Qualys Container Security

Release Notes

Version 1.6.8.2
September 16, 2020

Here's what's new in Container Security 1.6.8.2!

Container Runtime Security is now GA!

We're excited to announce that Container Runtime Security (CRS) is now generally available. CRS is a separately licensed feature in the Container Security module. It provides runtime visibility & enforcement capabilities for running containers. This allows customers to address various use cases for running containers around security best practice enforcement, file access monitoring, network access control.

CRS requires instrumentation of container images with the Qualys Container Runtime Instrumentation, which injects probes into the container image. Customers can configure instrumented images, containers with granular policies which govern container behavior, visibility. Based on these runtime enforcement policies - runtime events, telemetry can be viewed obtained from the backend via UI, API. Please see user documentation for more details.

Prerequisites

CRS is a separately licensed feature of Container Security. Customers need to have at least one host/sensor license for Container Security Scanning capabilities. In addition to this, customers need to be licensed for an appropriate number of containers for CRS. CRS relies on instrumenting a container image with Qualys instrumentation. This allows for in-container behavior visibility and enforcement. Please contact your Qualys Account Manager or Qualys Support if you are interested in this feature.

CRS Documentation

User Guide | API Guide

Container Runtime Security Deployment Workflow

Here's a look at the CRS UI elements and the deployment workflow.

Step 1: Build image, Push to registry, and Scan with registry sensor

You'll build the image and push it to the registry. Then you must scan the image with the registry sensor. This is a prerequisite for using runtime protection. You'll need to scan each image you want to instrument.

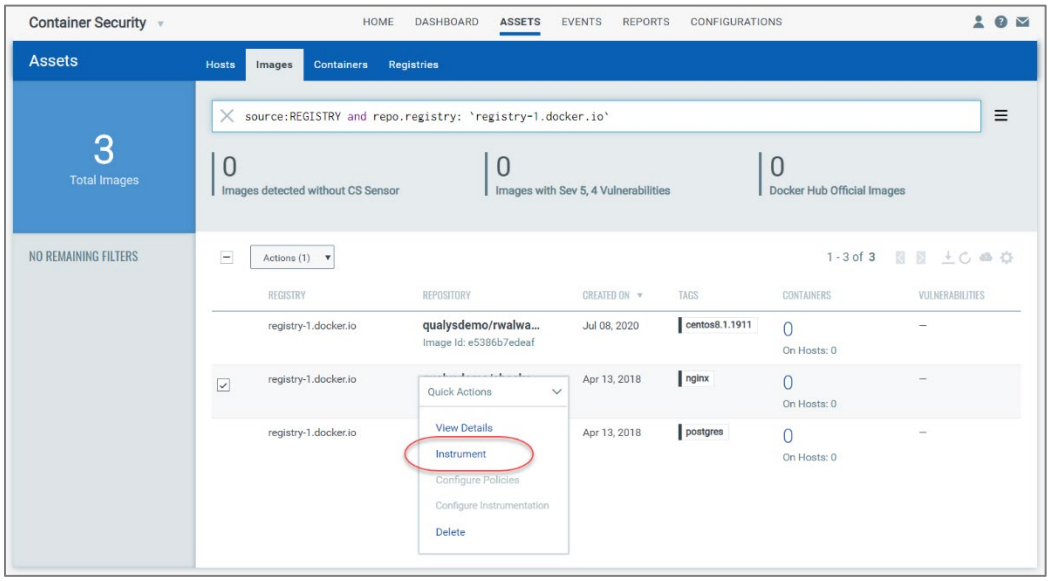
Step 2: Deploy the Instrumenter Service

This is the service that is needed to instrument your images. You'll deploy this service in your environment. Then 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.

Step 3: Instrument container images with Qualys instrumentation

After you build the image and push it into the registry, you'll want to instrument that image with our runtime security solution so that when the image is spun up as a running container it's protected. Once you have the protected image, you can run the image in your runtime environment as a running container. The alerts and notifications will be sent back to Qualys and you'll be able to view runtime events from the UI.

You'll see the new **Instrument** option on the Quick Actions menu under **Assets** > **Images**.

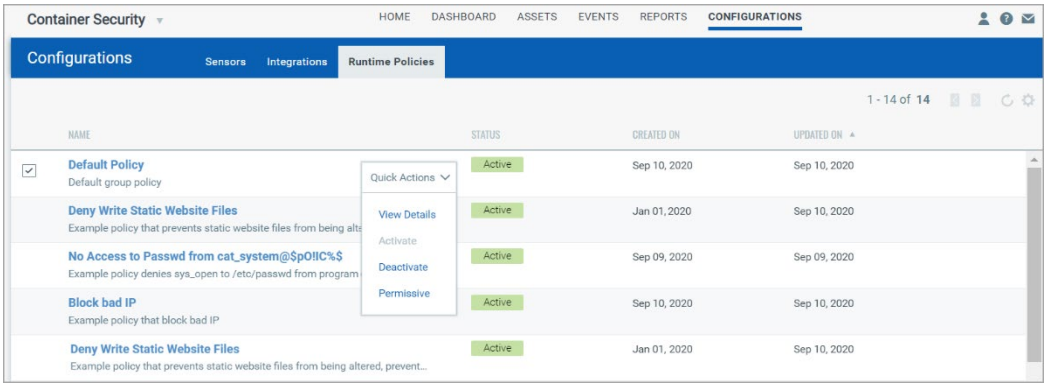


Step 4: Configure Policies and Instrumentation

You'll use the CRS API to create policies, and the UI to assign a policy to an instrumented image. You'll also want to set the policy enforcement level (determines whether policy rules are enforced) and select the log mode (determines which policy hits get logged).

View policies

Go to **Configurations** > **Runtime Policies**. We provide sample policies to help you get started. Select **View Details** for any policy to see more details like the policy rules.

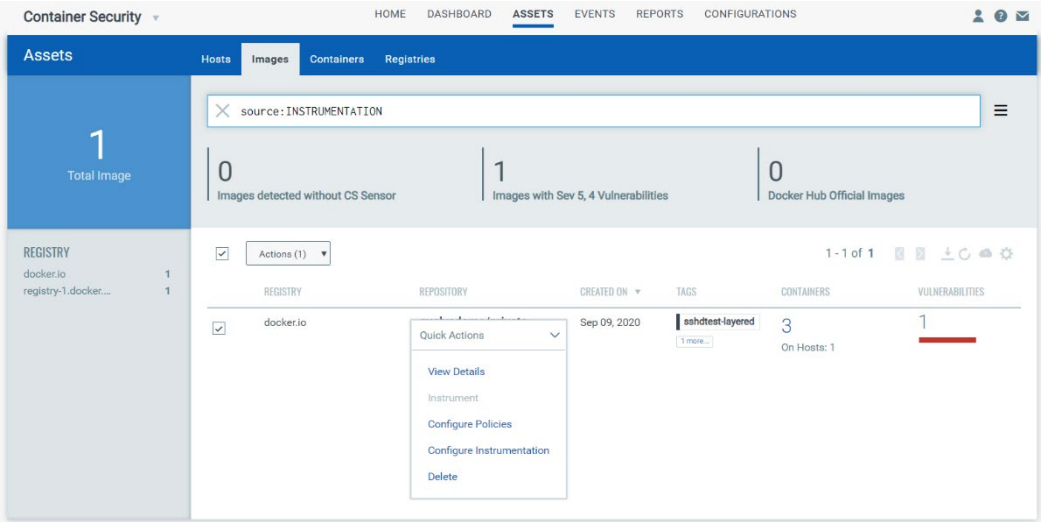


Select policy enforcement level

Select one of the policy enforcement options (**Activate**, **Deactivate**, **Permissive**) from the Quick Actions menu to determine whether or not the policy rules will be enforced on the containers that are spawned from the image. When testing new policies, we recommend you set the policy to Permissive mode, which allows you to see the rule hits without actually enforcing the rules.

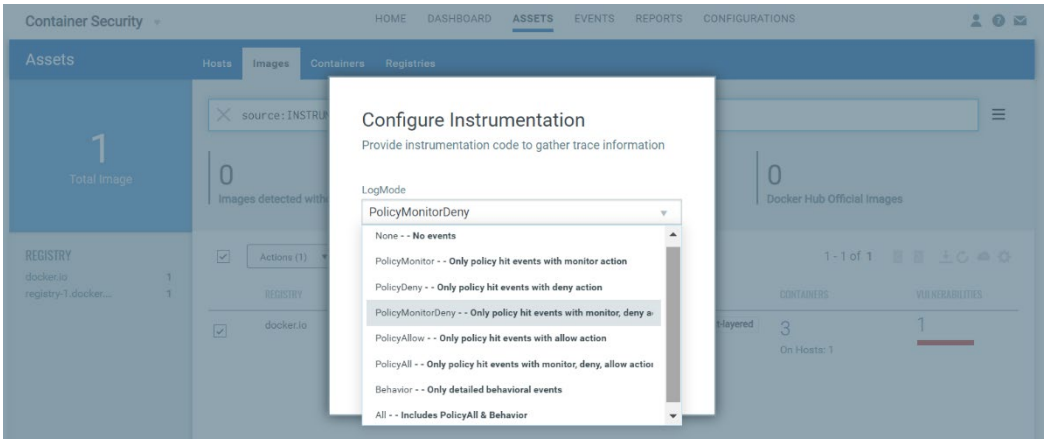
Apply policy to instrumented image

Go to **Assets** > **Images** and search for images with source: INSTRUMENTATION. Then choose **Configure Policies** to select the policy you want to apply to the image.



Choose log mode

Next, choose **Configure Instrumentation** from the Quick Actions menu of an instrumented image to choose a log mode. Your selection determines which policy hits get logged in the container security UI.

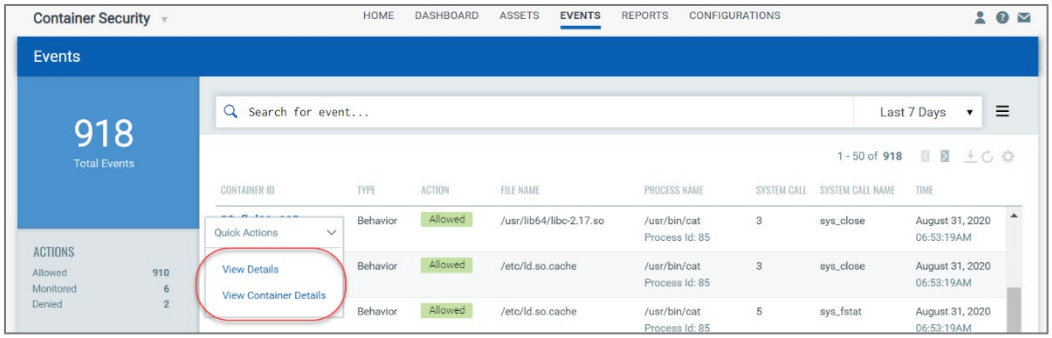


Step 5: Run container from instrumented image

When ready, spawn containers from the instrumented image. The policy applied to the instrumented image gets enforced on the container and activities are logged as per the log mode.

Step 6: View your events

Runtime events are listed on the **Events** tab. Here you can search events and drill-down into event details. Use options on the left side bar to quickly find events by the action taken (Allowed, Monitored, Denied) and the event type (Behavior, Standard). Use the search field above the list to find events by other event details like the container SHA, system call, process, etc.



You can choose from the following options on the Quick Actions menu for any event in the list:

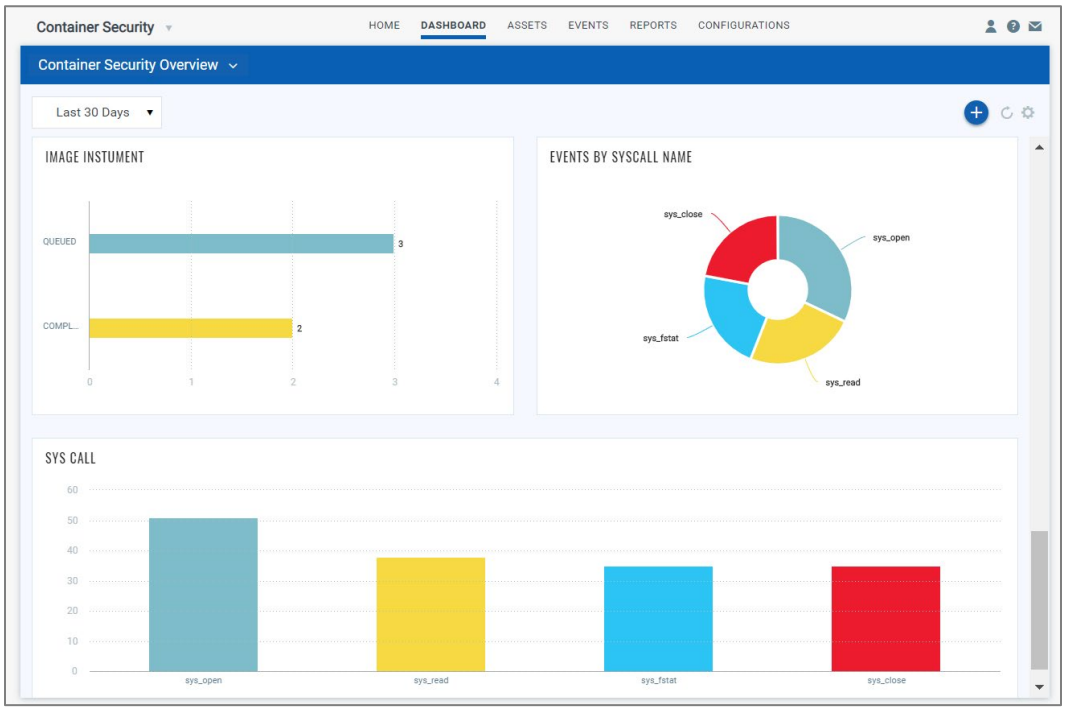
View Details – Get event details like the process, system call, file name and action.

View Container Details - Get container details, including events, runtime profile, container information, associations and vulnerabilities.

View event details on dashboard

Go to **Dashboard** and you'll see widgets with info about events like the number of events by action, event type and system call name. You'll also see the number of images that have been successfully instrumented and the number of images currently queued for instrumentation.

Check out this sample dashboard.



Issues Addressed

- We fixed an issue where a new vulnerability signature was released to address a false positive on an image/container but the scan after the signature update did not close the vulnerability. Now we'll remove the previous data and add the new vulnerability status based on the new signature.