



Qualys Container Security

Release Notes

Version 1.28

August 14, 2023

What's New?

[Malware Detection Powered by Qualys Deep Learning AI](#)

[Expiration Date for Reports](#)

[Enhancements to the Images Tab](#)

Container Security Sensor Updates

Upgrade your sensor to version 1.28 or later to benefit from the above-mentioned enhancements. Refer to the [Container Security Sensor 1.28 Release Notes](#) for the sensor updates.

API Changes

Refer to the [Container Security API 1.28 Release Notes](#) for the API changes in this release.

Issues Addressed

Qualys Container Security 1.28 brings you many more improvements and updates! [Learn more](#)

What's New?

Malware Detection Powered by Qualys Deep Learning AI

With this release, Qualys Container Security introduces malware detection, powered by Qualys Deep Learning AI, providing you with an effective way to protect against malware threats. You can now scan your container images for any potential malware files and ensure that no malicious container images are deployed into the production environment.

Some of its key benefits include:

- **Early Detection:** It detects malware threats at the early stage in the container lifecycle and ensures the integrity of container images is maintained in the registry.
- **High Accuracy:** It detects malwares with high precision, even when the malware is new or unknown.

To view the detected malwares for an image, go to **Assets > Images** and select **View Details** from the **Quick Actions** menu.

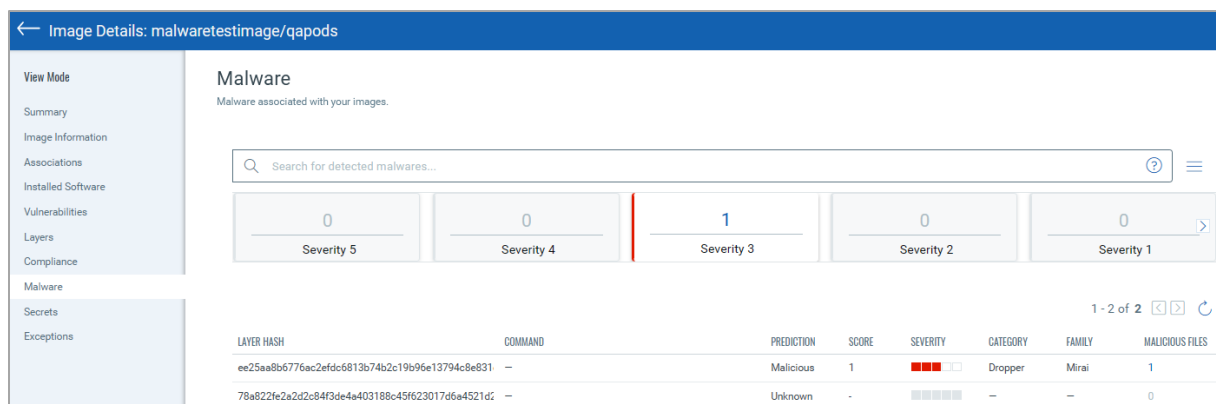


Figure 1: Malwares detected for an image

To view the details of malware, click the count in the **Malicious Files** column.

Additional Information On Files							
FILE HASH	PREDICTION	SCORE	SEVERITY	CATEGORY	FAMILY	FILE NAME	FILE TYPE
e684a0308c3a040f6a9f892eeae411	Malicious	1	■■■■□	Dropper	Mirai	libz.so.2	ELF

Close

Figure 2: Malware details

Notes:

- Malware detection is supported only for the registry sensor.
- The malware scan detects malicious files with UPX and ELF formats.

For more information, see Online Help: [Malware Scans](#).

Expiration Date for Reports

You can now set an expiration date for your reports. Reports are removed from your account after the specified date.

← Create New: Report

STEPS 3/5

- 1 Basic Details
- 2 Report Source
- 3 Report Schedule
- 4 Report Display
- 5 Review and Confirm

Report Schedule

On Demand **Schedule** **On Demand:** The report will run once it is created.

Report expires in *

1 Week

1 Day

1 Week

1 Month

3 Months

Next

In the **Reports** tab, you can see the time duration remaining before your report is deleted from your account.

REPORT NAME	STATUS	FILE FORMAT	CREATED AT	EXPIRES IN	TEMPLATE NAME	REPORT TYPE
	Incomplete	csv	3 hours ago	in 21 hours	Image Vulnerability	ON DEMAND
	Completed	csv	Apr 4, 2023	in 10 months	Image Vulnerability	SCHEDULED
	Completed	csv	Apr 4, 2023	in 10 months	Image Vulnerability	SCHEDULED
	Completed	csv	Apr 3, 2023	in 10 months	Image Vulnerability	SCHEDULED
	Completed	csv	Apr 3, 2023	in 10 months	Image Vulnerability	SCHEDULED

Note: The deletion job runs once a day. Therefore, if your report is expiring today, you may see the value as **scheduled for today** before the report is actually removed.

Enhancements to the Images Tab

The following enhancements are done in the **Assets > Images** tab in the context of secrets:

- You can now quickly filter out the images that have secrets using the **Images with Secrets** filter card. You can also find images based on the severity of the secrets associated with them, using the summary filters or a new search token, **secrets.severity**.

The screenshot shows the 'Assets > Images' tab. On the left, there's a sidebar with '72 Total Images' and a 'SECRETS' section showing counts for MEDIUM (2.43K), HIGH (1.98K), LOW (1.47K), and CRITICAL (690). Below that is a 'COMPLIANCE POSTURE' section with FAIL (115) and PASS (17). The main area has a search bar and filter cards: 'Images with Sev 5, 4 Vulne...' (48), 'Docker Hub Official Images' (0), 'Images with secrets' (65, highlighted with a red box), 'Images With Malware' (0), and 'Images no' (5). Below the filters is a table of images with secrets. The table has columns: REGISTRY, REPOSITORY, CREATED ON, TAGS, IMAGE TAGS, CONTAINERS, VULNERABILITIES, and COMPLIANCE. The first three rows show images from 'registry-1.docker.io' with repository 'zanwarprachi/s...' and various tags like 'logstash-based-wl...', 'static-fail-with...', and 'static-fail-with-...'. The 'VULNERABILITIES' column shows counts for 'On Hosts: 0' and '41', '2', and '2' respectively. The 'COMPLIANCE' column shows counts for '2', '2', and '2' respectively.

- In the **Secrets** section, you can now easily filter out the secrets by their severity using the severity filter cards, as shown below:

The screenshot shows the 'Image Details: 17e766c3243c' page. On the left is a sidebar with 'View Mode' and a list of sections: Summary, Image Information, Associations, Installed Software, Vulnerabilities, Layers, Compliance, Malware, Secrets, and Exceptions. The main area is titled 'Secrets' and shows 'Secrets detected for the image.' Below that is a search bar and filter cards: 'High' (25), 'Medium' (37), 'Low' (21), and 'Total Detected Secrets' (99, highlighted with a red box). Below the filters is a table of detected secrets. The table has columns: SECRET TYPE, CATEGORY, FILE PATH, DETECTED SECRETS, SEVERITY, SCANNED DATE, and LAYER SHA. The first three rows show secrets of type 'Stripe Secret Key', 'Shippo API Token', and 'Age Secret Key' from categories 'Stripe', 'Shippo', and 'Age' respectively, all located at '/root/secrets'. The 'DETECTED SECRETS' column shows '1' for each. The 'SEVERITY' column shows 'CRITICAL', 'LOW', and 'MEDIUM' respectively. The 'SCANNED DATE' column shows 'Jun 6, 2023 11:34 AM' for each. The 'LAYER SHA' column shows '1ca13120fdd4a1be782bc9e7...' for each.

The **Total Detected Secrets** card shows the number of total secrets detected for your image.

Issues Addressed

The following issue has been fixed with this release:

Registry scans failed because the registry sensor could not log in to a registry due to the presence of special characters in the login password.