Qualys Container Security

Release Notes

Version 1.8.1
January 12, 2021

Here's what's new in Container Security 1.8.1!

CLI Support for CRS Instrumenter

CLI Support for CRS Instrumenter

Applicable when Container Runtime Security (CRS) is enabled for your subscription.

We currently have an option in the Container Security UI that lets you instrument container images that have been scanned by a registry scan job (registry sensor). Starting with this release, you can use a new CLI mode option to instrument any image on your local host directly without the need for a registry scan. The image is not pushed to any repository because the instrumentation happens locally, and the new -layered instrumented image will appear on the local machine and in the Container Security UI.

How it works

We added new fields to the **deploy-instrumenter.sh** file for using CLI mode to instrument images, for identifying the image to instrument, and for identifying the runtime policy to apply to the instrumented image (optional). When you instrument an image using CLI mode, we'll immediately add in our solution and create the instrumented image (appended with -layered) at the same location. One command will instrument one image only, and then it will exit as soon as the instrumentation is done. The instrumented image will appear in the Container Security UI where you can view details about it.

Using CLI mode

1) Pull the docker CLI files from github. You can download them from https://github.com/Qualys/qualys_crs_instrumenter

2) Edit **deploy-instrumenter.sh** to configure user specific details for proxy and vault usage.

3) Run the docker CLI script with CLI mode enabled and the minimum required parameters. You must include --cli-mode to instrument CLI based images. Other required fields are endpoint and image. Policy is optional.

```
./deploy-instrumenter.sh --endpoint <endpoint> --cli-mode --image
<image> [--policy <policy id>]
```

For example:

```
./deploy-instrumenter.sh --endpoint "qualys_joe:my-
password@https://gateway.qg1.apps.qualys.com/crs/v1.3" --cli-mode --
image "6d9ae1a5c970" [--policy "5fd20b4321dabf0001fdc464"]
```

Where:

<endpoint> is in the format of username:password@url if you are not using a vault. Only url is needed for the endpoint when you are using a vault.

<image> is the image Id (e.g. "6d9ae1a5c970") or repository name:tag (e.g. "library/centos:centos72" or "java:latest") for the container image you want to instrument. The image must be present locally where you're running the CLI command.

<policy> is the policy Id (e.g. "5fd20b4321dabf0001fdc464") for the policy you want to immediately apply to the instrumented image.

Instrumented image in the UI

You'll see instrumented images on the **Assets** > **Images** list. Note that for these images there is no value shown in the **Registry** column since these were instrumented on the local host using the CLI mode (not pulled from the registry). Also, these images have not been scanned yet so there are no vulnerabilities shown.