Qualys Container Security

Release Notes

Version 1.6.2
December 16, 2019

Here’s what’s new in Container Security 1.6.2!

Container Runtime Security (Beta)

Search updated images and containers

CS version on the About page

Container Runtime Security (Beta)

Qualys Container Security 1.6.2 introduces runtime visibility and defense for containers (Container Runtime Security - CRS). CRS provides a function level firewall for containers that allows customers to get granular visibility into container behavior and enforce container activity behavior. CRS allows customers to protect container images and running containers with a Qualys CRS layer. Customers can apply granular behavior policies that provide runtime activity visibility and enforce (Allow, Deny, Alert) runtime behaviors.

We support the following registries for instrumentation:

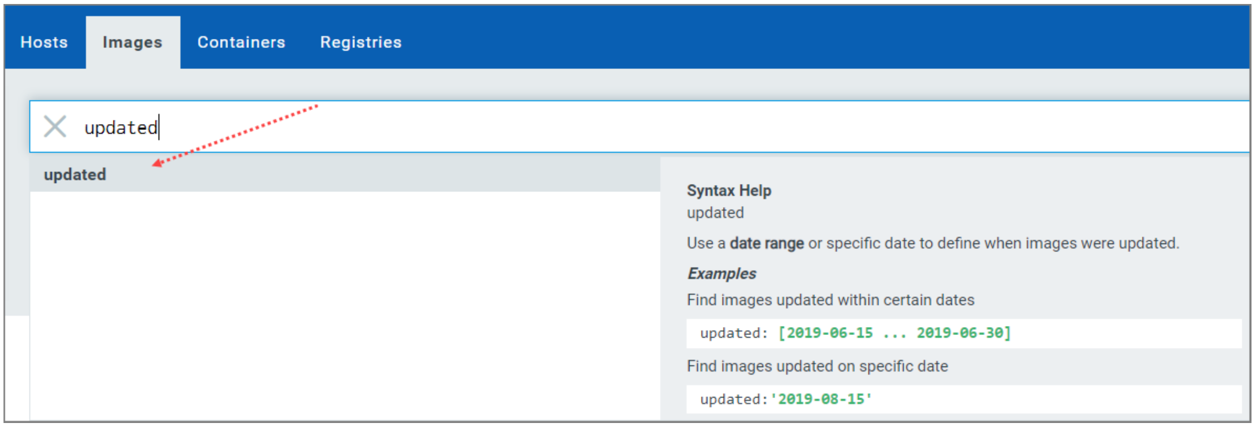
Public registries: Docker Hub

Private registries: v2-private registry: JFrog Artifactory (secure: auth + https).

Container Runtime Security (CRS) is not activated by default for existing and new customers. If you are interested and want to be part of the early preview program please contact your Qualys Account Manager or Qualys Support.

Search updated images and containers

You can now use the "updated" search token to search for updated images and containers.



Syntax Help
updated

Use a **date range** or specific date to define when images were updated.

Examples

Find images updated within certain dates

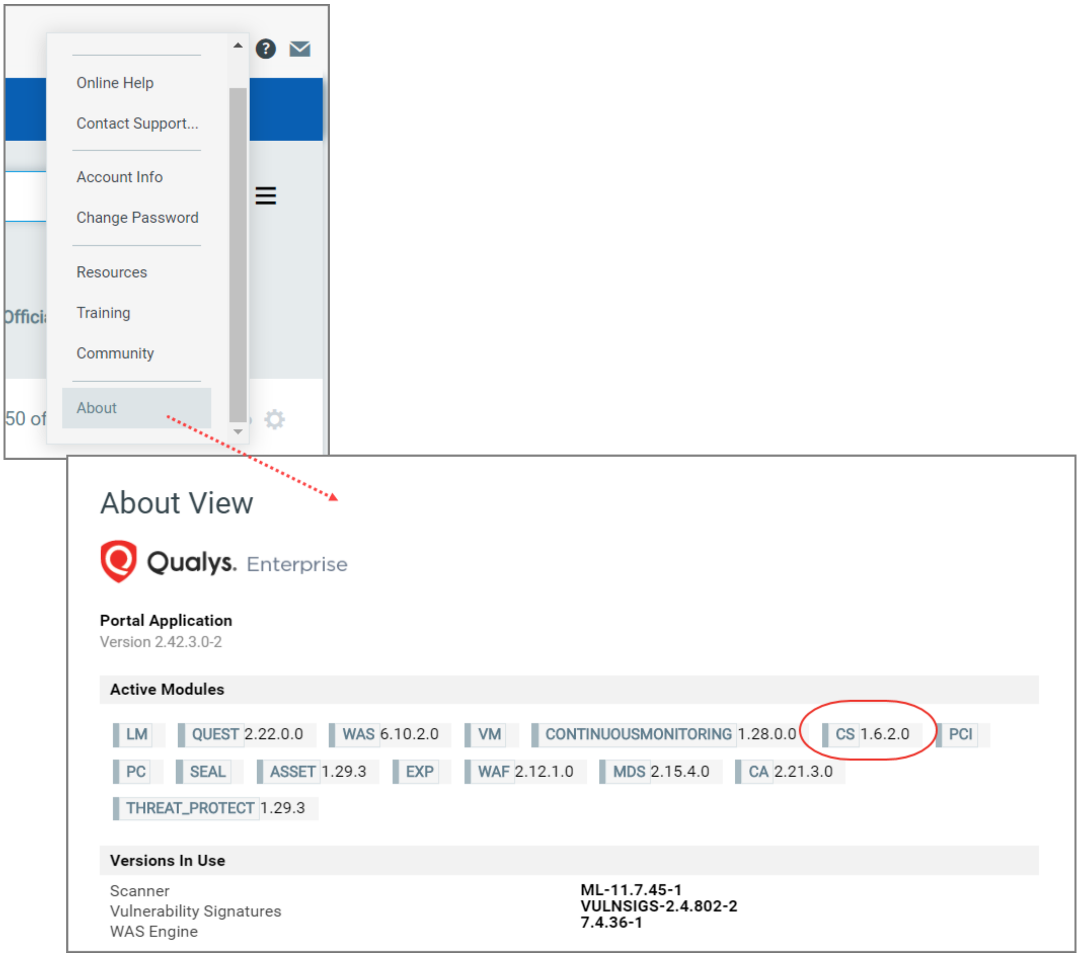
```
updated: [2019-06-15 ... 2019-06-30]
```

Find images updated on specific date

```
updated:'2019-08-15'
```

CS version on the About page

The Container Security version is now displayed on the About page of the CS UI.



About View

Qualys. Enterprise

Portal Application
Version 2.42.3.0-2

Active Modules

LM | QUEST 2.22.0.0 | WAS 6.10.2.0 | VM | CONTINUOUSMONITORING 1.28.0.0 | CS 1.6.2.0 | PCI | PC | SEAL | ASSET 1.29.3 | EXP | WAF 2.12.1.0 | MDS 2.15.4.0 | CA 2.21.3.0 | THREAT_PROTECT 1.29.3

Versions In Use

Scanner	**ML-11.7.45-1**
Vulnerability Signatures	**VULNSIGS-2.4.802-2**
WAS Engine	**7.4.36-1**