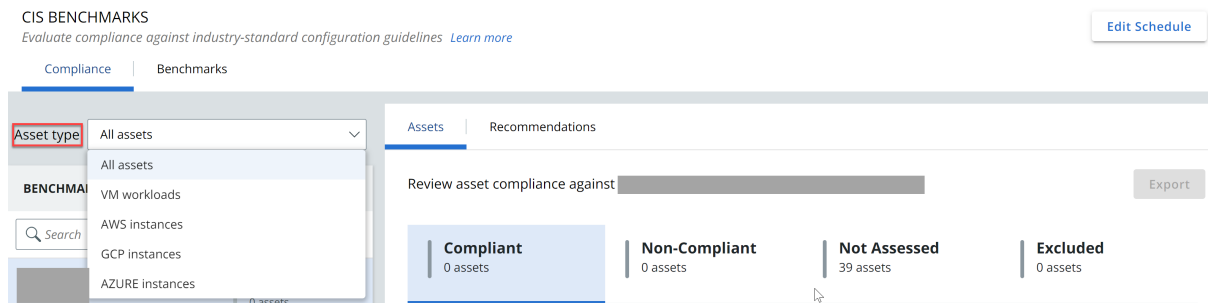
  

- **Azure and GCP workload support for Windows sensor**

The VMware Carbon Black Cloud Workload for Public Cloud now provides the ability to secure Azure and Google Cloud (GCP) workloads while simplifying the overhead of Azure subscriptions and GCP projects management.

Core capabilities include:

- Single and multiple Azure subscription and GCP project management.

- Auto-generated CI-CD agent installation packages.

- Enhanced visibility into inventory of protected and unprotected workloads.

- **Multi-account onboarding for Azure and GCP organizations**

  Cloud administrators or cloud account owners can onboard all Azure or GCP member accounts under an Azure Management Group or GCP organization by providing the App registration details of the Azure or service account of GCP management account with security audit policy. Carbon Black Cloud assumes the role to retrieve the member accounts and list them in the console.

# Resolved Issues - 14 December 2023

4

- **CBCUI-4879: Fixed an issue where the Japanese version of the Search Guide translated several search fields to Japanese**

    In the Carbon Black Cloud console, when the console language was set to Japanese, certain search fields in the Search Guide for both the **Alert** page and **Investigate** page were translated into Japanese. The issue was fixed because Carbon Black currently does not support Japanese search fields.

- **DSER-50870: Fixed issue that could result in assets matching Asset Group Dynamic criteria not properly joining the group when a group's criteria was manually updated**

- **CBCUI-4457: Organizations using Asset Groups can customize which Filters are shown in their Endpoints, VDI Clones, VM Workloads and Public Cloud pages**

- **DSER-50376: Asset Group Audit Log contains IP address information**

    In previous versions, some of the Asset Group Audit Log related entries are missing IP address information. Those entries now contain IP address information.

- **DSER-50806: Incorrect fields in the Inventory group facets**

    Fixed an issue where customers with MSM groups that have migrated to Asset Groups may have seen incorrect fields in the Inventory group facets. This issue impacted search and facet results, but did not affect group membership.

- **CBCUI-4776: Updates Policy information pawn in the Asset Groups details page to explain how policy ranking impacts the policy being selected**

# Known Issues

# 5

The items listed below are the known issues at the time the software version was released.

For items specific to Carbon Black Cloud on the VMware Cloud Services Platform, see the section Issues Specific to Carbon Black Cloud on the VMware Cloud Services Platform.

All other issues listed in the remaining sections apply to the core Carbon Black Cloud product.

Read the following topics next:

- API Key
- Carbon Black Cloud - All
- Container Essentials
- Endpoint Standard
- Enterprise EDR
- Issues Specific to Carbon Black Cloud on the VMware Cloud Services Platform
- Workloads
- XDR

## API Key

- **EA-24040: Mismatch with the CSV export data compared to the console between Nov 22 and Nov 24**

## Carbon Black Cloud - All

- **DSER-50283: Currently, the right rail of the Alert Triage page is not wrapping correctly**

  The command-line is visable if you scroll to the popout icon.

- **DSER-49788: Although the API is successfully fetching results for customers who have enabled APC uploads, they are not being displayed in the Cloud Analysis user interface**

- **DSER-49561: There is a reported anomaly on the Watchlists page in the Processes tab**

The report name is not populating correctly; it appears as "(Deleted)."

■ **DSER-48447: If a user tries to perform a bulk action to put sensors into bypass mode the audit log does not update if a sensor fails to move into bypass**

■ **DSER-47090: An alert with 4758 events is preventing the generation of an alert triage tree, leading to a visually cluttered page with numerous lines and ultimately causing browser crashes**

■ **DSER-46519: Currently users will not be able to find audit logs for downloading files from Inbox**

■ **DSER-45780: Endpoint Standard only environments are experiencing inconsistencies in hash signatures displayed across the following pages; alert page: alert detail VS alert triage**

■ **DSER-42250: Carbon Black encountered connectivity issues with certain endpoints receiving Maintenance mode responses instead of the correct response because device data was absent from the backend**

To resolve this, customers are required to manually uninstall these sensors.

■ **DSER-41165: Occasionally, the sensor sends 0s for the local IP or remote port, resulting in the UI displaying unexpected characters**

■ **DSER-40080: Updated reputation values are sometimes not reflected on the Malware Removal page**

Known malware that has the reputation changed to *Trusted Whitelist* or *Company* approved still appears on the malware removal page.

■ **DSER-31717: In release v22, Carbon Black Support does not initiate and sensor Update Sensor Requests in customer organizations**

■ **CBCUI-4724: Policy permissions file path deletes if no actions are selected**

When no actions are selected on existing policy rules, the Policy Permissions Paths are deleted.

■ **CBC-27346: Console does not display selected set of TTPs while updating a TTP rule**

When updating a TTP (Tactics, Techniques, and Procedures) rule type, the console does not display the previously selected set of TTPs. This behavior contrasts with console's ability to show previously selected watchlists when updating watchlist rules.

■ **DSER-42250: Sensor receives maintenance mode response when trying to authenticate**

Customers can experience connectivity issues with certain endpoints receiving a maintenance mode response instead of the correct response if device data is absent. To resolve the issue, customers must manually uninstall these sensors.

Associated with: EA-21807, EA-20280.

- **CBCUI-2937: Export feature on Observations page**

  The export feature on Observations page does not export the grouped counts and results when you have selected a **Group By** summary.

- **DSEN-21949: On the Observations tab ports are incorrectly swapped on certain netconns**

- **LC-2903: Investigate search doesn't warn the user when they search using a field that isn't indexed for that tab's API**

- **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.

# 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.

  Workaround: 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)**

- **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.

# Endpoint Standard

# Enterprise EDR

- **DSEN-23853: netconn_inbound field is always set to false for IDS observations**

- **DSEN-23733: EEDR hash banning does not work for processes that are already running**

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

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

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

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

## Issues Specific to Carbon Black Cloud on the VMware Cloud Services Platform

- **CBC-17603: Avira upload for Reputation will not be available upon release due to a bug regarding timing out of malware reporting, causing false negative results**

  This means the ability to opt-in to automatically upload potential malware to Avira will be temporary disabled.

- **CBC-17619: Some API permissions have an incorrect name, using "threathunter" in place of "org"**

- **CBC-17721: The integrationServices routes for audit logs and notification APIs are not yet available**

  This only affects the API calls, and not the Notifications via email or the ability to view Audit Logs in the Carbon Black Cloud console.

## Workloads

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

- **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.

- **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.

# XDR

- **CBCUI-3007: Observations Alert Details**

  Clicking the Close action on an Observation's Alert Details right pane closes the Alert but the console incorrectly says there was an error.

- **DSEN-23805: Windows 3.9.1 MR1 sensor does not report TLS properties for IDS alerts**

- **CBC-26691: netconn_tls_cipher doesn't return or index a human-readable cipher suite value**

- **DSER-45927: XDR-enabled Alerts page doesn't support searching on type: INTRUSION_DETECTION_SYSTEM**

# What's New - 16 November 2023

<span style="color:gray; font-size:3em">6</span>

**Build 1.20**

To see changes made in previous releases, see Chapter 2 Archive of 2023 Improvements and Resolved Issues and VMware Carbon Black Cloud on VMware Cloud Services Platform Release Notes - 2022 Archive.

This release includes:

Read the following topics next:

■ Alert Triage Page

■ Containers

■ Enterprise EDR

■ New Tools

## Alert Triage Page

■ **Better visibility of file events on the Alert Triage tree**

Alert Triage page includes a visual tree diagram that highlights all alert-related inter-process, process-to-network and process-to-file operations. Carbon Black Cloud has improved visibility in this tree to ensure visibility of all *filemod* operations that report on scanned files, renamed files, detected ransomware operations and suspicious dropped files.

The following image displays an example of the way Alert Triage can visualize all such *filemod* operations:
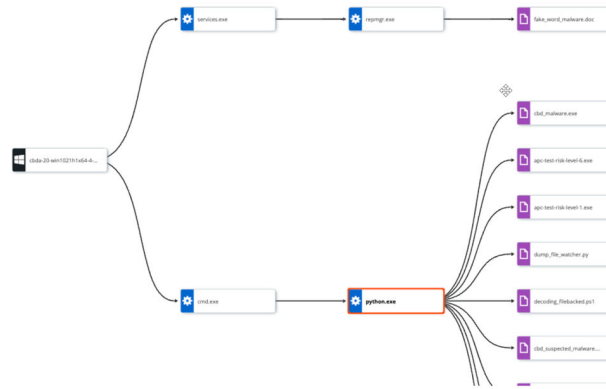
# Containers

- **API for Container Setup has been published**

  An API for container setup has been published to automate the installation and monitoring of Container Security functionality. More information and details about the API are on the Developer Network, Announcing the Setup API for Carbon Black Cloud Container Security.

- **Protecting containers running on standalone and ECS environments**

  Carbon Black Cloud is excited to extend Container support to additional platforms beyond Kubernetes. The new Non-Kubernetes sensor enhances security in container environments outside of Kubernetes, offering critical features:

  - **Containerized Sensor:** A dedicated sensor to ensure security in diverse container orchestration platforms like Amazon EKS, and Docker Enterprise.

  - **Enhanced Visibility:** Comprehensive image scanning for vulnerabilities, secrets, and malware.

  - **Detect and Respond:** Seamless integration with Linux sensors for proactive threat response.

- **Windows Support for** *cbctl*

  Carbon Black is pleased to announce the addition of native Windows binary support for *cbctl*. This update is tailored for DevOps and DevSecOps professionals who require *cbctl* functionality on Windows platforms.

  - **Windows Compatibility:** *cbctl.exe* is now available for Windows, enabling seamless execution on Windows-based systems.

  - **User-Friendly**: Easily access *cbctl.exe* through existing binary distribution channels, simplifying integration into your workflow.

  To get started with *cbctl* on Windows, download the binary from your cluster's CLI configuration page.

- **Remote Upgrade of Kubernetes Sensor**

You can now remotely manage the Kubernetes Sensor directly from the Carbon Black Cloud console. This update streamlines operations by allowing users to upgrade or downgrade the sensor without direct administrative access to the cluster.

The key benefits are:

▪ **Operator-Managed**: Upgrades and downgrades are handled by the operator, requiring no manual intervention.

▪ **Feature Management**: The system automatically toggles supported features based on the selected sensor version.

▪ **Configuration Preservation**: The customized values remain intact, and cluster configurations are not altered during the process.

# Enterprise EDR

▪ **Exclusion of Module Load Reporting for Common, Trusted Windows Dynamic-link Libraries (DLLs)**

As of this release, module load (modload) events that are generated when a process loads a common, trusted Windows DLL are no longer reported by default. The exclusion of these modload events yields operational and performance benefits for Enterprise EDR customers. These events are safe to exclude because they are inherently normal and expected.

If you wish to undo this change, you can re-activate the collection of these modload events by enabling the 'Collect common library load events' setting on the Sensor tab of the **Policies** page.



▪ **Geolocation of Auth Event Remote IPs**

The Auth Events tab on the **Investigate** page offers a 'Remote Location' configurable filter and a 'Remote Location' configurable column, which display the geolocation associated with a public remote IP address.

# New Tools

- **New tools for integrating Carbon Black Cloud in your Ecosystem**

  - Carbon Black Cloud Python SDK 1.5.0 now has support for the Alerts v7 API.

    - https://developer.carbonblack.com/2023/10/announcing-the-release-of-v1.5.0-of-carbon-black-cloud-python-sdk/

  - Carbon Black Cloud Syslog Connector 2.0 has been released. This is a full refresh of the syslog connector to use the Alerts v7 API. It also makes it easy to configure multiple Alert conditions and multiple organizations with the more powerful configuration file capabilities.

    - https://developer.carbonblack.com/2023/10/announcing-the-carbon-black-cloud-syslog-connector-2.0.0-release/

# Resolved Issues - 16 November 2023

# 7

Read the following topics next:

- All
- Containers

## All

- **DSER-41452: Users can now use filters on Endpoints page to select from the top 200 values in each filter category**

  Associated with: EA-21470.

- **DSER-28322: Device names, in addition to device IDs, have been added to the audit logs generated by the following endpoint actions:**

  - Enable / Disable bypass
  - Quarantine / Unquarantine assets
  - Start / pause background scan
  - Manage Sensor Gateway Connection
  - Delete Hash

## Containers

- **CBC-32511: Aggregate hardening events to reduce network egress**

- **CNS-3787: Enable secret scanner by default for runtime scanning**

- **CNS-3733: Added a *pending configuration* state to health reports**

# What's New - 19 October 2023

<span style="float:right; font-size:3em; color:#999;">8</span>

**Build 1.19**

To see changes made in previous releases, see VMware Carbon Black Cloud on VMware Cloud Services Platform Release Notes - 2022 Archive.

This release includes:

Read the following topics next:

- Enterprise EDR
- Removed Observed Alerts
- Workloads

## Enterprise EDR

- **Observations Filters**

  As part of the first phase of enhancements regarding increased visibility into scripts, customers can now filter for scripts using Observations Filters, and view additional telemetry in both Observation Details and the Process Analysis table. In Process Analysis, the ability to filter for scriptloads using filters already existed, but the table for each scriptload event now has all additional telemetry.

## Removed Observed Alerts

- **Removed Observed Alerts from Email Notifications**

  Accompanying the V7 Alerts API release in June 2023, Carbon Black announced a change to Observed Alerts. Observed Alerts were events that might have had interesting security context, but were not determined to be a threat by Carbon Black. Observed Alerts were not designed to be actionable and did not require a full investigation. For this reason, Carbon Black removed Observed Alerts from the Alerts page to encourage customers to focus their energy on more pressing alerts.

For compatibility purposes only, these alerts are still present within the V6 Alerts API and the Enriched Events API. Before this release, the alerts were also present in email notifications. Due to recent console changes, customers have not been able to view those Observed Alerts in the console if navigating from an email notification. Carbon Black plans to remove Observed Alerts from the remaining legacy APIs in the coming months once the APIs are deprecated, so Carbon Black has also removed Observed Alerts from email notifications in this release. Customers no longer receive any Observed Alert email notifications from this point forward.

# Workloads

- **Multi-account onboarding (AWS Organization)**

  This feature enables a cloud administrator or a cloud account owner, to onboard all AWS member accounts under an AWS organization by providing the IAM role of the AWS management account with security audit policy. Carbon Black Cloud assumes the role to retrieve the AWS member accounts and list them in the console.

# Resolved Issues - 19 October 2023

Read the following topics next:

- [All](#)
- [Enterprise EDR](#)
- [Issues Specific to Carbon Black Cloud on the VMware Cloud Services Platform](#)

## All

- **CBCUI-4024: Investigate page excluding Observations**

  On the **Investigate** page, customers can see all observations when they select "All Available", including the previously-excluded "observations with future timestamps".

- **DSER-35532: Sensors can be updated to their current version**

  Sensors can be updated to their current version. Updating sensors schedules a sensor upgrade job for the sensor(s) listed. Upon completion of the job, the sensors remain persistently in a 'Pending Update' state, with no option to cancel. This changes improves sensor upgrade jobs to set status of sensors being updated to their current version to 'Successful Update'.

- **DSER-39404: Bulk device actions include device names for less than 200 devices**

  Bulk device actions, for example policy change, only include device names if the action is for less than 200 devices. Otherwise, only the device count is included. This change improves audit log entries to include a list of device IDs when the bulk operation is completed.

- **DSER-44788: Support for the UNINSTALL_SENSOR option**

  This change adds support for the UNINSTALL_SENSOR option for *device_actions* API using a search criteria to specify devices. This also adds support for the option to uninstall sensors on the endpoints page using the *Uninstall all # assets matching search* option, which was previously displayed in the UI but not supported by the API.

- **CBCUI-4562: The permission name for Script Deobfuscation has been updated on API Access Levels**

The permission name now displays with Category: Deobfuscation, Permission name: script deobfuscation.

- **DSER-44788: Bulk uninstall action fails when selecting sensor count greater than query row limit**

  This change adds support for the "UNINSTALL_SENSOR" option for device_actions API using a search criteria to specify devices. This also adds support for the option to uninstall sensors on the endpoints page using the "Uninstall all # assets matching search" option, which was previously displayed in the UI but not supported by the API.

## Enterprise EDR

- **DSER-28686: In the Observations Tab, users can filter scriptload events**

  For each scriptload Observation, there is now a UI Card in the right rail showing the following telemetry: script name, full path, SHA256, available reputation, and available signature data.

  In the **Process Analysis Page**, where users could already filter for scriptloads using Event Type, the drop-down for each scriptload now has the following additional telemetry: script name, full file path, script content, content length, SHA256, available reputation, and available signature data.

## Issues Specific to Carbon Black Cloud on the VMware Cloud Services Platform

- **DSER-46342: Fixed an issue with sensor registration failing when sensors had trailing white spaces in their hostname**

- **DSER-48643: MSSP partner interaction**

  Fixed an issue with MSSP partner interaction and the edit notification modal so that all users in both the child or and parent org appear in recipients drop-down and can be edited.

- **DSER-35532: EA: Update to the Current Version Leaves Sensors Stuck in 'Pending Update'**

- **DSER-39404: EA: Audit Log: Bulk policy change-> Include device IDs**

- **DSER-46342: Trimming issue where sensor registration failure due duplicate key constraint of contact_email_id_key**

- **DSER-48643: MSSP cannot add multiple notification MSSP parent recipients in MSSP child org**

# Update - 26 September 2023

# 10

**Important**  Carbon Black has recently improved the **Investigate** experience in Carbon Black Cloud. We are interested in hearing from you regarding these improvements.

To provide feedback regarding the Investigate experience, please complete the customer feedback form here.

For more information about the Observations Experience for Carbon Black Cloud, see the UEX article: Make Way for Observations - Enriched Events are fully removed from the CBC UI.

You can also view the 8 minute video walkthrough regarding how you can take full advantage of all the functionality on Investigate page.

- **Enriched Events on Investigate is now retired**

  The **Investigate** and **Alert Triage** pages no longer show the Enriched Event experience. This completes the upgrade to the **Observations** experience on these pages. This means:

  - The **New investigate experience** toggle has been removed from the **Investigate** and **Alert Triage**.

  - Events, Applications, Devices, Network tabs have been removed.

  The underlying Enriched Events API is deprecated and will be decommissioned in July 2024.

- **Updates to the Investigate page**

  - **Export** puts all available fields in the CSV.

  - **Process Name** column added to "View By" Process and added as **Configure Table** option.

- **Added a quick tour button on the Investigate page**

  We have introduced a **quick tour** button on the **Investigate** page that allows you to review the features and benefits of this Observations experience at your leisure.
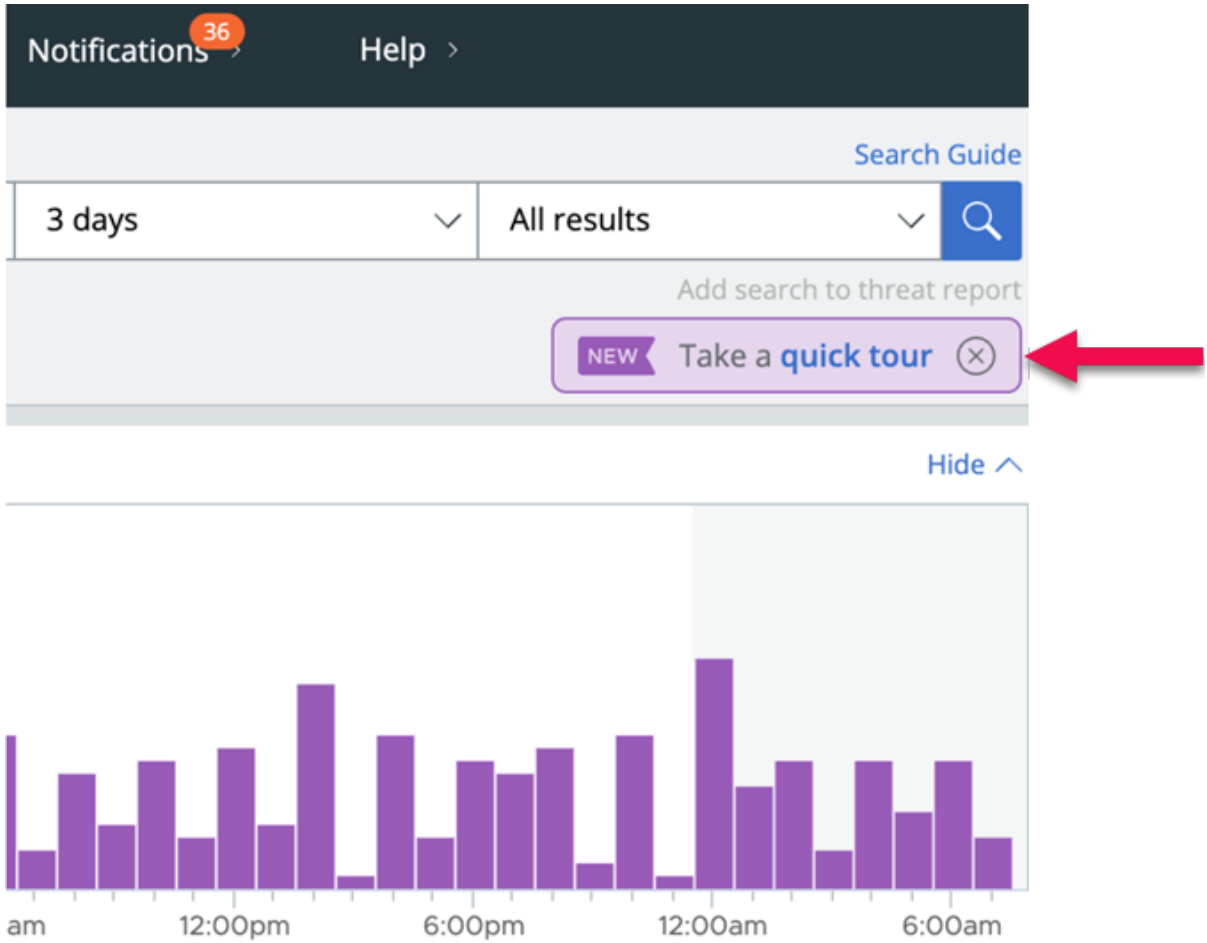
# What's New - 14 September 2023

<div style="text-align: right; font-size: 48px; color: #cccccc;">11</div>

**Build 1.18**

To see changes made in previous releases, see VMware Carbon Black Cloud on VMware Cloud Services Platform Release Notes - 2022 Archive.

This release includes:

Read the following topics next:

- Endpoint Standard
- Enhanced Email Notification Rollout
- Host-based Firewall
- New Total Prevented Actions - Alerts Widget
- Sensor Upgrade Pages

## Endpoint Standard

- **Core Prevention Exclusions**

  We are excited to announce enhancements to Core Prevention rules that will make managing and tuning Core Prevention rules more flexible. With the release of Core Prevention Exclusions, you will now be able to create granular, process-based exclusions within each category to allow business-critical processes to run in the event of a false positive block. Prior to these updates, the only remedy to a Core Prevention false positive was to disable the Core Prevention category entirely, which is not recommended. You will now be able to create specific exclusions that will allow you to leave the category enabled while ensuring that your use cases are not interrupted.

  For the first time, customers will be able to create process exclusions based on a variety of attributes related to either the primary or parent process including process path, command line, hash, and certificate. This allows you to hone in on processes with more specificity than before and create exclusions for specific workflows, such as scripting activity leveraging command lines.

  For more information, please see the Announcement Blog and the Core Prevention section of the VMware Carbon Black Cloud on Cloud Services Platform User Guide.

*The ability to add exclusions to a specific Core Prevention category.*



*The Add Exclusion pane lets you choose between Process or Parent Process and select which attribute you would like to exclude.*

*The ability to add multiple attributes across primary and parent processes.*



# Enhanced Email Notification Rollout

- **Enhancements to alert email notifications**

  Carbon Black is excited to announce enhancements to alert email notifications that is rolling out over the coming months to all notification rules. Carbon Black is introducing additional fields such as parent and child process information, process username, MITRE ATT&CK information, and other highly requested fields. These fields are going to first become available to newer notification rules and then to all notification rules over the coming months.

# Host-based Firewall

- **Custom Alert Severity Score**

    Host-based Firewall now allows customers to set the alert severity score on a per-rule basis. This allows you to promote or demote Host-based Firewall alerts relative to other Carbon Black Cloud alerts, improving the alert management experience and expediting investigation and remediation tasks. The alert severity score displays during Host-based Firewall rule creation only for the **Block and alert** rule type. You can choose an alert severity score between level 1 to level 10, with level 10 being the highest alert severity. By default, the alert severity score is set at level 4.

# New Total Prevented Actions - Alerts Widget

- **The previously named Total Prevented Actions widget has been changed to Total Prevented Actions - Observations**

    In the previous release, the "Prevented Malware" widget changed to "Total Prevented Actions" which uses Enriched Events or Observations to count the number of blocks that have occurred in your environment. Although this provides a higher level of insight into the number of events in your environment that have been blocked, it is often necessary to view this metric in terms of Alerts.

    In order to better replicate the old "Prevented Malware" widget, we have added a new "Total Prevented Actions - Alerts" widget. This widget communicates how many alerts are associated with a prevented action and allows you to pivot to the Alerts page. This widget is now available on the Dashboard in the widget drawer. Click "Add Widget" in the top right corner of the Dashboard, or "Open" in the bottom right corner, to add this widget to your dashboard. The previously named "Total Prevented Actions" widget has been changed to "Total Prevented Actions - Observations".

Total Prevented Actions - Alerts

TOTAL
730

Non-malware

| Known malware | 0 | Suspect malware | 0 |
| Non-malware | 730 | PUPs | 0 |
| Unknown | 0 | Company banned list | 0 |
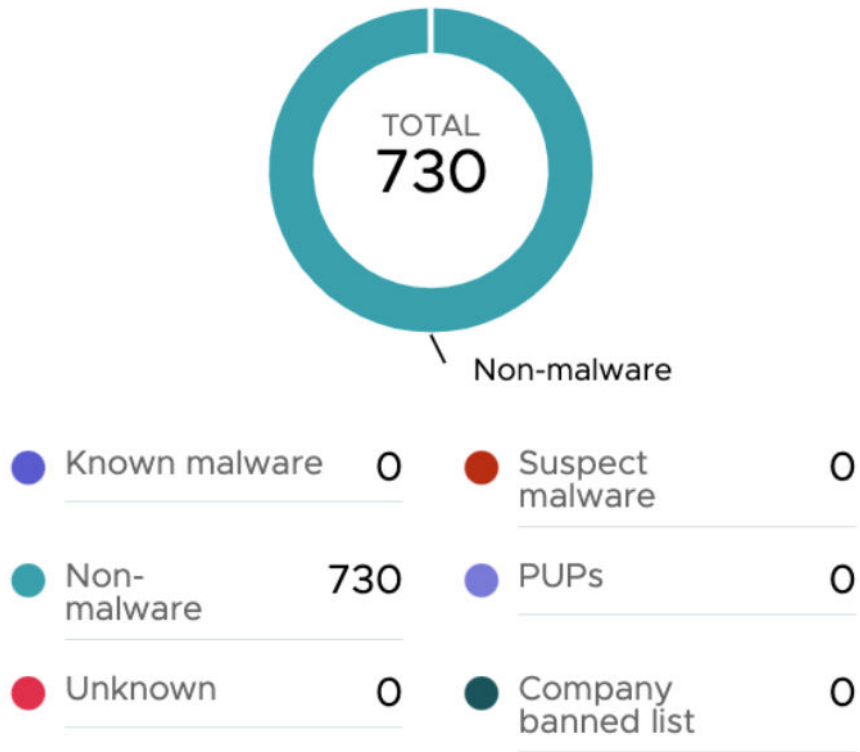
*Alert severity and grouping not applied*

## Sensor Upgrade Pages

- **Sensor Upgrade Pages error status message**

  Following the launch of Containers and Kubernetes support, the Carbon Black Cloud Sensor Upgrade Page/APIs have been updated to return a clear error status message that indicates these endpoints must be updated using the Cluster page.

| | | | | |
|---|---|---|---|---|
| **Name** | | **Target sensor versions** Windows 4.0.0.701 | | **Actions** ⌄ |
| **Status** Stopped | | | | |
| **Requested** 11:06 PM, May 10, 2023 | | | | |

| **All** 1 sensors | **Updated** 0 sensors | **Failed** 1 sensors | **In Progress** 0 sensors | **Not Started** 0 sensors |
|---|---|---|---|---|

🔍 Search          OS  All ⌄          Sensors  All ⌄

| NAME ▼ | OS ▽ | SENSOR ▽ | DEVICES ID ▽ | DETAILS |
|---|---|---|---|---|
| | Windows | 3.9.1.2451 | | K8s sensors must be updated from the Clusters page |

# Resolved Issues - 14 September 2023

<div style="text-align: right; font-size: 3em;">12</div>

Read the following topics next:

- Issues Specific to Carbon Black Cloud on the VMware Cloud Services Platform

- Investigate Page

- Kubernetes

## Issues Specific to Carbon Black Cloud on the VMware Cloud Services Platform

- **DSER-48406: New devices, that match the a deleted criteria, continue to get assigned policy from the deleted criteria**

- **DSER-46691: EA: Workloads not assigning to the default standard policy at time of install**

- **DSER-48320: Observations Histogram Timeline Issues with Custom Date Range**

- **CBCUI-3678: Alerts Page wildcard search UI changes**

- **CBCUI-3325: Implement the redesigned Netconn Expando, second revision**

- **CBCUI-4169: Cypress: fix notifications test cleanup**

- **CBAPI-4852: Update Alert search to enable wildcard searching**

## Investigate Page

- **LC-3893: Investigate page > Observations tab visible columns**

  **Investigate page > Observations tab** does not always Export the visible columns in the displayed search results in the downloadable CSV file.

- **LC-3894: Investigate page > Observations tab IPv4**

  The Export CSV returns IPv4 addresses in integer format rather than the expected dotted decimal (e.g. 10.11.12.13) format.

# Kubernetes

- **DSER-49127: Carbon Black Cloud Device Actions API**

  Enhanced Carbon Black Cloud Device Actions API to not send de-register requests to Kubernetes-derived sensors. This prevents such sensors from getting in an undesired state.

# What's New - 16 August 2023                                      13

**Build 1.17**

To see changes made in previous releases, see VMware Carbon Black Cloud on VMware Cloud Services Platform Release Notes - 2022 Archive.

This release includes bug fixes, enhancements, and improvements.

- Watchlist Table Footer
- Field Description in Search Guide

Read the following topics next:

- Alerts Experience Enhancements
- CIS Benchmarks
- Container
- Host-Based Firewall
- Reveal
- Support for macOS
- Workloads

## Alerts Experience Enhancements

Following the updates to our V7 Alerts API in June, Carbon Black is excited to announce some significant enhancements to our Alerts experience in the VMware Carbon Black Cloud console.

These enhancements improve alert triage in the VMware Carbon Black Cloud and allow for easier management, consumption, and triage of alerts. For more information on all of these features, please see Alerts Experience Enhancements Announcement and <Tech Zone overview videos>.

These enhancements include, but are not limited to:

- **Additional metadata to search on across all alerts**

    Introduction of new alert metadata such as process command line and username, parent and child process information, netconn data, additional device fields, MITRE categorization where available, and more.
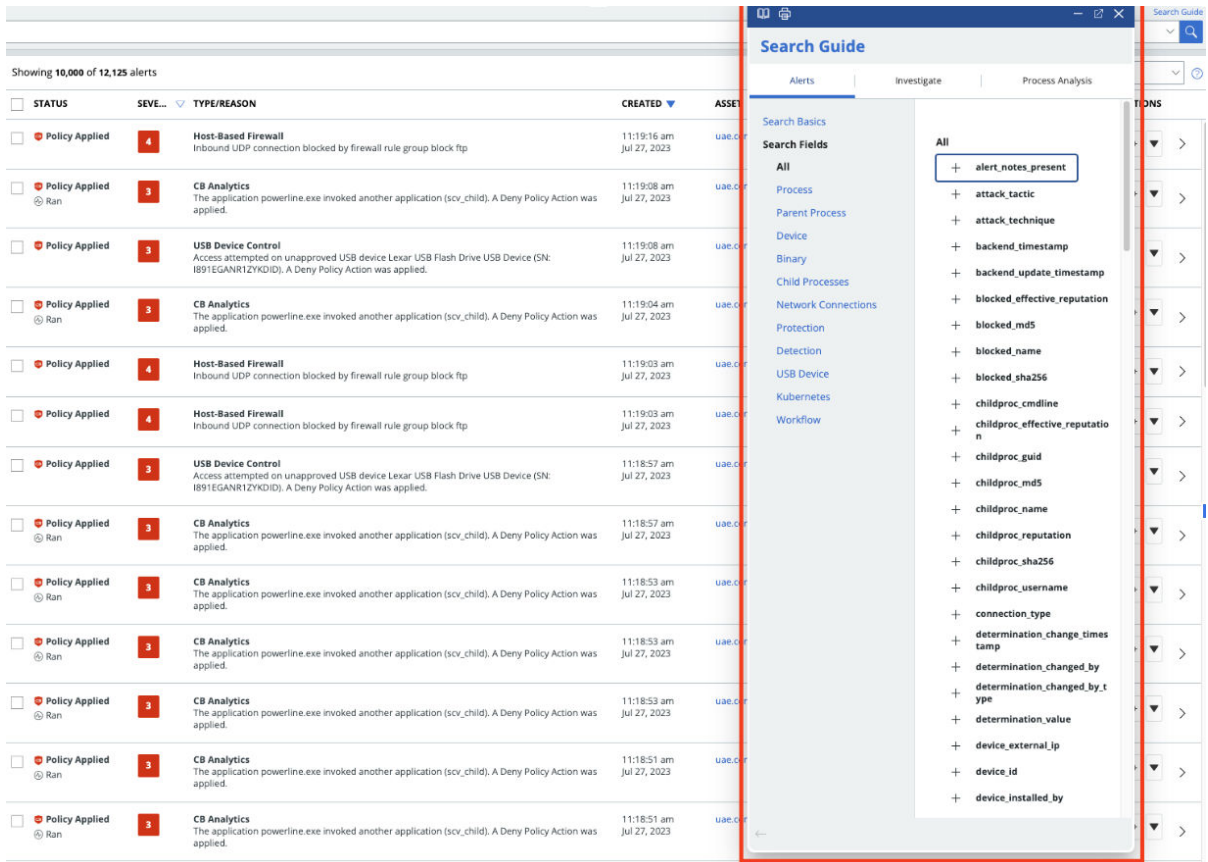
- **New full screen alert details view**

  Users can now view the updated alerts screen with a full alert details view.
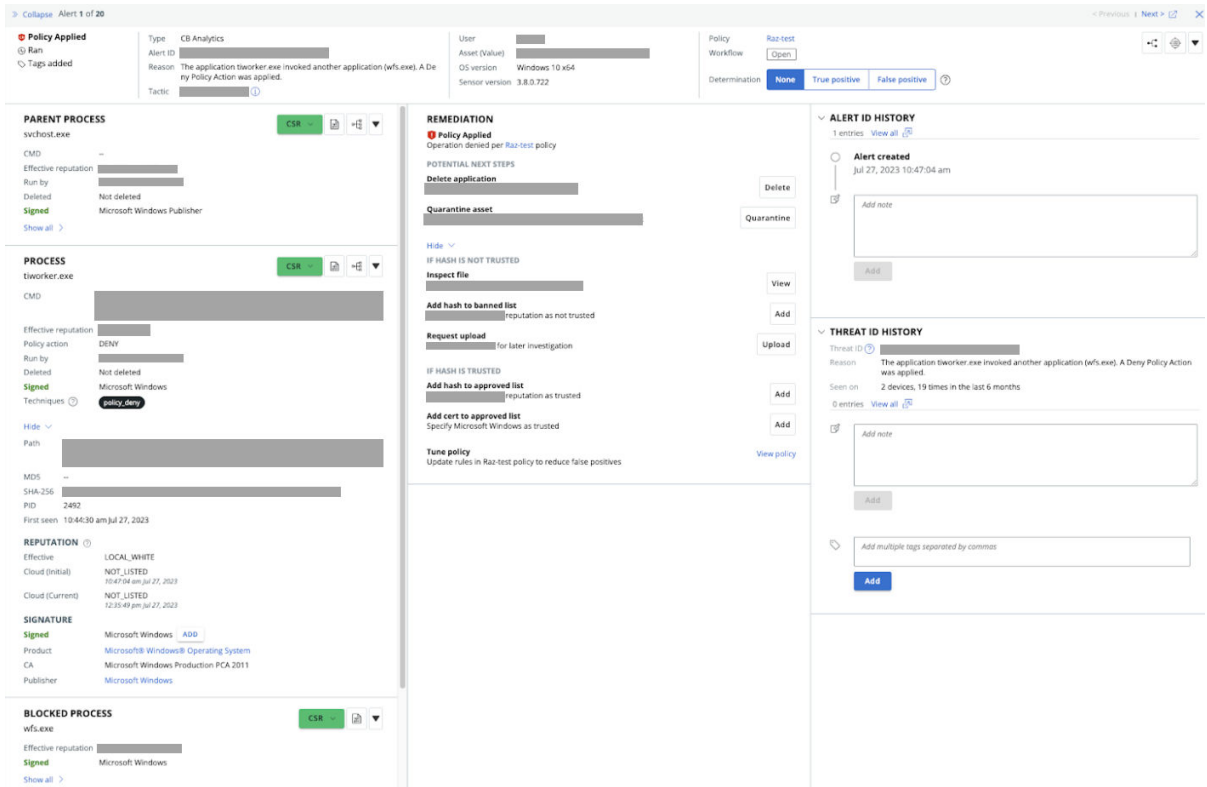
- **New customizable alert filters and table columns**

  Users can now view new alert filers and table columns.

  Additional alert columns for the primary alerts table.
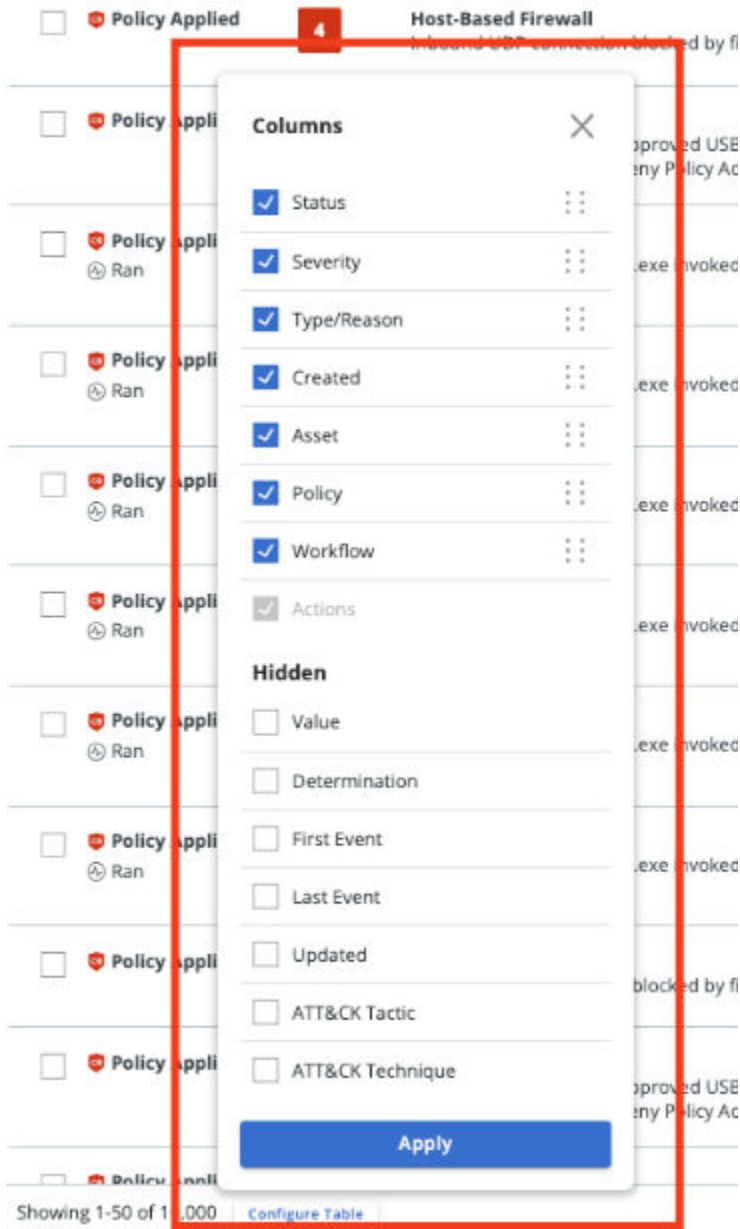
Additional ways to filter alerts.
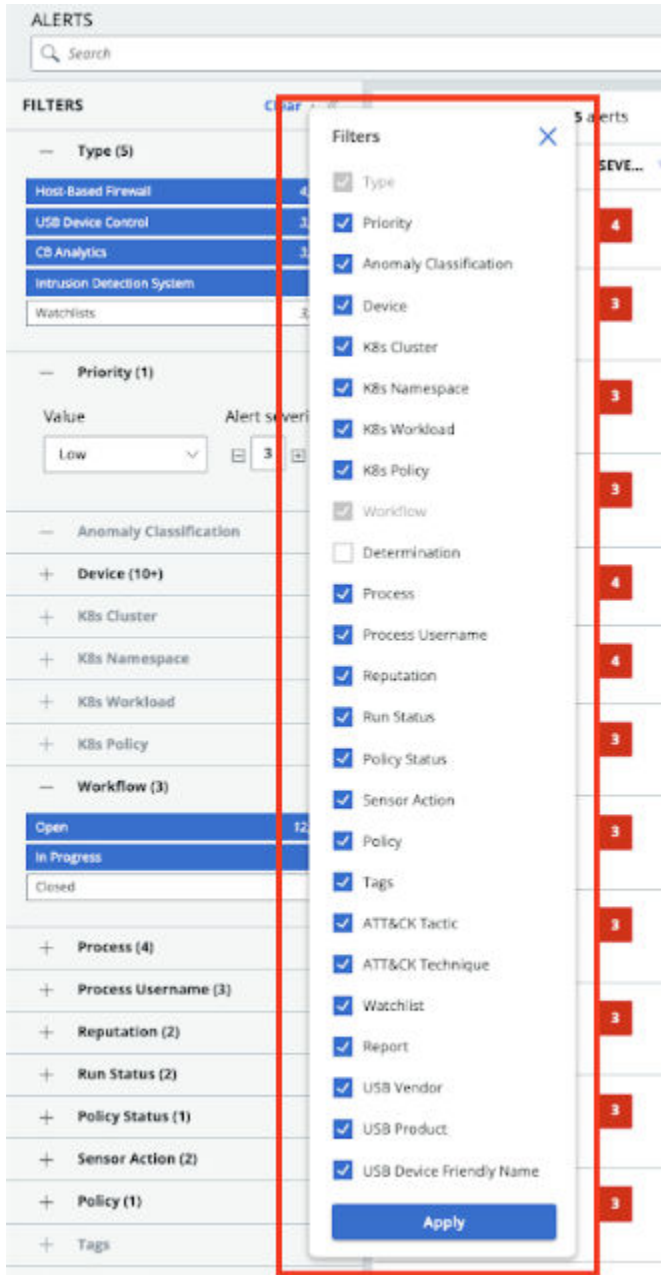
- **Ability to mark alerts as "In Progress" and track the alert status workflow**

  Introducing an in-product alert workflow management, allowing you to mark alerts as "In Progress" and help you better manage alert triage across your SOC team. The **Workflow** column displays the status of the alert, where users can change the workflow of an alert to **Open**, **Closed**, or **In Progress**.

  For further information about editing the alert workflow, see the following section of the VMware Carbon Black Cloud on CSP User Guide: Editing the Alert Workflow (vmware.com).

Users can view all previous changes to the workflow status of the alert in the **Alert ID History** card. The enhanced Alert History visibility shows a history of all alert workflow state transitions (ie. Open -> In Progress), comments, determination, closure information, and other items.

For further information about the enhanced alert details, see the following section of the VMware Carbon Black Cloud on CSP User Guide: View Alert Details (vmware.com)

■ **Alert Determination feature**

Users can now mark an alert as a True Positive or a False Positive alert. Providing feedback about alerts also enhances the accuracy of the classification system over time for some Watchlists.

For further information, see the following section of the VMware Carbon Black Cloud on CSP User Guide: Add Determination for Alerts (vmware.com).

■ **Enhanced Group By: Threat ID view**

Users now have easier management and consumption of grouped alerts in an improved group by ThreatID view.

For further information, see the following section of the VMware Carbon Black Cloud on CSP User Guide: Group By: Threat ID (vmware.com).

■ **Better note management**

Users now have the ability to add notes to both individual alerts as well as alerts grouped by ThreatID. Users can add notes to the Alert ID History and Threat ID History panes.

For further information, see the following section of the VMware Carbon Black Cloud on CSP User Guide: Add Notes (vmware.com).

# CIS Benchmarks

■ **Assets deployed in AWS Cloud are supported from this release**

CIS Benchmarks now supports AWS Instances. This feature is available with Windows sensor 3.9 and currently supports following windows servers: Windows server 2012, Windows Server 2012 R2, Windows server 2016, Windows server 2019 and Windows server 2022. This feature is available to all Workload customers. Carbon Black will be onboarding existing customers in a phased manner.

The CIS Benchmarks recommendations tab now allows users to select whether to view All Assets, VM Workloads, or AWS Instances. On the left navigation pane, users can choose All Assets, VM Workloads, or AWS Instances from the asset type drop-down menu. After selecting the asset type, the compliance reflects the values based on the selection and all tabs show the asset type selected.
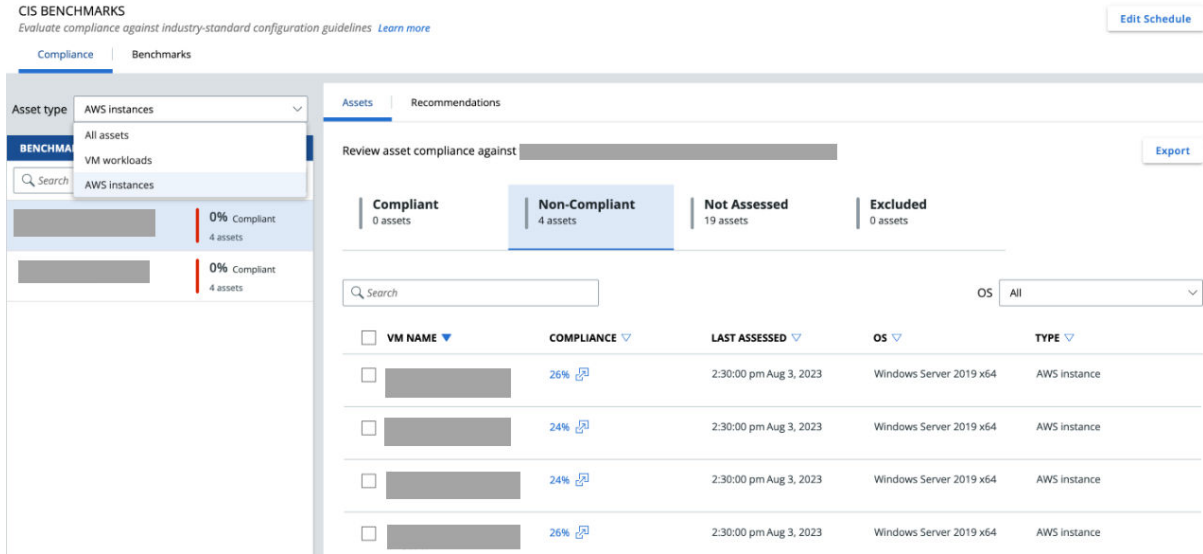
# Container

- **Cloud Native Detection and Response**

    Containers and Kubernetes have become synonymous with the modern application transformation as organizations increasingly adopt multi-cloud and hybrid technology infrastructures. However, the growth in cloud native architectures and containers also expands an organization's attack surface. As Security Operations Center (SOC) teams are tasked with learning the complexities of cloud native environments, they also are challenged with containers running in production with limited-to-no security coverage, disparate tools that create gaps in coverage, and limited visibility into the different layers of these applications.

    VMware Carbon Black's new Cloud Native Detection and Response (CNDR) capabilities deliver enhanced threat detection for containers and Kubernetes within a single, unified platform. CNDR provides VMware Carbon Black customers with unified visibility, security, and control in highly dynamic and complex modern application environments. These enhancements aim to deliver runtime protection for Linux containers to provide a scalable approach for protecting applications from emerging threats and helping eliminate blind spots for attackers to exploit.

    Container Advance customers can now enjoy the benefits of CNDR by using the latest Kubernetes Sensor. Cloud Native Detect and Response will help detect and respond to kubernetes and container-based attacks by grouping events and alerts based on their Kubernetes metadata, including container and Kubernetes context, and make workload posture risk accessible for quick assessment of the asset.
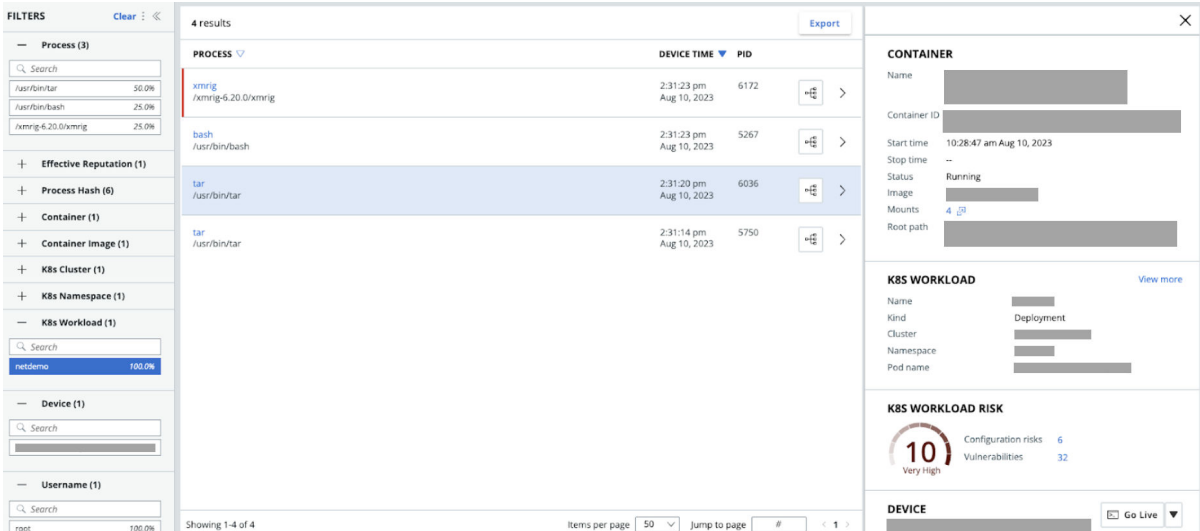
Customers can evaluate threats in cloud Cloud Native environments by overlaying Kubernetes and containers data on top of the existing process tree.
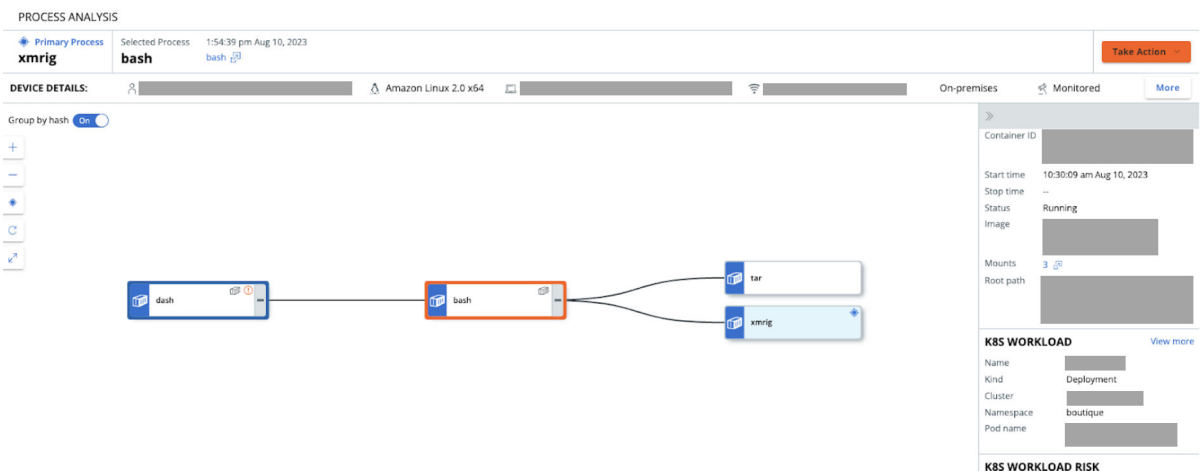


Customers can query for Kubernetes and container-based events to investigate Cloud-Native environment easily, create a watchlist, and trigger Kubernetes and containers threats alerts. Use the in-product Search Guide to access a full list of available search terms to help you create advanced queries.

For more information about the new capabilities, see the following sections of the VMware Carbon Black Container User Guide:

■ Investigating Container Events on the Investigate Page (vmware.com) https://docs.vmware.com/en/draft/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-0A5757F1-67D2-4258-9B3A-09EA62410100.html

■ Investigate Containers Events on the Process Analysis Page (vmware.com)

■ Triaging Kubernetes Alerts (vmware.com)

■ **Secret Detection**

Not only is secret detection an important part of customers' container security strategy, but it is crucial to keeping sensitive data out of the hands of attackers. Typically, attackers have a specific secret in mind, and these secrets are exposed due to errors early in the development lifecycle.

With VMware Carbon Black Container, customers can now scan all executable files in their containerized applications to detect secrets. This adds to the existing image scanning and malware detection capabilities available to Carbon Black Container customers.

Container customers can now scan images for secrets using the latest Kubernetes sensor and CLI for CI/CD integration. The scanner looks for files, environment variables, and command parameters to make sure secrets are not included in the images in any way. The obfuscated secrete, and its source shows up on the image page at the console and the CLI output to help identify the secret source and mitigate the risk. See the product documentation for more information.



- **CNS-3196: New k8s workload risk categories**

- **CNS-3185: The Workloads table's facets is now extended with exclusions capability**

# Host-Based Firewall

- **Navigate directly to rule from alert**

  Carbon Black Cloud Host-based Firewall (HBFW) allows you to create rules that govern network behaviors of applications across endpoints in your environment. Within this feature set, HBFW gives the option to create rules that block a behavior and generate an associated alert. Users can now get additional granularity when investigating that alert by navigating directly to the HBFW rule that triggered the alert with just one click from the Alert details view. This helps users to understand what generated the alert and also to make any associated changes to the rule so that it more appropriately fits their environment needs.

# Reveal

- **API Support for the Reveal Powershell**

  The Reveal Powershell de-obfuscation feature now has API support for use in integrations.  For more details on the Developer Network see: https://developer.carbonblack.com/2023/07/announcing-vmware-carbon-black-cloud-reveal-api/.

# Support for macOS

- **Support for macOS assets as part of its Vulnerability Management**

  This release of Carbon Black Cloud adds support for macOS assets as part of its Vulnerability Management solution. Details on supported sensor and OS versions can be found in Carbon Black Cloud documentation for macOS Sensor OER.

  With the addition of macOS support, Vulnerability Management is now able to deliver a risk-prioritized list of CVEs for all major operating systems that are the likeliest victims of attacks originating from OS and application vulnerabilities. The set of capabilities available for macOS mirror those of other OS types with the ability to automatically assess vulnerabilities without requiring one-off on-demand scans, simplify operations with intelligent risk-prioritization, and provide visibility of these CVEs directly within the Carbon Black Cloud console.

# Workloads

- **Azure and Google Cloud**

  The VMware Carbon Black Cloud Workload for Public Cloud now provides the ability to secure Azure and Google Cloud (GCP) workloads while simplifying the overhead of Azure subscriptions and GCP projects management.

  Core capabilities include:

  - Single and multiple Azure subscription and GCP project management.

  - Auto-generated CI-CD agent installation packages.

  - Enhanced visibility into inventory of protected and unprotected workloads.

  Carbon Black recommends 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:

  - **Vulnerability Assessment**: VMware Carbon Black Cloud Workload provides InfoSec and Cloud admins with a list of OS and Application vulnerabilities across protected workloads. 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 Cloud admin can view the inventory of the Azure and GCP workloads 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 Azure and GCP footprint.

    - Get access to a richer data set about Public Cloud workloads including but not limited to Azure/GCP tags, their vulnerabilities, and trigger various management actions.

    - Use auto-deregistering of Azure and GCP workloads after termination to enhance the management of ephemeral 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, and Ansible are supported.

- **Public Cloud Account Management**: Infosec admin and Azure/GCP admin can easily manage their Azure subscriptions/GCP projects and regions. They can:

    - Add a single subscription/project.

    - Leverage bulk import of subscriptions/projects to facilitate quick onboarding of existing subscriptions/projects.

    - Search and export onboarded subscriptions/projects and regions into an easy-to-consume format.

# Resolved Issues - 16 August 2023

14

Read the following topics next:

- Container
- Enterprise EDR
- Issues Specific to Carbon Black Cloud on the VMware Cloud Services Platform
- Reveal

## Container

- **CNS-3124: Workload summary - fixed table height**

- **CNS-3108: Vulnerabilities page - cant fetch the "All" tab - getting 500 from the server**

## Enterprise EDR

- **DSER-48535: netconn_community_id value wasnot compliant**

  The **netconn_community_id** value emitted by the Carbon Black Cloud Data Forwarder was not compliant with the corelight reference implementation documented here.

- **LC-3907: The netconn_community_id value returned by Process Search API**

  The **netconn_community_id** value returned by Process Search API and the Process Analysis page was not compliant with the corelight reference implementation documented here.

## Issues Specific to Carbon Black Cloud on the VMware Cloud Services Platform

- **DSER-48749: Watchlist Table Footer cropped if Watchlist Description is more than 3 lines**

- **DSER-46831: Documentation: Inaccurate field description in Search Guide**

# Reveal

- **CBCUI-3879: Investigate page can sometimes exclude Observations that are visible on the Alert Triage page**

- **CBCUI-3877: Investigate page > Processes tab does not show Alert badge for processes that have an associated Alert**

# Update - 26 July 2023

Read the following topics next:

- XDR Enhancements

## XDR Enhancements

- **Network Traffic Analysis**

    NTA (Network Traffic Analysis) is a new type of Observation introduced with this release.

    Unlike many of Carbon Black's traditional static detections, NTA uses traffic analysis to monitor network activity and historical data to identify anomalies within the network.

    This initial rollout includes a set of three unique detectors called "profilers". These detectors work by establishing a profile for expected traffic and detecting activity that occurs outside of the expected profile.

    - User Agent Profiler: Identifies unusual user agents in HTTP connections being made from a local device compared to the user agents, typically observed from HTTP connections originating from the device.

    - IP Profiler: Identifies anomalous IP address connections associated with a device, compared to those seen typically.

    - Port Profiler: Identifies connections to or from a local host that have an unusual, remote IP address. These anomalies are compared to remote IPs that host typically connects to or receives connections to.

- **Policy Enhancements**

    Customers can turn off XDR data collection by clicking **Enforce > Policies > Sensor Settings**. Disabling XDR data collection prevents the recording of XDR specific enhanced network telemetry, including Intrusion Detection System (IDS) and NTA alerts and observations.

# What's New - 13 July 2023

**Build 1.16**

To see changes made in previous releases, see VMware Carbon Black Cloud on VMware Cloud Services Platform Release Notes - 2022 Archive.

This release includes bug fixes, enhancements, and improvements.

Read the following topics next:

- Data Forwarder
- Endpoint Standard
- Enterprise EDR
- Host-Bast Firewall
- Investigate
- Managed Detection and Response
- Sensor Upgrade Pages

## Data Forwarder

- **Data Forwarder launches Alert Forwarder version 2.0.0**

  Following the launch of the v7 Alerts API in the 1.15 release, the Carbon Black Cloud Data Forwarder now makes support available for these new Alerts. Because the Alerts schema has significantly changed and is no longer compatible with the existing "Alerts" Data Forwarder, Carbon Black Cloud now offers the ability to select explicit versions of the Alert Forwarder:

  - The existing Alert Forwarder is called the "1.0.0" version.
  - The new Alert Forwarder is called the "2.0.0" version.

  All users of the **Settings > Data Forwarder** page in the Carbon Black Cloud console now displays a new Schema configuration drop-down menu when selecting the Alert type. By default the Alert Forwarder offers you the "2.0.0" version of the Alert Forwarder, and always defaults to the latest version of the Alert Forwarder.

All users of the v2 Data Forwarder Config API can view a new optional input parameter "version_constraint" as well as a new return value on all GET requests called "current_version". Those API callers who create or edit Alert Forwarders from now on will default to the 1.0.0 Alert Forwarder version if they do not specify the "version_constraint" parameter.

For more Data Forwarder news, read:

- about the new Alert Forwarder release and our plans for the future here (requires logging into UEX)

- the Alert Forwarder schema

- updates to the Data Forwarder Config API

- Carbon Black's commitment to semantic versioning in Data Forwarder

- about migration guidance for developers who have automated any applications, scripts, or other integrations against the Alert Forwarder to make your adoption of the new 2.0.0 Alert Forwarder schema as easy as possible.

# Endpoint Standard

- **Hash Origins Data Retention**

  In order to streamline development cycles, Carbon Black is changing data retention of hash origin device prevalence from 6 months to 3 months for customers who are licensed for Endpoint Standard but not Enterprise EDR. There is no impact to Alerts or Events data.

- **Device Control - Export Device Inventory and Approvals**

  Carbon Black Cloud gives visibility and control over USB mass storage devices detected in your environment with the ability to block untrusted devices and approve trusted devices. The Carbon Black Cloud UI maintains a list of these USB mass storage devices that have been detected in your environment, as well as the trusted devices which have been approved. With this release, you can now export those lists of detected devices in the inventory page and the list of approved devices from the approvals page.

# Enterprise EDR

- **XDR Release 2**

  - Alert Forwarder version 2.0.0 makes Intrusion Detection System alerts available, that were not visible in the version 1.0.0 Alert Forwarder. See List item. for more information.

  - Netconn details updates on Observations, Alert Triage, and Process Analysis.

# Host-Bast Firewall

- **Export Host-Based Firewall Policy Rules**

  Carbon Black Cloud Host-Based Firewall allows users to block, allow, and alert on the network behavior of applications across windows endpoints and workloads. This feature replaces legacy firewall solutions with a lightweight, rule-based solution that's easy to manage at enterprise scale. The Carbon Black Cloud User Interface provides a centralized console to create and manage all host-based firewall rules. With the release of this export capability, you can now export the full set of rule groups, rules, and associated rule parameters from the host-based firewall policy page.

# Investigate

- **Observations Update**

  Host Based Firewall and Intrusion Detection System (IDS) alerts now report up to 100 identical observations per alert. After 100, Carbon Black Cloud suppresses additional duplicate observations. This reduces system fatigue and helps speed up searches.

# Managed Detection and Response

- **Enhancements to Audit Log Content**

  The Managed Detection and Response Audit log content has improved to include user information and current notification settings.  Audit log entries are added each time a user selects either the Manage Detection page or the Notifications page and updates, adds, or deletes current notification selections. The following is an example of the new Audit Log content for Managed Detection and Managed Detection and Response notification updates.



# Sensor Upgrade Pages

- **Sensor Upgrade Pages Improvements**

When a user requests to stop a sensor upgrade, it transitions to a "Stopping" state. There can be several minutes delay between the user's stop request and the resulting changes being processed in the backend, this new status exposes that the request is received and is being processed.

When a user requests to create a new sensor upgrade, it transitions to an "Initializing" state. Larger jobs take significantly longer to initialize than smaller jobs, up to a few minutes, and can display in a confusing state in the console. This new "Initializing" state exposes that work is still being done to prepare the upgrades.

# Resolved Issues - 13 July 2023

# 17

Read the following topics next:

■ Audit and Remediation

## Audit and Remediation

■ **DSER-47984: Failure caused by string query results in the form "6E075145"**

If a string from query results is of the form "6E075145", the code was trying to parse it as a java Double value and the parsed result is "Infinity" that causes failure.

Added fix to parse such strings as java String.

■ **DSER-47639: LQ-Device-API capability to handle envoy path**

■ **DSER-47932: In VDP, using the same CSV_EXPORT_BUCKET_NAME for lq-diff json and csv export**

# What's New - 15 June 2023

<span style="float:right">**18**</span>

**Build 1.15**

To see changes made in previous releases, see VMware Carbon Black Cloud on VMware Cloud Services Platform Release Notes - 2022 Archive.

This release includes bug fixes, enhancements, and improvements.

Read the following topics next:

- V7 Alerts API
- Investigate > Observations
- Endpoint Standard
- Sensor Update Status tab

## V7 Alerts API

- **Announcing the Alerts V7 API**

  The new Alerts V7 API is ready for public use and integration on June 15th. This is the first of many upcoming enhancements to the VMware Carbon Black Cloud Alerts experience. The Alerts V7 API introduces a handful of new features including:

  - Overhauled alert schema with additional metadata, such as: process command line and username, parent and child process information, netconn data, additional device fields, and MITRE categorization when available.

  - Easier management and consumption of grouped alerts.

  - Ability to mark alerts as **In Progress**.

  - Ability to mark alerts as **True Positive** or **False Positive**.

  - Additional fields available for both searching and filtering.

  - Enhanced note management with the ability to add notes to both individual alerts as well as to threats. Alerts are grouped by threat.

  The new Alerts V7 API improves alert management and allows for easier management, consumption, and triage of alerts in the Carbon Black Cloud. For more information, please see the CBC Alerts API Announcement on the Developer Network, available on June 15th.

For customers with existing integrations, detailed information to move from v6 to v7 API will be published shortly followed by an updated version of the Carbon Black Cloud Python SDK.  The Data Forwarder also is soon releasing an updated schema version which aligns with Alerts v7 API. Integrations such as Splunk and QRadar will be progressively updated in future releases to take advantage of the new Alerts data available.

# Investigate > Observations

- **Investigate > Observations replaces Enriched Events**

  The **Observations** tab on the **Investigate** page, which has been in preview mode since March 2023, is now the default experience. You might notice various changes that are best seen in the video at the bottom of this Carbon Black TechZone post.

  You can opt-out of **Observations** and use the **Enriched Events** tab by clicking the **New Investigate experience** toggle in the top-right corner of the **Observations** tab. The option to revert to **Enriched Events** will be removed later this year.

  To provide any feedback on the new experience, use the Observations Feedback Form.

- **Investigate > Observations improvements**

  When you use **Group By**, the results not only display how many matches there are for each value of that field, but also how many unique values exist for the rest of the displayed columns. "--" signifies there are no values for that column in that group. You can click on the **Observations** count column for any row to explore the variations in the single group.

Showing **368** groups with max **10,000** results (**38,312** total results) ⓘ  | View By [ Device ▽ ] | Group by [ Remote IP ⊗ ] [ Select ▽ ] | Export

| OBSERVATIONS | REMOTE IP ▽ | TIME ▼ | DEVICE ▽ | DEVICE GROUP ▽ | OS ▽ | USERNAME ▽ | LOCAL IP | POLICY ▽ |
|---|---|---|---|---|---|---|---|---|
| 8726 | 0.0.0.27 | 6:00:15 am Jun 7, 2023 -1:46:59 pm Jun 8, 2023 | 14+ | -- | 2+ | 14+ | -- | 1+ |
| 7 | 52.168.112.67 | 7:26:54 am Jun 7, 2023 -1:43:03 pm Jun 8, 2023 | 5+ | -- | 1+ | 1+ | 5+ | 1+ |
| 8 | 20.189.173.1 | 9:37:59 am Jun 7, 2023 -1:39:11 pm Jun 8, 2023 | 6+ | -- | 1+ | 1+ | 6+ | 1+ |

The **Observations** tab **Group By** list did not include an equivalent for **Enriched Events** "Applications" sub-tab. You can now group by applications by selecting **Process Hash** in the **Group By** list on the **Observations** tab.

The **Observations** tab adds a **View By** capability to allow you to quickly switch between four ways to analyze your search results:

a   Observations, the default view

b   Devices

c   Network

d   Process Hash

This equates to the static sub-tabs under the **Enriched Events** page, in combination with the **Group By** feature.

**ATT&CK Tactic** and **ATT&CK Technique** filters now include the Tactic or Technique name alongside the ATT&CK ID for ease of selection - e.g. "TA0010 - Exfiltration" rather than just "TA0010".

The **Observation Details** in the right navigation pane improves the organization of the data, specifying **What Triggered This Observation** as the header for the variety of evidence available such as Threat and Rule.

A new "Observations Deep Dive" video highlights all the new and hidden features of **Observations** and **Investigate**.

Use the improved Observations feedback form to report any further bugs or gaps in the **Observations** tab as compared to **Enriched Events**.

- **Actions added to Network details**

  You can access the Network details:

  a   Investigate > Observations > right pane.

  b   Process Analysis > Events > expanded details.

  c   Alert Triage > Observations> expanded details.

  The Network details pane now has a new **Find in VirusTotal** action to lookup either the remote domain or remote IP address.

# Endpoint Standard

- **Observed Alerts Are Now Observations**

  Accompanying the V7 Alerts API release, Carbon Black Cloud are also announcing a change to "Observed Alerts". Observed Alerts are events that might have had interesting security context, but are not determined to be a threat by Carbon Black. Observed Alerts are not designed to be actionable and do not require a full investigation.

  Moving forward, Observed Alerts are no longer present on the **Alerts** page or in the new V7 Alerts API. Observed Alerts now exist on the **Investigate** page as Observations. Customers can find these Observations by navigating to the **Investigate** page and filtering on Carbon Black Cloud. The non-alerted Observations present in this section include the Observed Alerts that used to be available on the Alerts page.

  Customers leveraging the V6 Alerts API and original Alert Forwarder are not affected by this change and have access to these Observed Alerts until the V6 API is deprecated.
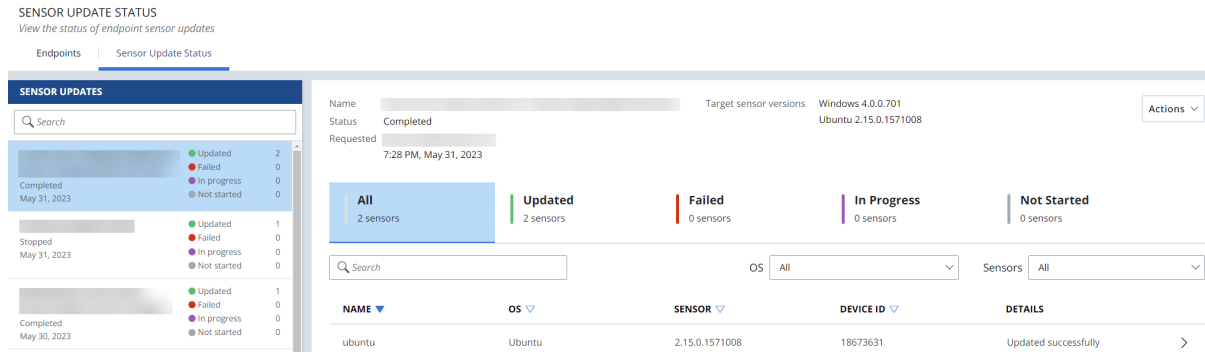
# Sensor Update Status tab

- **Increase in the device upgrade limit from 10,000 to 250,000**

You can now add up to 250,000 sensors to an upgrade request (job) in the Carbon Black Cloud console.

- **Updated User Interface for the Sensor Update Status tab on any Inventory page in the Carbon Black Cloud console**

  The new Sensor Update Status tab addresses customer feedback to allow increased visibility and control of the sensor update progress. The new Sensor Update Status tab improves mass sensor management and provides more flexibility for larger enterprise environments.



With the new Sensor Upgrade Status tab you can:

- Name or re-name a group of sensors with a unique name that you want to update in the Carbon Black Cloud console. This improves the organization of the sensor upgrades. **Note:** You must provide a unique name for each sensor group to avoid errors.

- Review the status of the Sensor upgrades by sensors that are **Not Started**, **In Progress**, **Failed**, or **Updated**. This improves the use case of not knowing the status of a sensor upgrade.

- Search for a specific device name within a sensor update.

# Resolved Issues - 15 June 2023

<span style="color:grey; font-size:large">19</span>

Read the following topics next:

- [All](#)

- [Workloads](#)

## All

- **DSER-41526: Update UI to reflect "Quarantine" action now supported for Linux Sensors 2.13**

## Workloads

- **CWP-15738: An Install Sensor pop-up shows only 3.9.1.2668 for all CWP and VCDR customers**

# What's New - 11 May 2023

<div style="text-align: right">20</div>

**Build 1.14**

To see changes made in previous releases, see VMware Carbon Black Cloud on VMware Cloud Services Platform Release Notes - 2022 Archive.

This release includes bug fixes, enhancements, and improvements.

Read the following topics next:

- Audit and Remediation
- Container
- MDR
- Alert Details Panel
- Observations Page

## Audit and Remediation

- **New Recommended Query Category - Sensor Analysis**

  A new category of Recommended Query is now available on the Live Query > New Query page. This category is titled "Sensor Analysis" and provides recommendations for querying the Windows Live Query Extension Tables introduced with the 3.8 Windows Sensor Release.

  See the VMware Carbon Black Cloud User Guide for more information on our Live Query Extension Tables.

## Container

- **The Kubernetes connectivity map contains new UI enhancements including a new side panel for top connection and statistics**

  The new Kubernetes connectivity map design focuses on the most relevant data to create a better visual experience. The map introduces bar charts that display a visual summary about the connection types to evaluate the network traffic in a cluster. The interactive experience allows customers to explore the network activity of different areas of the cluster. The map helps customers to understand the behaviour of a cluster and to highlight areas of interest.

Figure 20-1. **Kubernetes connectivity map**
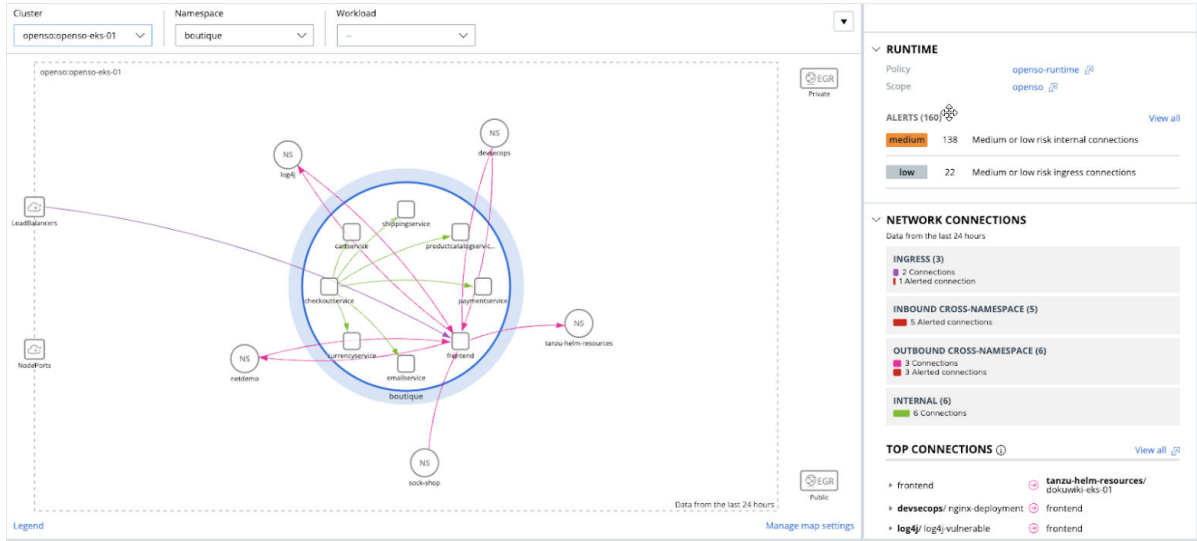


- **New User Guide Available for VMware Carbon Black Container**

  A new VMware Carbon Black Container User Guide is available.  This standalone guide contains all information required to install, configure, and manage your container environment.

  - The HTML version of this guide is embedded in the main VMware Carbon Black Cloud User Guide.

  - All context-sensitive help links in the product have been redirected to the new guide and topics.

  - The container-related topics previously embedded throughout the main guide have been removed.  All container content is in the new guide.

  - You can download a standalone VMware Carbon Black Container User Guide PDF from the Carbon Black Cloud landing page Quick Links or from the HTML preface page for the containers guide.

  This is version one of this guide and we encourage your feedback.  If you want to provide feedback regarding a topic or the guide itself, please use the feedback option on the respective page.

# MDR

- **New Frequently Asked Questions Section Available for VMware Carbon Black Managed Detection and Response**

  A new VMware Carbon Black Managed Detection and Response FAQs section is available. You can view the Managed Detection and Response FAQs in the VMware Carbon Black Cloud User Guide.

This section answers the questions that are frequently asked by Carbon Black Managed Detection and Response customers:

- Most common questions

- Product and service level objective FAQs

- Evaluation FAQs

- Analyst team FAQs

- Communication FAQs

- Configuration FAQs

- Reporting FAQs

- General FAQs

# Alert Details Panel

- **Anomaly Classification feature for E-EDR customers**

  The Anomaly Classification feature detects and automatically identifies alerts that are most likely to be relevant.

  The feature filters alerts into three categories:

  - Not Anomalous.

  - Remove Baseline.

  - Anomalous.

  Customers can use the **Alert Details** pane to provide a **True Positive** or **False Positive** alert determination for anomalous alerts.

- **New section in the Alert Details side panel**

  A new section explaining what triggered an alert, including information about the rule or policy, observations, and MITRE ATT&CK.

# Observations Page

- **Updates to the Observations page**

  New updates to the **Observations** page including:

  - Revised details side panel.

  - New configurable columns (remote IP, local IP, process hash, and port).

  - New feedback form is available from the information icon next to the toggle that turns on the new experience.

# Resolved Issues - 11 May 2023

21

Read the following topics next:

- All
- Workflow
- Container

## All

- **CBCUI-3196: Expandable Manage Related Alerts section**

  The Manage Related Alerts section is now expandable and the above buttons in workflow modals have been moved

- **CBCUI-2677: Removed the updated column in the UAE alerts grouped view**

- **CBCUI-3284: Missing parent process details/error toast on side panel open**

- **CBCUI-1793: Group action for quarantining assets**

  A group action can quarantine all assets in a group

- **DSER-34353: HTTP Status 500**

  The Audit Log API returns HTTP Status 500 whenever a user requests (fromRow + maxRows) > 10000

- **CBCUI-2645: Process Card**

  Ensure the Process Card contains all necessary fields, particularly the Process Username field

- **CBCUI-1856: Fixed the identify ineligible assets in multi-select bulk actions**

# Workflow

- **CBCUI-2509: New 'Mark In Progress' section has been added for ungrouped alerts**

# Container

- **CNS-2324: Fixed an issue with not closing the eBPF module in the network tracer upon an interface detachment**

- **CNS-2105: Fixed an issue with the "health_reports" API search**

  Fixed an issue where the "health_reports" API search did not work as expected when involving the ":" character.

# Update - 25 April 2023

<span style="font-size:4em">22</span>

Read the following topics next:

- CIS Benchmarking

## CIS Benchmarking

- **Non-Assessed Asset View for CIS Benchmarking**

  In the first release of CIS Benchmarks, assets were displayed under different tabs based on compliance assessment status as *"Compliant", "Non-Compliant",* or *"Excluded"*. Our latest release brings the addition of a new tab called *"Not Assessed"* that allows users to check the compliance posture for assets which were not assessed.

# What's New - 13 April 2023

<span style="color:gray; font-size:200%">23</span>

**Build 1.13**

To see changes made in previous releases, see VMware Carbon Black Cloud on VMware Cloud Services Platform Release Notes - 2022 Archive.

This release includes:

- API and Integration Docs Modal on the API Access page

- Updates on the Investigate Page for Dismiss Alert

- New facets added for USE and for XDR

# Resolved Issues - 13 April 2023

Read the following topics next:

- All

- Issues Specific to Carbon Black Cloud on the VMware Cloud Services Platform

## All

- **CBAPI-4549: Updated API and Integration Docs Modal on API Access page**

## Issues Specific to Carbon Black Cloud on the VMware Cloud Services Platform

- **DSER-46243: Fixed issue on the Investigate Page where *Dismiss Alert* shows the *Undismiss Alert* popup**

- **CBCUI-2584: Added new facet categories**

  Added new facet categories for UAE and XDR:

  - Process Username

  - K8s Policy

  - Watchlist

  - Report

  - USB Vendor

  - USB Product

  - USB Device Friendly Name

# What's New - 15 March 2023

<span style="float:right; font-size:3em; color:#999;">25</span>

To see changes made in previous releases, see VMware Carbon Black Cloud on VMware Cloud Services Platform Release Notes - 2022 Archive.

This release includes bug fixes, enhancements, and improvements.

Read the following topics next:

- XDR
- Identity Intelligence
- Anomaly Classification
- New Observations Tab
- Investigate Page
- Alert Triage page
- New APIs

## XDR

- **Introducing the release of XDR, a new add-on to Enterprise EDR**

    Observations enhancements for XDR

    - New filter category added for Application Protocol (for example, TLS, HTTP).

    - New optional column, **Application Protocol**, added to the *Observations* search results table.

    For more information, see Exploring XDR Data on the Observations Page and Investigate - Observations in the VMware Carbon Black Cloud User Guide.

    **Note:** XDR requires the Carbon Black Cloud Windows Sensor 3.9.1 MR1+.

- **Additional searchable netconn fields**

    netconn_application_protocol, netconn_bytes_received, netconn_bytes_sent, netconn_first_packet_timestamp, netconn_ja3_local_fingerprint, netconn_ja3_local_fingerprint_fields, netconn_ja3_remote_fingerprint, netconn_ja3_remote_fingerprint_fields, netconn_last_packet_timestamp,

netconn_remote_device_id, netconn_remote_device_name, netconn_request_headers, netconn_request_method, netconn_request_url, netconn_response_headers, netconn_response_status_code, netconn_server_name_indication, netconn_tls_certificate_issuer_name, netconn_tls_certificate_subject_name, netconn_tls_certificate_subject_not_valid_after, netconn_tls_certificate_subject_not_valid_before, netconn_tls_version, triggered_alert_id

For more information, see the in-product *Search Guide*.

- **Enhancements to Process Analysis**

  Newly designed "expando" for NetConn events, making all available netconn metadata available on each event:

  - Includes Application Layer Details where the Application Protocol is "HTTP" or "TLS".

  - Includes MITRE Tactic and/or Technique where available.

  For more information, see Exploring XDR Data on the Process Analysis Page in the VMware Carbon Black Cloud User Guide.

- **Enhancements to the Alerts page**

  VMware Carbon Black XDR customers now have available a preview of the New Alerts experience that upgrades the Alerts page in Carbon Black Cloud.

  VMware Carbon Black XDR customers can view the IDS Alerts generated by the XDR microIDS, and see the Alerts labeled with "Alert Type" categories that are compatible with their Observation Types.

  For more information, see Exploring XDR Data on the Alerts Page in the VMware Carbon Black Cloud User Guide.

# Identity Intelligence

- **Introducing the Identity Intelligence feature in Enterprise EDR with a new *Auth Events* tab on the *Investigate* page**

  Identity Intelligence introduces additional visibility into end users and their authentication activity. When activated, Enterprise EDR collects various types of Windows authentication events, that are reported on a new *Auth Events* tab on the *Investigate* page. Users can search and filter through Windows authentication events for anomalous authentication behavior and correlate authentication and process activity.

  Collection of authentication events is deactivated by default, but can be activated per Policy.

  **Note:** Auth Events requires the Carbon Black Cloud Windows Sensor 3.9.1 MR1+.

  For more information, see Investigate - Auth Events in the VMware Carbon Black Cloud User Guide.

- **New authentication event search fields**

New authentication event search fields include:

auth_cleartext_credentials_logon, auth_daemon_logon, auth_domain_name, auth_elevated_token_logon, auth_event_action, auth_failed_logon_count, auth_failure_status, auth_failure_sub_status, auth_interactive_logon, auth_logon_id, auth_logon_type, auth_privileges, auth_remote_device, auth_remote_ipv4, auth_remote_logon, auth_remote_port, auth_restricted_admin_logon, auth_auth_user_id, auth_auth_user_principal_name, auth_username, auth_virtual_account_logon, windows_event_id

**Note:** See the *Search Guide* for more details.

- **Filter authentication events results**

  Users can filter the authentication events results by:

  - Windows Event ID

  - Username

  - User ID

  - Logon Type

  - Logon ID, Domain

  - Remote Device

  - Remote IP

  - Port

  - Privileges

  - Interactive Logon

  - Remote Logon

  - Process, Device

  - Policy

  - Parent (Parent Process)

- **Group authentication event results**

  Group authentication event results using one or more of the following criteria:

  - Windows Event ID

  - Username

  - Device

  - Remote IP

  - Time (1 minute, 10 minutes, 1 hour, 1 day)

- **Export feature in the *Auth Events* tab**

Introducing the **Export** feature to the *Auth Events* tab. Users can now export process event results from the *Auth Events* tab, similar to how process results can be exported from the *Investigate* page.

The new **Export** button:

▪ Exports up to 10,000 authentication event results at a time.

▪ Exports authentication event results in CSV format.

▪ **Events Detail pane**

View extensive details about each authentication event in the Event Details pane.

Pivot to new searches from the Event Details pane:

▪ Click hyperlinked values for single-attribute pivots:

   ▪ Windows Event ID

   ▪ Username

   ▪ Logon ID

   ▪ CMD

   ▪ Product

   ▪ Publisher

   ▪ Policy

▪ Use the Investigate dropdown menu for multi-attribute pivots:

   ▪ Username and device

   ▪ Device & remote IP: if the event contains a Remote IP value

   ▪ Username and Windows event ID

# Anomaly Classification

▪ **Introducing the Anomaly Classification feature in Enterprise EDR**

With the help of machine learning models, the Anomaly Classification feature allows users to reduce noise and surface relevant Watchlist alerts. The machine learning system classifies Watchlist alerts as *Anomalous*, *Not Anomalous*, or *Not Classified* to help analysts to focus on anomalous alerts and respond to them faster.

Anomaly Classification improves the accuracy and speed of threat detection while reducing the workload of security analysts. Furthermore, analysts can provide determination feedback to help train the machine learning systemby marking alerts as *True positive* or *False positive*. Providing determination feedback enhances alert classification accuracy over time.

Anomaly Classification provides the following features:

▪ A new *Anomalous* indicator on anomalous alerts.

- Users can filter alerts by Anomaly Classification type on the *Alerts* page:

  - Anomalous

  - Not Anomalous

  - Not Classified

**Note:** This feature supports Carbon Black Advanced Threats and AMSI Threat Intelligence watchlists. Anomaly Classification is currently only available for the following customers:

- Customers with XDR.

- Customers in the US regions.

For more information, see Anomaly Classification in the VMware Carbon Black Cloud User Guide.

# New Observations Tab

- **Introducing the Observations tab to the Investigate page**

  The *Investigate* page now offers an optional *Observations* tab experience, which is an opt-in upgrade to the *Enriched Events* tab.

  - The Observations tab is available to Enterprise EDR organizations that have added the XDR subscription.

  - The Observations tab is available in preview mode for Endpoint Standard organizations, as an opt-in feature. Use the **New Investigate experience** toggle to preview the Observations tab.

  - Data from Enriched Events is available in the Observations tab.

  - You receive a feedback prompt when choosing to view the Enriched Events tab.

  - More details are available in the Carbon Black Community article here: https://community.carbonblack.com/t5/Endpoint-Standard-Discussions/Introducing-Observations-to-the-CBC-Investigate-Page/m-p/117302.

  **Note:** Some Observations might display experimental category names. The Observation type names were finalized in February 2023 and all data generated since then is labeled correctly.

  - **Benign Events** is now **Contextual Activity**

  - **UNKNOWN** is now **CB Analytics**

  For more information, see Investigate - Observations in the VMware Carbon Black Cloud User Guide.

- **New filter categories**

  - Type (observation types)

  - Attack Tactic

- Attack Technique

**Note:** The **Event Type** category on the Observations tab is the new name for the **Type** category on the Enriched Events tab.

- **Histogram**

  With the Histogram feature, you can:

  - Visualize the frequency of matching search results over selected time period.

  - Select one or more time intervals (bars) to drill into activity in time ranges of interest.

  - Return to the previous time range selections using the **Back** button.

  - Hide the histogram with the **Hide/Show** button.

- **Group By views**

  In the **Group By** views, you can summarize your search results by a number of grouping categories, including:

  - Observation Type

  - Device

  - Username

  - Remote IP

  - Local IP

  - ATT&CK Tactic

- **MITRE ATT&CK Tactic and Technique**

  MITRE ATT&CK Tactic and Technique are now visible on the Observations tab as columns and in the right Observation Details pane.

  - All are mapped to MITRE ATT&CK v10 standardized techniques and tactics

  - In cases where the MITRE Tactic or Technique are available, the matching **mitre_**-prefixed TTPs are hidden on the Investigate right pane

  **Note:** Not all Observation types are always instrumented with MITRE Tactic and Technique, such as Contextual Activity and Intrusion Detection System.

- **New optional columns in the Observations search results table**

  New optional columns are available on the Observations search results table, including:

  - ATT&CK Tactic

  - Direction

  - Local IP

  - OS

  - Policy

- ■ Remote IP

- ■ **Enhanced netconn pane**

  An enhanced netconn pane in the Observations right pane includes a visual indication of the direction from where the netconn originated.

# Investigate Page

- ■ **Enhancements to the Investigate page**

  The *Investigate* page includes the following new features:

  - ■ After you receive any search results on the *Investigate* page, all subsequent interactions with the *Investigate* page automatically initiate search requests on your behalf, including clicking on Filters, and clicking or click-and-drag in the histogram

  - ■ If an Alert ID is shown on the Investigate page, a **View all alerts for this event** link to the Alerts page displays. The link now displays in cases where there is only a single alert, not just when there are multiple alerts associated.

  - ■ New searchable fields on both the *Processes* tab and the *Observations* tab:

    - ■ attack_tactic, attack_technique, attack_tid, netconn_actions, netconn_community_id, observation_description, observation_id, observation_type, rule_id

    - ■ Some fields are also searchable on the *Process Analysis* page.

# Alert Triage page

- ■ **Enhancements to the Alert Triage page**

  - ■ Coordinates with the "New Investigate experience" toggle on the *Observations* tab on the *Investigate* page, to show *Observations* data instead of Enriched Events for customers opting in to the *Observations* view.

  - ■ Better organization of the detailed metadata available when expanding individual *Observations*.

# New APIs

- ■ **New APIs now available are Observations, Threat Metadata and Authentication Events.**

  For further information, see CBC Platform APIs.

# What's New - 14 March 2023

**Build 1.12**

To see changes made in previous releases, see VMware Carbon Black Cloud on VMware Cloud Services Platform Release Notes - 2022 Archive.

This release includes bug fixes, enhancements, and improvements.

Read the following topics next:

- Containers
- Managed Detection and Response
- Process Analysis

## Containers

- **Containers**
    - Dataplane charts are more customizable
    - Introduced a **Risk** widget for Workload Risk
    - Redesigned the Clusters page

## Managed Detection and Response

- **Enhancements to the Daily Summary Report**

    Carbon Black is providing more detail to customers about alerts reviewed by Managed Detection and Response.

    - Renamed the "Unlikely Threats" section to "Unlikely Threats by Device" to more easily identify devices that are creating the most alerts.
    - Added a new section called "Unlikely Threats by Alert" that provides a a list of the first 100 unlikely threats.
    - General format improvements

# Process Analysis

- **Enhancements to the Process Analysis page**

  The following enhancements are available on the Process Analysis page:

  - New searchable fields: attack_tactic, attack_technique, attack_tid, netconn_actions, netconn_community_id, observation_description, observation_id, observation_type, rule_id

  - New filter categories:

    - Attack Tactic

    - Attack Technique

- **Export feature added to the Process Analysis page**

  Introducing the **Export** feature to the *Process Analysis* page. Users can now export process event results from the *Process Analysis* page, similar to how process results can be exported from the *Investigate* page.

  The new **Export** button:

  - Exports up to 10,000 process event results at a time.

  - Exports process event results in CSV format.

# Resolved Issues - 14 March 2023

**27**

Read the following topics next:

- All
- Containers
- Endpoint Standard

## All

- **DSER-42944: App Services to expose CSR Audit log in tenant orgs**

- **DSER-43728: Sensor did not go into quarantine**

## Containers

- **CNS-600: Fixed CLI missing violations for scanning custom rules**

- **CNS-1908: Updated Syft version to 0.74.0**

- **CNS-632: Fixed ScanFailed Model did not unpack CLI version and therefore cluster-scanning never stopped**

## Endpoint Standard

- **DSER-38213: Malware Removal failed: device not found**

# What's New - 13 February 2023

# 28

**Build 1.11**

To see changes made in previous releases, see VMware Carbon Black Cloud on VMware Cloud Services Platform Release Notes - 2022 Archive.

This release includes bug fixes, enhancements, and introduces the following new features:

Read the following topics next:

- All

- Workloads

## All

- **Microsoft Azure Active Directory is officially supported in Carbon Black Cloud as a SAML Identity Provider for use in user authentication and Single Sign-On (SSO)**

  For more information about enabling SAML with Microsoft Azure Active Directory see: Enable SAML Integration with Microsoft Azure Active Directory (vmware.com).

## Workloads

- **The VMware Carbon Black Cloud Workload product now includes Center for Internet Security (CIS) Benchmarks**

  The VMware Carbon Black Cloud Workload product now includes Center for Internet Security (CIS) Benchmarks under Hardening for helping enterprises measure and report compliance of organizational workload assets against industry standard benchmarks published by CIS. By curating standard benchmarks, organizations will be able to gauge compliance against CIS level 1 recommendations that matter and improve their security posture. Infrastructure administrators can investigate non compliant assets and remediate them or exclude them from future compliance measurements. Lastly security analysts will be able to report on compliance of organizational windows server assets in release 1.

This feature will be available with Windows sensor 3.9 and currently supports following windows flavors:

- Windows server 2012, Windows Server 2012 R2, Windows server 2016, Windows server 2019 and Windows server 2022.

- This feature will be available to all Workload customers. We will be onboarding existing customers in a phased manner.

For more information about CIS Benchmarks see: CIS Benchmarks (vmware.com).

# Resolved Issues - 13 February 2023

<div style="text-align: right">29</div>

Read the following topics next:

- User Interface
- Kubernetes Events

## User Interface

- **CNS-1760: Fixed issues for the build phase scope usage**

- **CNS-146: Added an indication for rule selection in the policy**

## Kubernetes Events

- **CNS-1795: Added a link to workload details in the Kubernetes Events**

# What's New - 26 January 2023

To see changes made in previous releases, see VMware Carbon Black Cloud on VMware Cloud Services Platform Release Notes - 2022 Archive.

The Carbon Black Cloud team has released the following new features:

- **Carbon Black Cloud Host-Based Firewall**

  Carbon Black Cloud Host-based Firewall enables users to block, allow, and alert on the network behavior of applications across windows endpoints and workloads. This feature replaces legacy firewall solutions with a lightweight, rule-based solution that's easy to manage at enterprise scale.

  Security analysts require visibility into and control over endpoint network traffic to ensure they can detect and respond to attacks before they spread to other devices in the network. With remote work increasing due to the COVID-19 pandemic, security teams have an increased need for visibility and control over employee's network activity when they're working outside of the corporate network.

  VMware Carbon Black Cloud Host-based Firewall enables security teams to further consolidate their security stack by integrating firewall management capabilities directly into their endpoint and workload protection platform. By including Host-based Firewall capabilities in the Carbon Black Cloud platform, SOCs can leverage a single platform for more use cases, increasing their overall efficiency and reducing the resources needed to run their SOC.

  Host-based Firewall is available as an add-on SKU for customers who have Endpoint Standard, Endpoint Advanced, or Endpoint Enterprise, or Workload Advanced or Workload Enterprise.

- **Sensor Gateway for Carbon Black Cloud Workloads**

  The Carbon Black Cloud Workloads team introduced the new sensor gateway feature on January 24, 2023. For details, see the VMware Carbon Black Cloud Workload 1.2.2 Release Notes.

# What's New - 12 January 2023

<div style="text-align: right">31</div>

**Build 1.10**

To see changes made in previous releases, see Chapter 2 Archive of 2023 Improvements and Resolved Issues.

This release includes bug fixes, enhancements, and introduces the following new features:

Read the following topics next:

- Endpoint Standard
- Managed Detection & Response
- Container Essentials

## Endpoint Standard

- **Core Prevention Policy Configurations**

  Since late 2020, the Carbon Black Threat Analysis Unit (TAU) has been crafting and publishing high-fidelity prevention rules to 3.6+ Windows sensors. These rules protect customers from a variety of different types of late-breaking, high-impact attacks without the need for customers to change policy configurations.

  Despite the high-fidelity and low false positive rate of these preventions, we recognize that customers sometimes have business-critical assets that perform certain behaviors and trigger false positives. In this release, we are providing customers with new configuration options to set TAU-published prevention categories to **Alert Only** if necessary within their policies. Upon expanding the Core Prevention dropdown, there are 6 Rule Configs* that have the options of **Alert** and **Alert and Block**.

Figure 31-1.



For more information on the categories shown here, see Core Prevention in the VMware Carbon Black Cloud User Guide.

Upon expanding each category, you can choose whether you want the Core Prevention category to be active.

Figure 31-2.



We expect that you will not need to adjust these configurations regularly, but they are here to assist in the event of a non-remediable false positive. In a future release, you will be able to add exclusions to these configurations without needing to disable prevention completely.

**Rule Lookup for Core Prevention Alerts**

If you receive an alert that a Core Prevention rule generated, you can see what Core Prevention category caused the alert directly from the Alerts page. In the right pane, a new **Rule** field informs you the category that is responsible for the alert.

Figure 31-3.



Clicking on the link will take you directly to the Policies page with the appropriate Rule Config selected. In this case, Defense Evasion was responsible for the alert.

*Rule Configs: A Rule Config is a type of setting within the policy page that allows users to make adjustments to Carbon Black-defined rulesets. Modifications can include toggling between "Alert Only" and "Block and Alert" on a per-operating system basis when the configuration applies to multiple operating systems. In future releases, Rule Configs will support process exclusions and other types of user modifications.*

# Managed Detection & Response

- **Updated Managed Detection (MD) and Managed Detection & Response (MDR) Daily Summary**

  The updated Managed Detection (MD) and Managed Detection & Response (MDR) Daily Summary provides better context of the past day's activity and improved reliability to ensure large reports make it to your inbox. Of note:

  - Certain alerts previously incorrectly classified as "Not Reviewed" are correctly classified as "Unlikely Threat."

  - Unlikely Threats are now grouped by Device.

  - Updated descriptions clarify which product (Managed Detection vs Managed Detection & Response) you've purchased and which CB Analytics alerts are reviewed by the MD/R Analyst team.

  **Note** You can opt into receiving a Daily Summary via email from the Cabron Black Cloud Console in **Settings** -> **Managed Detection**.

# Container Essentials

- **Carbon Black Cloud Container now supports Kubernetes version 1.26**

- **Known Malware Detection in Container Images**

  Using Image File Reputation and Malware Detection for Carbon Black Container, users can now scan all executable files in containers to detect malicious files and malware. Just like vulnerabilities and Kubernetes workload posture, users can now scan images for malware at runtime and in the build phase through CI/CD integration.

  You can use the cbctl to scan containers during the build phase to detect containers with suspected or banded files and to block risk containers early in the SDLC.

  The new File Reputations widget allows users to better understand the number of images running with suspicious files, as well as their distribution by Reputation.
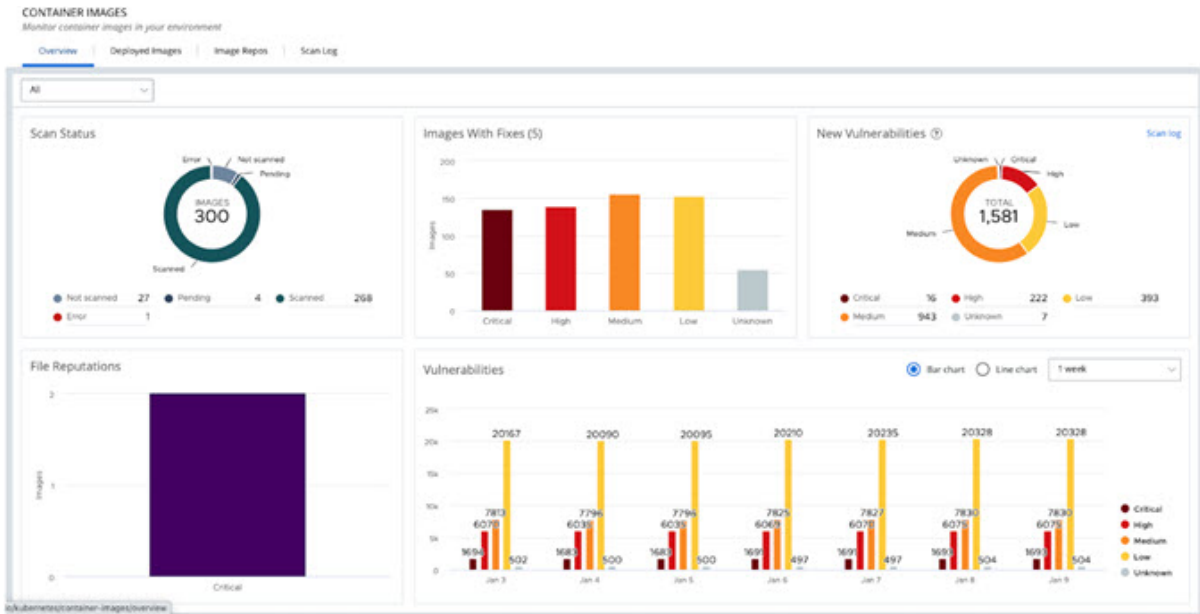
Next to the container image name is a new malware badge for those images running with suspicious or critical files. A list of suspicious or truly malicious files is added to the image information page, to help focus the user's attention to the most risky field.
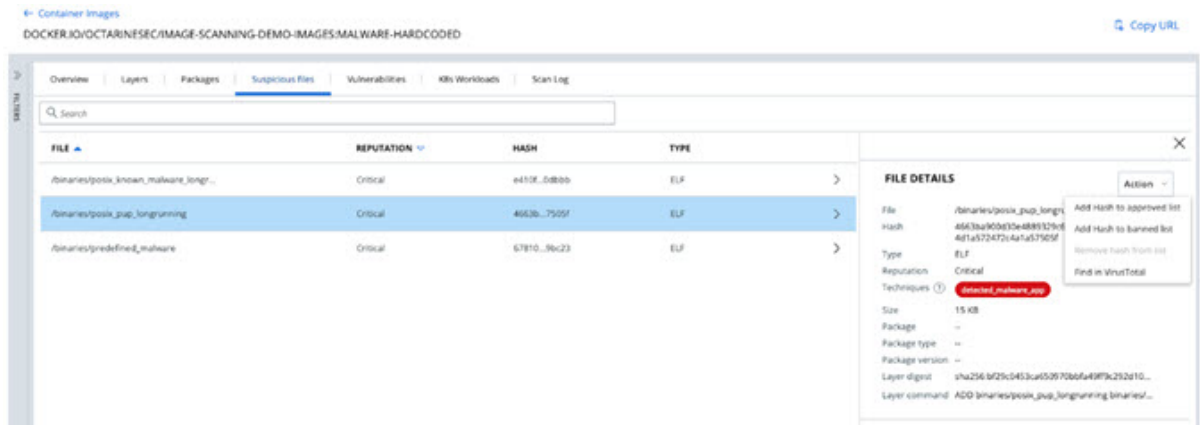


The visual indication for malware is now included in the layer page to help users easily identify the layer and command which introduce to malware for easy resolution.

# Resolved Issues - 12 January 2023

# 32

Read the following topics next:

- Carbon Black Cloud - All
- Container Essentials

## Carbon Black Cloud - All

- **CBCUI-2293: Updated URL for AWS**

  Updated the URL for the **Settings > AWS Accounts** page from */settings/public-cloud* to */settings/public-cloud/aws*.

## Container Essentials

- **CNS-519: Updated risk analyzer to take into account known malware**

- **CNS-1064: Risk score under CB vulnerability page no longer shows CVSS v2 Instead of v3**

- **CNS-1496: Removed the severities filter from the overview page**

- **CNS-1511: Fixed texts that the map/connections are from last 24h to the actual/correct 2h**

- **CNS-1583: Removed cluster setup/edit misleading success message**

- **CNS-1645: Added required RBAC to File Reputations**