Qualys Container Security

Release Notes

Version 1.6.8.5

October 15, 2020

Here's what's new in Container Security 1.6.8.5!

Easy Install of CRS Instrumenter Service

We now have 3 easy install options for deploying the CRS instrumenter service in your environment. These options have been designed to work with a minimum set of configuration parameters to make the install easy on customers with fewer steps.

These options are available:

Option 1: Run instrumenter using docker CLI based command

Option 2: Run docker compose file

Option 3: Run kubernetes instrumenter.yml

Please refer to the Container Runtime Security User Guide for complete details on how to deploy the instrumenter service using the options listed above.

Support instrumentation for CentOS 7 and 8.1.1911 docker images

Starting with this release you can instrument CentOS 7 and CentOS 8.1.1911 images with Qualys instrumentation for Container Runtime Security (CRS). We support instrumentation for CentOS 7 and 8.1.1911 images with glibc-2.17-307.el7.1.x86_64 and glibc-2.28-72.el8.centos.x86_64.rpm based docker images.

When you choose to instrument an image from the Container Security UI, the instrumenter service will be used to pull down the unprotected image, package our solution into it, and then push it back to the registry as a protected image.

Issues Addressed

- Host associations will now be kept intact after reprovisioning of the sensor (that was deleted in backend).
- We fixed issues that were causing Registry scans not to complete.
- Now we'll show the correct value in the STATUS column when you download the Sensors list in CSV format from the UI.
- We fixed an issue where duplicate images/containers were being fetched with next pagination call.
- We will now show the lastFoundOnHost value in the API response for /v1.1/images and /v1.1/images/{imageid}
- We updated the API User Guide to replace pageNo with pageNumber.