



Adding Container Image Scanning to your Codefresh Pipelines with anchore



JEREMY VALANCE

Jeremy Valance

Solutions Architect

anchore

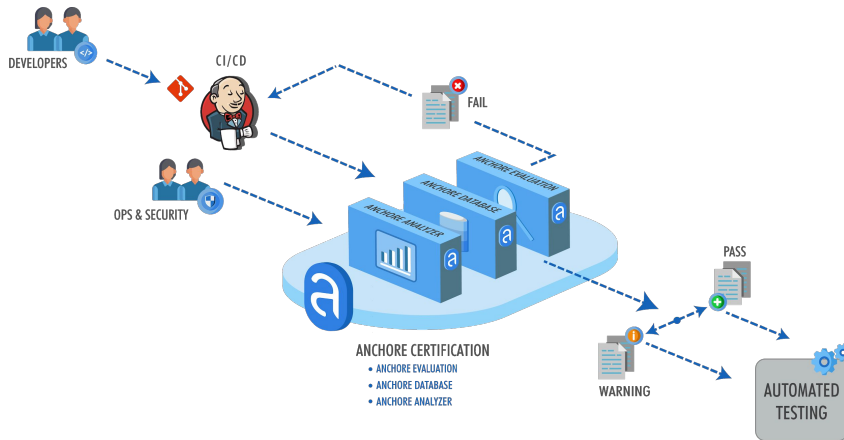


Agenda

- Introduction
- Container Security Models
- Scanning with Anchore in a CodeFresh Pipeline
- Live Demo
- Q&A

Container Security

- Should involve securing all pieces of the container lifecycle (image, registry, container runtime, and host).
- Mandatory image scanning step in CI/CD process.
- “Shift left” to catch vulnerabilities early in the development lifecycle.
- Methods and tooling for notifications and remediation are available when vulnerabilities are found within a container image.



Why do we need to scan images?

- Container images greatly increase speed of development and release.
- Images are static archive files that include all components to run a given app or service.
- Libraries and components within the image may contain vulnerabilities.
- If not scanned, images with vulnerable packages can make their way into production environments.
- Developers may accidentally leave secrets or credentials within images.
- Image metadata and Dockerfiles may contain sensitive configurations like unused exposed ports or running as a root user.

What does container image scanning do?

- Anchore analysis tools will inspect container images and generate a detailed manifest of the image, a virtual 'bill of materials' that includes official operating system packages, unofficial packages, configuration files and language modules and artifacts.
- Policies rules can be created to govern security vulnerabilities,, configuration file contents, secrets, manifest changes, exposed ports or any user defined checks.
- Image scanning is focused on gaining a deep understanding of the contents of the images, and does not scan proprietary source code.

How do Anchore policies work?

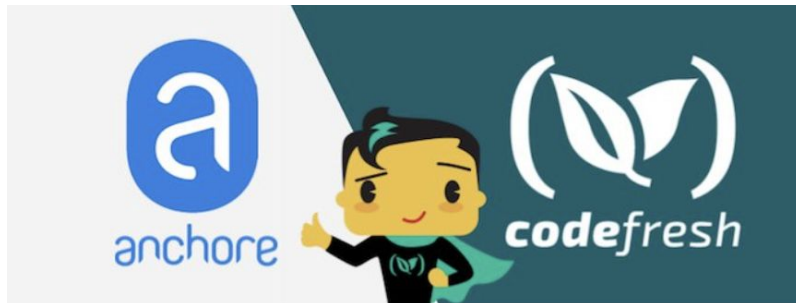
- Anchore first analyzes the container image, then conducts a policy evaluation on it.
- Anchore policies are made up of a set of user-defined rules such as:
 - Security vulnerabilities
 - Image manifest changes
 - Configuration file contents
 - Presence of credentials in an image
 - Exposed ports
 - Package whitelists and blacklists
- Policies can be created through API, CLI, or Enterprise UI.
- Policies can be enforced through CI/CD, API or CLI.

Example Policy

```
{
  "id": "48e6f7d6-1765-11e8-b5f9-8b6f228548b6",
  "name": "Example Policy",
  "rules": [
    {
      "action": "STOP",
      "gate": "dockerfile",
      "id": "ce7b8000-829b-4c27-8122-69cd59018400",
      "params": [
        {
          "name": "ports",
          "value": "22"
        }
      ]
    }
  ]
}
```


Scanning with Anchore in a Codefresh pipeline

- All configuration detailed within codefresh.yml file.
- First step builds image from Dockerfile and pushes to Codefresh registry automatically.
- Second step scans image with Anchore and evaluates the policy rules against the analyzed data.
- Final step (depending on the result of step two), will push the image to Dockerhub.



How do I use it?

- Anchore Engine Open Source: <https://github.com/anchore/anchore-engine>
- Anchore Enterprise: <https://anchore.com/enterprise>
- Github examples:
 - Image Fail: https://github.com/valancej/node_critical_fail
 - Image Pass: https://github.com/valancej/node_critical_pass

See our blog post
complete with
codefresh yaml at:
[Codefresh.io/blog](https://codefresh.io/blog)

<https://codefresh.io/blog>

Adding Anchore Container Image Scanning to Your Codefresh Pipelines

Security-Testing | November 20, 2018



The image shows a superhero character with a yellow face and black suit, standing between the Anchore logo (a blue circle with a white 'a') and the Codefresh logo (a white leaf-like shape inside parentheses). The word 'anchore' is written in blue below the logo, and 'codefresh' is written in white below the logo.

Build Image

In the first step of the pipeline, we build a sample Docker image from a Dockerfile as defined in our codefresh.yaml:

```
1 build_image:
2   title: Building Docker Image
3   image: build
```

Summary

- Container images should be scanned as a step in CI/CD process.
- Policies should be created and enforced at the CI/CD layer to increase confidence in deployments.



anchore

Questions?

anchore

Get the open source at
anchore.com/opensource

Anchore.com

() **codefresh**

Schedule a 1:1 with our
DevOps Experts
-and-
Sign up for FREE! 120
builds/month

Codefresh.io



Thank You

See our upcoming Codefresh Live events at:

codefresh.io/events

