



Qualys Container Security

Release Notes

Version 1.12

October 1, 2021

Here's what's new in Container Security 1.12!

[Container Security Sensor URL Added to About Page](#)

[OS Information Added to Image and Container Details](#)


[Improved UI Messages for Empty Data Lists](#)

Container Security 1.12 brings you more improvements and updates! [Learn more](#)

Container Security Sensor URL Added to About Page

We've added the Container Security Sensor URL to the **Help > About** page in the UI, making this information easier to access. Any host with a Container Security sensor installed must be able to reach the Container Security Sensor URL. Note that this sample is from an account on US Platform 2. If you're on a different platform, then you'll see a different URL in your account. This UI change will be visible when both Container Security 1.12 and Cloud Platform 3.8 are available on your platform.

About View



Portal Application
Version 3.7.0.0-10

Active Modules

PS 1.3.0.0-3	QUEST 2.28.0.0	APISEC	WAS 6.19.0.0-93	VM	UD 1.1.0	PC	XDR
EDR 1.6.0-10	MDS 2.17.1.0-92	CA 3.7.0.0	SDR 1.3.0.2	CONTINUOUSMONITORING 1.31.0.0			
FIM 3.0.1.0-11	OCA 1.6.0.1	CS 1.11.0.5-2	PCI	SAC	ITAM 2.0.0.0-4	ICS 0.9.1.0-73	
SEM	CERTVIEW 2.8.2.0-20	CLOUDVIEW 1.17.0.2-1	ASSET 2.7.0	QGS 1.3.2.0-11			
PM 1.5.1.1-7	WAF 2.13.0.0	THREAT_PROTECT 2.7.0	SCA				

Versions In Use

Scanner	ML-12.6.41-1
Vulnerability Signatures	VULNSIGS-2.5.267-2
WAS Engine	8.10.61-1
Online Help	3.7.18-1

External Scanners

External Scanners listed are for WAS scans only.

In order to work properly, the Web Malware Detection service may use multiple source IPs that change over time. The Web Malware Detection service only performs normal user requests for web content and it does not perform any testing, so the Web Malware Detection service IP addresses should not need to be whitelisted.

Security Operations Center (SOC)

64.39.96.0/20 (64.39.96.1-64.39.111.254)
2602:FDAA:0:2108::/64
2600:0C02:1020:2881::/64
2600:C08:2015:4400::/64
2600:0C02:1020:2111::/64
2600:0C02:1020:2224::/64

Scanner Appliances

Security Operations Center (SOC)

qualysguard.qg2.apps.qualys.com:443
qgadmin.qg2.apps.qualys.com:443
qualysapi.qg2.apps.qualys.com:443
distribution.qg2.apps.qualys.com:443
monitoring.qg2.apps.qualys.com:443
scanservice1.qg2.apps.qualys.com:443
all in 64.39.96.0/20 (64.39.96.1-64.39.111.254)

Cloud Agents

Hosts on which agents are installed must be able to reach the URL below.

Container Security

Hosts on which container security sensor is installed must be able to reach the URL below.

[Close](#)

OS Information Added to Image and Container Details

For each image/container, we've added the Operating System name to the Image Details and Container Details pages in the UI. This is the same Operating System information that appears when you fetch image or container details using the Container Security API.

Image Details

Go to **Assets > Images**, and select **View Details** for any image in the list. You'll now see **OS Name** under **Image Information**.

← Image Details: centos

View Mode

Summary

Image Information

Associations

Installed Software

Vulnerabilities

Layers

Compliance

Image Information

Last known information for this image

Repository Name:	centos
Image Id (SHA):	7e6257c9f8d8d4cfff5e155f196d67150b871bbe8c02761026f803
Created on:	Aug 10, 2020 6:20:09 UTC
Author:	-
Docker Version:	18.09.7
OS Name:	CentOS Linux 7.8.2003
Size:	193.91 MB
Associated Containers:	6 (6 Running, 0 Stopped)

Container Details

Go to **Assets > Containers**, and select **View Details** for any container in the list. You'll now see **OS Name** under **Container Information**.

← View Details: hamilton

View Mode

Summary

Container Details

Network

Services/Users

Installed Software

Associations

Vulnerabilities

Compliance

Container Information

Last known information for this Container

9830c5ac

Created on : Sep 10, 2020 12:06:25 UTC

Last Scanned : a year ago

Drift : False

State : **RUNNING**

Duration : a year ago

Container ID :	9830c5ac	Status :	RUNNING
Name :	hamilton	Privileged :	False
Image Id :	7e6257c9f	Run as Root :	True
Command :	/bin/bash	OS Name :	CentOS Linux 7.8.2003
Environment :	PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin		
Host Name :	container3		
IP Address :	10.11.12.13		
Container SHA :	9830c5ac21a1a2e5f5f157195932903d3fb81106 affba9b16d52d71		

Improved UI Messages for Empty Data Lists

We've improved the messages that appear in the UI when a data list is empty to clearly indicate why the list is empty. These changes will be visible when both Container Security 1.12 and Cloud Platform 3.8 are available on your platform.

Here are the possible messages you'll see for an empty data list:

No records found.

This means there are no records to display. For example, the Images list will be empty if you have no images.

There are no records matching your query.

This means you have records and you've entered a valid search query but none of your records match the query.

Invalid search query.

This means you have records but you've entered an invalid search query. Fix your query and try again.

The application is currently unavailable. Please contact your system admin or try again in some time.

This means the application is unavailable for some reason and we're unable to display records.

Issues Addressed

- We fixed an issue where customers got a credentials error when configuring an AWS ECR connector when a wildcard was used for the Resource element.
- Now a duplicate rule ID is not allowed for a particular policy ID.
- Now you can use `pageNumber` and `pageSize` input parameters when using the v1.1 API for fetching controls.
- We fixed an issue where users were unable to sort the containers list by last scanned date.
- We fixed the alignment of the mouse-over tool tip for icons that appear in the UI.
- Now when using the API to fetch image and container details, the response will include the published date for a vulnerability.
- We fixed an issue where fetching a detailed images list with a `LastScanDate` range of 1 minute resulted in a 500 error and 0 records. Now a response code of 200 will be returned even if there are 0 records.

The following fixes will be visible in the UI when both Container Security 1.12 and Cloud Platform 3.8 are available on your platform:

- You'll now see Container Security dashboard templates in VMDR.
- On the Assets > Hosts tab, you can now search for hosts using the `lastActivity` search token.
- We removed search tokens pertaining to vulnerability status since these are not applicable in the container security UI. We removed `software.vulnerabilities.status` and `drift.software.vulnerabilities.status` completely, and removed `vulnerabilities.status` from the Installed Software tab inside image and container details.