



Qualys Container Security

Release Notes for Sensor

Version 1.31.0

January 8, 2024

What's New?

[Creating Custom Secret Detectors](#)

[Prioritizing Sensor PODs](#)

[Introducing a new argument – --limit-resource-usage](#)

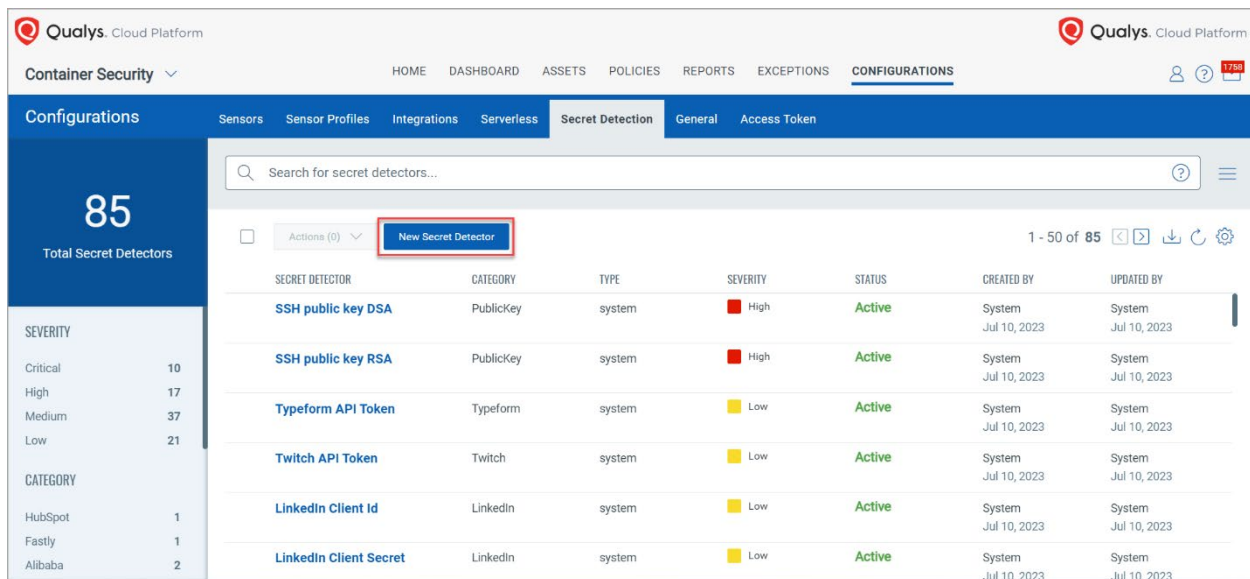
What's New?

Creating Custom Secret Detectors

Starting this release, you can now create, edit, delete custom (non-system) type secret detectors.

Note: You cannot create System type Secret Detector. However, you can edit the Severity, and Status of a System Secret Detector.

In the **Configurations > Secret Detection** tab, you can see the **New Secret Detector** button to create a new secret detector.



The screenshot shows the Qualys Cloud Platform interface for Container Security. The 'Configurations' tab is selected, and the 'Secret Detection' sub-tab is active. A sidebar on the left shows '85 Total Secret Detectors' and a filter for 'SEVERITY' with counts: Critical (10), High (17), Medium (37), and Low (21). The main area displays a table of secret detectors. A 'New Secret Detector' button is highlighted in the top left of the table area.

SECRET DETECTOR	CATEGORY	TYPE	SEVERITY	STATUS	CREATED BY	UPDATED BY
SSH public key DSA	PublicKey	system	High	Active	System	System
SSH public key RSA	PublicKey	system	High	Active	System	System
Typeform API Token	Typeform	system	Low	Active	System	System
Twitch API Token	Twitch	system	Low	Active	System	System
LinkedIn Client Id	LinkedIn	system	Low	Active	System	System
LinkedIn Client Secret	LinkedIn	system	Low	Active	System	System

Fill in the required details for the new secret detector and save the secret detector form. The new Secret Detector will be visible in the Secret Detector's list.

Note: Wild card characters are disabled for the **Regex** field of a Secret Detector. A query search requires the exact matching of the string (non-wildcard entry) to avoid identification of the redundant entries.

Important: Regex field does not support “\” backlash character as it can give false-positive search results later.

Secret Detector Details

Secret Detector Name *

Enter Secret Detector name

63 characters remaining

Category *

Enter Category

63 characters remaining

Severity *

Critical

▼

Regex *

Enter Regex

256 characters remaining

Status

☒ Active ☐ Inactive

Keywords ⓘ

Enter Keywords

Cancel

Save

Prioritizing Sensor PODs

PriorityClass is used in Kubernetes to prioritize Pods in the case of resource contention. With this release, Qualys has added support to the **PriorityClass**. It is named as “qualys-priority-class” in the Sensor deployment yaml file. You can set the `priority` value and `preemptionPolicy`. The Priority that you assign to the CS sensor POD gets applied to the image scanning PODs which are being spun up by the CS sensor.

To know more about prioritizing Qualys PODs, refer to the [Container Security Sensor Deployment Guide](#).

Introducing a new argument - *--limit-resource-usage*

With this release, Qualys has introduced a new sensor argument which needs to be applied during sensor installation. This argument reduces memory consumption for the given sensor leading to better performance of the scans.

Issues Addressed

The following issues are fixed in this release:

- Registry sensors failed to support multiarch OCI images and threw an error – “Cannot find manifest for <image name> from registry; skipping it.”
- SCA, Secret, Malware scans were consuming more memory. Now with the use of “--limit-resource-usage”, memory usage during the security scanning is reduced.

Known Issues

List of the known issues:

- Due to a change in the containerd environment configuration for GKE 1.27 or later, or EKS 1.26 or later versions, Container sensor is unable save the container images. This is impacting some types of the container image scan - Static, SCA, Secret, and Malware.
- Sensor is creating zombie process during a scan in an openshift air-gapped cluster.
- Scanning PODs do not tolerate the following taints.
taints:
effect: NoExecute
key: CriticalAddonsOnly
value: “true”