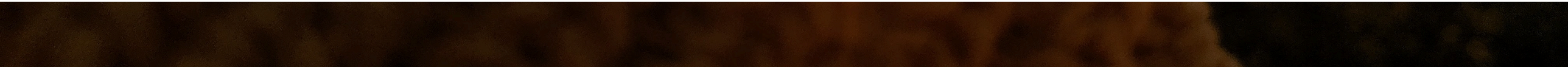
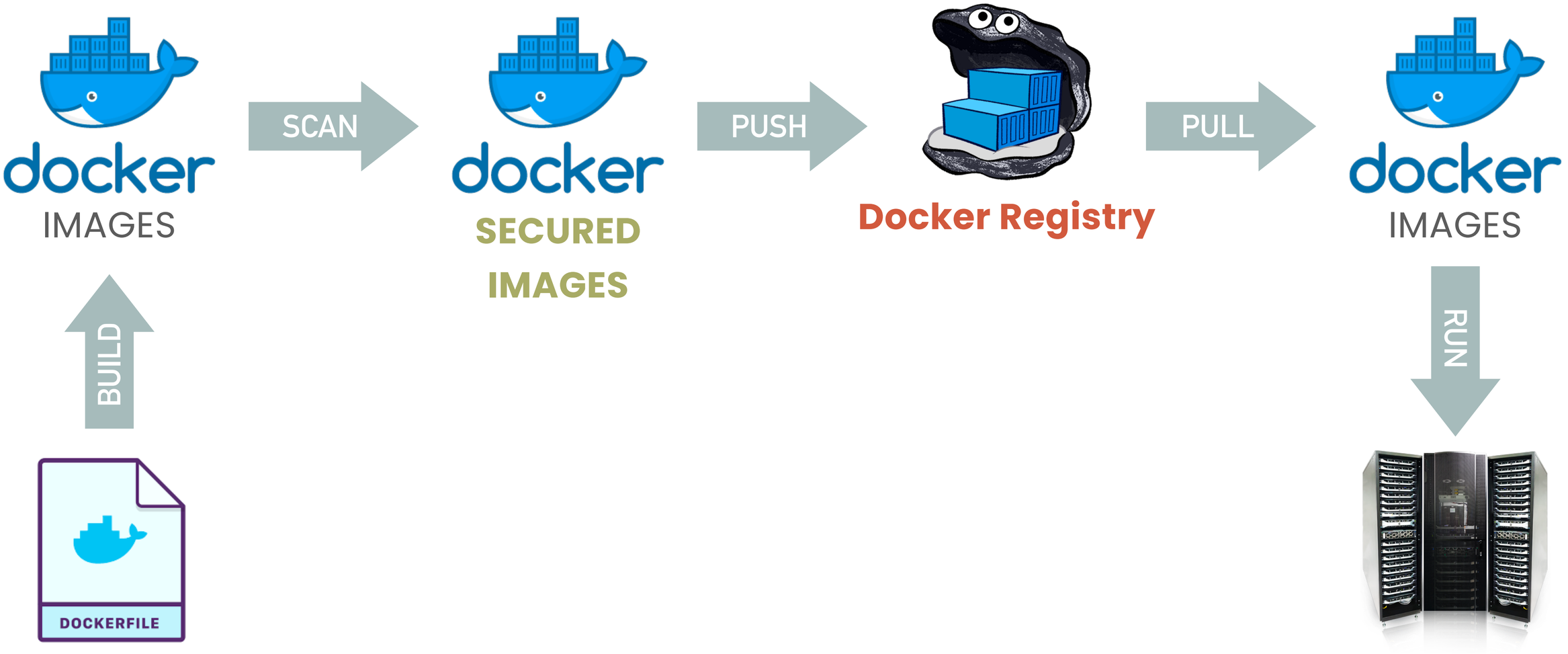
INTRODUCTION TO DOCKER

INTRODUCTION TO DOCKER

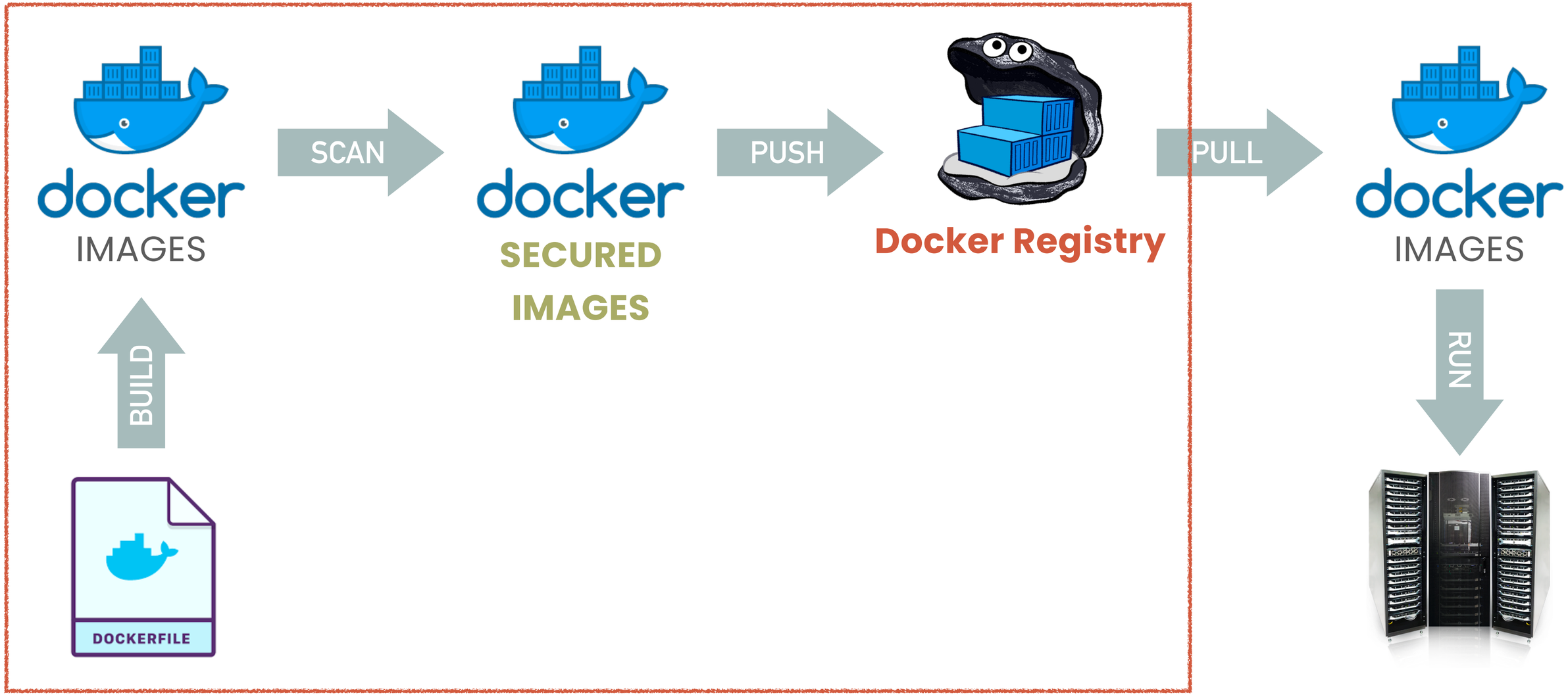
Multi Stage Build, Security Scan and Publish to Registry



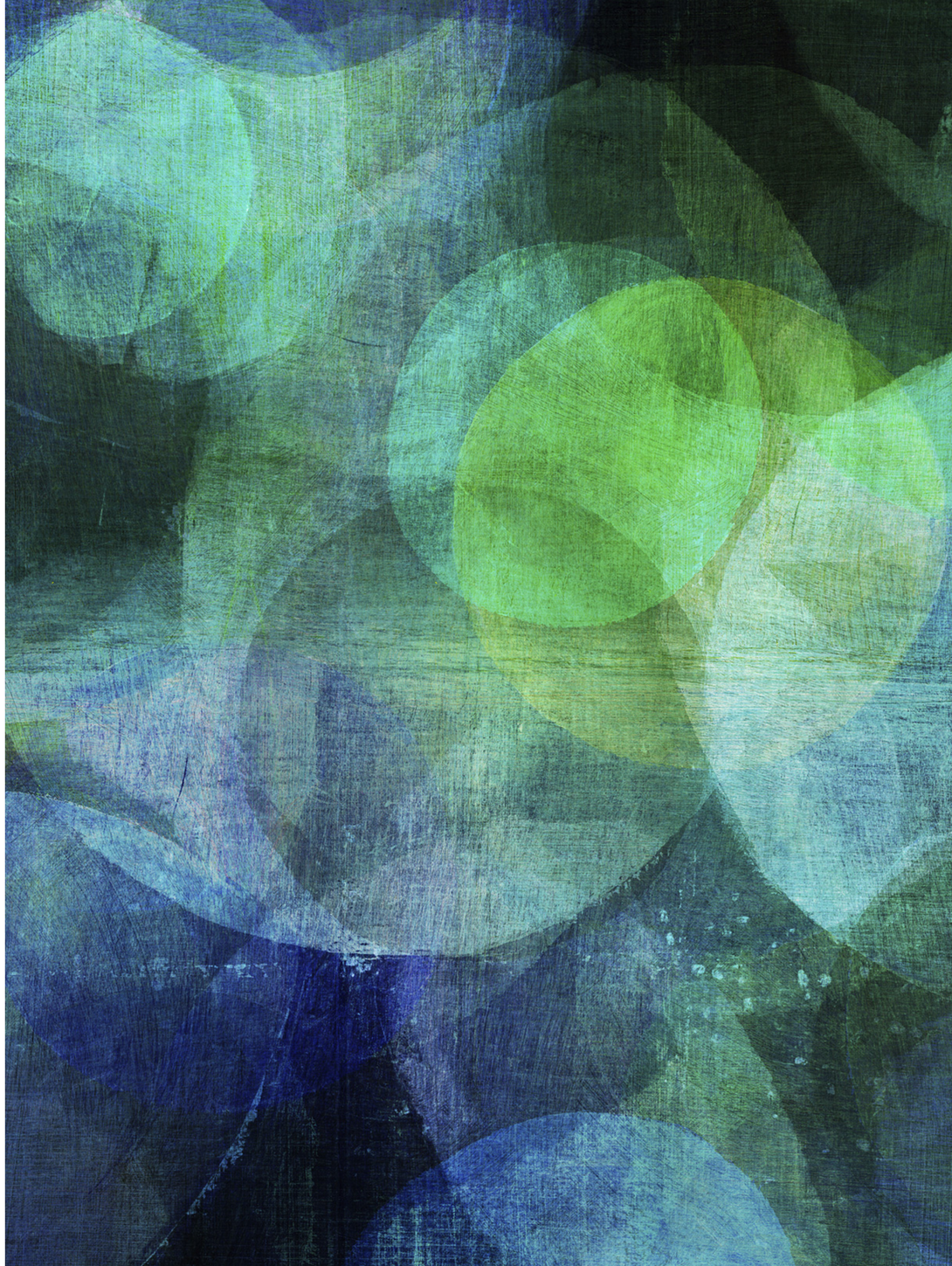
DEVELOPMENT WORKFLOW WITH DOCKER



DEVELOPMENT WORKFLOW WITH DOCKER

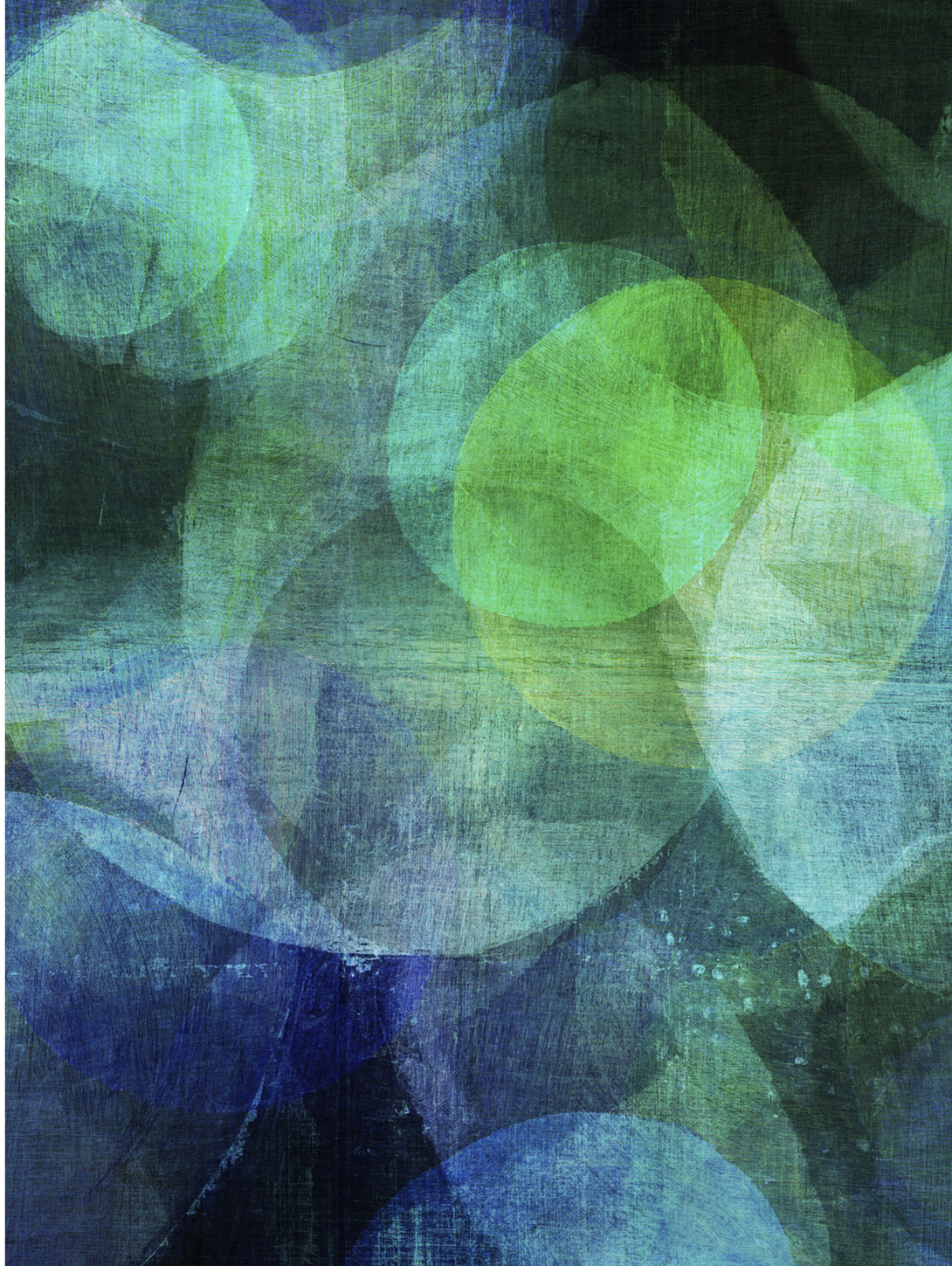


AGENDA



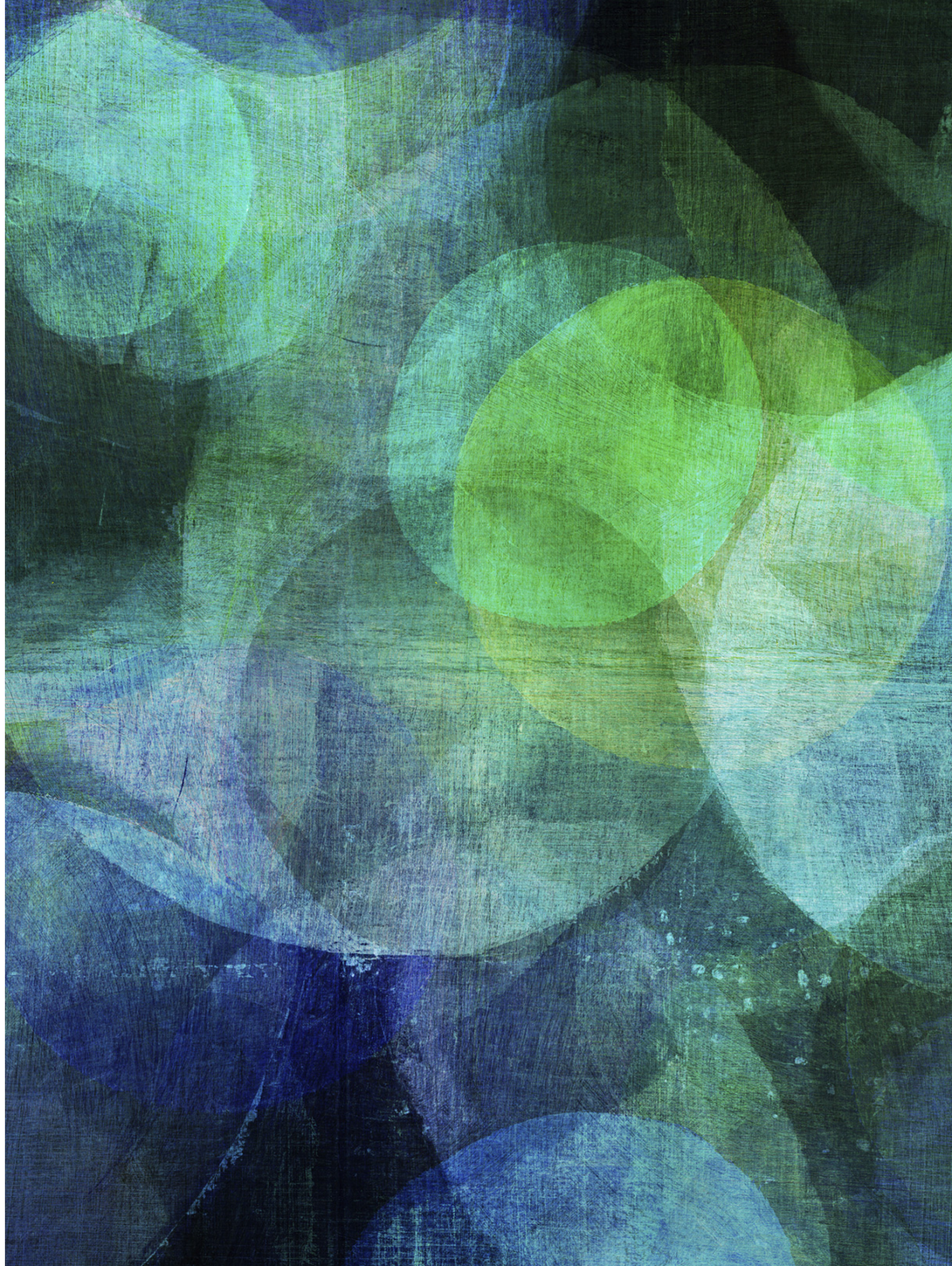
AGENDA

- Multi Stage Build



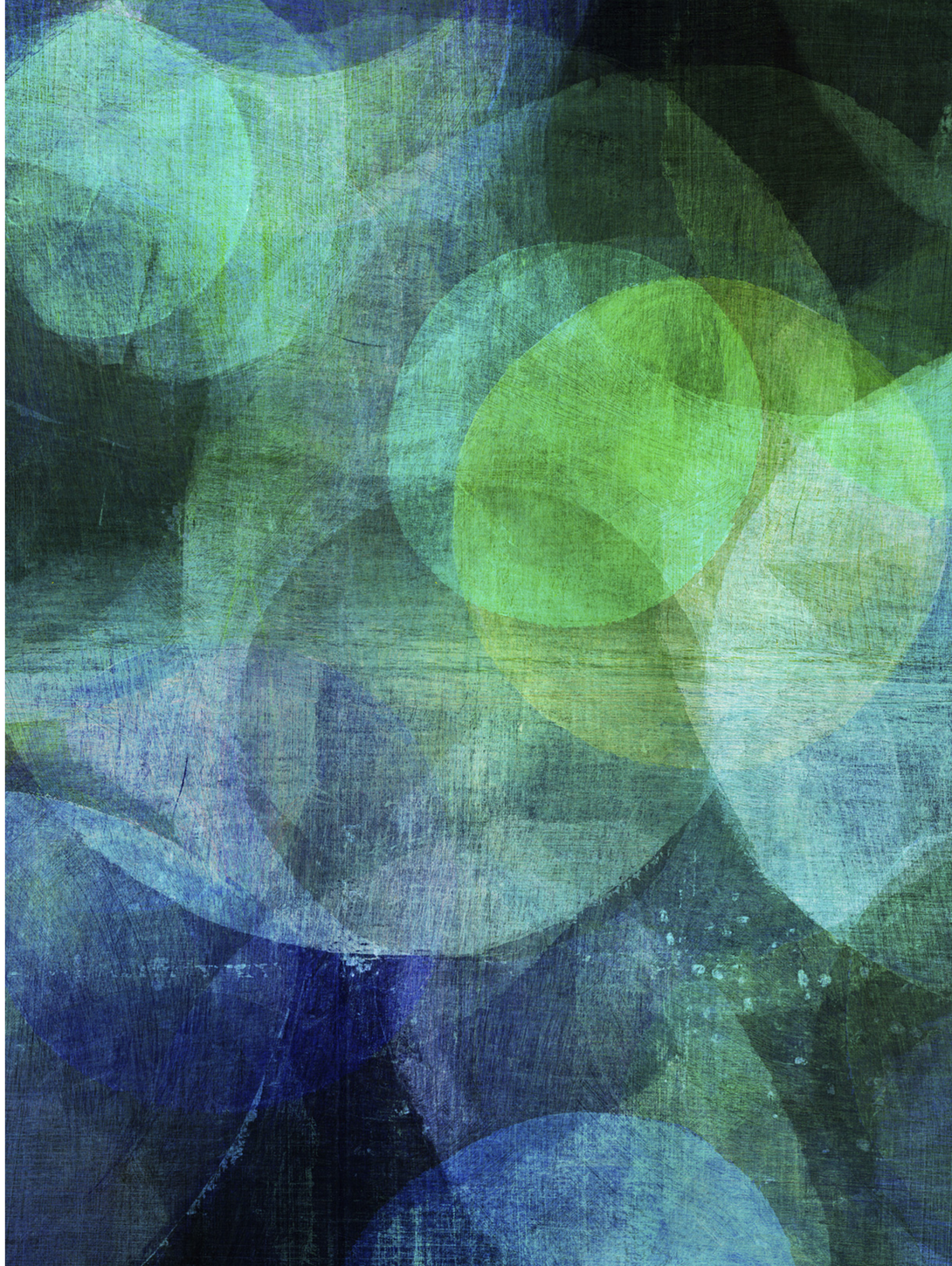
AGENDA

- Multi Stage Build
- Docker Scan



AGENDA

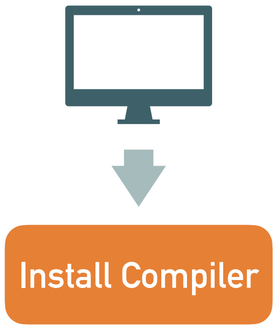
- Multi Stage Build
- Docker Scan
- Docker Registry



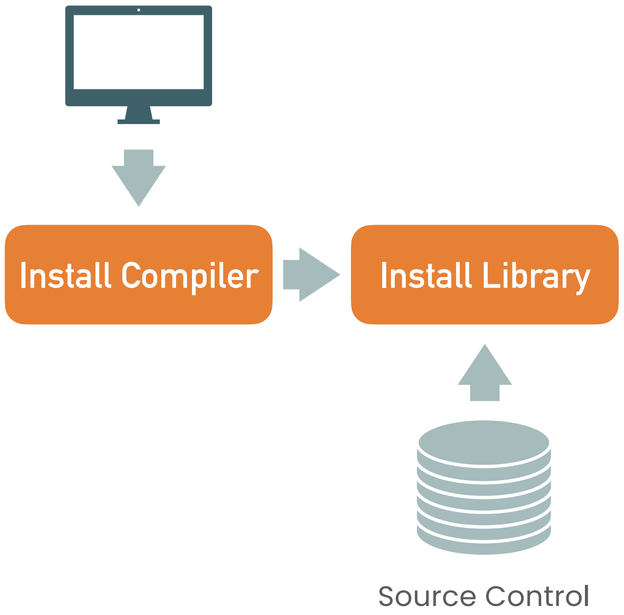
MULTI STAGE BUILD

CHALLENGING ABOUT BUILDING DOCKER IMAGE

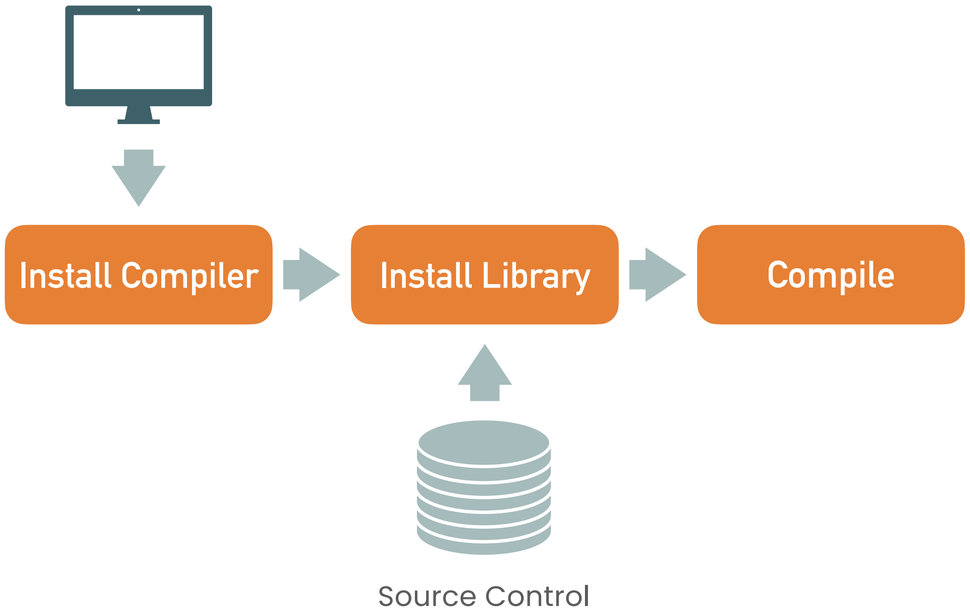
CHALLENGING ABOUT BUILDING DOCKER IMAGE



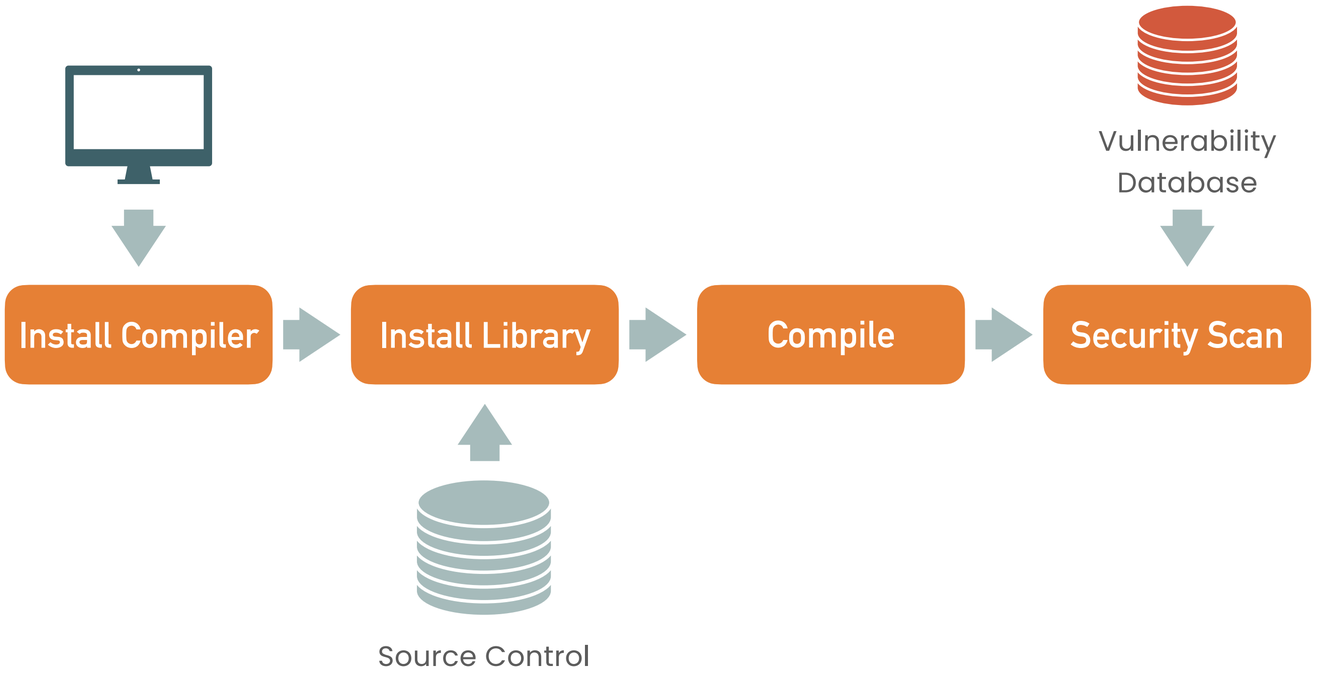
CHALLENGING ABOUT BUILDING DOCKER IMAGE



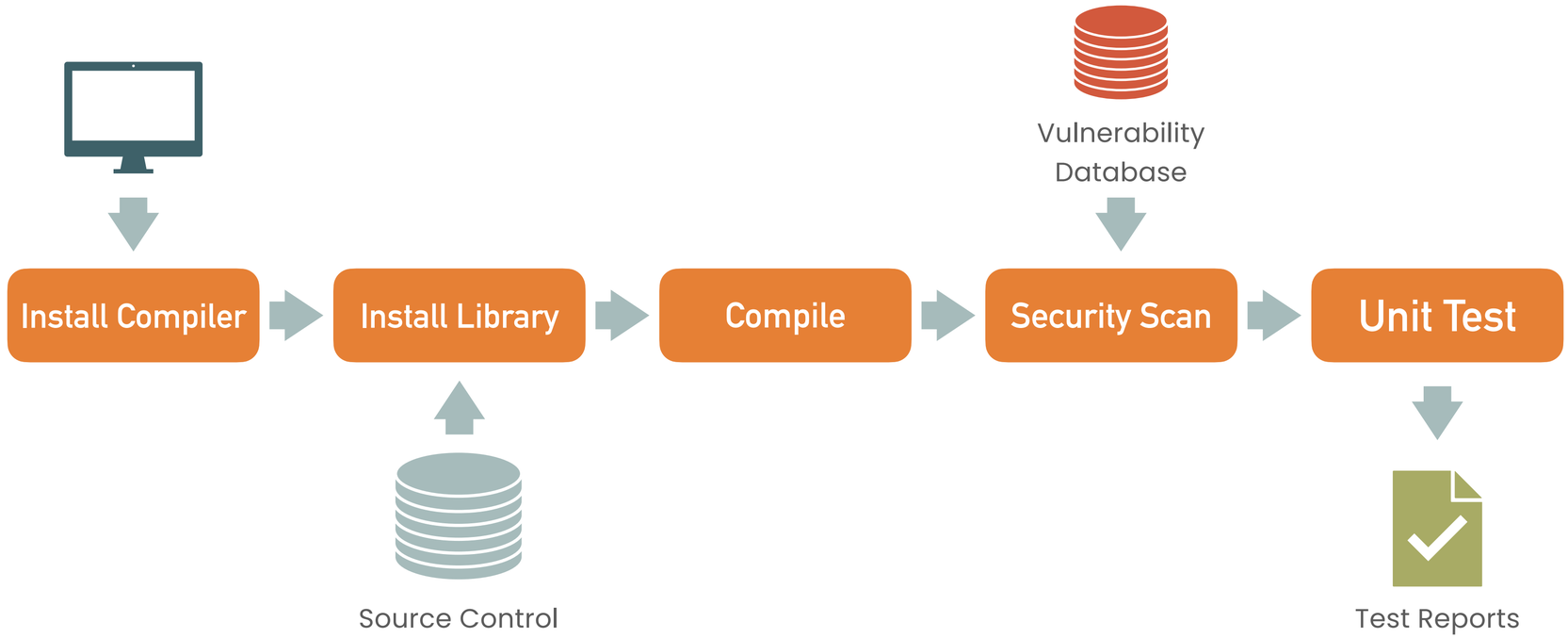
CHALLENGING ABOUT BUILDING DOCKER IMAGE



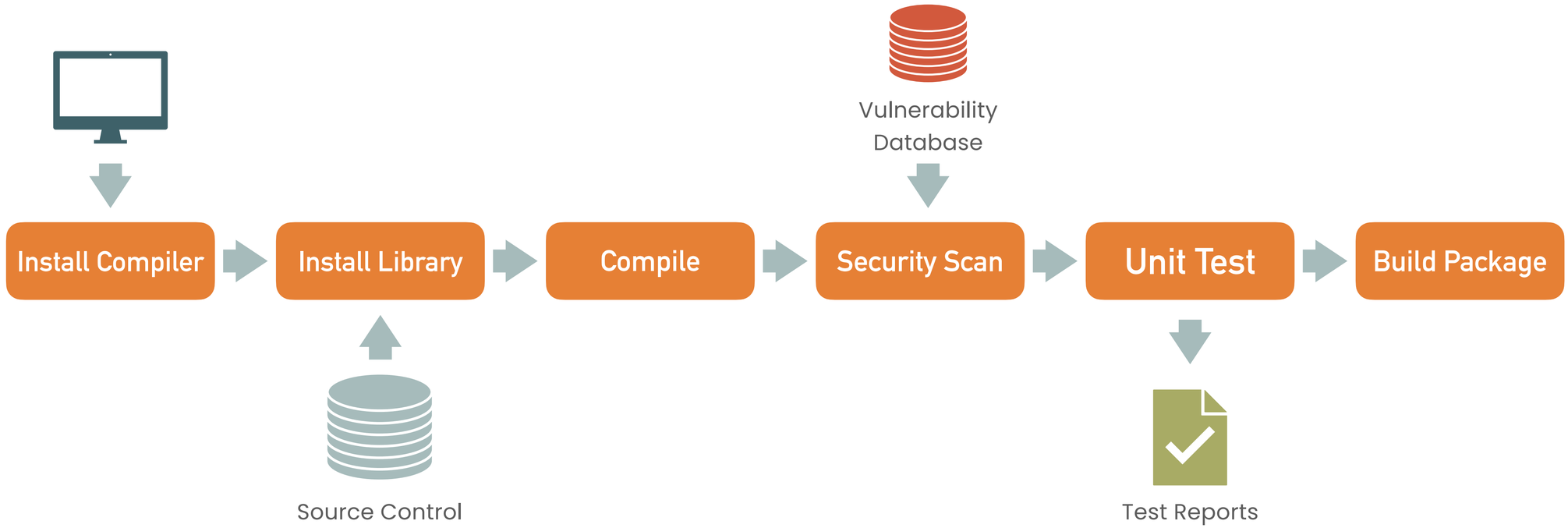
CHALLENGING ABOUT BUILDING DOCKER IMAGE



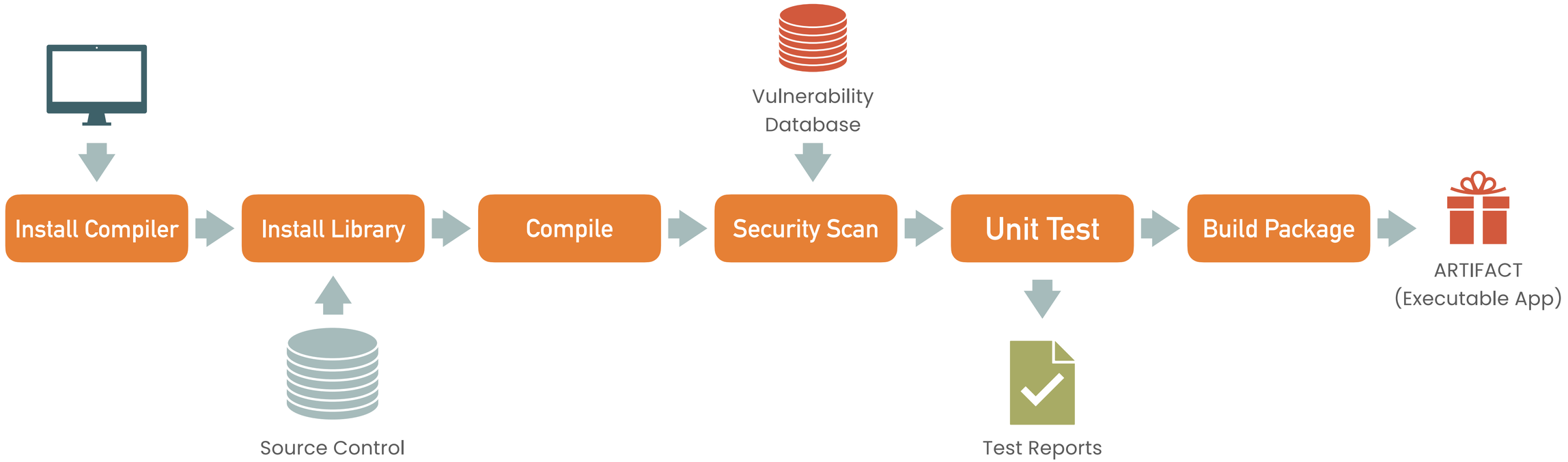
CHALLENGING ABOUT BUILDING DOCKER IMAGE



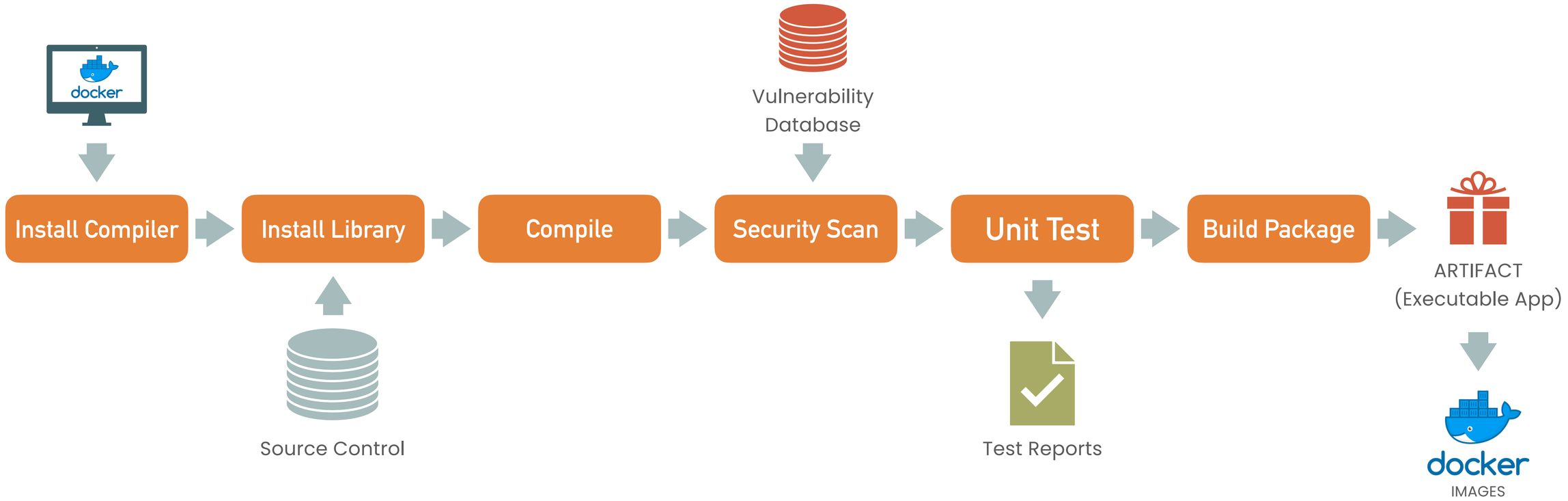
CHALLENGING ABOUT BUILDING DOCKER IMAGE



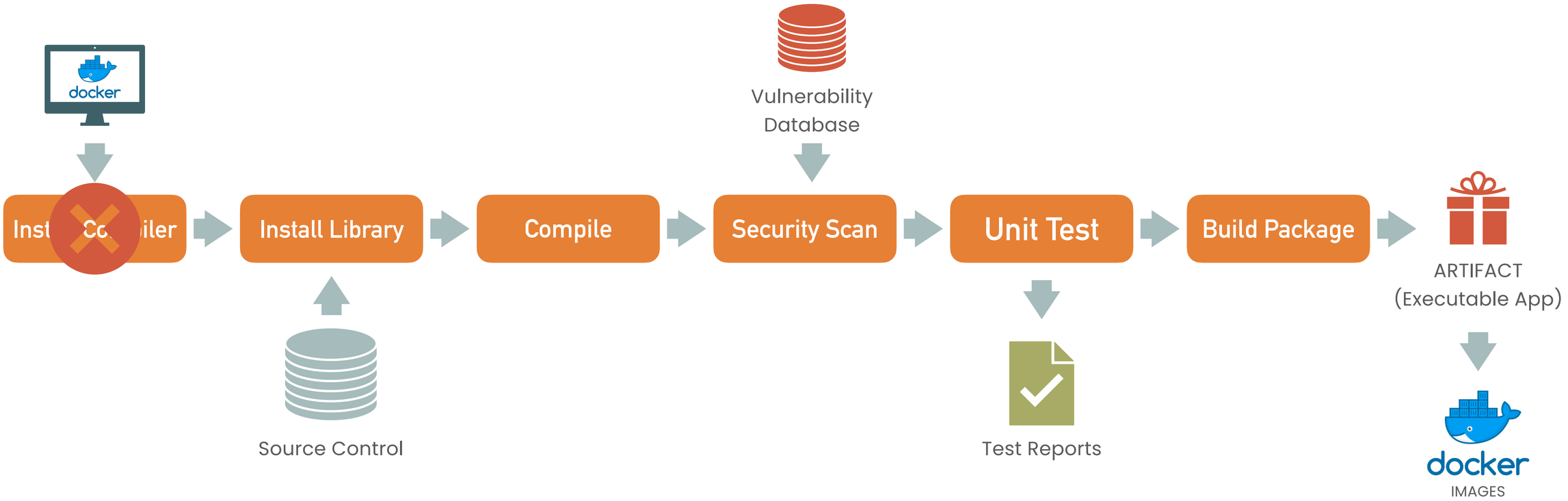
CHALLENGING ABOUT BUILDING DOCKER IMAGE



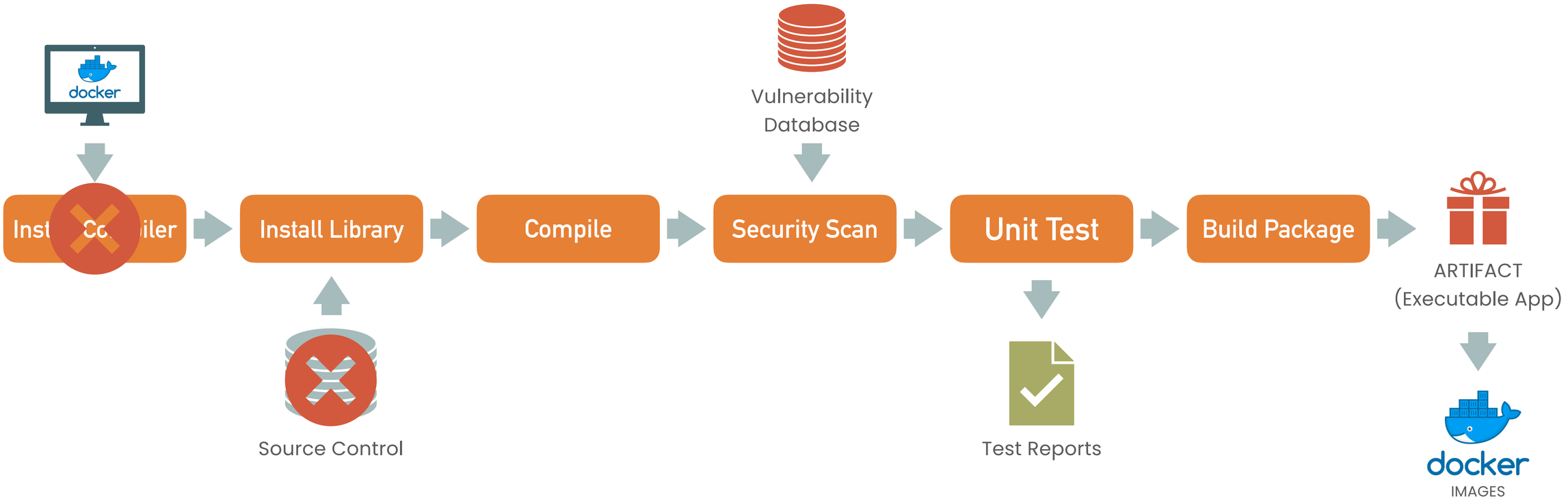
CHALLENGING ABOUT BUILDING DOCKER IMAGE



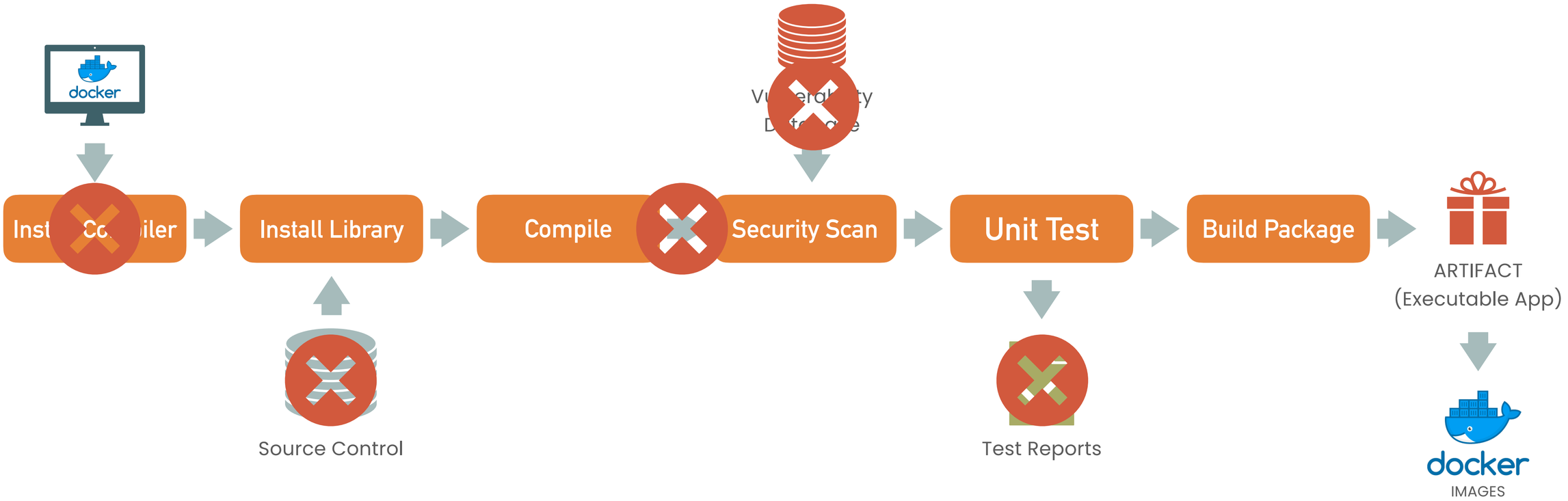
CHALLENGING ABOUT BUILDING DOCKER IMAGE



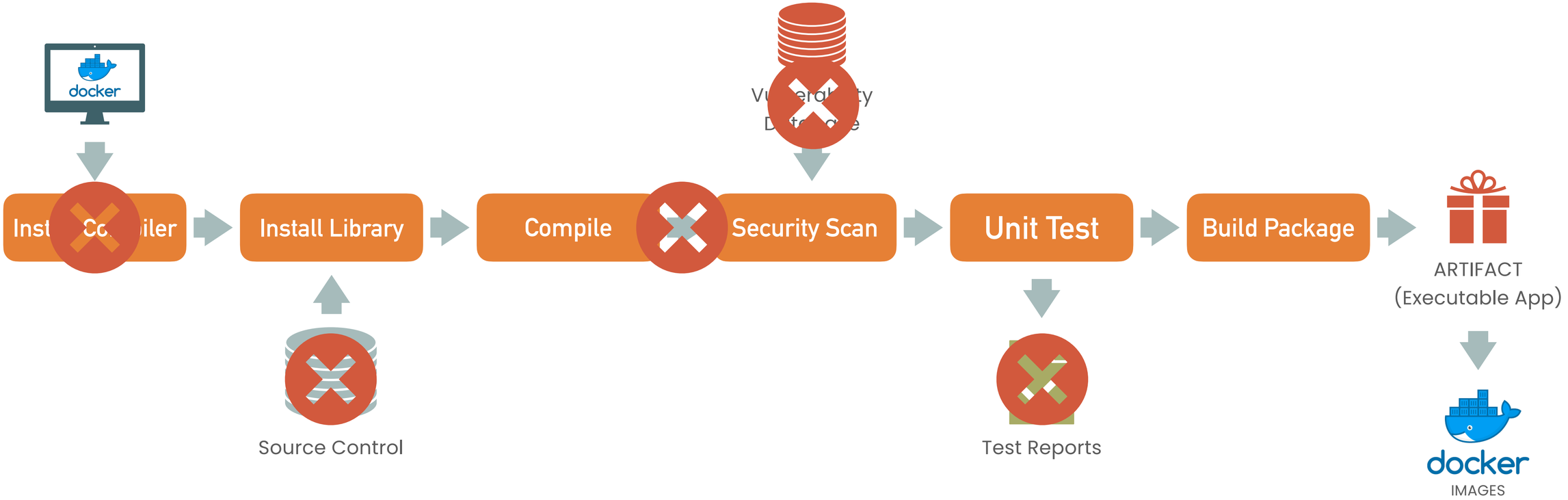
CHALLENGING ABOUT BUILDING DOCKER IMAGE

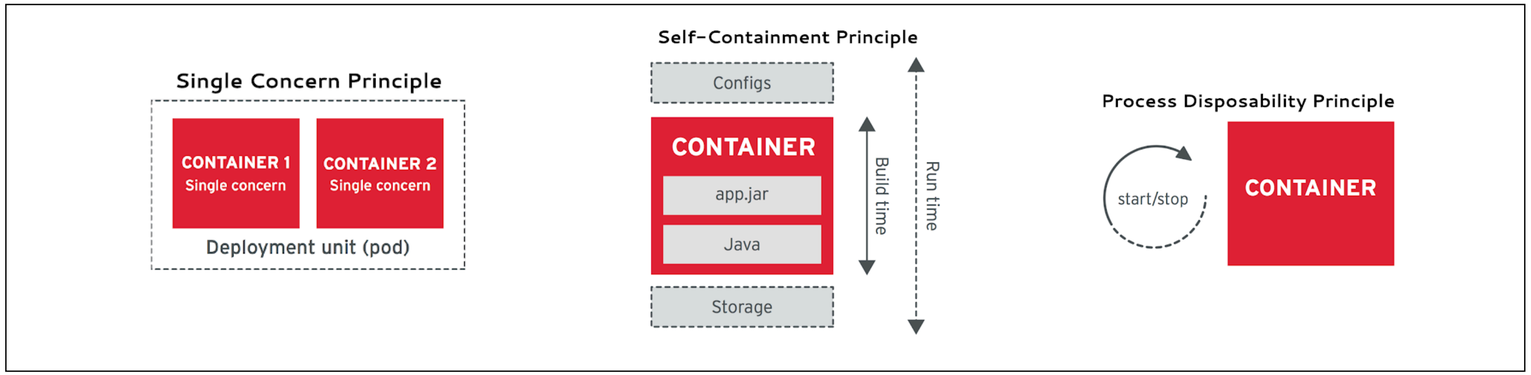


CHALLENGING ABOUT BUILDING DOCKER IMAGE



CHALLENGING ABOUT BUILDING DOCKER IMAGE





DOCKER FOR BUILD AND DOCKER FOR RUN

DOCKER FOR BUILD AND DOCKER FOR RUN

DOCKER FOR BUILD AND DOCKER FOR RUN

DOCKER FOR BUILD AND DOCKER FOR RUN

DOCKER FOR BUILD

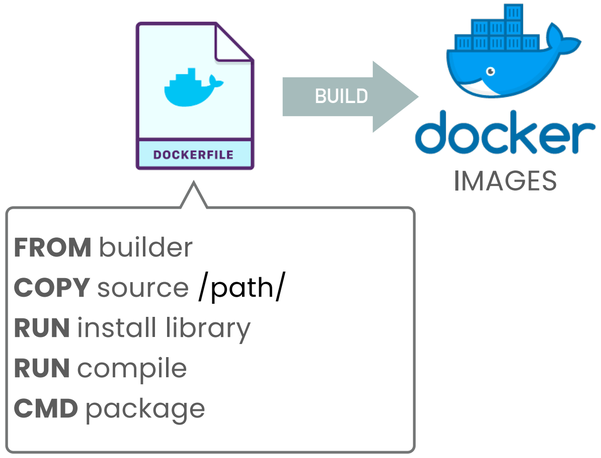
DOCKER FOR RUN

FROM builder
COPY source /path/
RUN install library
RUN compile
CMD package

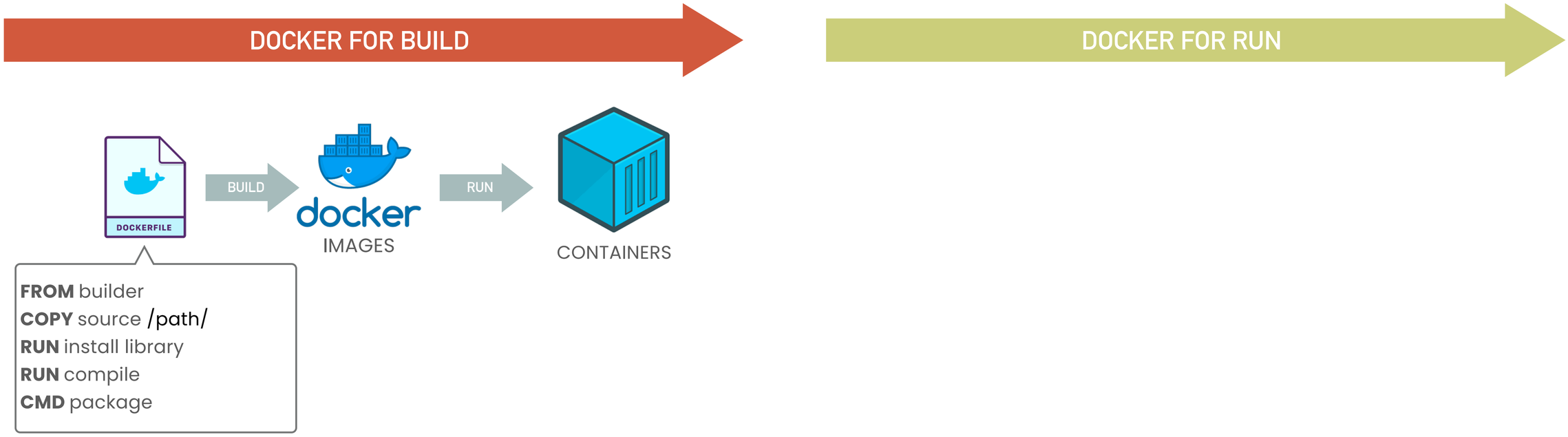
DOCKER FOR BUILD AND DOCKER FOR RUN

DOCKER FOR BUILD

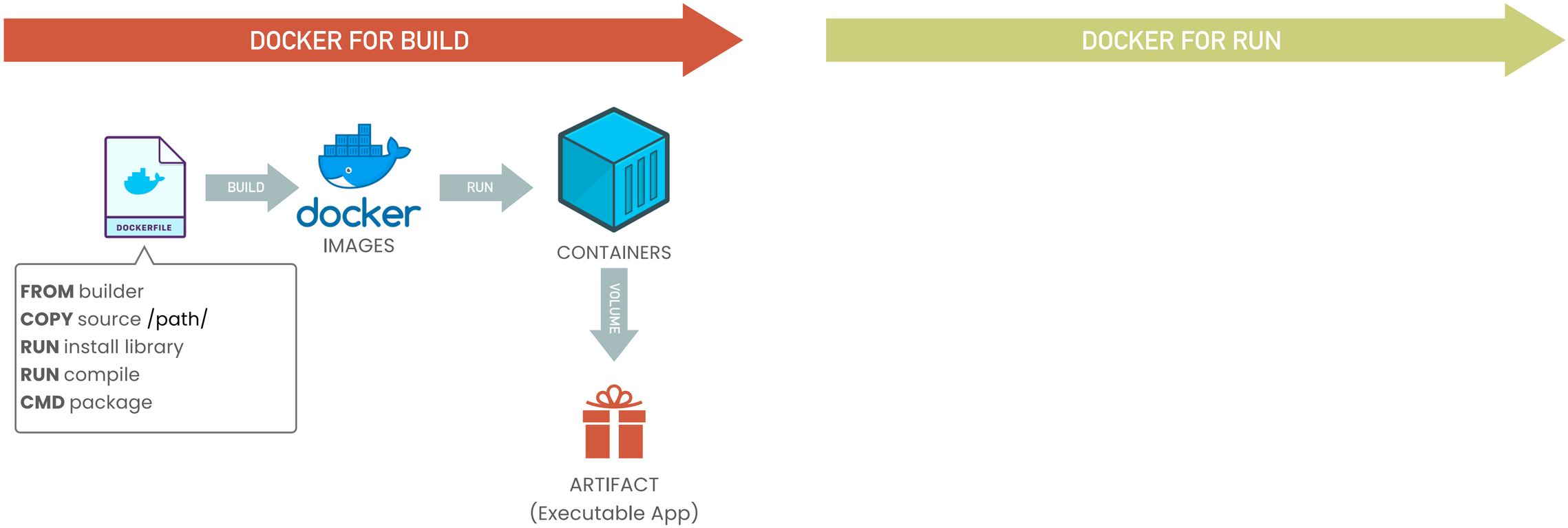
DOCKER FOR RUN



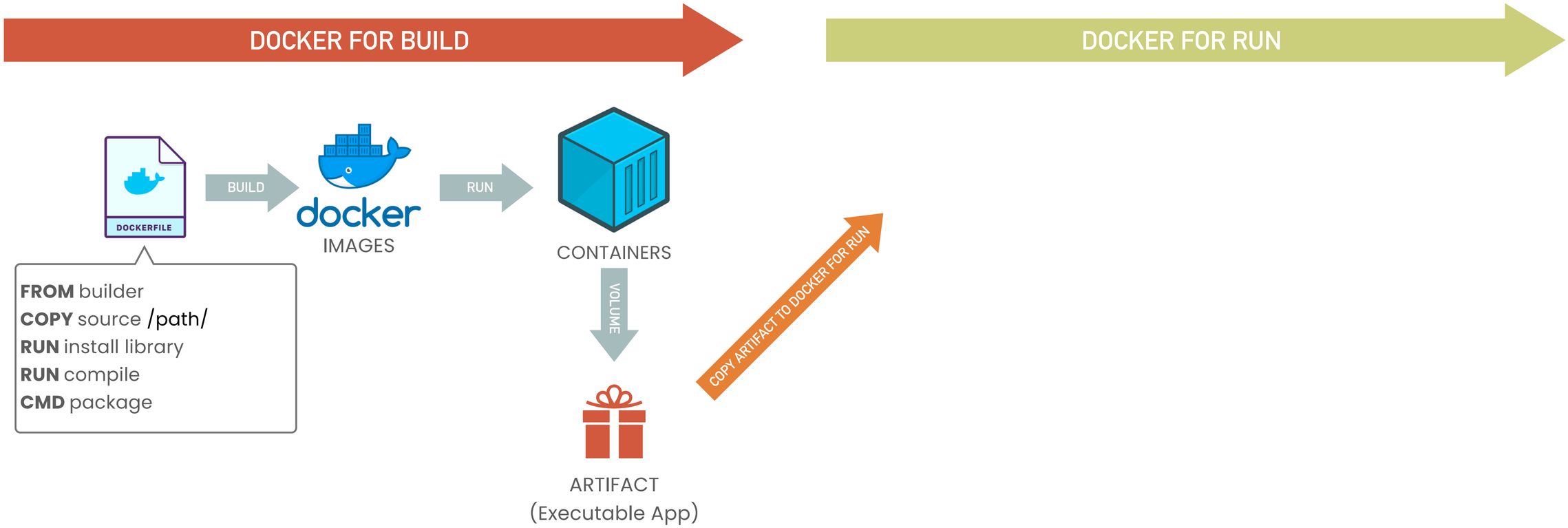
DOCKER FOR BUILD AND DOCKER FOR RUN



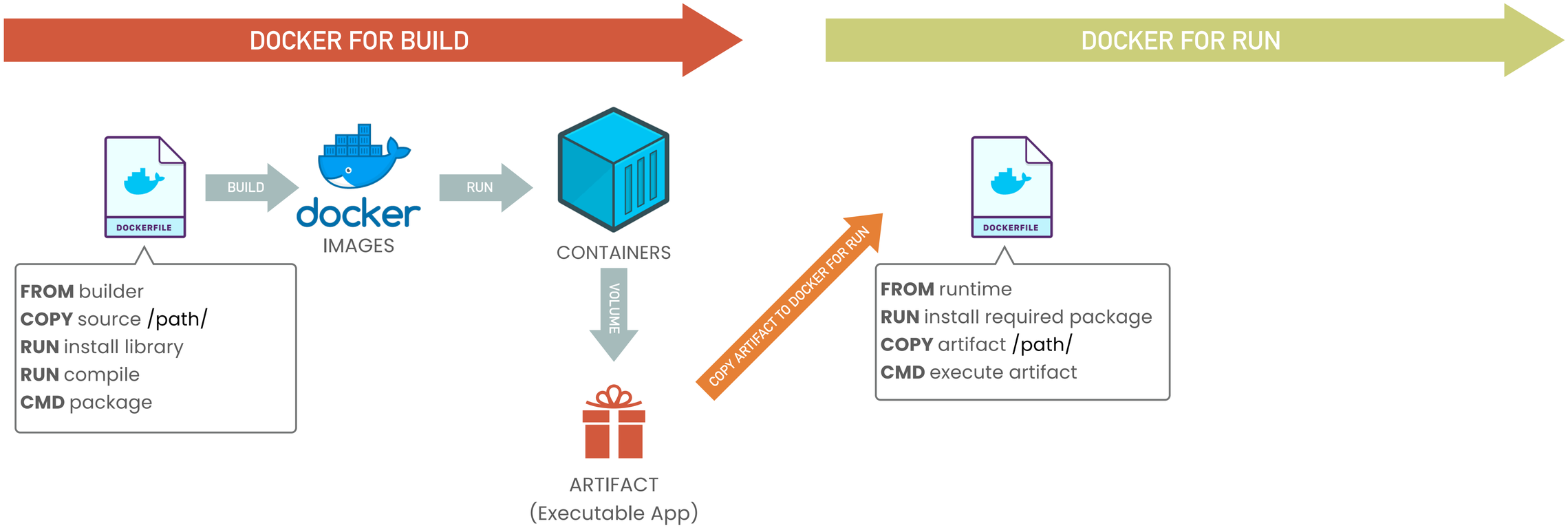
DOCKER FOR BUILD AND DOCKER FOR RUN



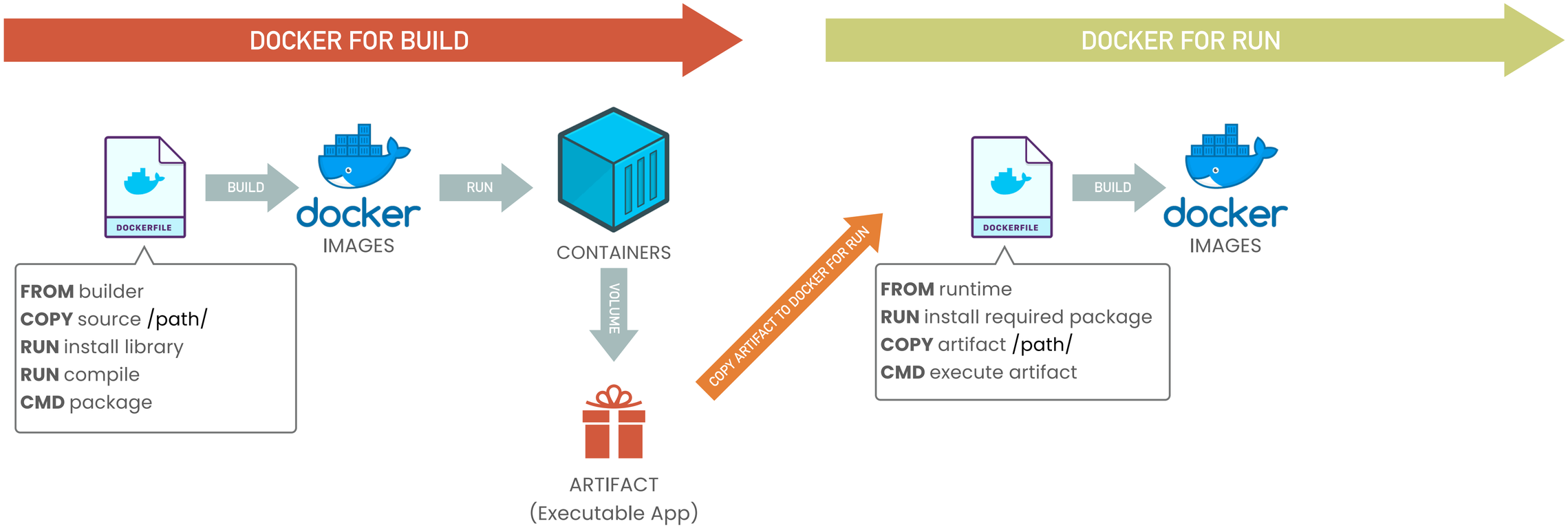
DOCKER FOR BUILD AND DOCKER FOR RUN



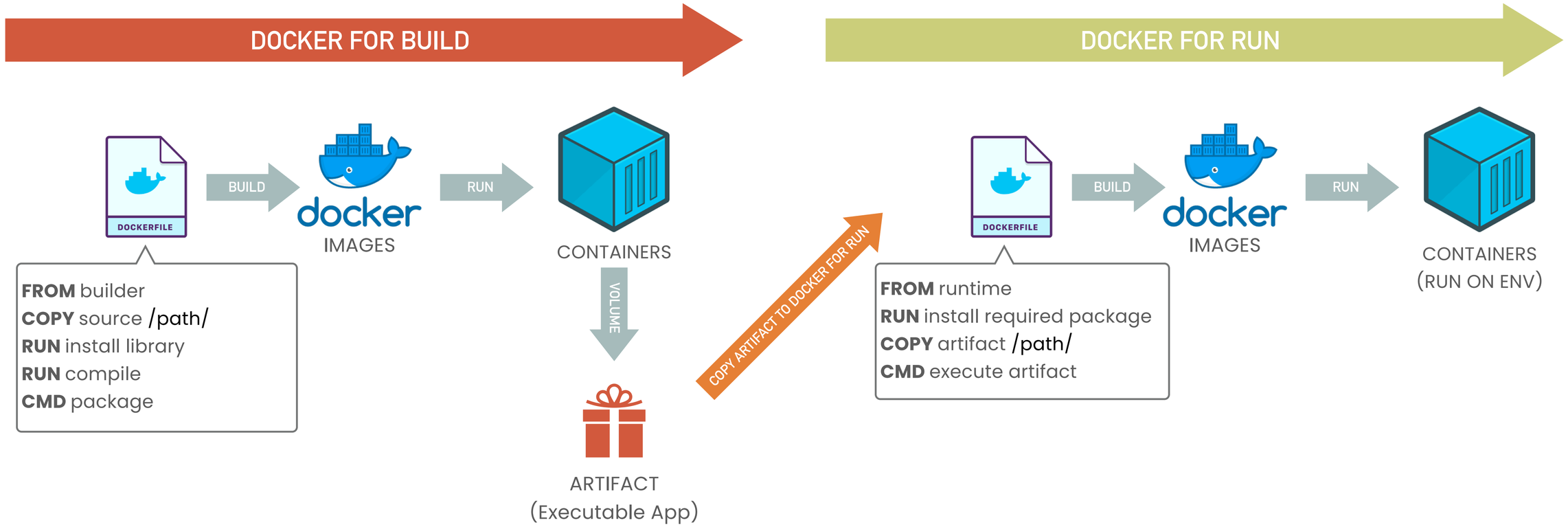
DOCKER FOR BUILD AND DOCKER FOR RUN



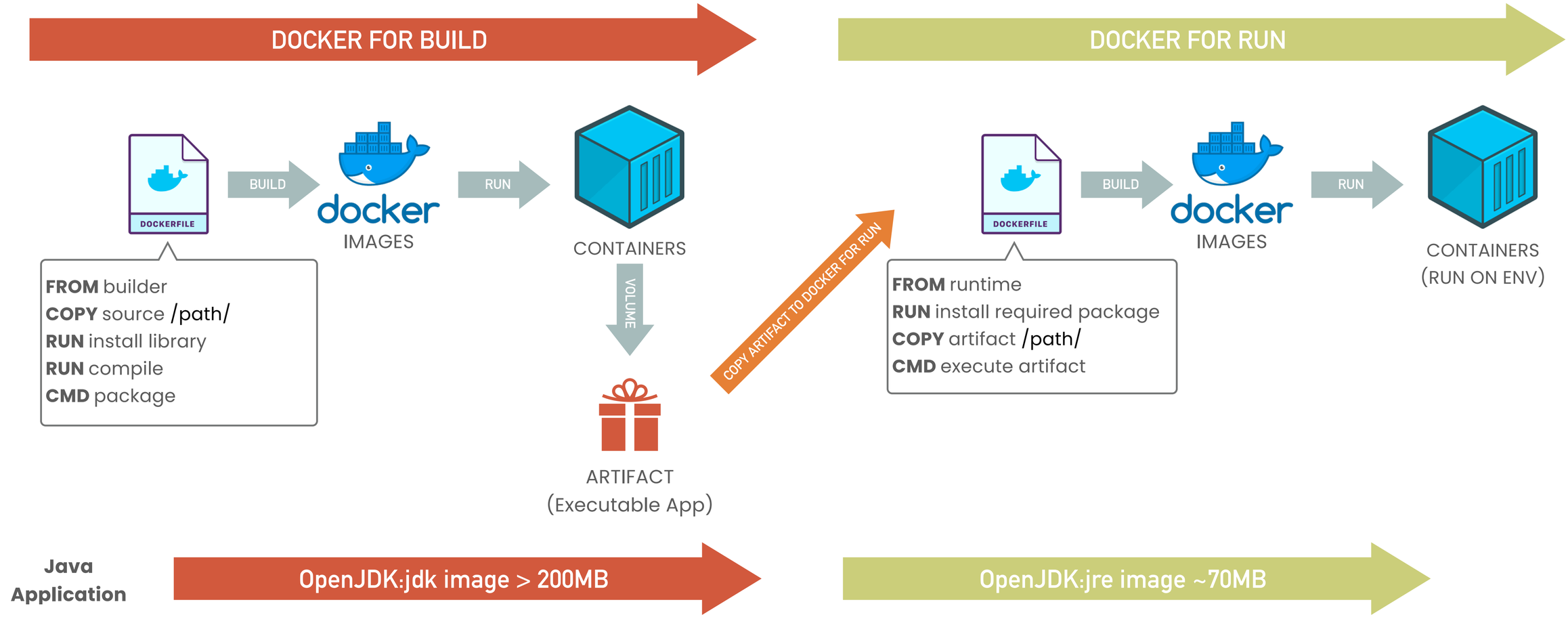
DOCKER FOR BUILD AND DOCKER FOR RUN



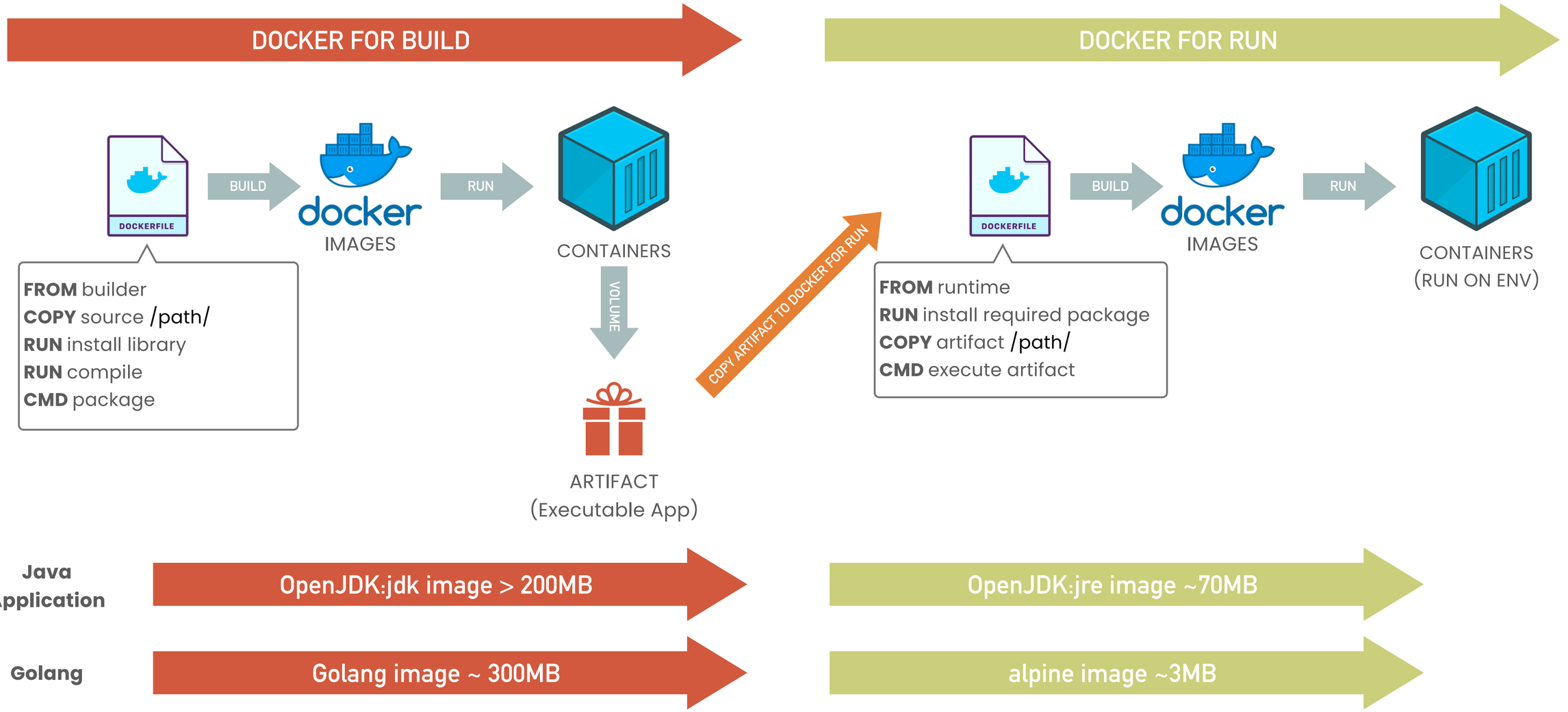
DOCKER FOR BUILD AND DOCKER FOR RUN



DOCKER FOR BUILD AND DOCKER FOR RUN

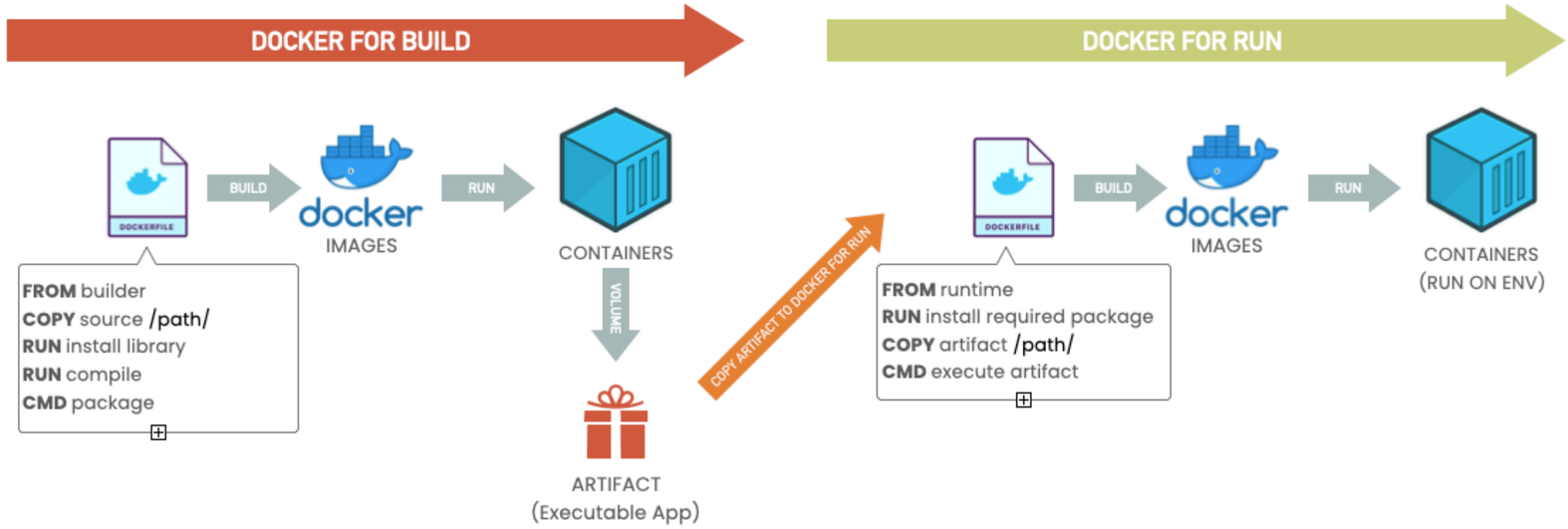


DOCKER FOR BUILD AND DOCKER FOR RUN

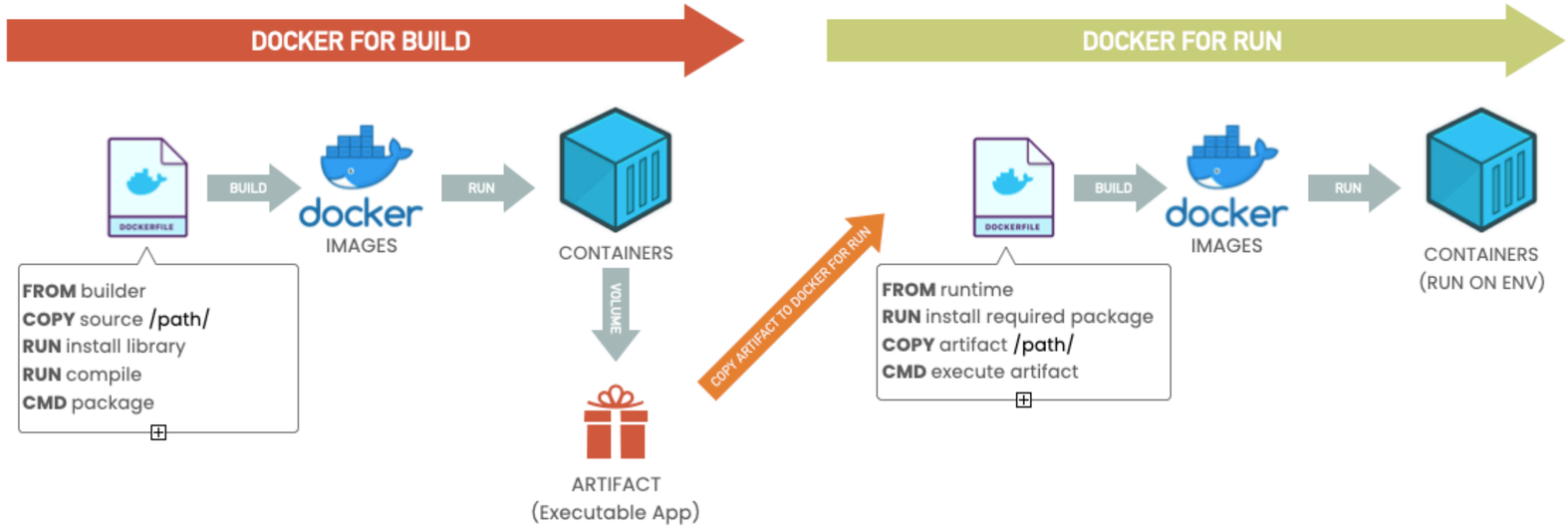


DOCKER FOR BUILD AND DOCKER FOR RUN

DOCKER FOR BUILD AND DOCKER FOR RUN



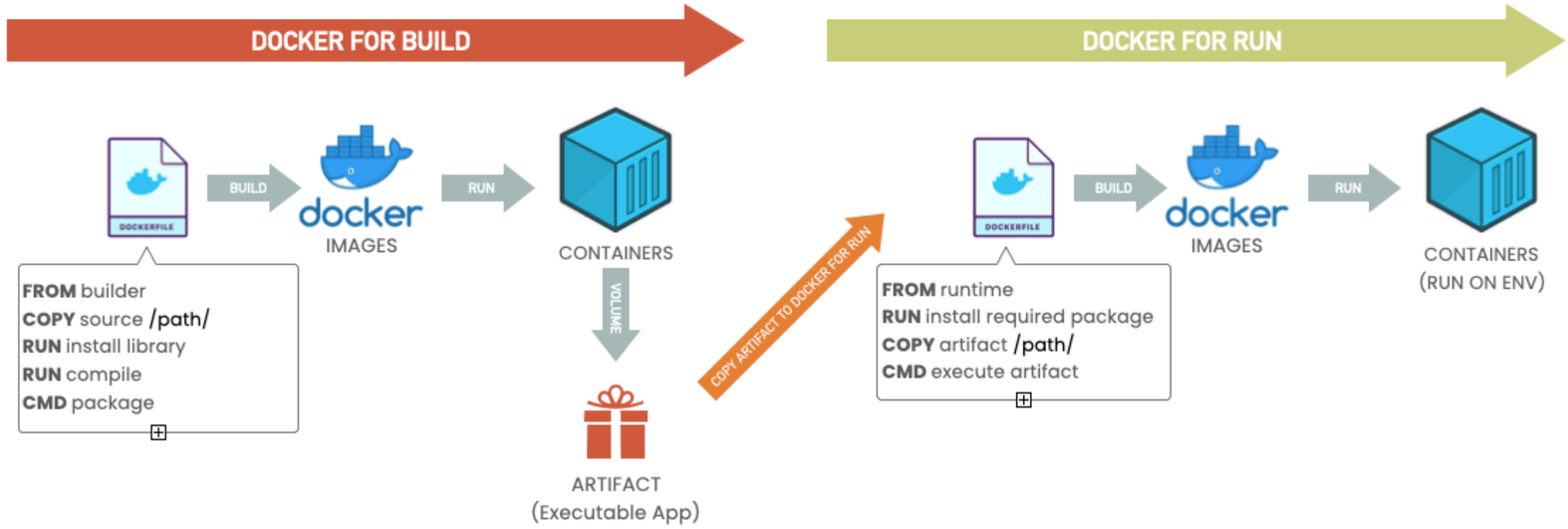
DOCKER FOR BUILD AND DOCKER FOR RUN



Dockerfile.build

```
# syntax=docker/dockerfile:1
FROM golang:1.16
WORKDIR /go/src/github.com/alexellis/href-counter/
COPY app.go ./
RUN go get -d -v golang.org/x/net/html \
  && CGO_ENABLED=0 GOOS=linux go build -a
-installsuffix cgo -o app .
```

DOCKER FOR BUILD AND DOCKER FOR RUN



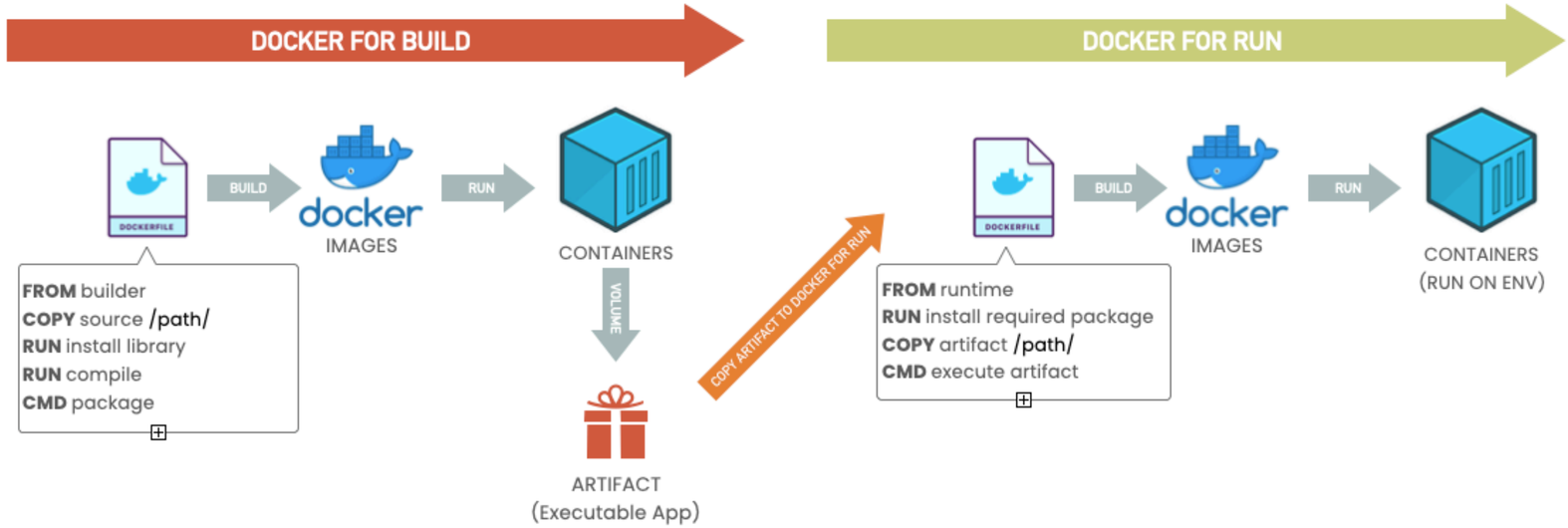
Dockerfile.build

```
# syntax=docker/dockerfile:1
FROM golang:1.16
WORKDIR /go/src/github.com/alexellis/href-counter/
COPY app.go ./
RUN go get -d -v golang.org/x/net/html \
  && CGO_ENABLED=0 GOOS=linux go build -a
-installsuffix cgo -o app .
```

Dockerfile

```
# syntax=docker/dockerfile:1
FROM alpine:latest
RUN apk --no-cache add ca-certificates
WORKDIR /root/
COPY app ./
CMD ["./app"]
```

DOCKER FOR BUILD AND DOCKER FOR RUN



Dockerfile.build

```
# syntax=docker/dockerfile:1
FROM golang:1.16
WORKDIR /go/src/github.com/alexellis/href-counter/
COPY app.go ./
RUN go get -d -v golang.org/x/net/html \
  && CGO_ENABLED=0 GOOS=linux go build -a
-installsuffix cgo -o app .
```

build.sh

```
#!/bin/sh
echo Building alexellis2/href-counter:build

docker build --build-arg https_proxy=$https_proxy --build-arg http_proxy=$http_proxy \
    -t alexellis2/href-counter:build . -f Dockerfile.build

docker container create --name extract alexellis2/href-counter:build
docker container cp extract:/go/src/github.com/alexellis/href-counter/app ./app
docker container rm -f extract

echo Building alexellis2/href-counter:latest

docker build --no-cache -t alexellis2/href-counter:latest .
rm ./app
```

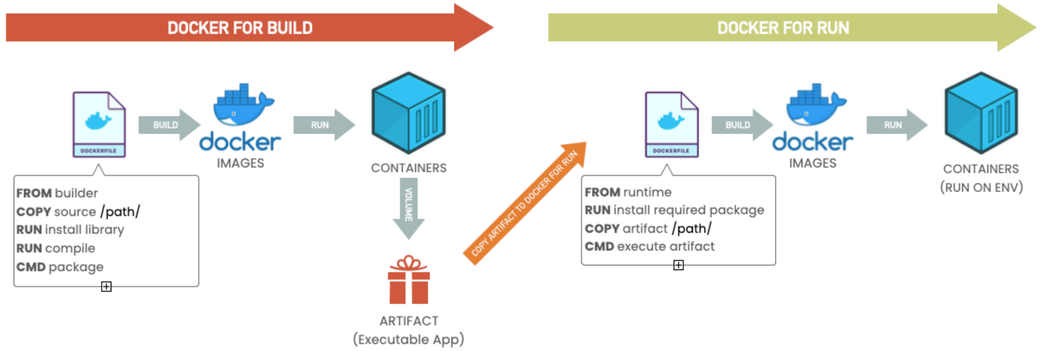
Dockerfile

```
# syntax=docker/dockerfile:1
FROM alpine:latest
RUN apk --no-cache add ca-certificates
WORKDIR /root/
COPY app ./
CMD ["./app"]
```

USE MULTI-STAGES BUILD

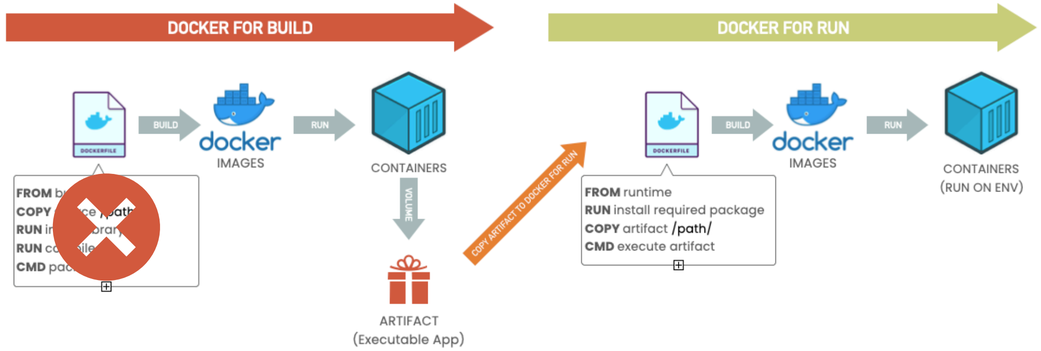
Use multiple **FROM**

USE MULTI-STAGES BUILD



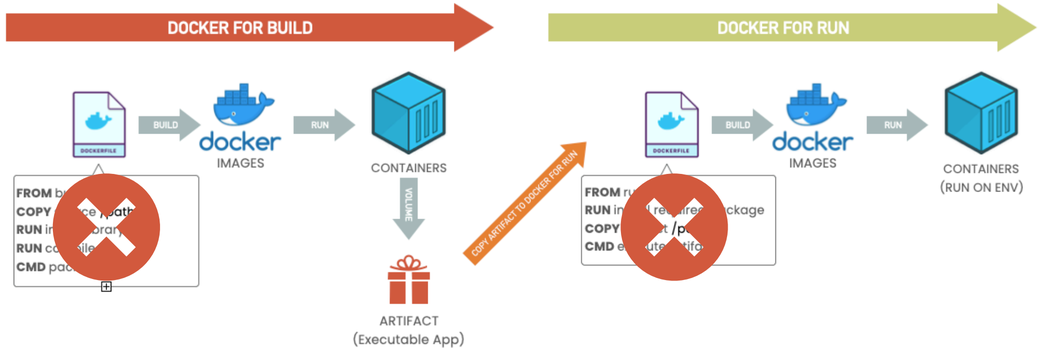
Use multiple **FROM**

USE MULTI-STAGES BUILD



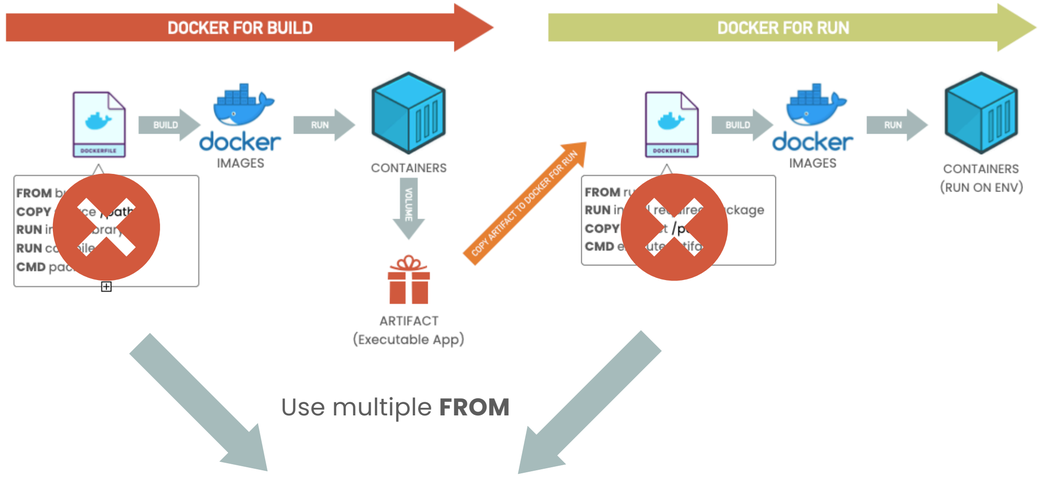
Use multiple **FROM**

USE MULTI-STAGES BUILD

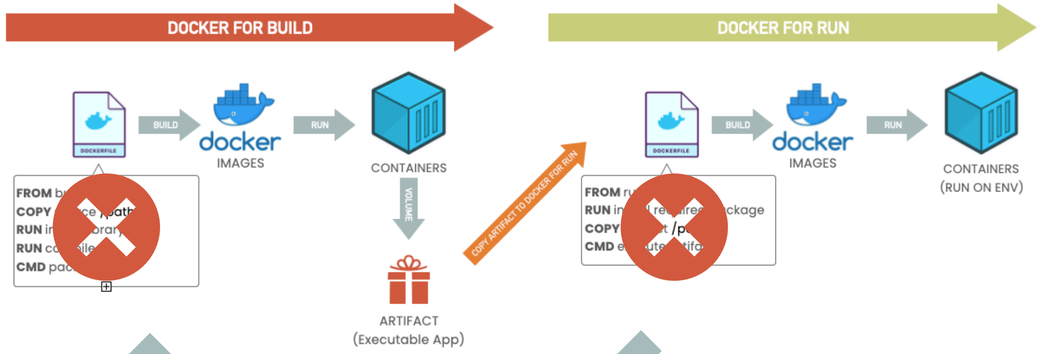


Use multiple **FROM**

USE MULTI-STAGES BUILD



USE MULTI-STAGES BUILD



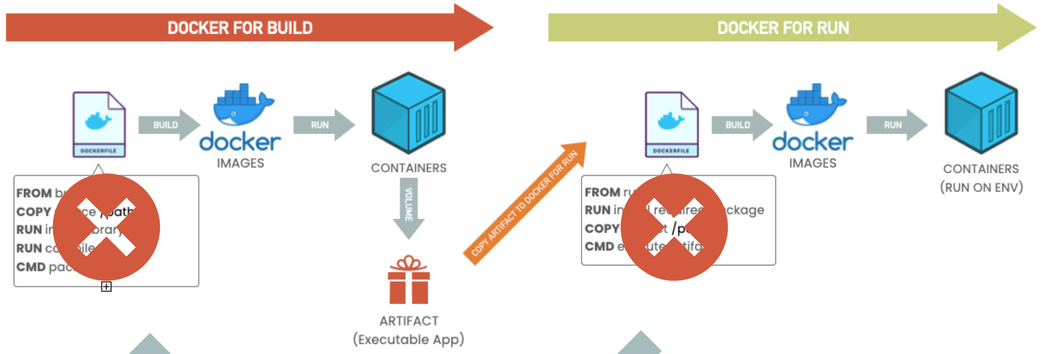
Use multiple **FROM**

DOCKERFILE

FROM jdk **AS** builder
COPY source /path/
RUN install library
RUN compile
CMD package **artifact**

FROM jre **AS** runtime
RUN install required package
COPY --from=builder **artifact** /path/
CMD execute **artifact**

USE MULTI-STAGES BUILD



Use multiple **FROM**

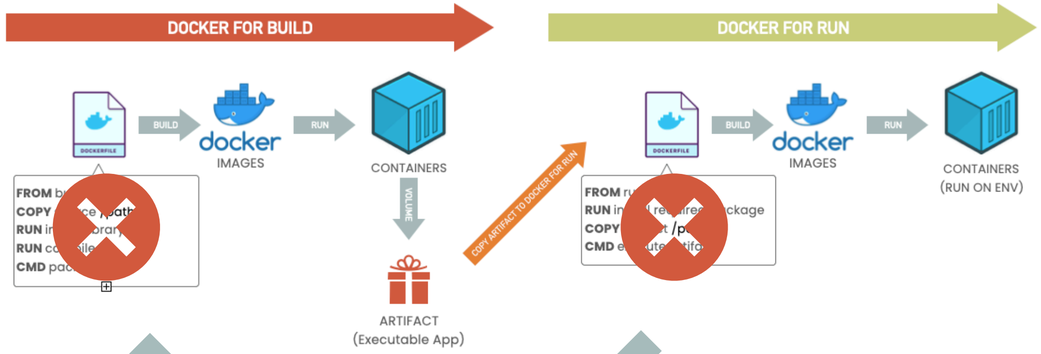
DOCKERFILE

```
FROM jdk AS builder
COPY source /path/
RUN install library
RUN compile
CMD package artifact

FROM jre AS runtime
RUN install required package
COPY --from=builder artifact /path/
CMD execute artifact
```

```
$ docker build .
```

USE MULTI-STAGES BUILD



Use multiple **FROM**

DOCKERFILE

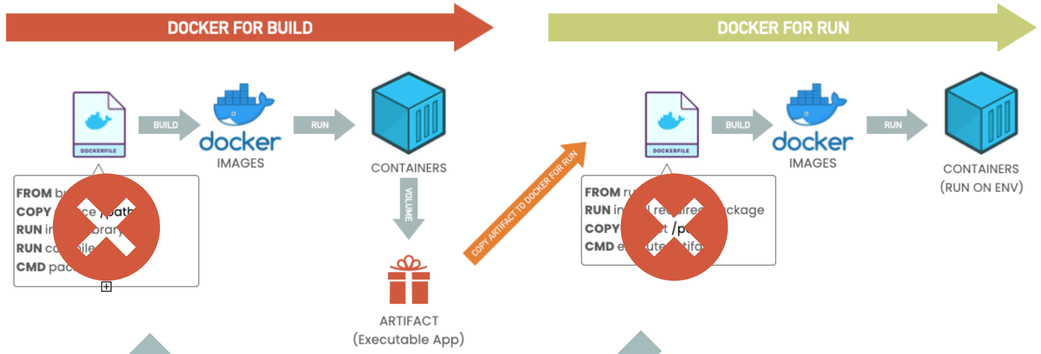
FROM jdk **AS** builder
COPY source /path/
RUN install library
RUN compile
CMD package **artifact**

FROM jre **AS** runtime
RUN install required package
COPY --from=builder **artifact** /path/
CMD execute **artifact**

```
$ docker build .
```

docker
IMAGES

USE MULTI-STAGES BUILD



Use multiple **FROM**

DOCKERFILE

FROM jdk **AS** builder
COPY source /path/
RUN install library
RUN compile
CMD package **artifact**

FROM jre **AS** runtime
RUN install required package
COPY --from=builder **artifact** /path/
CMD execute **artifact**

```
$ docker build .
```

docker
IMAGES

jre image
~70MB

alpine image
~3MB

DOCKER (SECURITY) SCAN

DOCKER IMAGE SCAN COMMAND

DOCKER IMAGE SCAN COMMAND

```
$ docker scan [OPTION] <image[:tag]>
```

DOCKER IMAGE SCAN COMMAND

```
$ docker scan [OPTION] <image[:tag]>
```

```
Docker Scan relies upon access to Snyk, a third party provider, do you consent to proceed using Snyk? (y/N)
y

Testing ubuntu...

✗ Low severity vulnerability found in util-linux/libblkid1
  Description: Integer Overflow or Wraparound
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-1534917
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, e2fsprogs@1.45.5-2ubuntu1, util-linux/mount@2.34-0.1ubuntu9.1, util-linux/fdisk@2.34-0.1ubuntu9.1, util-linux/libuuid1@2.34-0.1ubuntu9.1,
util-linux@2.34-0.1ubuntu9.1, sysvinit/sysvinit-utils@2.96-2.1ubuntu1, util-linux/bsdutils@1:2.34-0.1ubuntu9.1, util-linux/libfdisk1@2.34-0.1ubuntu9.1, util-linux/libmount1@2.34-0.1ubuntu9.1, util-
linux/libsmartcols1@2.34-0.1ubuntu9.1
  From: util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  and 23 more...

✗ Medium severity vulnerability found in util-linux/libblkid1
  Description: CVE-2021-3996
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-2387723
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, e2fsprogs@1.45.5-2ubuntu1, util-linux/mount@2.34-0.1ubuntu9.1, util-linux/fdisk@2.34-0.1ubuntu9.1, util-linux/libuuid1@2.34-0.1ubuntu9.1,
util-linux@2.34-0.1ubuntu9.1, sysvinit/sysvinit-utils@2.96-2.1ubuntu1, util-linux/bsdutils@1:2.34-0.1ubuntu9.1, util-linux/libfdisk1@2.34-0.1ubuntu9.1, util-linux/libmount1@2.34-0.1ubuntu9.1, util-
linux/libsmartcols1@2.34-0.1ubuntu9.1
  From: util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  and 23 more…

Package manager:   deb
Project name:      docker-image|ubuntu
Docker image:      ubuntu
Platform:          linux/amd64
Base image:        ubuntu:20.04

Tested 93 dependencies for known vulnerabilities, found 30 vulnerabilities.

Base Image    Vulnerabilities  Severity
ubuntu:20.04  30               0 critical, 0 high, 8 medium, 22 low

Recommendations for base image upgrade:

Major upgrades
Base Image              Vulnerabilities  Severity
ubuntu:impish-20211015  20               0 critical, 0 high, 8 medium, 12 low


For more free scans that keep your images secure, sign up to Snyk at https://dockr.ly/3ePqVcp
```

DOCKER IMAGE SCAN COMMAND

```
$ docker scan [OPTION] <image[:tag]>
```

```
Docker Scan relies upon access to Snyk, a third party provider, do you consent to proceed using Snyk? (y/N)
y
Testing ubuntu...

✗ Low severity vulnerability found in util-linux/libblkid1
  Description: Integer Overflow or Wraparound
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-1534917
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, e2fsprogs@1.45.5-2ubuntu1, util-linux/mount@2.34-0.1ubuntu9.1, util-linux/fdisk@2.34-0.1ubuntu9.1, util-linux/libuuid1@2.34-0.1ubuntu9.1, util-linux@2.34-0.1ubuntu9.1, sysvinit/sysvinit-utils@2.96-2.1ubuntu1, util-linux/bsdutils@1:2.34-0.1ubuntu9.1, util-linux/libfdisk1@2.34-0.1ubuntu9.1, util-linux/libmount1@2.34-0.1ubuntu9.1, util-linux/libsmartcols1@2.34-0.1ubuntu9.1
  From: util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  and 23 more...

✗ Medium severity vulnerability found in util-linux/libblkid1
  Description: CVE-2021-3996
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-2387723
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, e2fsprogs@1.45.5-2ubuntu1, util-linux/mount@2.34-0.1ubuntu9.1, util-linux/fdisk@2.34-0.1ubuntu9.1, util-linux/libuuid1@2.34-0.1ubuntu9.1, util-linux@2.34-0.1ubuntu9.1, sysvinit/sysvinit-utils@2.96-2.1ubuntu1, util-linux/bsdutils@1:2.34-0.1ubuntu9.1, util-linux/libfdisk1@2.34-0.1ubuntu9.1, util-linux/libmount1@2.34-0.1ubuntu9.1, util-linux/libsmartcols1@2.34-0.1ubuntu9.1
  From: util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  and 23 more…

Package manager:   deb
Project name:      docker-image|ubuntu
Docker image:      ubuntu
Platform:          linux/amd64
Base image:        ubuntu:20.04

Tested 93 dependencies for known vulnerabilities, found 30 vulnerabilities.

Base Image    Vulnerabilities  Severity
ubuntu:20.04  30               0 critical, 0 high, 8 medium, 22 low

Recommendations for base image upgrade:

Major upgrades
Base Image              Vulnerabilities  Severity
ubuntu:impish-20211015  20               0 critical, 0 high, 8 medium, 12 low


For more free scans that keep your images secure, sign up to Snyk at https://dockr.ly/3ePqVcp
```

DOCKER IMAGE SCAN COMMAND

```
$ docker scan [OPTION] <image[:tag]>
```

```
Docker Scan relies upon access to Snyk, a third party provider, do you consent to proceed using Snyk? (y/N)
y

Testing ubuntu...

✗ Low severity vulnerability found in util-linux/libblkid1
  Description: Integer Overflow or Wraparound
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-1534917
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, e2fsprogs@1.45.5-2ubuntu1, util-linux/mount@2.34-0.1ubuntu9.1, util-linux/fdisk@2.34-0.1ubuntu9.1, util-linux/libuuid1@2.34-0.1ubuntu9.1, util-linux@2.34-0.1ubuntu9.1, sysvinit/sysvinit-utils@2.96-2.1ubuntu1, util-linux/bsdutils@1:2.34-0.1ubuntu9.1, util-linux/libfdisk1@2.34-0.1ubuntu9.1, util-linux/libmount1@2.34-0.1ubuntu9.1, util-linux/libsmartcols1@2.34-0.1ubuntu9.1
  From: util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  and 23 more...

✗ Medium severity vulnerability found in util-linux/libblkid1
  Description: CVE-2021-3996
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-2387723
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, e2fsprogs@1.45.5-2ubuntu1, util-linux/mount@2.34-0.1ubuntu9.1, util-linux/fdisk@2.34-0.1ubuntu9.1, util-linux/libuuid1@2.34-0.1ubuntu9.1, util-linux@2.34-0.1ubuntu9.1, sysvinit/sysvinit-utils@2.96-2.1ubuntu1, util-linux/bsdutils@1:2.34-0.1ubuntu9.1, util-linux/libfdisk1@2.34-0.1ubuntu9.1, util-linux/libmount1@2.34-0.1ubuntu9.1, util-linux/libsmartcols1@2.34-0.1ubuntu9.1
  From: util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  and 23 more…

Package manager:   deb
Project name:      docker-image|ubuntu
Docker image:      ubuntu
Platform:          linux/amd64
Base image:        ubuntu:20.04

Tested 93 dependencies for known vulnerabilities, found 30 vulnerabilities.

Base Image    Vulnerabilities  Severity
ubuntu:20.04  30               0 critical, 0 high, 8 medium, 22 low

Recommendations for base image upgrade:

Major upgrades
Base Image              Vulnerabilities  Severity
ubuntu:impish-20211015  20               0 critical, 0 high, 8 medium, 12 low


For more free scans that keep your images secure, sign up to Snyk at https://dockr.ly/3ePqVcp
```

DOCKER IMAGE SCAN COMMAND

```
$ docker scan [OPTION] <image[:tag]>
```

```
Docker Scan relies upon access to Snyk, a third party provider, do you consent to proceed using Snyk? (y/N)
y
```

```
Testing ubuntu...

✗ Low severity vulnerability found in util-linux/libblkid1
  Description: Integer Overflow or Wraparound
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-1534917
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, e2fsprogs@1.45.5-2ubuntu1, util-linux/mount@2.34-0.1ubuntu9.1, util-linux/fdisk@2.34-0.1ubuntu9.1, util-linux/libuuid1@2.34-0.1ubuntu9.1, util-linux@2.34-0.1ubuntu9.1, sysvinit/sysvinit-utils@2.96-2.1ubuntu1, util-linux/bsdutils@1:2.34-0.1ubuntu9.1, util-linux/libfdisk1@2.34-0.1ubuntu9.1, util-linux/libmount1@2.34-0.1ubuntu9.1, util-linux/libsmartcols1@2.34-0.1ubuntu9.1
  From: util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  and 23 more...

✗ Medium severity vulnerability found in util-linux/libblkid1
  Description: CVE-2021-3996
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-2387723
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, e2fsprogs@1.45.5-2ubuntu1, util-linux/mount@2.34-0.1ubuntu9.1, util-linux/fdisk@2.34-0.1ubuntu9.1, util-linux/libuuid1@2.34-0.1ubuntu9.1, util-linux@2.34-0.1ubuntu9.1, sysvinit/sysvinit-utils@2.96-2.1ubuntu1, util-linux/bsdutils@1:2.34-0.1ubuntu9.1, util-linux/libfdisk1@2.34-0.1ubuntu9.1, util-linux/libmount1@2.34-0.1ubuntu9.1, util-linux/libsmartcols1@2.34-0.1ubuntu9.1
  From: util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  and 23 more…

Package manager:   deb
Project name:      docker-image|ubuntu
Docker image:      ubuntu
Platform:          linux/amd64
Base image:        ubuntu:20.04

Tested 93 dependencies for known vulnerabilities, found 30 vulnerabilities.

Base Image    Vulnerabilities  Severity
ubuntu:20.04  30               0 critical, 0 high, 8 medium, 22 low

Recommendations for base image upgrade:

Major upgrades
Base Image              Vulnerabilities  Severity
ubuntu:impish-20211015  20               0 critical, 0 high, 8 medium, 12 low


For more free scans that keep your images secure, sign up to Snyk at https://dockr.ly/3ePqVcp
```

DOCKER IMAGE SCAN COMMAND

```
$ docker scan [OPTION] <image[:tag]>
```

Please make sure the image and/or repository exist

```
Docker Scan relies upon access to Snyk, a third party provider, do you consent to proceed using Snyk? (y/N)
y
```

```
Testing ubuntu...

✗ Low severity vulnerability found in util-linux/libblkid1
  Description: Integer Overflow or Wraparound
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-1534917
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, e2fsprogs@1.45.5-2ubuntu1, util-linux/mount@2.34-0.1ubuntu9.1, util-linux/fdisk@2.34-0.1ubuntu9.1, util-linux/libuuid1@2.34-0.1ubuntu9.1, util-linux@2.34-0.1ubuntu9.1, sysvinit/sysvinit-utils@2.96-2.1ubuntu1, util-linux/bsdutils@1:2.34-0.1ubuntu9.1, util-linux/libfdisk1@2.34-0.1ubuntu9.1, util-linux/libmount1@2.34-0.1ubuntu9.1, util-linux/libsmartcols1@2.34-0.1ubuntu9.1
  From: util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  and 23 more...

✗ Medium severity vulnerability found in util-linux/libblkid1
  Description: CVE-2021-3996
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-2387723
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, e2fsprogs@1.45.5-2ubuntu1, util-linux/mount@2.34-0.1ubuntu9.1, util-linux/fdisk@2.34-0.1ubuntu9.1, util-linux/libuuid1@2.34-0.1ubuntu9.1, util-linux@2.34-0.1ubuntu9.1, sysvinit/sysvinit-utils@2.96-2.1ubuntu1, util-linux/bsdutils@1:2.34-0.1ubuntu9.1, util-linux/libfdisk1@2.34-0.1ubuntu9.1, util-linux/libmount1@2.34-0.1ubuntu9.1, util-linux/libsmartcols1@2.34-0.1ubuntu9.1
  From: util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  and 23 more…
```

```
Package manager:   deb
Project name:      docker-image|ubuntu
Docker image:      ubuntu
Platform:          linux/amd64
Base image:        ubuntu:20.04

Tested 93 dependencies for known vulnerabilities, found 30 vulnerabilities.

Base Image    Vulnerabilities  Severity
ubuntu:20.04  30               0 critical, 0 high, 8 medium, 22 low

Recommendations for base image upgrade:

Major upgrades
Base Image              Vulnerabilities  Severity
ubuntu:impish-20211015  20               0 critical, 0 high, 8 medium, 12 low


For more free scans that keep your images secure, sign up to Snyk at https://dockr.ly/3ePqVcp
```

IMAGE VULNERABILITY DB (WITH CVSS V3 RATING)

IMAGE VULNERABILITY DB (WITH CVSS V3 RATING)

0.1 - 3.9 | 4.0 - 6.9 | 7.0 - 8.9 | 9.0 - 10.10

IMAGE VULNERABILITY DB (WITH CVSS V3 RATING)

0.1 - 3.9 | 4.0 - 6.9 | 7.0 - 8.9 | 9.0 - 10.10

```
✗ Low severity vulnerability found in util-linux/libblkid1
  Description: Integer Overflow or Wraparound
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-1534917
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, ...
  From: util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  and 23 more...


✗ Medium severity vulnerability found in util-linux/libblkid1
  Description: CVE-2021-3996
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-2387723
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, ...
  From: util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  and 23 more…
```

IMAGE VULNERABILITY DB (WITH CVSS V3 RATING)

0.1 - 3.9 | 4.0 - 6.9 | 7.0 - 8.9 | 9.0 - 10.10

```
✗ Low severity vulnerability found in util-linux/libblkid1
  Description: Integer Overflow or Wraparound
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-1534917
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, ...
  From: util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  and 23 more...


✗ Medium severity vulnerability found in util-linux/libblkid1
  Description: CVE-2021-3996
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-2387723
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, ...
  From: util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  and 23 more…
```

IMAGE VULNERABILITY DB (WITH CVSS V3 RATING)

0.1 - 3.9 | 4.0 - 6.9 | 7.0 - 8.9 | 9.0 - 10.10

```
✗ Low severity vulnerability found in util-linux/libblkid1
  Description: Integer Overflow or Wraparound
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-1534917
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, ...
  From: util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  and 23 more...


✗ Medium severity vulnerability found in util-linux/libblkid1
  Description: CVE-2021-3996
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-2387723
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, ...
  From: util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1
  and 23 more…
```

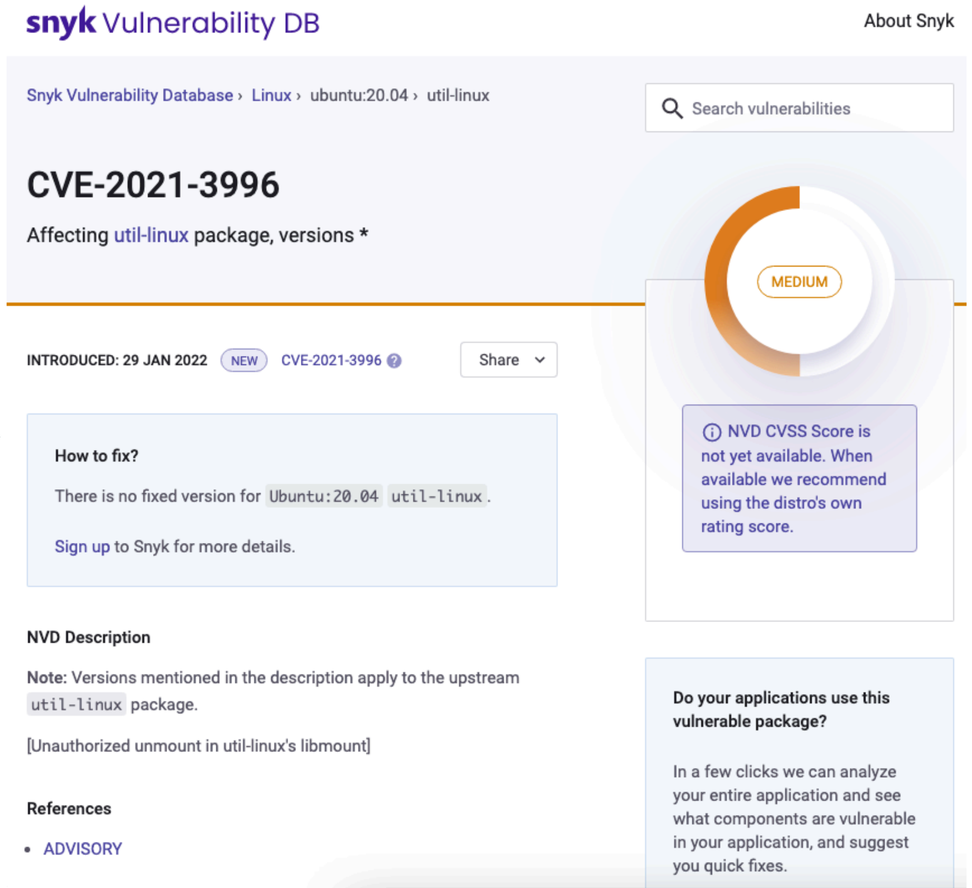


IMAGE SCAN SUMMARY RESULT AND RECOMMENDATION

IMAGE SCAN SUMMARY RESULT AND RECOMMENDATION

```
Package manager:   deb
Project name:      docker-image|ubuntu
Docker image:      ubuntu
Platform:          linux/amd64
Base image:        ubuntu:20.04

Tested 93 dependencies for known vulnerabilities, found 30 vulnerabilities.

Base Image    Vulnerabilities  Severity
ubuntu:20.04  30               0 critical, 0 high, 8 medium, 22 low

Recommendations for base image upgrade:

Major upgrades
Base Image              Vulnerabilities  Severity
ubuntu:impish-20211015  20               0 critical, 0 high, 8 medium, 12 low


For more free scans that keep your images secure, sign up to Snyk at https://dockr.ly/3ePqVcp
```

IMAGE SCAN SUMMARY RESULT AND RECOMMENDATION

```
Package manager:   deb
Project name:      docker-image|ubuntu
Docker image:      ubuntu
Platform:          linux/amd64
Base image:        ubuntu:20.04

Tested 93 dependencies for known vulnerabilities, found 30 vulnerabilities.

Base Image    Vulnerabilities  Severity
ubuntu:20.04  30               0 critical, 0 high, 8 medium, 22 low

Recommendations for base image upgrade:

Major upgrades
Base Image              Vulnerabilities  Severity
ubuntu:impish-20211015  20               0 critical, 0 high, 8 medium, 12 low


For more free scans that keep your images secure, sign up to Snyk at https://dockr.ly/3ePqVcp
```

IMAGE SCAN SUMMARY RESULT AND RECOMMENDATION

```
Package manager:   deb
Project name:      docker-image|ubuntu
Docker image:      ubuntu
Platform:          linux/amd64
Base image:        ubuntu:20.04

Tested 93 dependencies for known vulnerabilities, found 30 vulnerabilities.

Base Image    Vulnerabilities  Severity
ubuntu:20.04  30               0 critical, 0 high, 8 medium, 22 low

Recommendations for base image upgrade:

Major upgrades
Base Image              Vulnerabilities  Severity
ubuntu:impish-20211015  20               0 critical, 0 high, 8 medium, 12 low


For more free scans that keep your images secure, sign up to Snyk at https://dockr.ly/3ePqVcp
```

IMAGE SCAN SUMMARY RESULT AND RECOMMENDATION

```
Package manager:   deb
Project name:      docker-image|ubuntu
Docker image:      ubuntu
Platform:          linux/amd64
Base image:        ubuntu:20.04

Tested 93 dependencies for known vulnerabilities, found 30 vulnerabilities.

Base Image    Vulnerabilities  Severity
ubuntu:20.04  30               0 critical, 0 high, 8 medium, 22 low

Recommendations for base image upgrade:

Major upgrades
Base Image              Vulnerabilities  Severity
ubuntu:impish-20211015  20               0 critical, 0 high, 8 medium, 12 low


For more free scans that keep your images secure, sign up to Snyk at https://dockr.ly/3ePqVcp
```

IMAGE SCAN FOR AUTOMATION PROCESS

IMAGE SCAN FOR AUTOMATION PROCESS

```
$ docker scan --json ubuntu:latest
```

IMAGE SCAN FOR AUTOMATION PROCESS

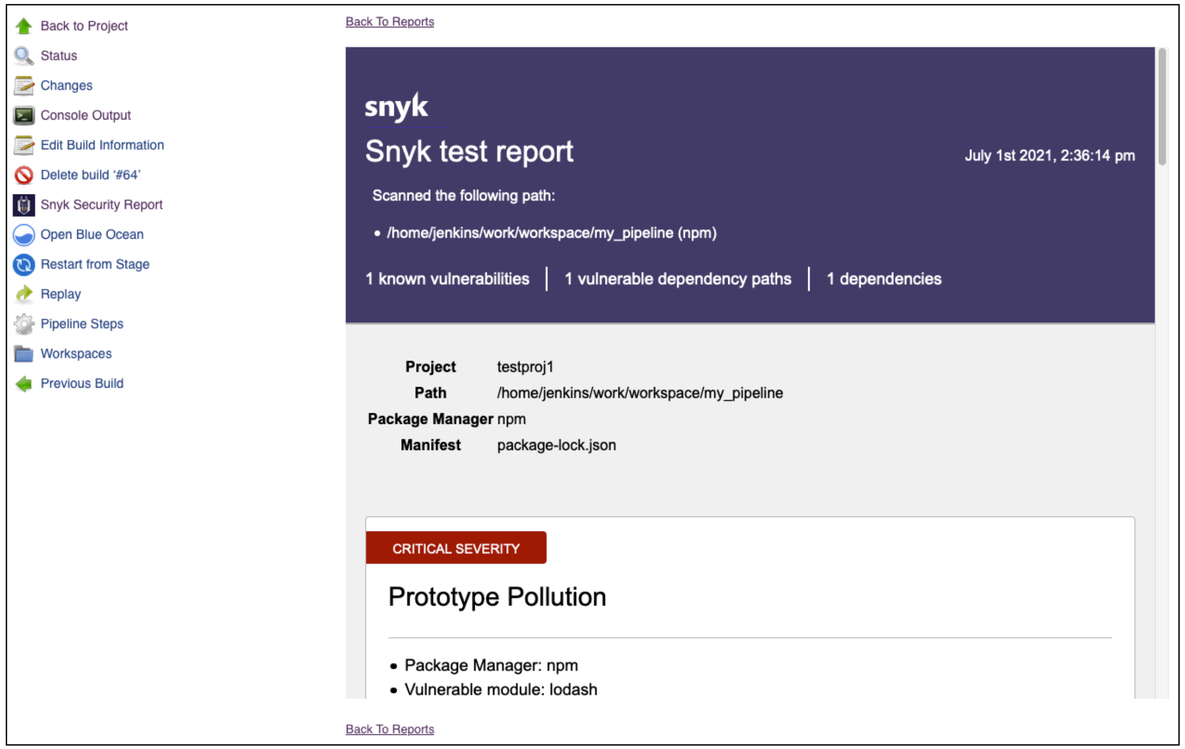
```
$ docker scan --json ubuntu:latest
```


```
{
  "vulnerabilities": [
    {
      "title": "Improper Check for Dropped…",
      "credit": [
        ""
      ],
      "packageName": "bash",
      "language": "linux",
      "packageManager": "ubuntu:20.04",
      "description": "## NVD Description\n<i>…",
      "identifiers": {
        "ALTERNATIVE": [],
        "CVE": [
          "CVE-2019-18276"
        ],
```

IMAGE SCAN FOR AUTOMATION PROCESS

```
$ docker scan --json ubuntu:latest
```


```
{
  "vulnerabilities": [
    {
      "title": "Improper Check for Dropped…",
      "credit": [
        ""
      ],
      "packageName": "bash",
      "language": "linux",
      "packageManager": "ubuntu:20.04",
      "description": "## NVD Description\n<i>…",
      "identifiers": {
        "ALTERNATIVE": [],
        "CVE": [
          "CVE-2019-18276"
        ],
```

MORE FOR IMAGE SCAN (--HELP)

MORE FOR IMAGE SCAN (--HELP)

```
$ docker scan --help
```

MORE FOR IMAGE SCAN (--HELP)

```
$ docker scan --help
```

```
Usage:  docker scan [OPTIONS] IMAGE

A tool to scan your images

Options:
      --accept-license    Accept using a third party scanning provider
      --dependency-tree   Show dependency tree with scan results
      --exclude-base      Exclude base image from vulnerability scanning (requires --file)
  -f, --file string       Dockerfile associated with image, provides more detailed results
      --group-issues      Aggregate duplicated vulnerabilities and group them to a single one (requires --json)
      --json              Output results in JSON format
      --login             Authenticate to the scan provider using an optional token (with --token), or web base token if empty
      --reject-license    Reject using a third party scanning provider
      --severity string   Only report vulnerabilities of provided level or higher (low|medium|high)
      --token string      Authentication token to login to the third party scanning provider
      --version           Display version of the scan plugin
```

DOCKER REGISTRY

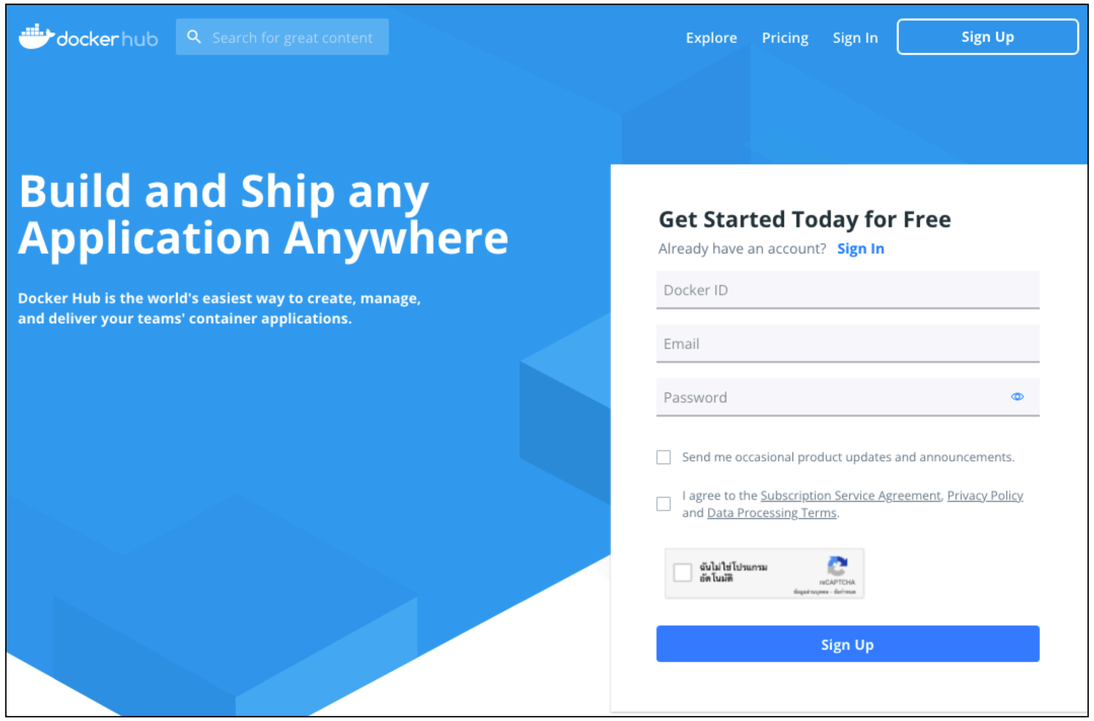
DOCKER REGISTRY (HUB.DOCKER.COM)

DOCKER REGISTRY (HUB.DOCKER.COM)

Docker Registry

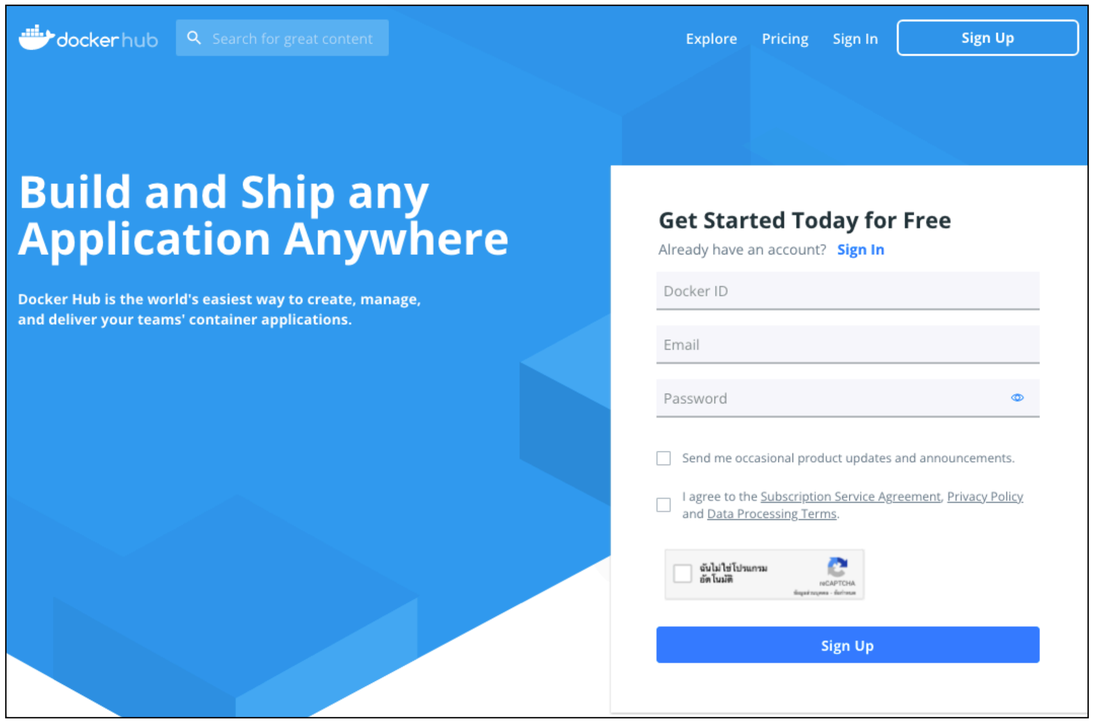
DOCKER REGISTRY (HUB.DOCKER.COM)

Docker Registry



DOCKER REGISTRY (HUB.DOCKER.COM)

Docker Registry

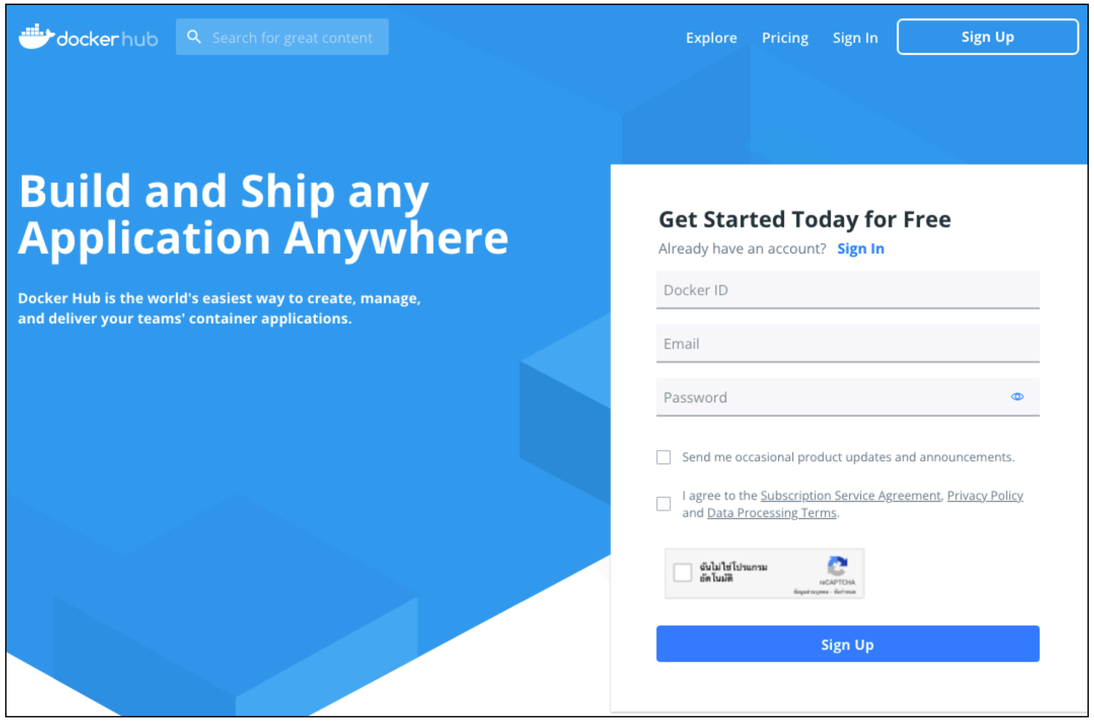


elastic

https://www.docker.elastic.co/

DOCKER REGISTRY (HUB.DOCKER.COM)

Docker Registry



elastic

https://www.docker.elastic.co/

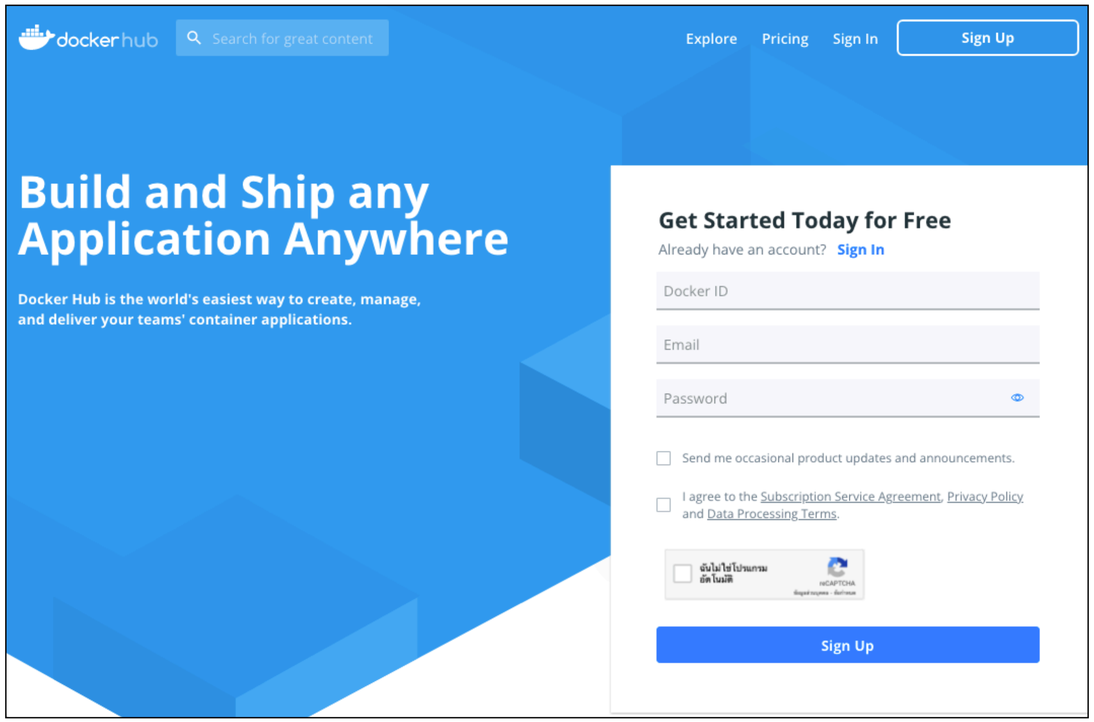
Amazon ECR

Azure Container Registry

Google Container Registry

DOCKER REGISTRY (HUB.DOCKER.COM)

Docker Registry



elastic

https://www.docker.elastic.co/

Amazon ECR

Azure Container Registry

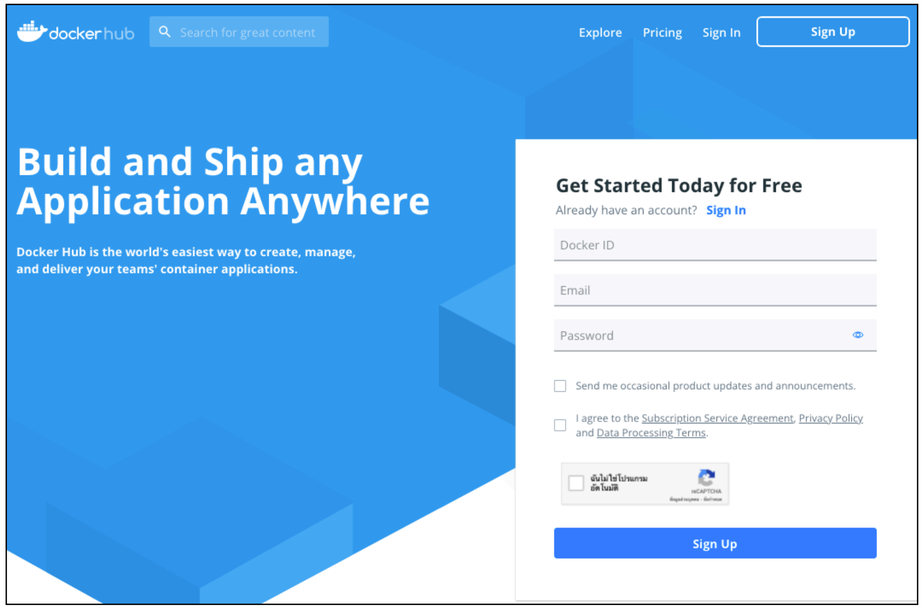
Google Container Registry

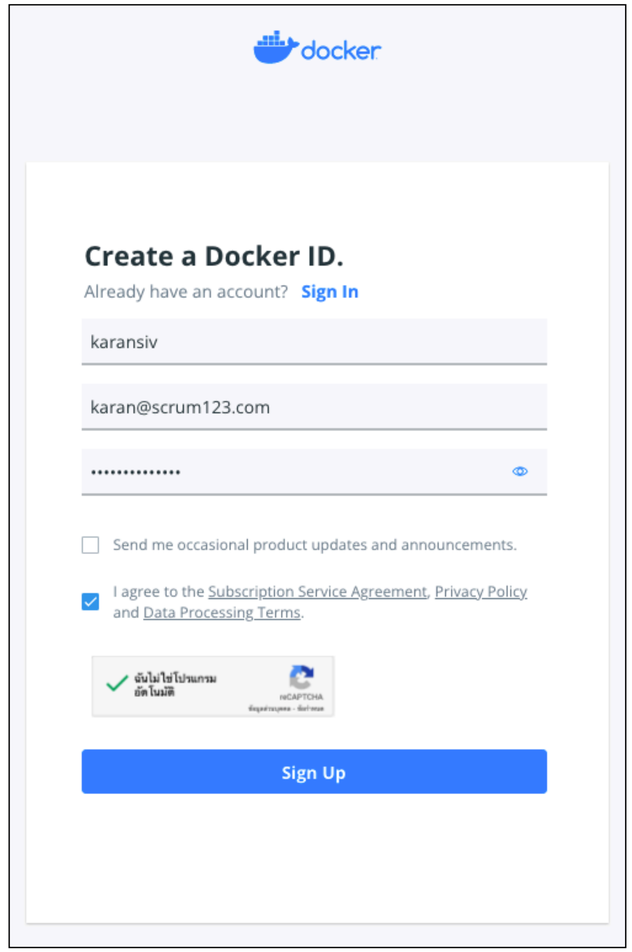
goharbor.io

JFrog Artifactory

SIGN UP ON HUB.DOCKER.COM

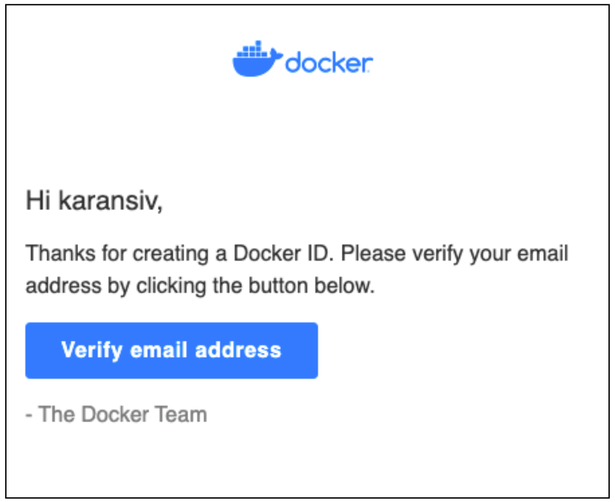
SIGN UP ON HUB.DOCKER.COM

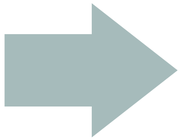


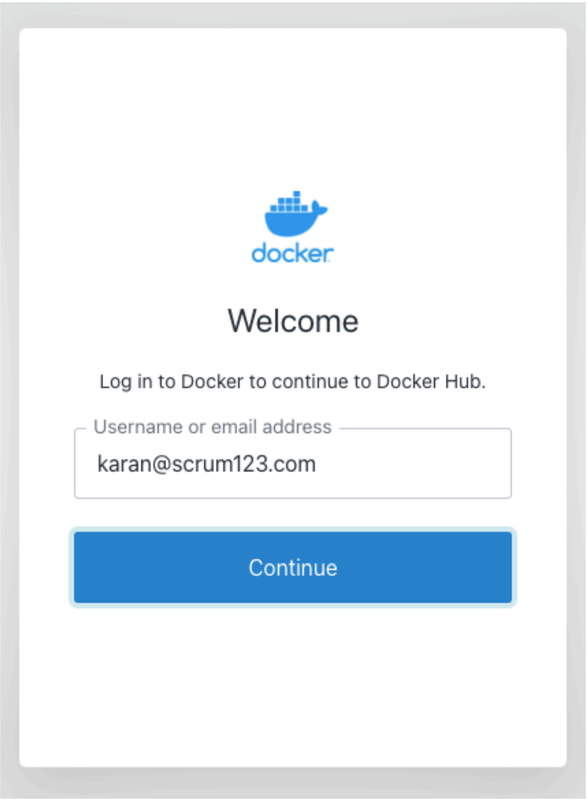


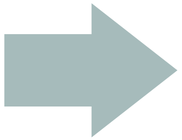
SIGN UP ON HUB.DOCKER.COM

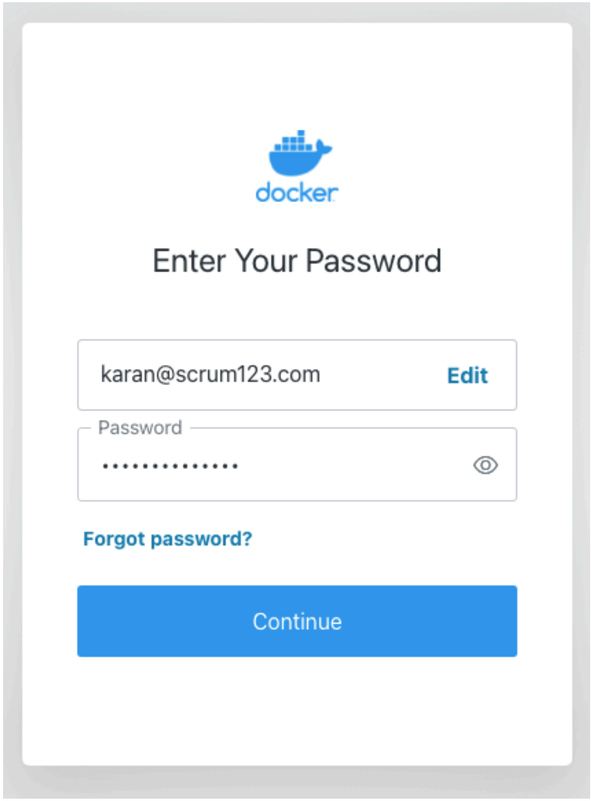
SIGN UP ON HUB.DOCKER.COM





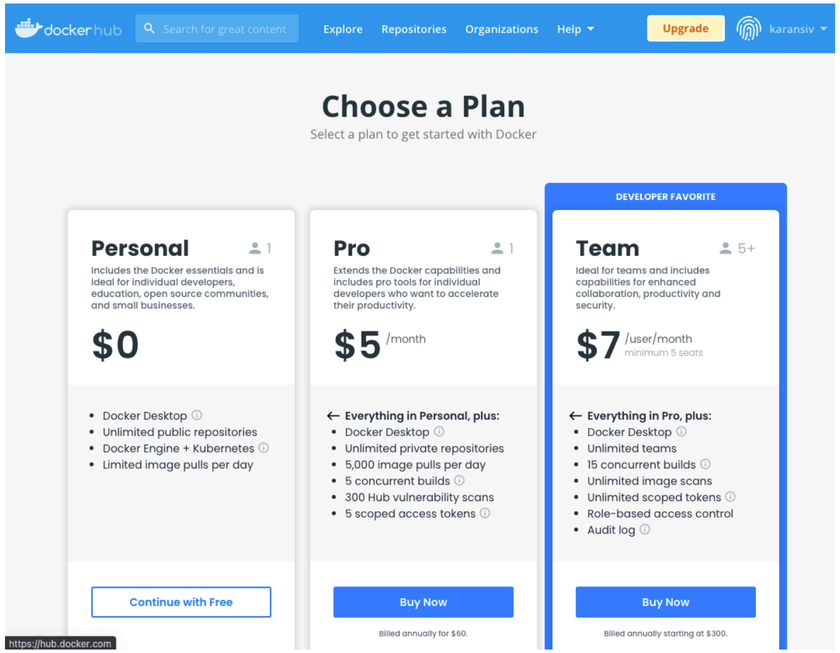


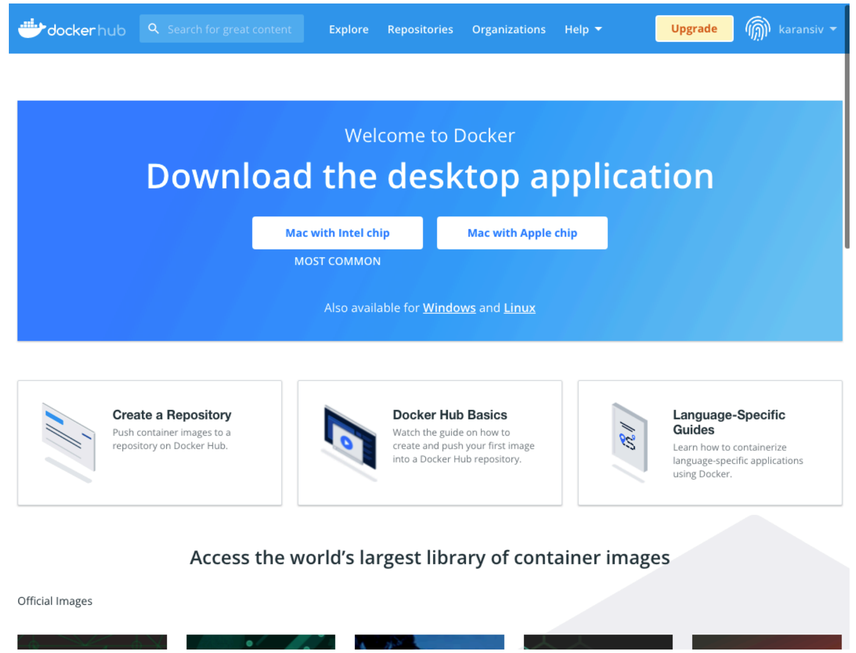




SIGN UP ON HUB.DOCKER.COM

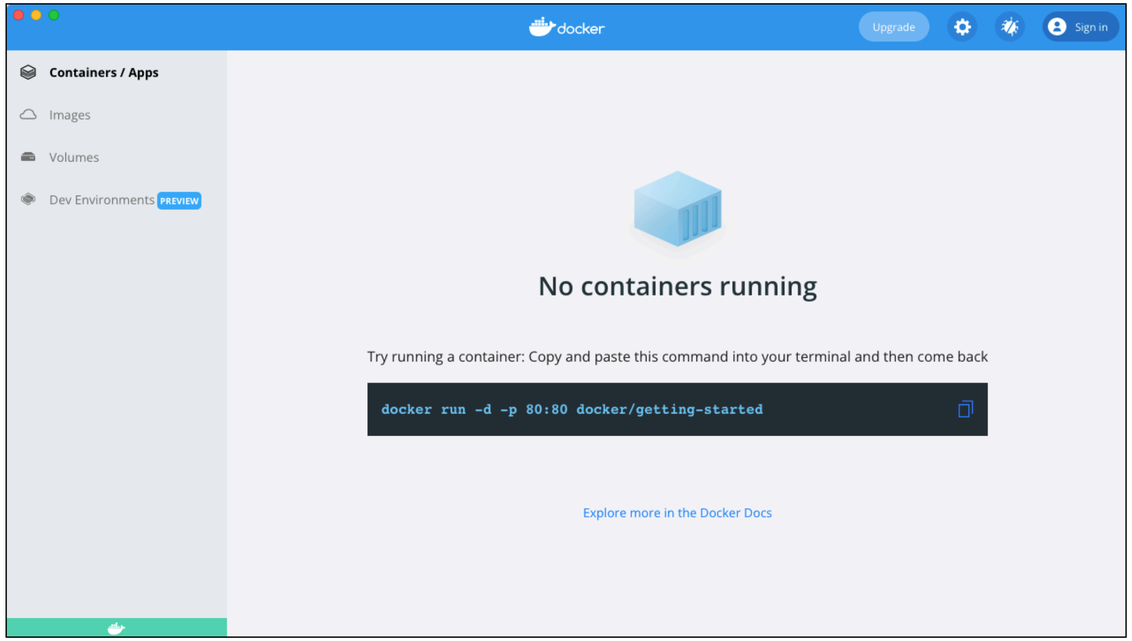
SIGN UP ON HUB.DOCKER.COM

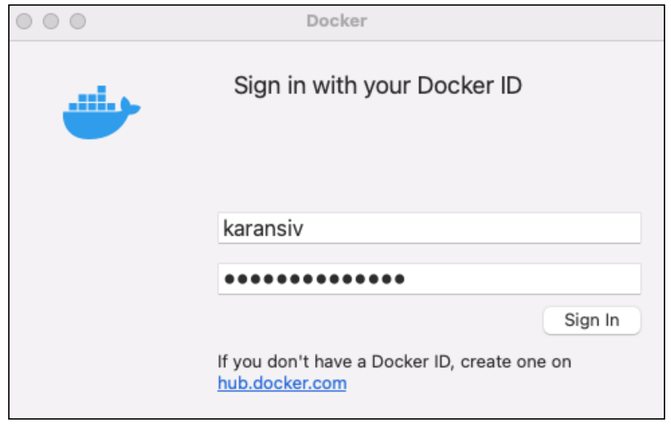




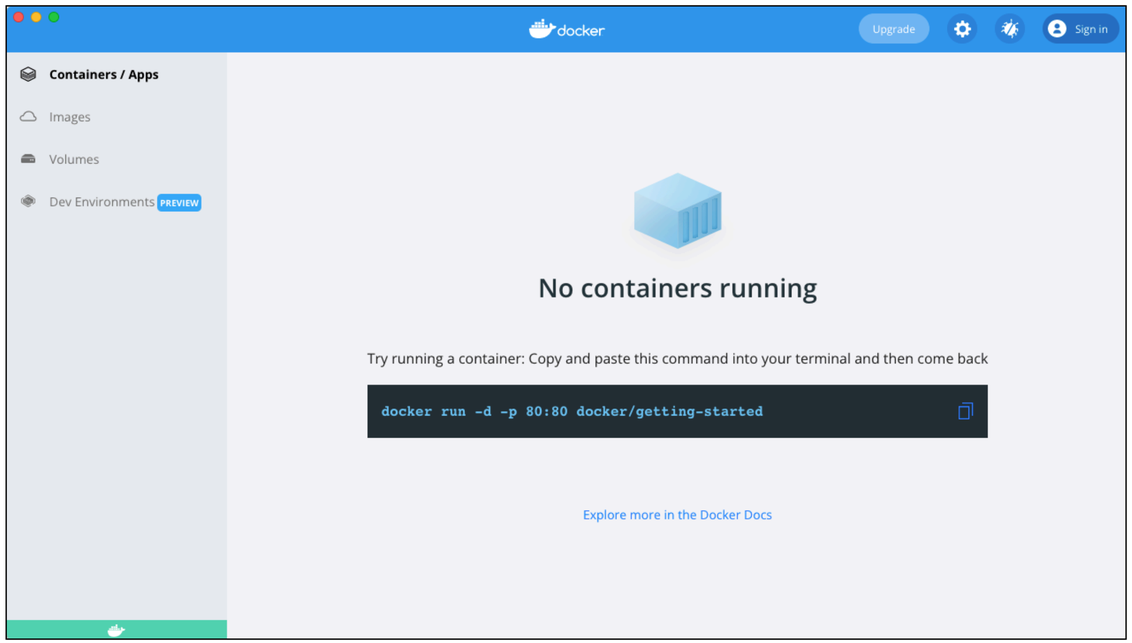
SIGN IN DOCKER DESTOP

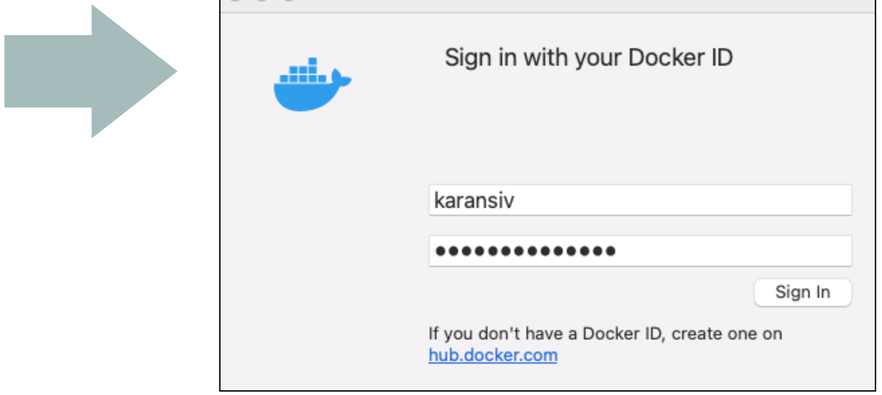
SIGN IN DOCKER DESTOP





SIGN IN DOCKER DESTOP





DOCKER PUSH COMMAND

DOCKER PUSH COMMAND

```
$ docker push [OPTION] NAME[:tag]
```

DOCKER PUSH COMMAND

```
$ docker push [OPTION] NAME[:tag]
```

Example :

```
$ docker push karansiv/application:0.0.1
```

DOCKER PUSH COMMAND

```
$ docker push [OPTION] NAME[:tag]
```

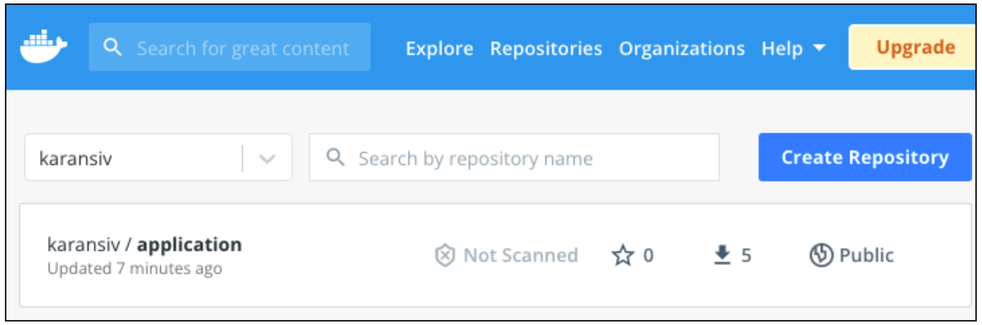
Example :

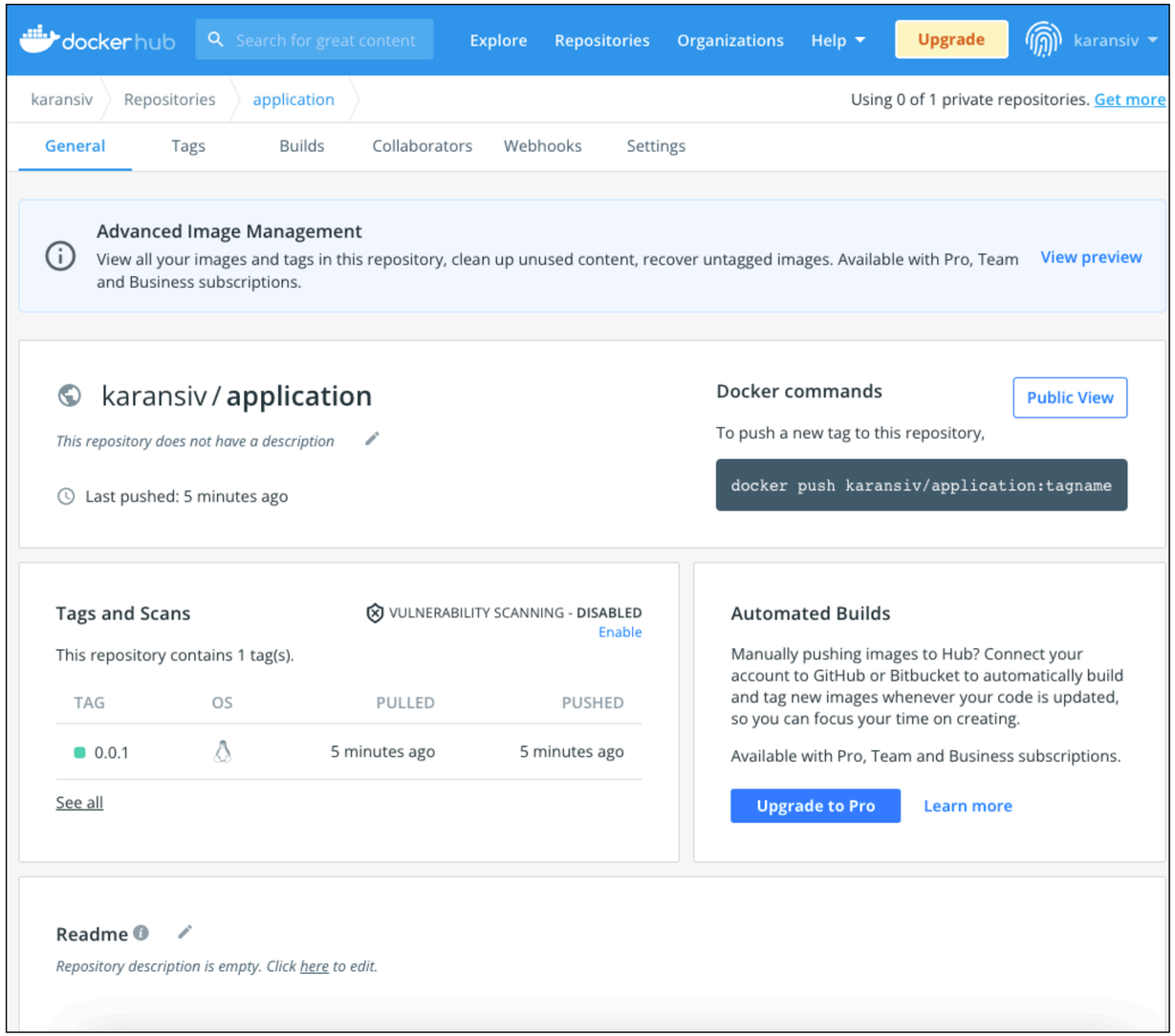
```
$ docker push karansiv/application:0.0.1
```

```
The push refers to repository [docker.io/karansiv/application]
57cf4935a684: Pushed
b79069e91828: Pushed
0eba131dffd0: Mounted from library/ubuntu
0.0.1: digest:
sha256:2e64722cdb0275c0068d7786755b7a0e179410796bf2484a890c3f879aefb6b7 size: 952
```

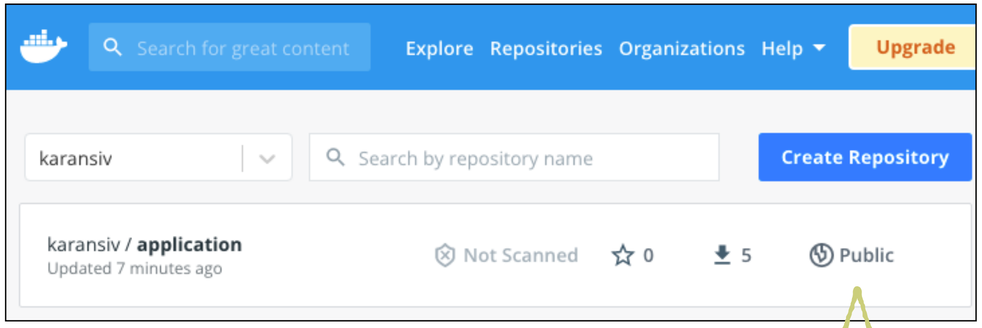
DOCKER REMOTE REPOSITORY (HUB.DOCKER.COM)

DOCKER REMOTE REPOSITORY (HUB.DOCKER.COM)

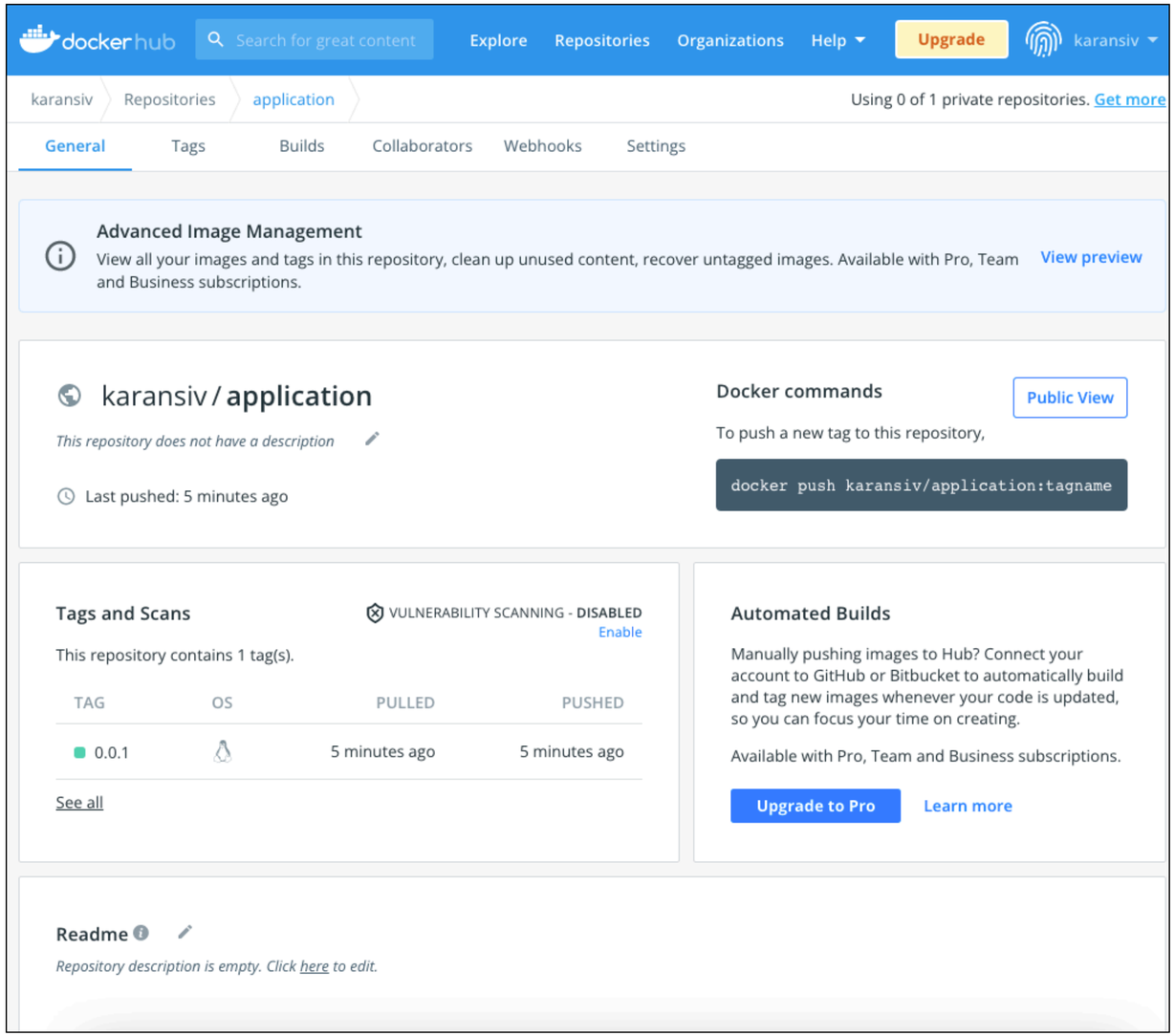




DOCKER REMOTE REPOSITORY (HUB.DOCKER.COM)

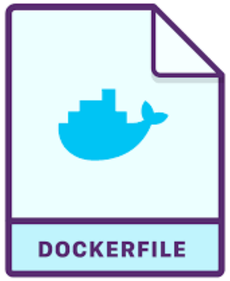


You get **one private repository for free** with your Docker Hub user account. If you **need more private** repositories for your user account, **upgrade your Docker Hub plan** from your Billing Information page.

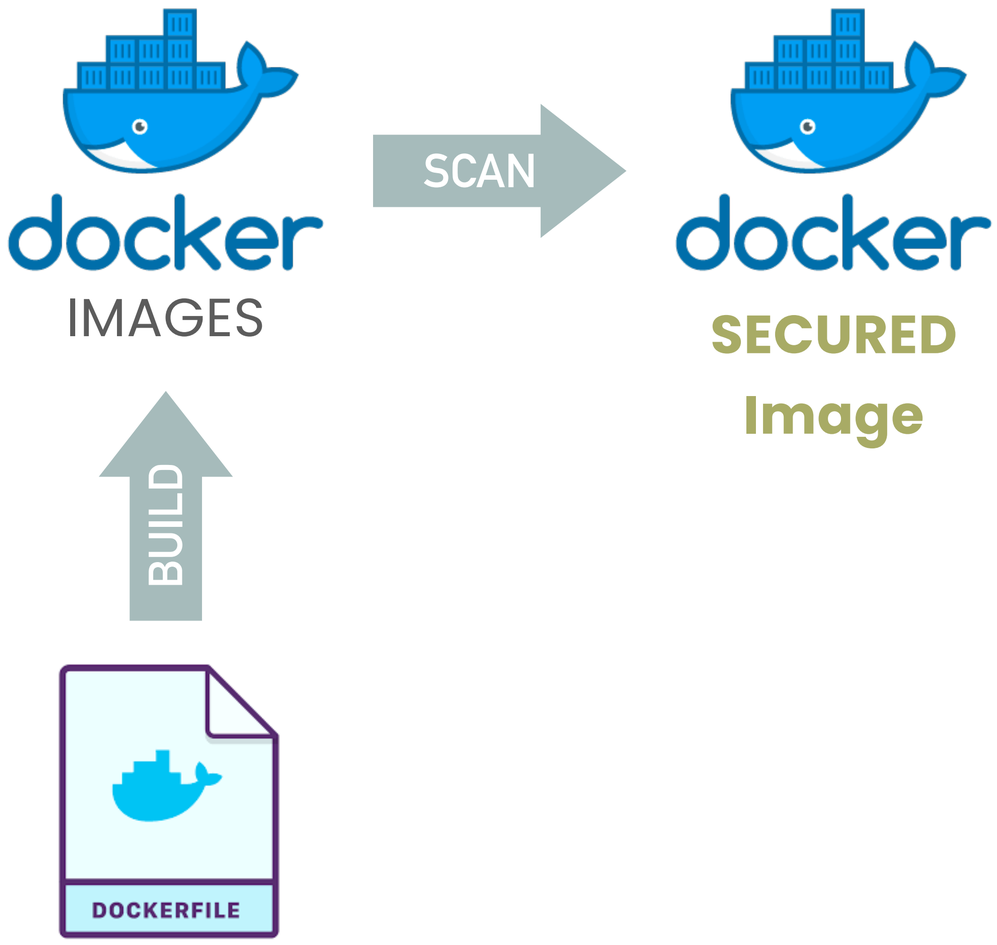


DEVELOPMENT WORKFLOW WITH DOCKER

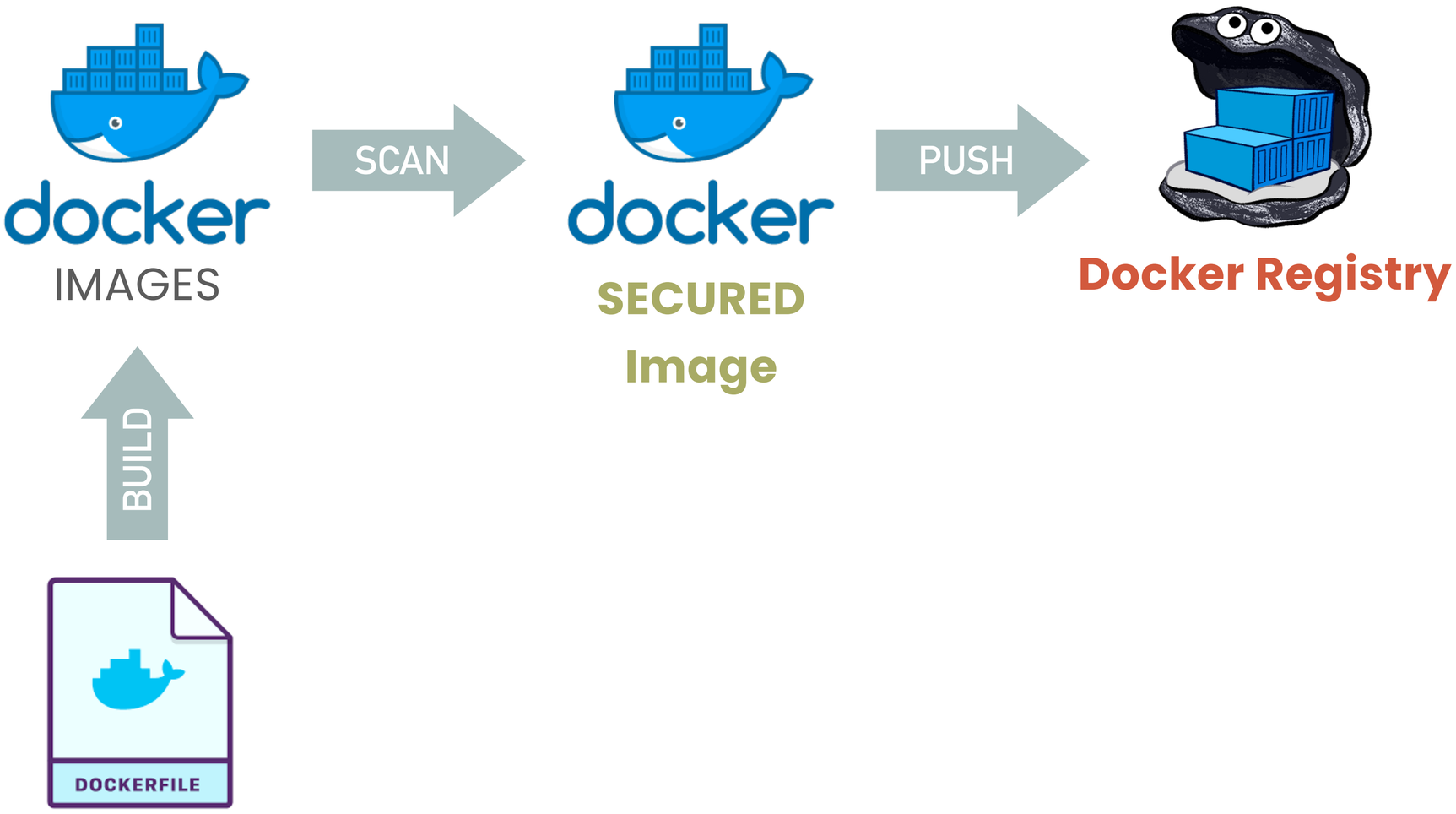
DEVELOPMENT WORKFLOW WITH DOCKER



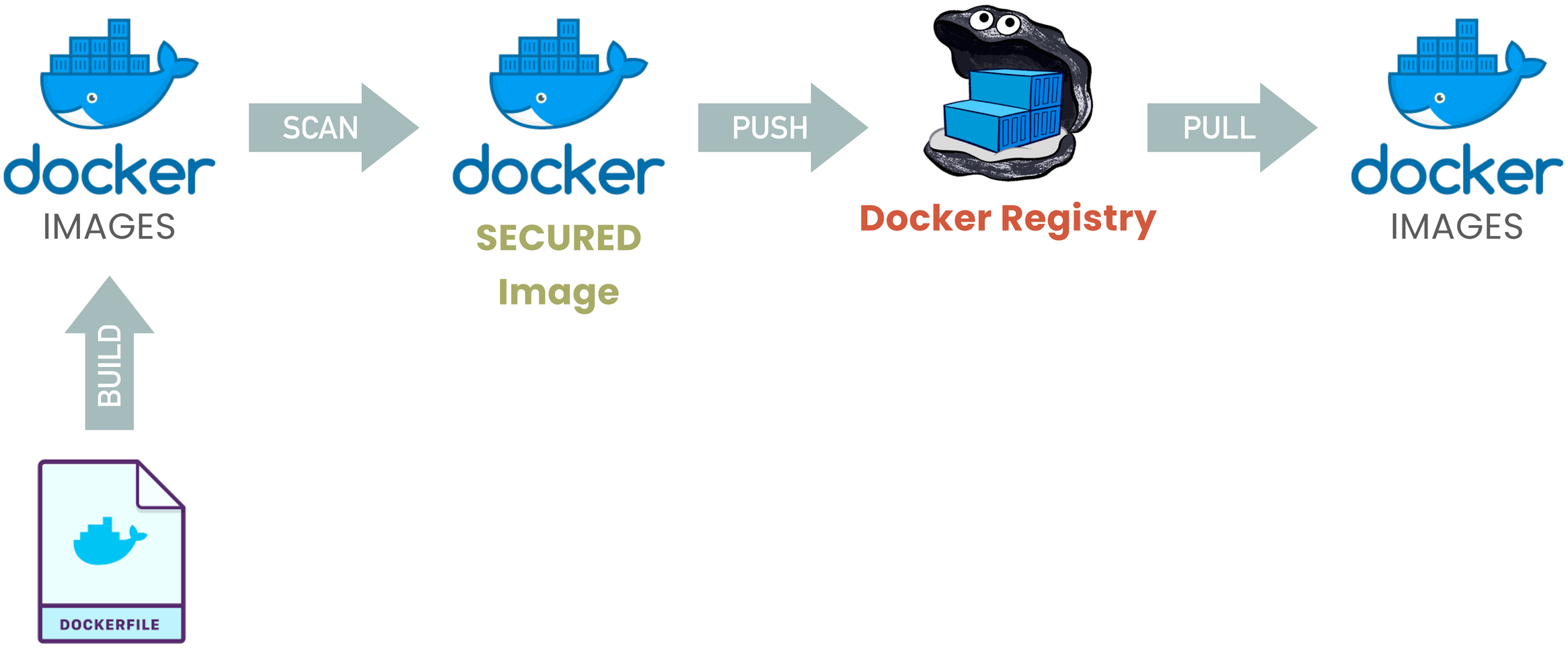
DEVELOPMENT WORKFLOW WITH DOCKER



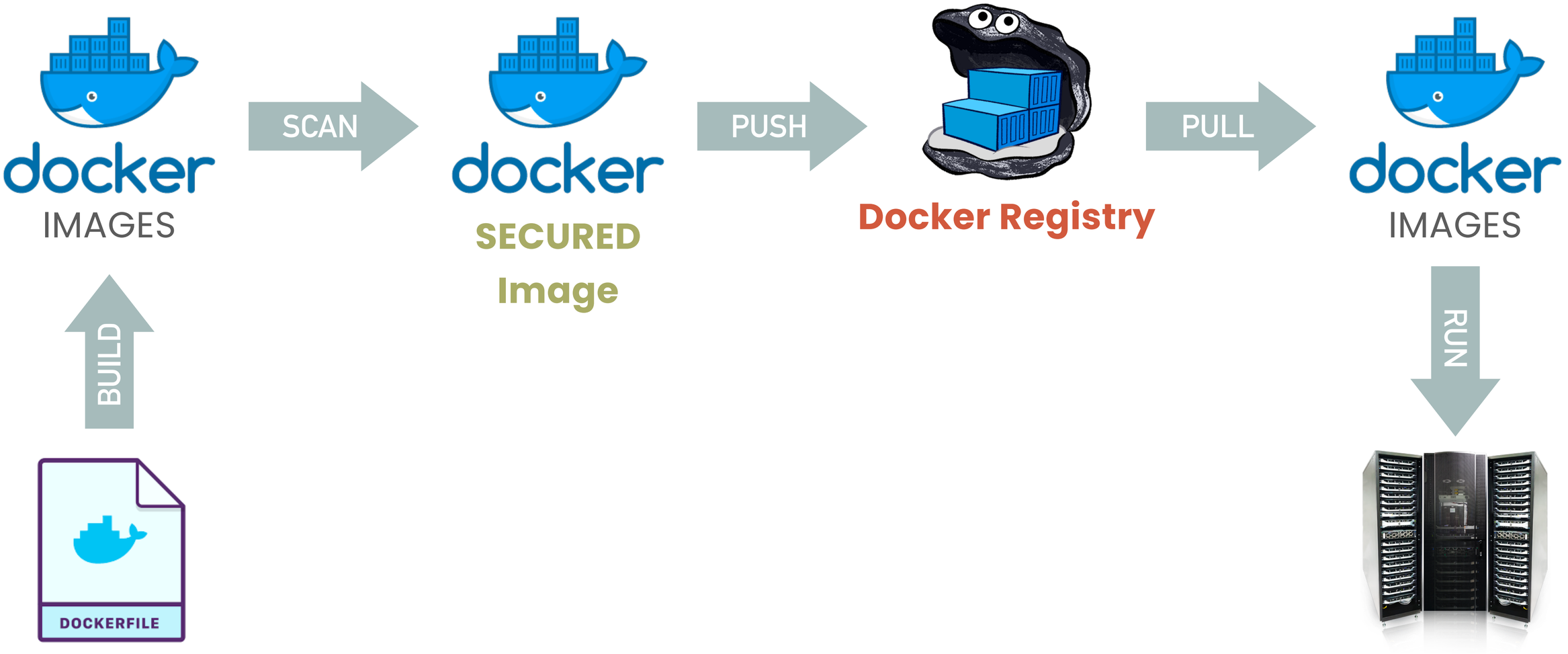
DEVELOPMENT WORKFLOW WITH DOCKER



DEVELOPMENT WORKFLOW WITH DOCKER



DEVELOPMENT WORKFLOW WITH DOCKER



THANK YOU