





# INTRODUCTION TO DOCKER

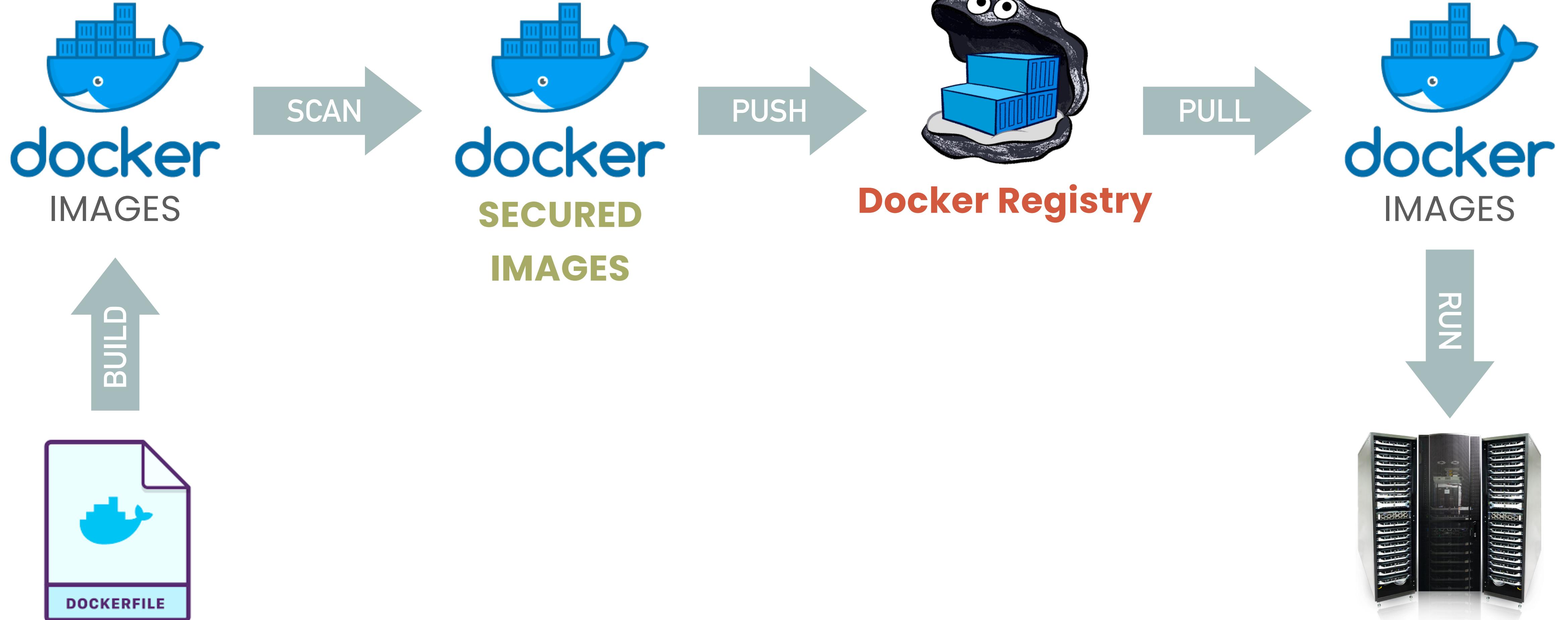


# INTRODUCTION TO DOCKER

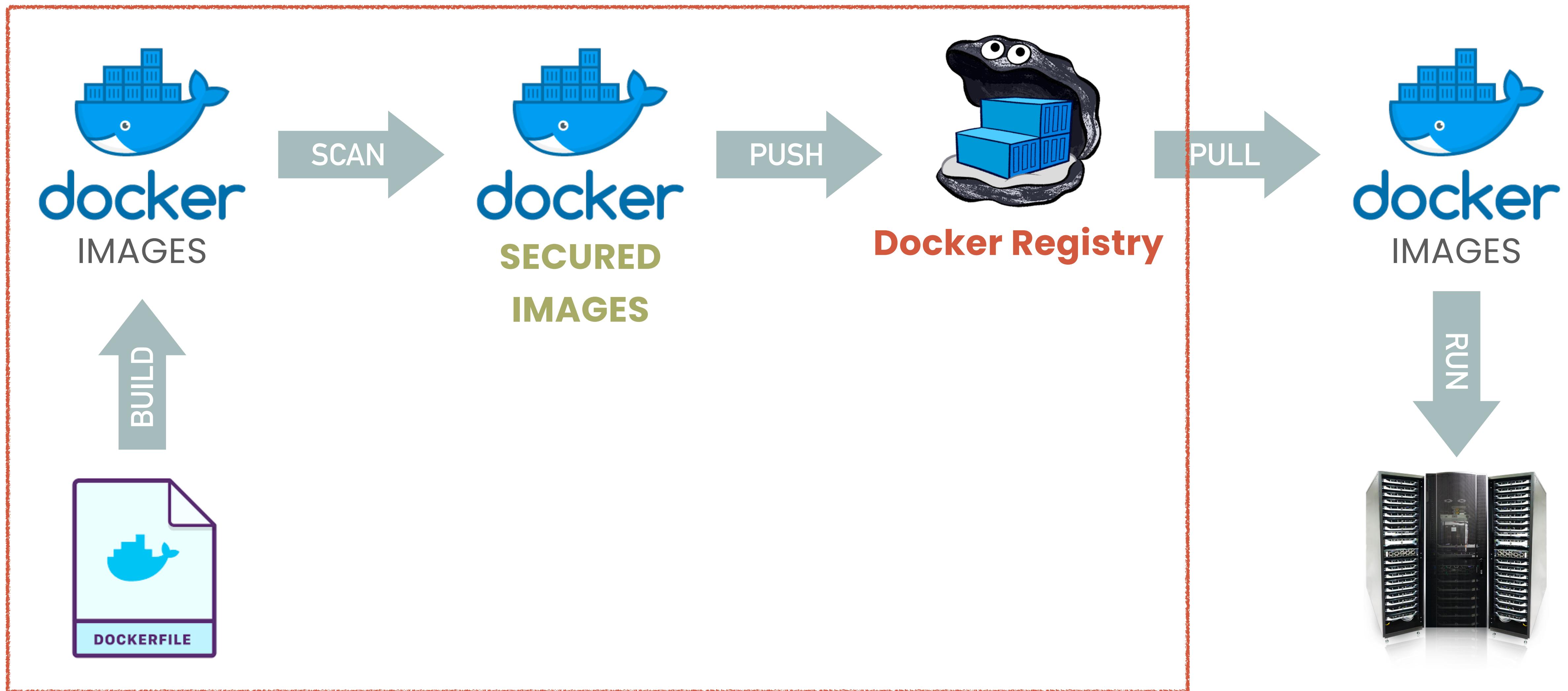
---

Multi Stage Build, Security Scan and Publish to Registry

# DEVELOPMENT WORKFLOW WITH DOCKER

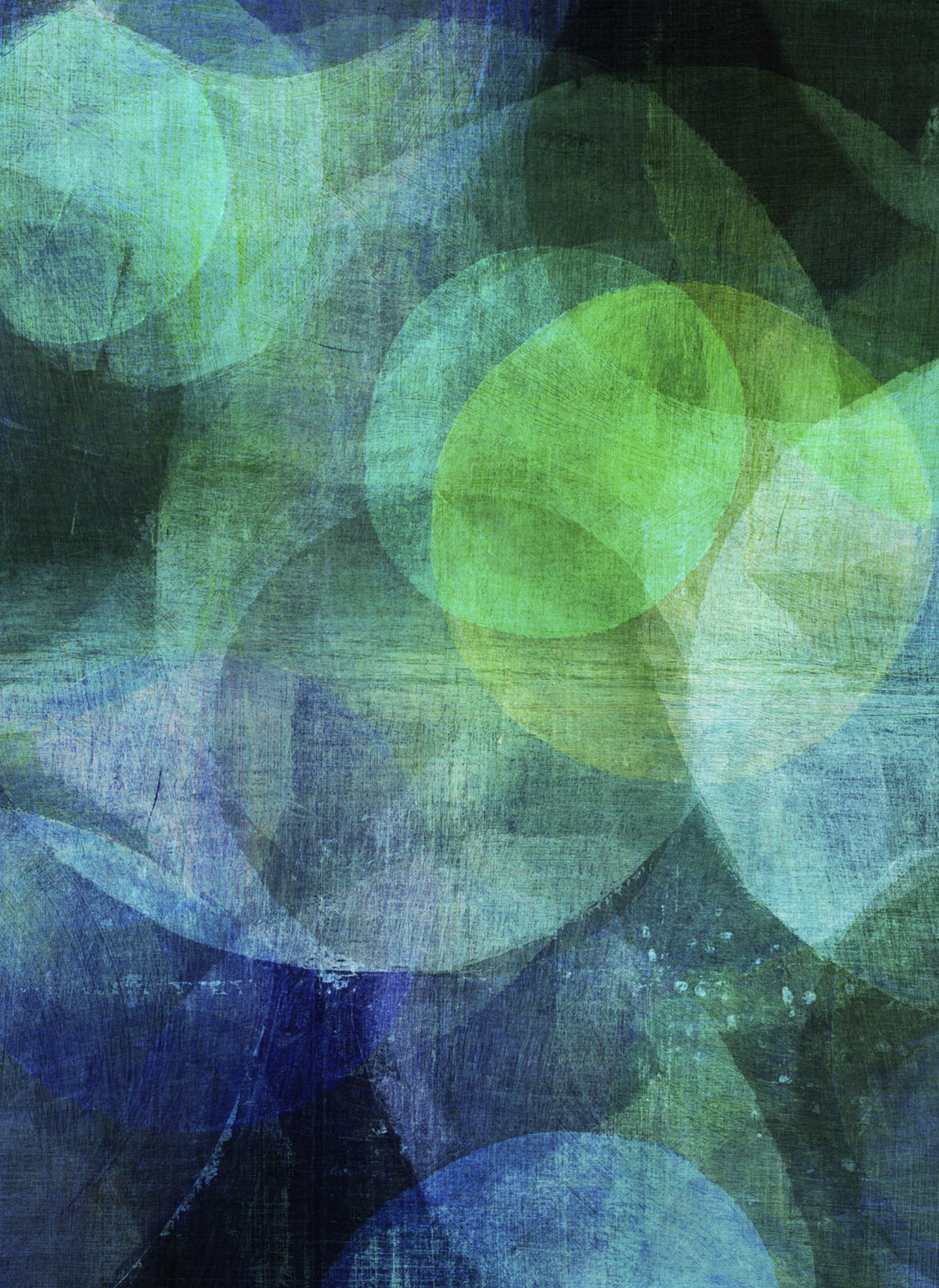


# DEVELOPMENT WORKFLOW WITH DOCKER



# AGENDA

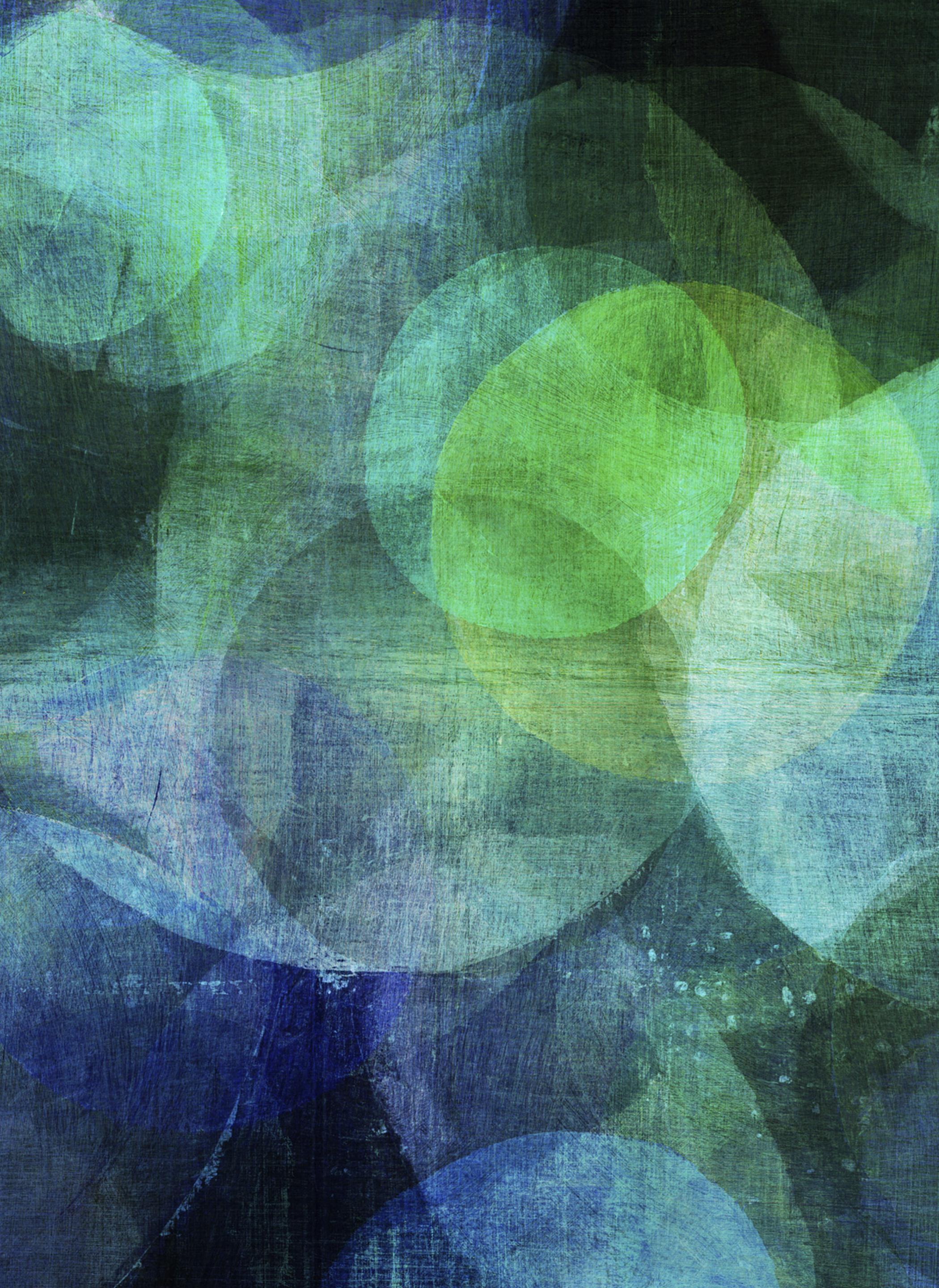
---



# AGENDA

---

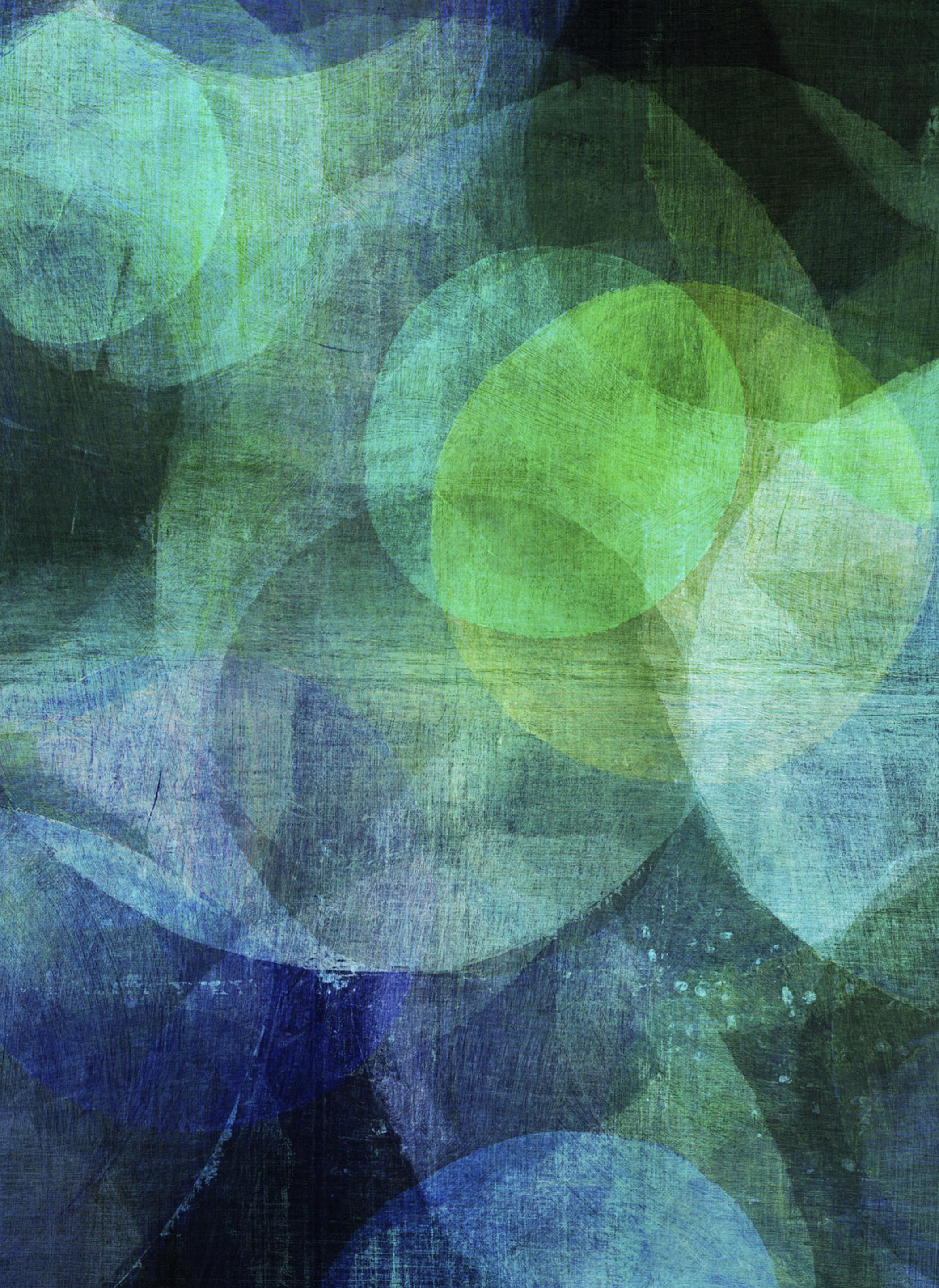
- Multi Stage Build



# AGENDA

---

- Multi Stage Build
- Docker Scan



# AGENDA

---

- Multi Stage Build
- Docker Scan
- Docker Registry

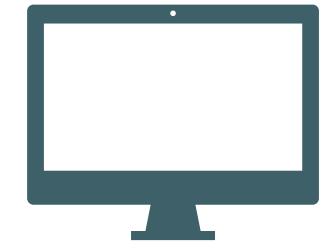


# MULTI STAGE BUILD

---

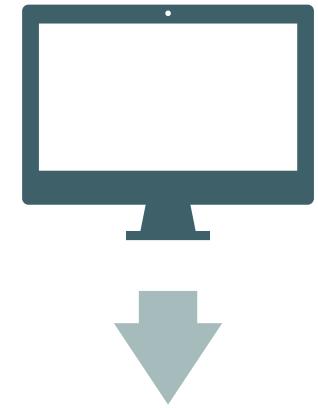
# CHALLENGING ABOUT BUILDING DOCKER IMAGE

---



# CHALLENGING ABOUT BUILDING DOCKER IMAGE

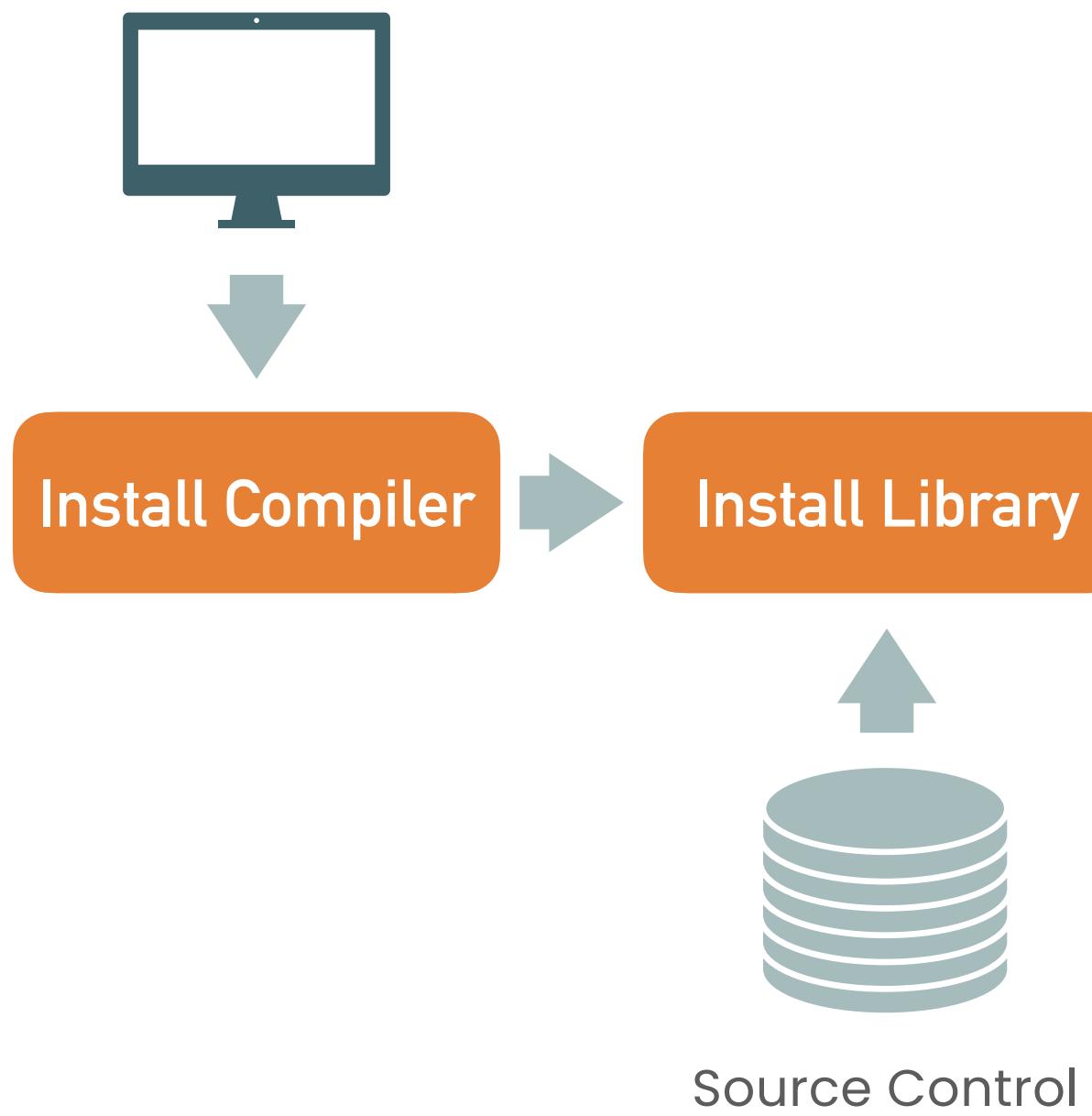
---



Install Compiler

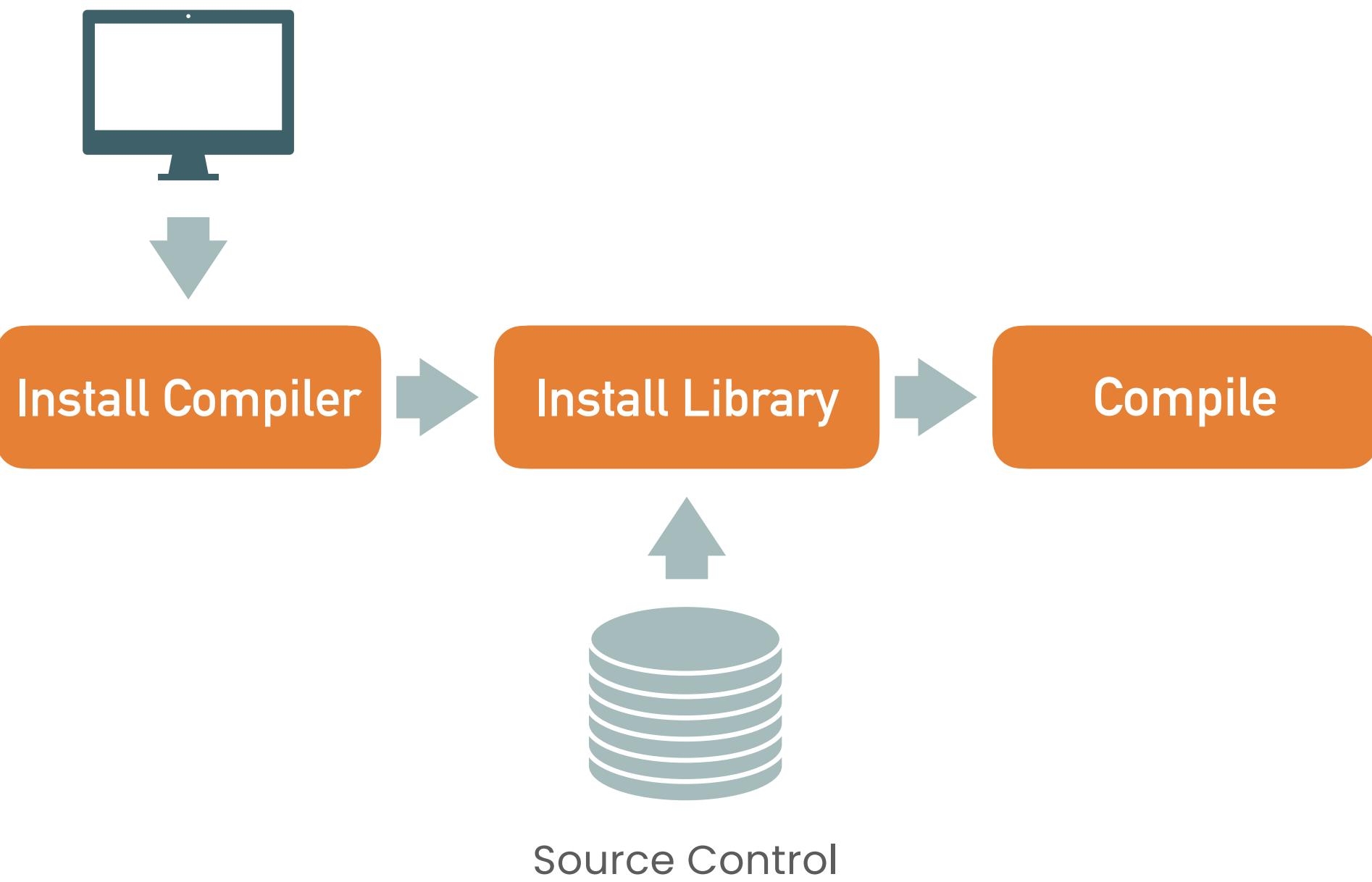
# CHALLENGING ABOUT BUILDING DOCKER IMAGE

---



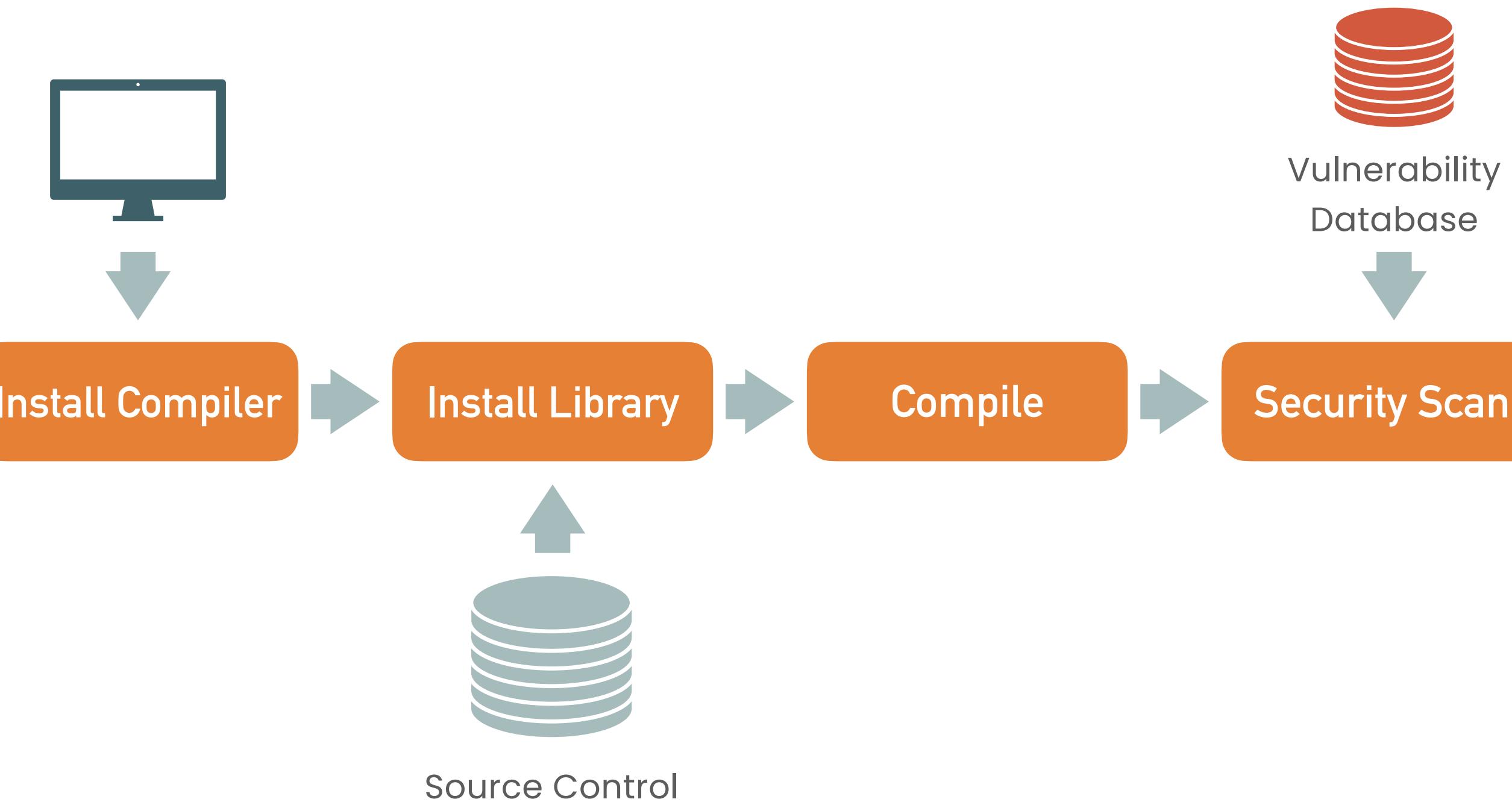
# CHALLENGING ABOUT BUILDING DOCKER IMAGE

---

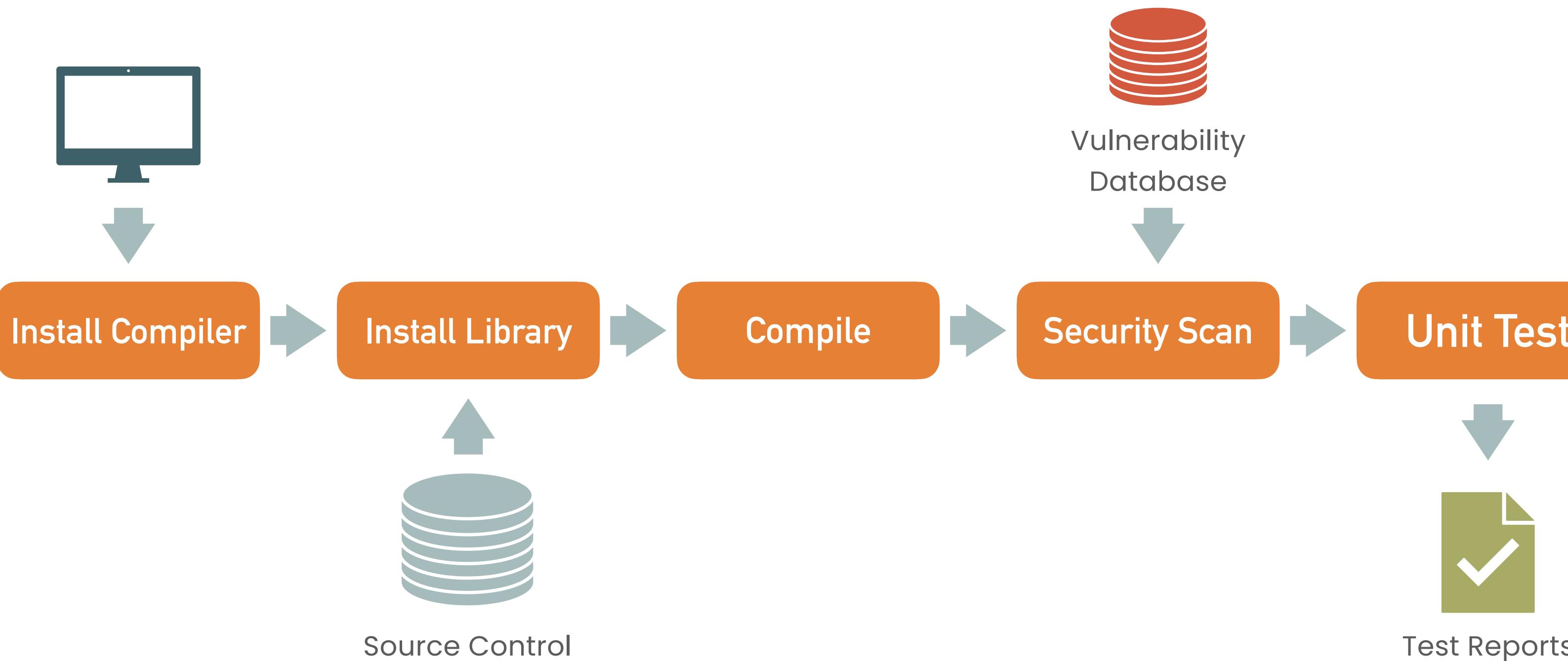


# CHALLENGING ABOUT BUILDING DOCKER IMAGE

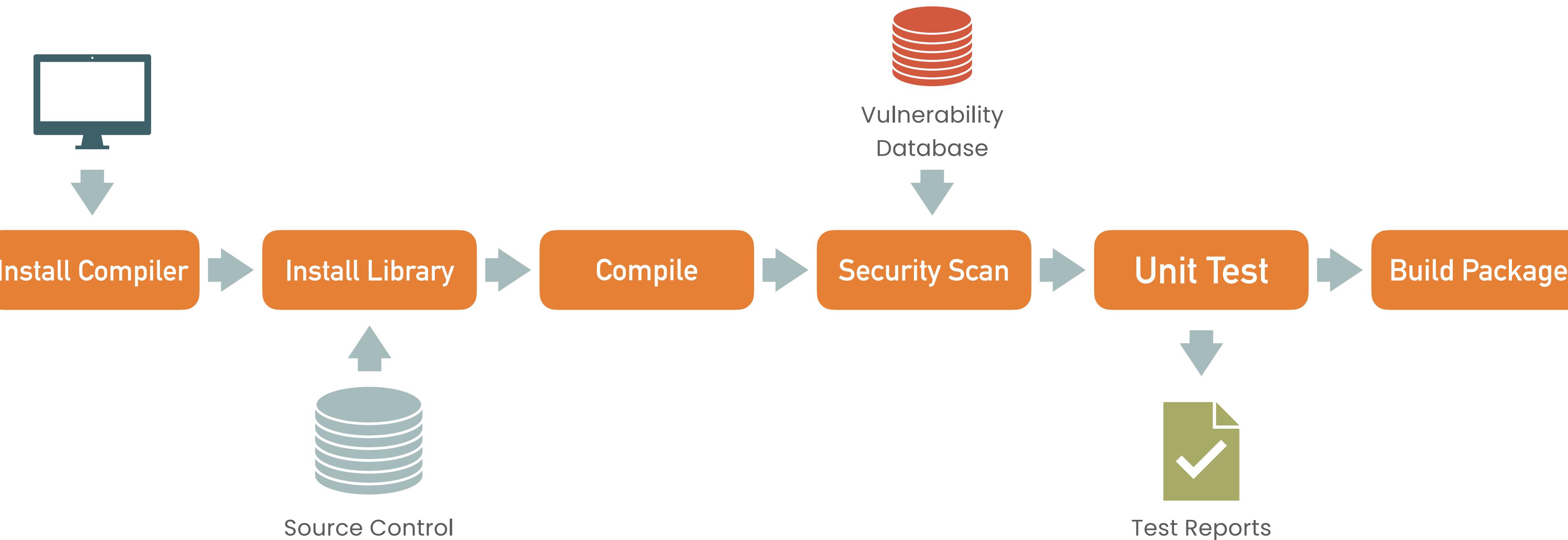
---



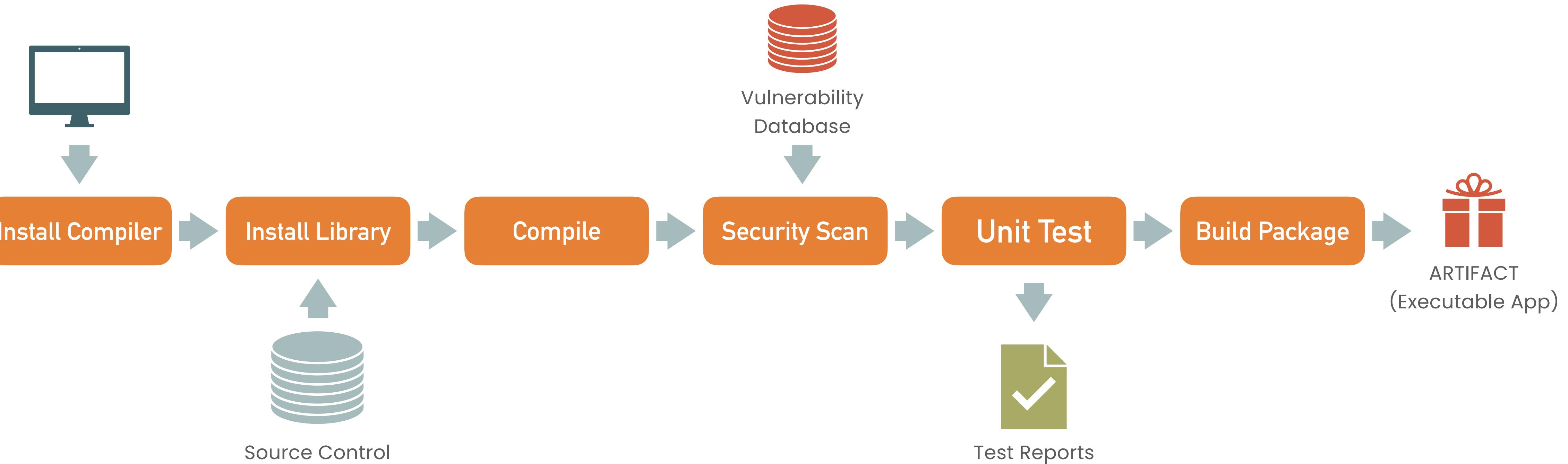
# CHALLENGING ABOUT BUILDING DOCKER IMAGE



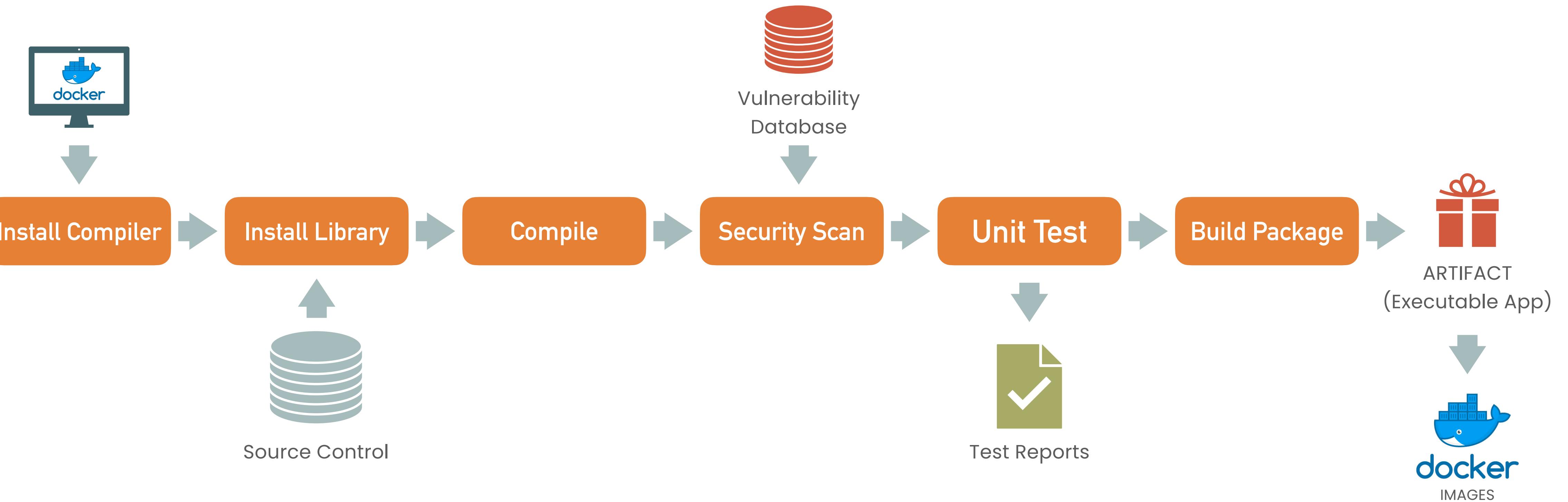
# CHALLENGING ABOUT BUILDING DOCKER IMAGE



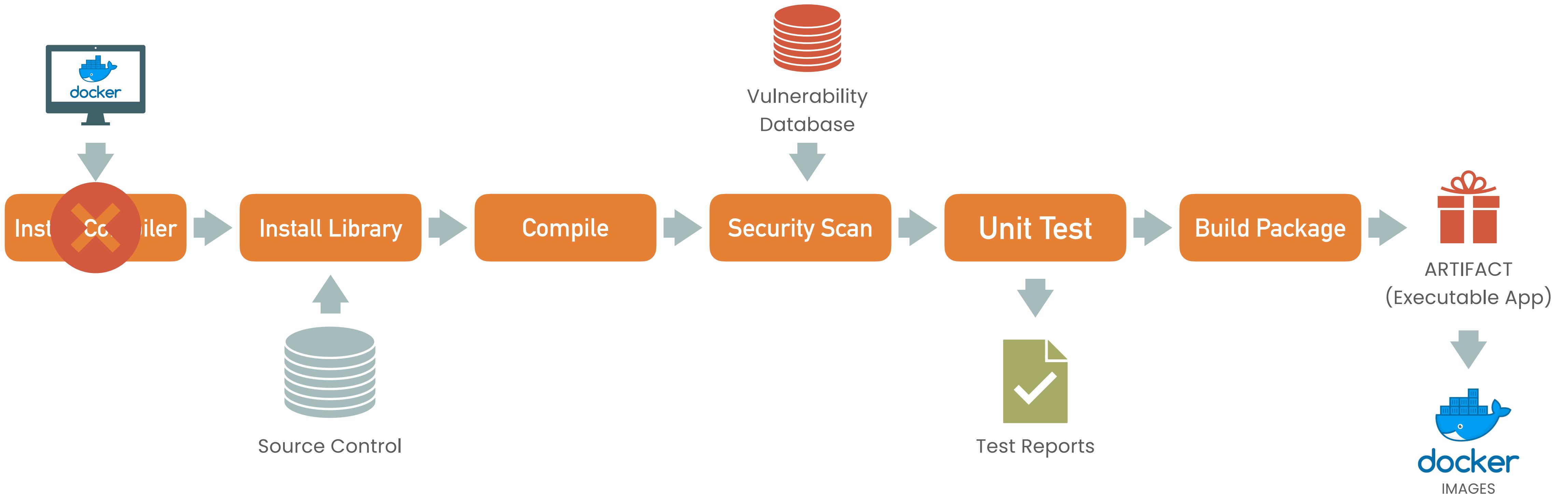
# CHALLENGING ABOUT BUILDING DOCKER IMAGE



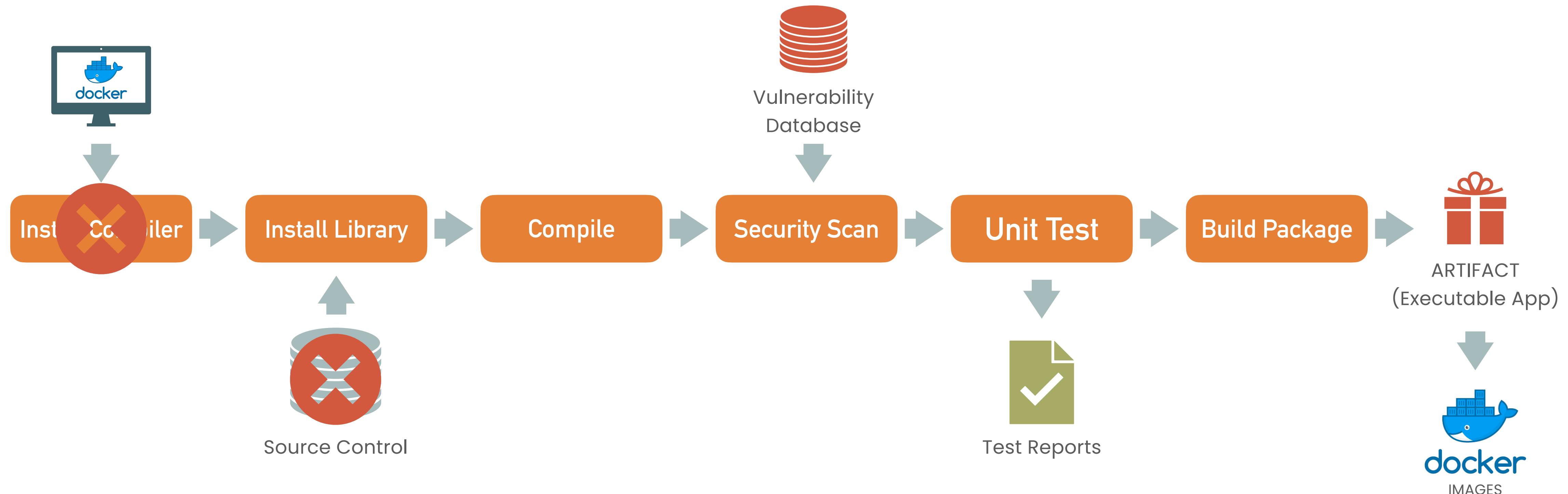
# CHALLENGING ABOUT BUILDING DOCKER IMAGE



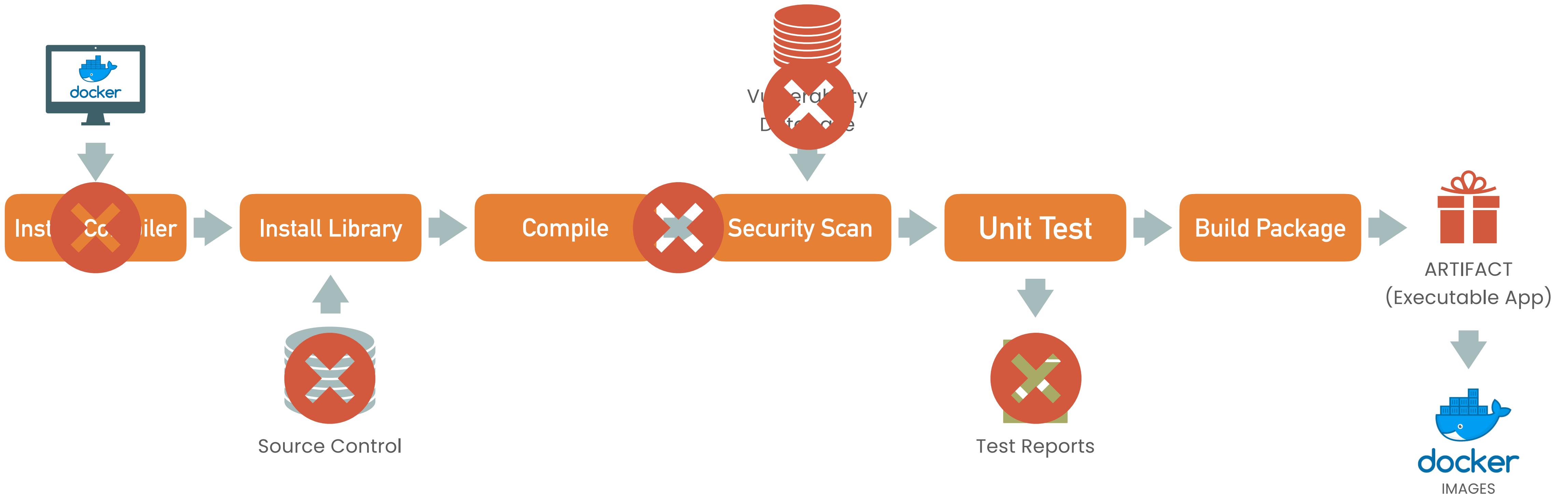
# CHALLENGING ABOUT BUILDING DOCKER IMAGE



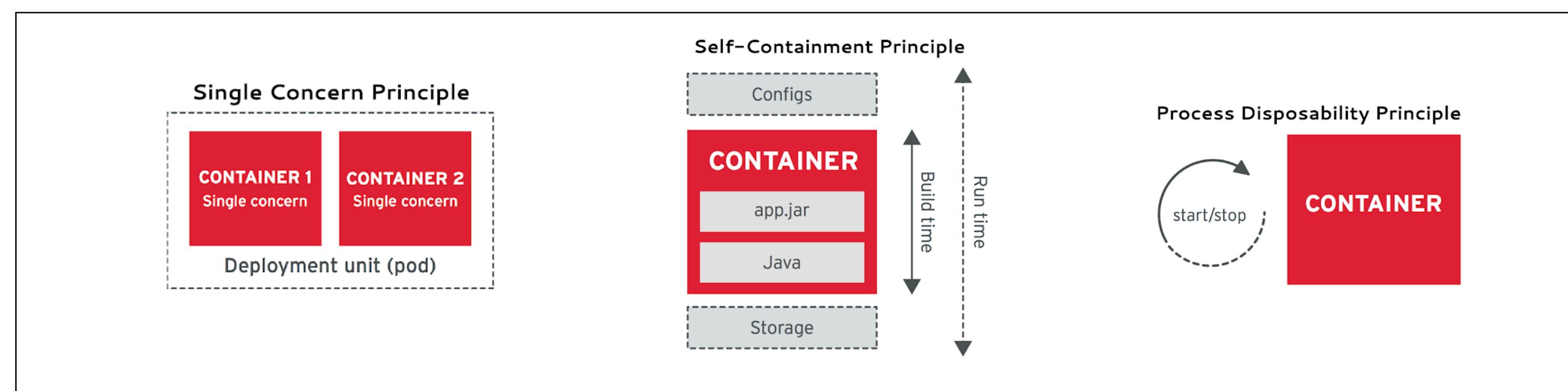
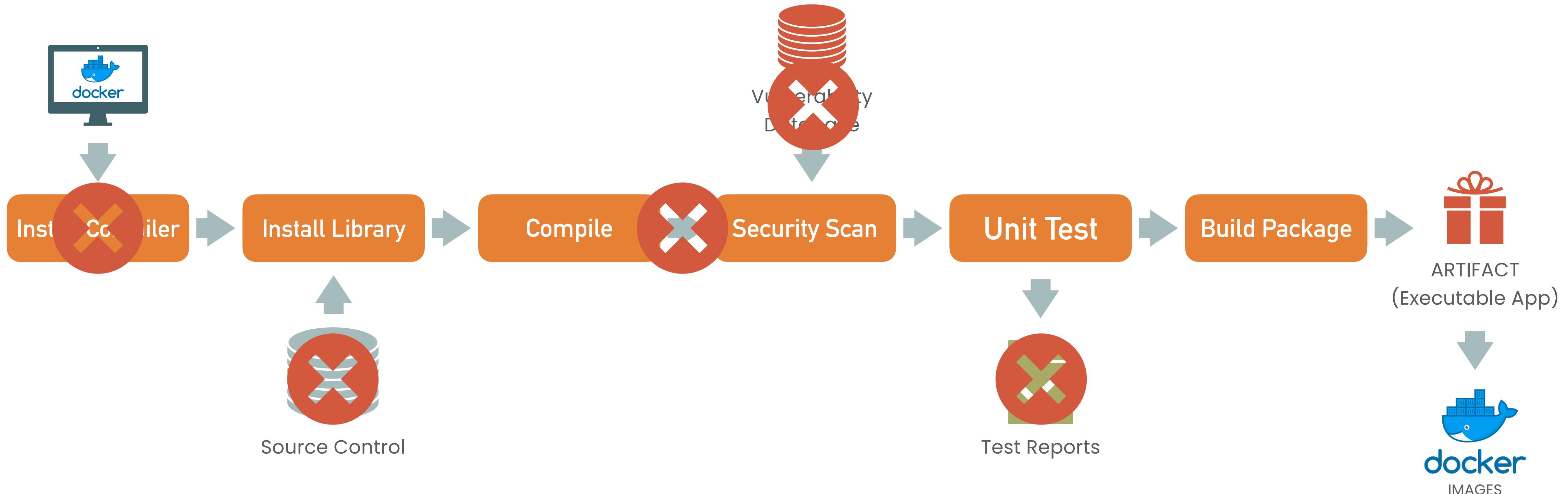
# CHALLENGING ABOUT BUILDING DOCKER IMAGE



# 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



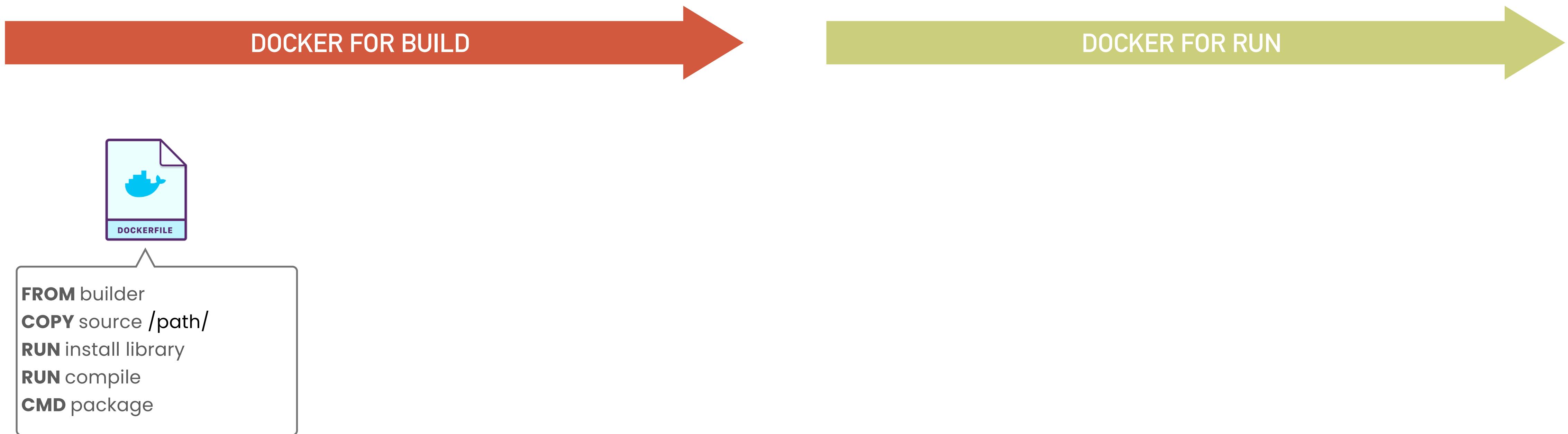
# DOCKER FOR BUILD AND DOCKER FOR RUN

---



# DOCKER FOR BUILD AND DOCKER FOR RUN

---



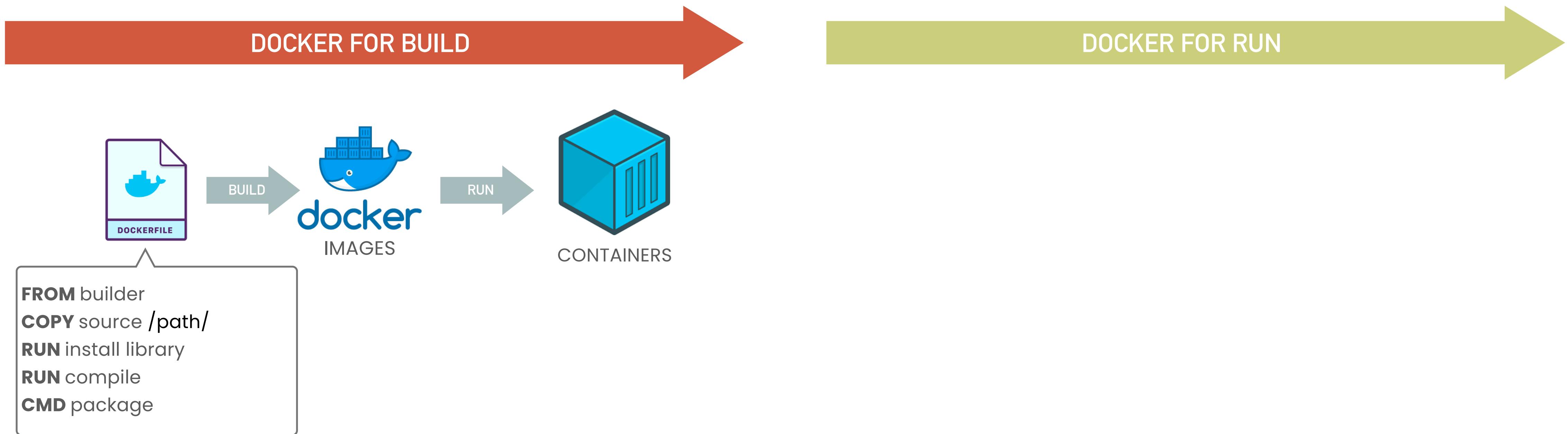
# DOCKER FOR BUILD AND DOCKER FOR RUN

---

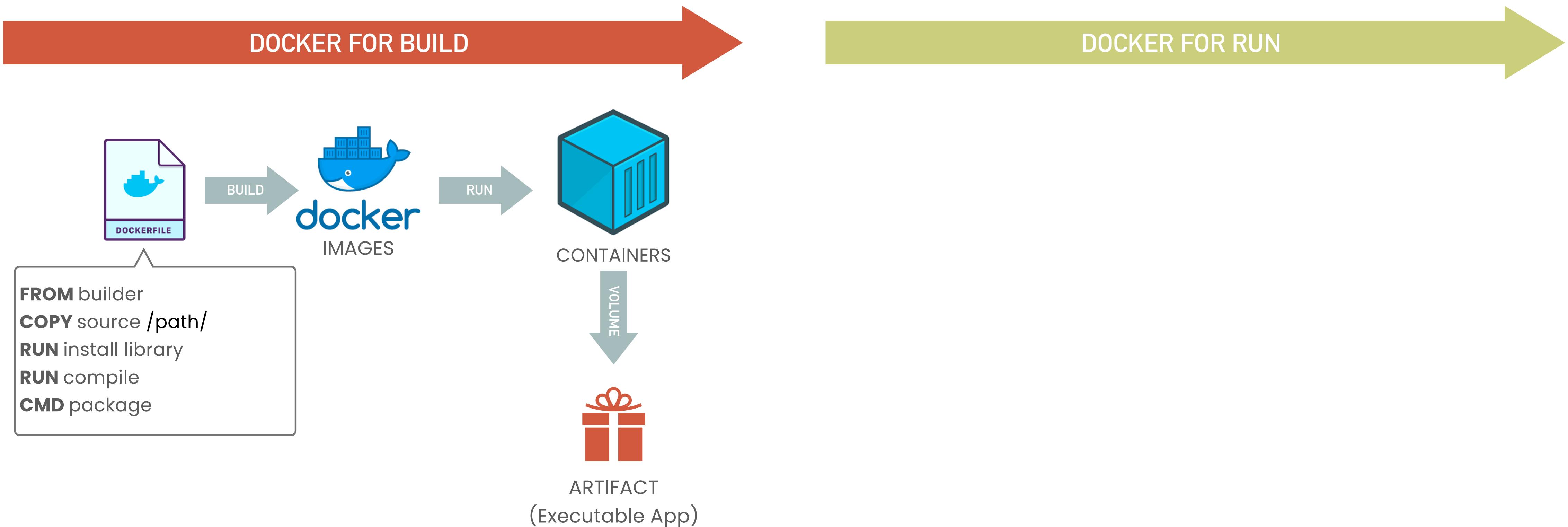


# DOCKER FOR BUILD AND DOCKER FOR RUN

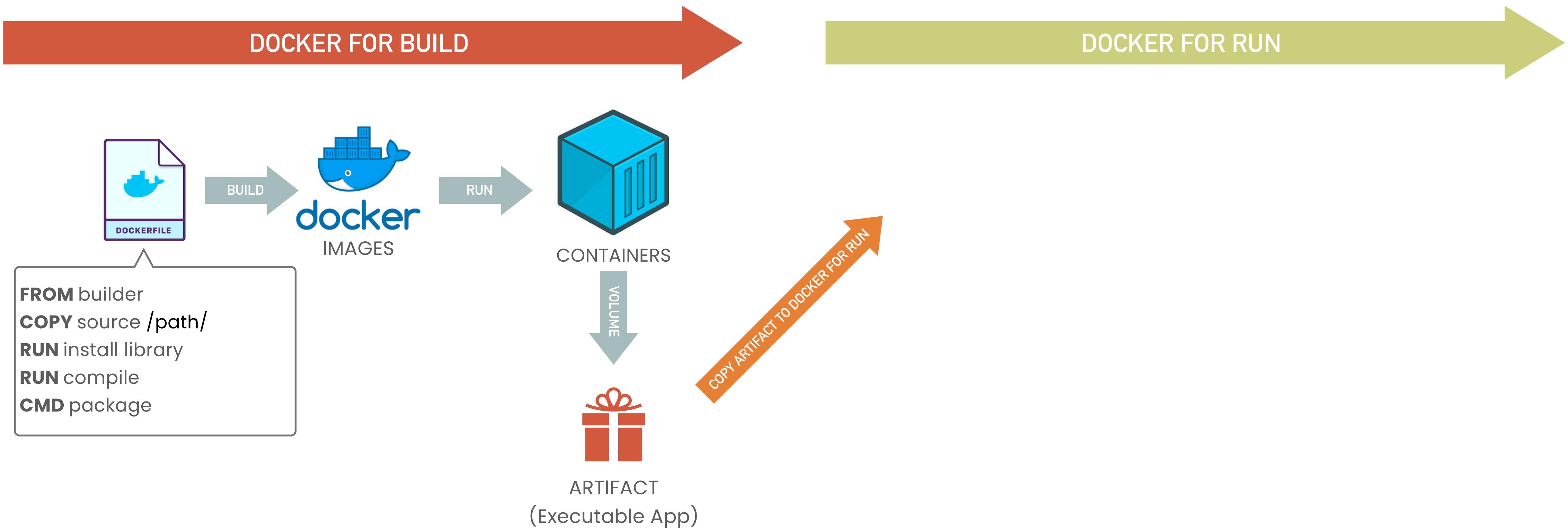
---



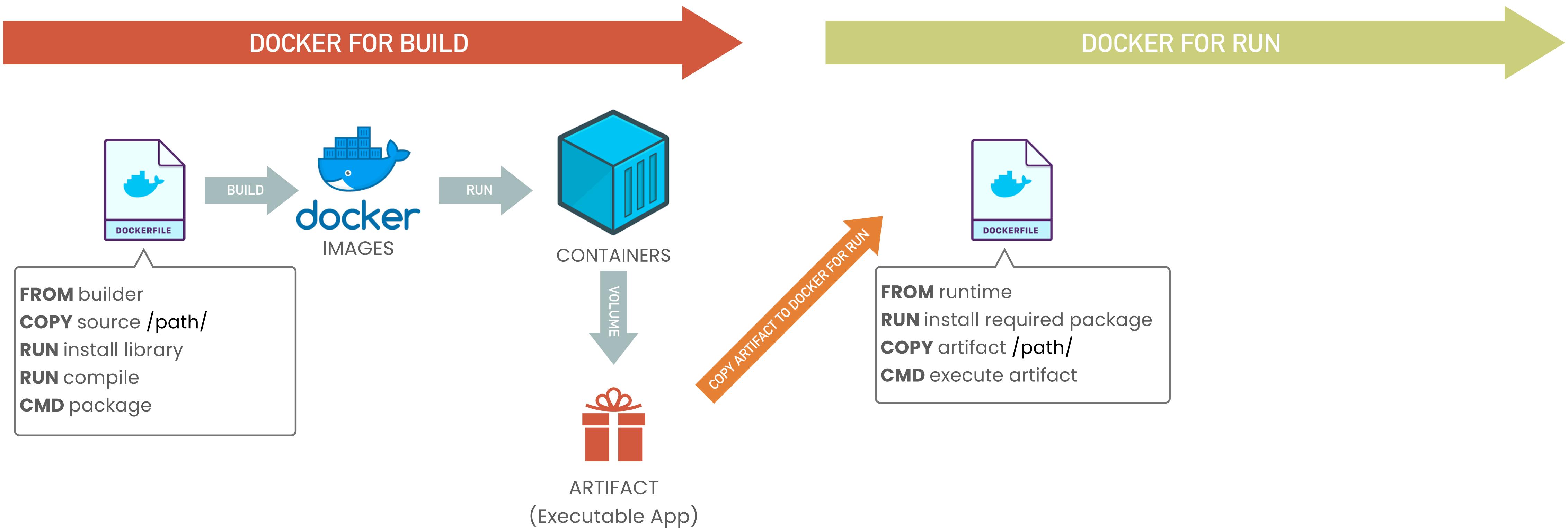
# DOCKER FOR BUILD AND DOCKER FOR RUN



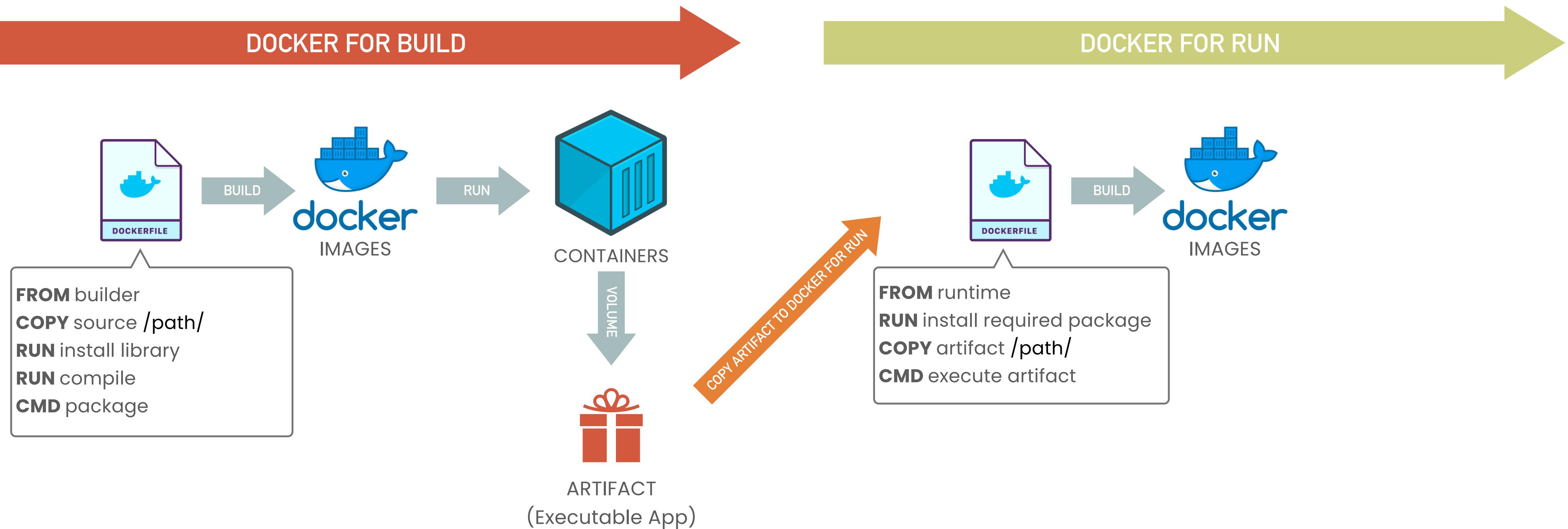
# DOCKER FOR BUILD AND DOCKER FOR RUN



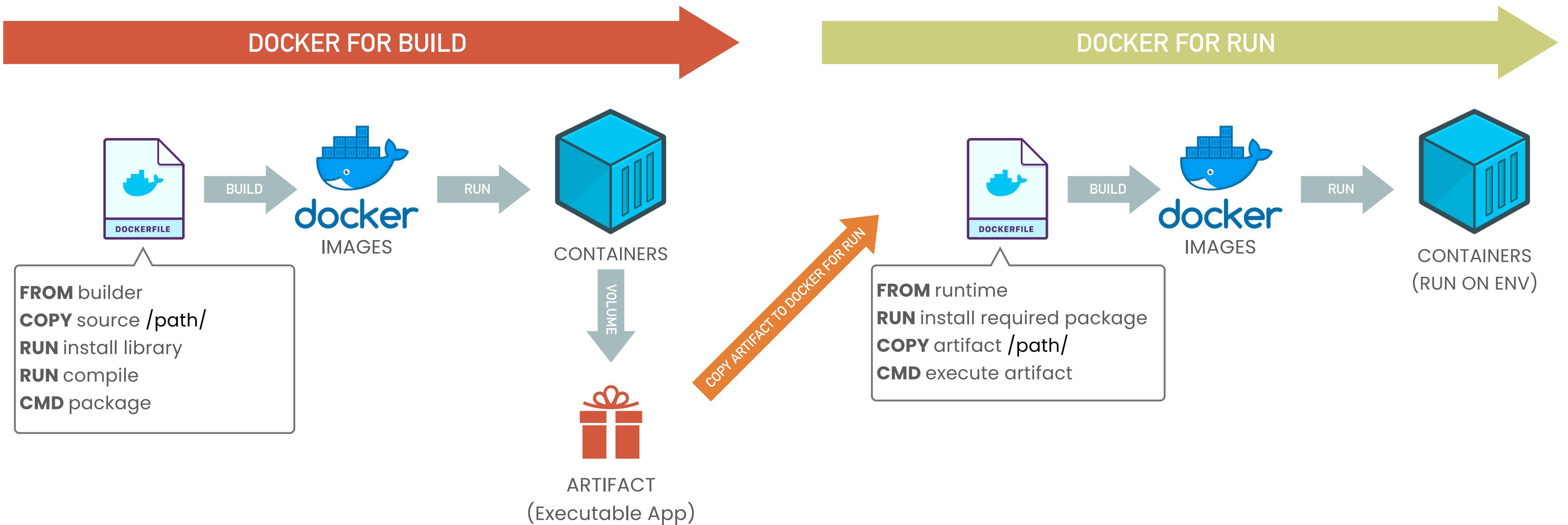
# DOCKER FOR BUILD AND DOCKER FOR RUN



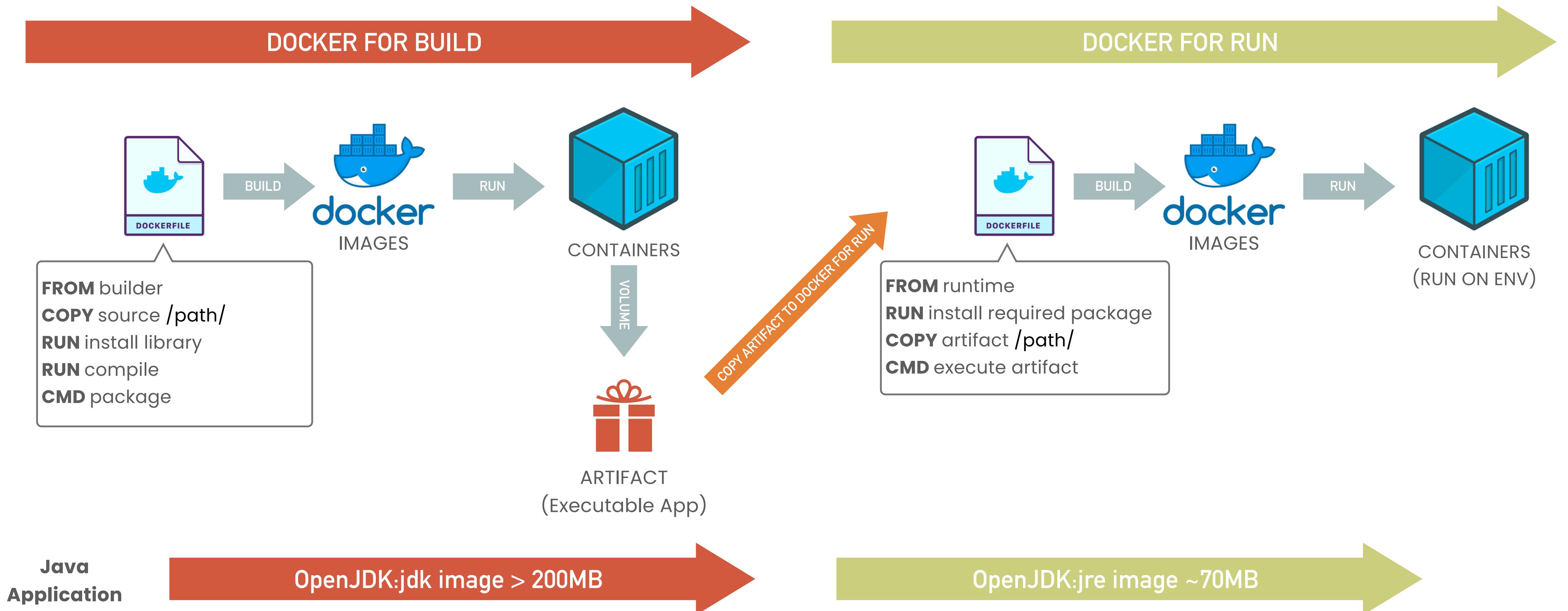
# DOCKER FOR BUILD AND DOCKER FOR RUN



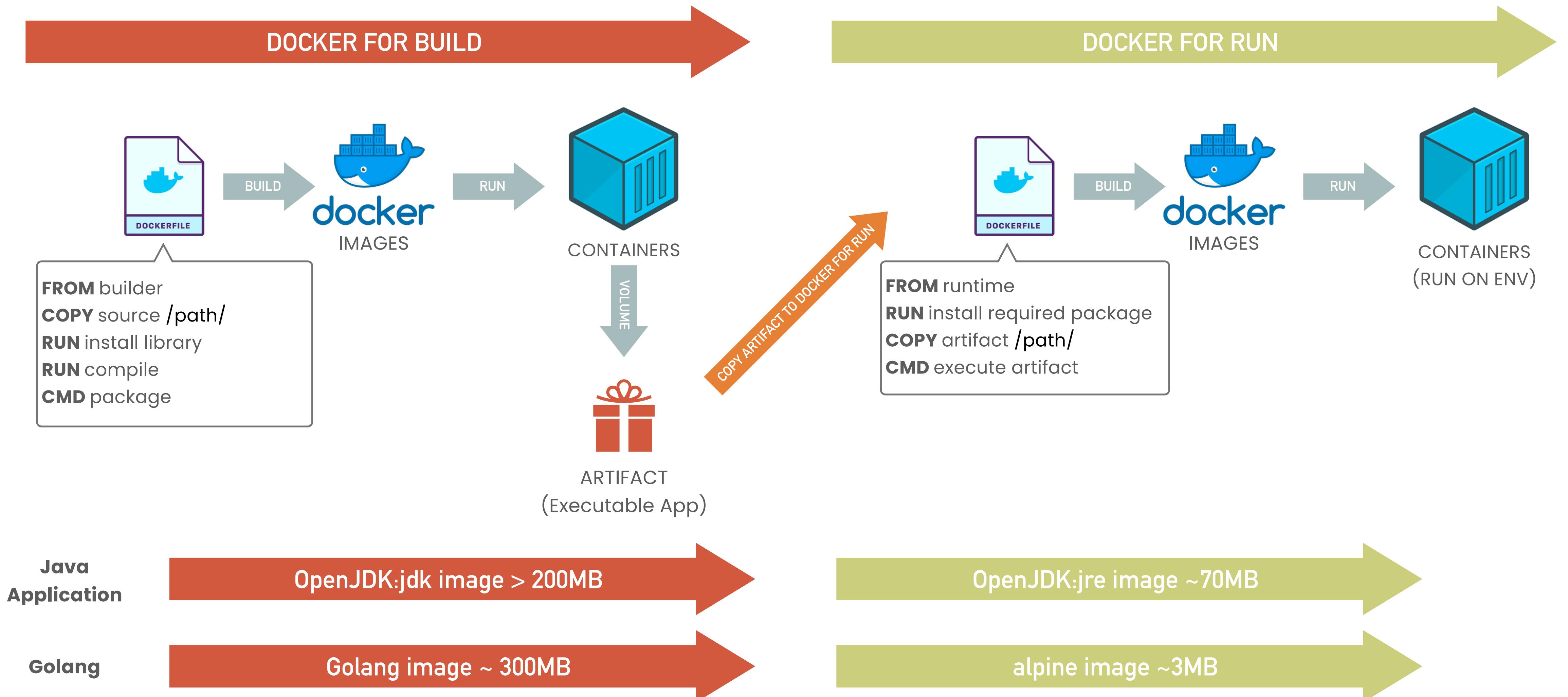
# DOCKER FOR BUILD AND DOCKER FOR RUN



# DOCKER FOR BUILD AND DOCKER FOR RUN



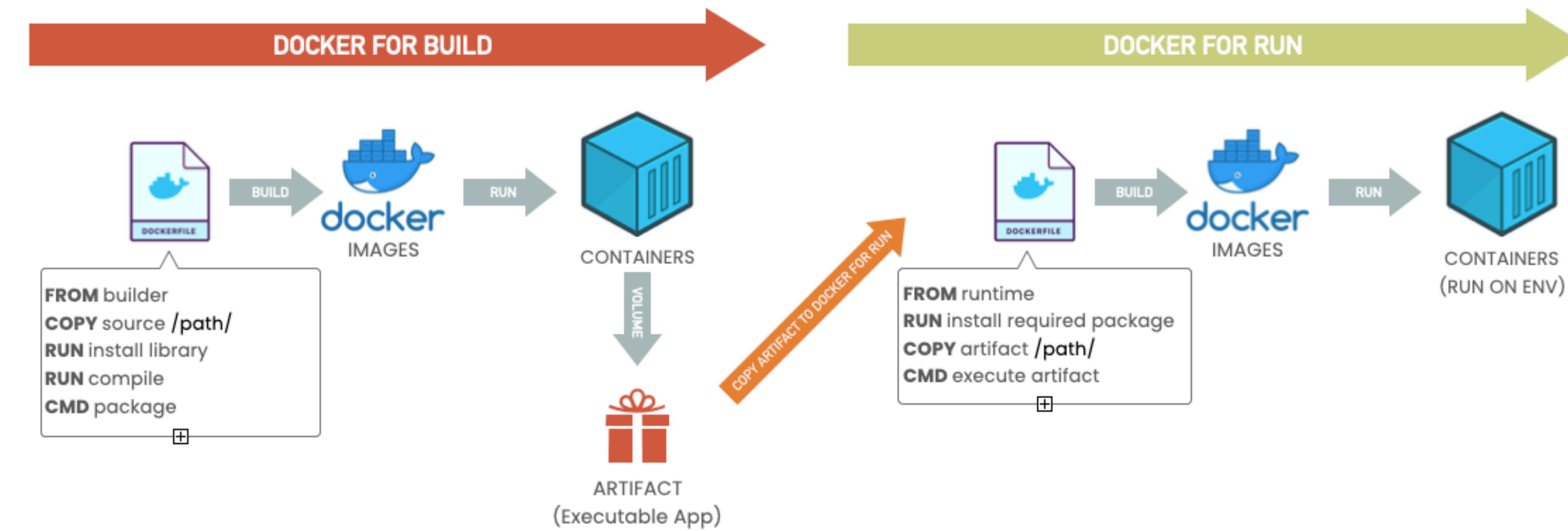
# DOCKER FOR BUILD AND DOCKER FOR RUN



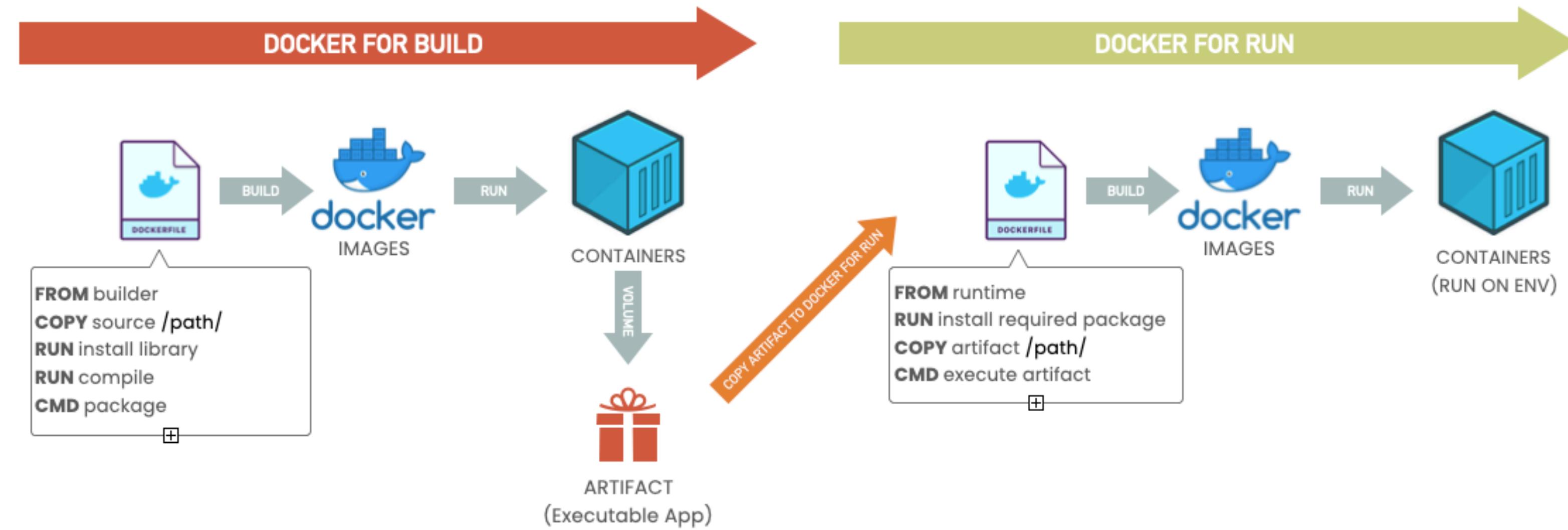
# DOCKER FOR BUILD AND DOCKER FOR RUN

---

# DOCKER FOR BUILD AND DOCKER FOR RUN



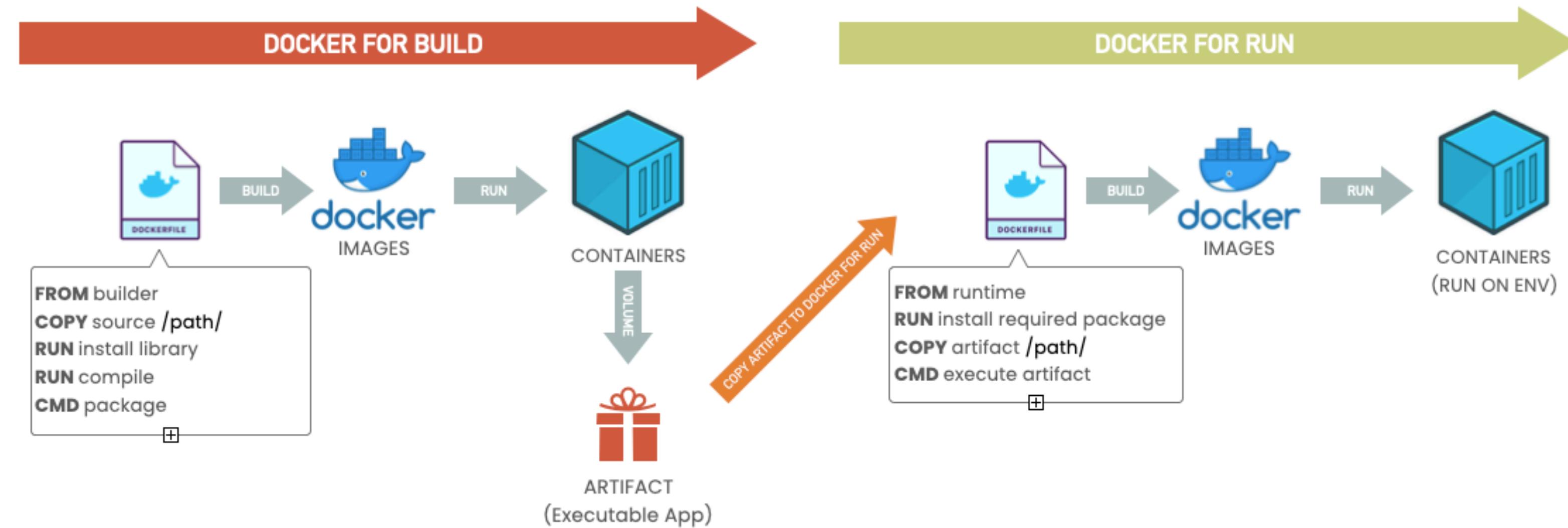
# DOCKER FOR BUILD AND DOCKER FOR RUN



## 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



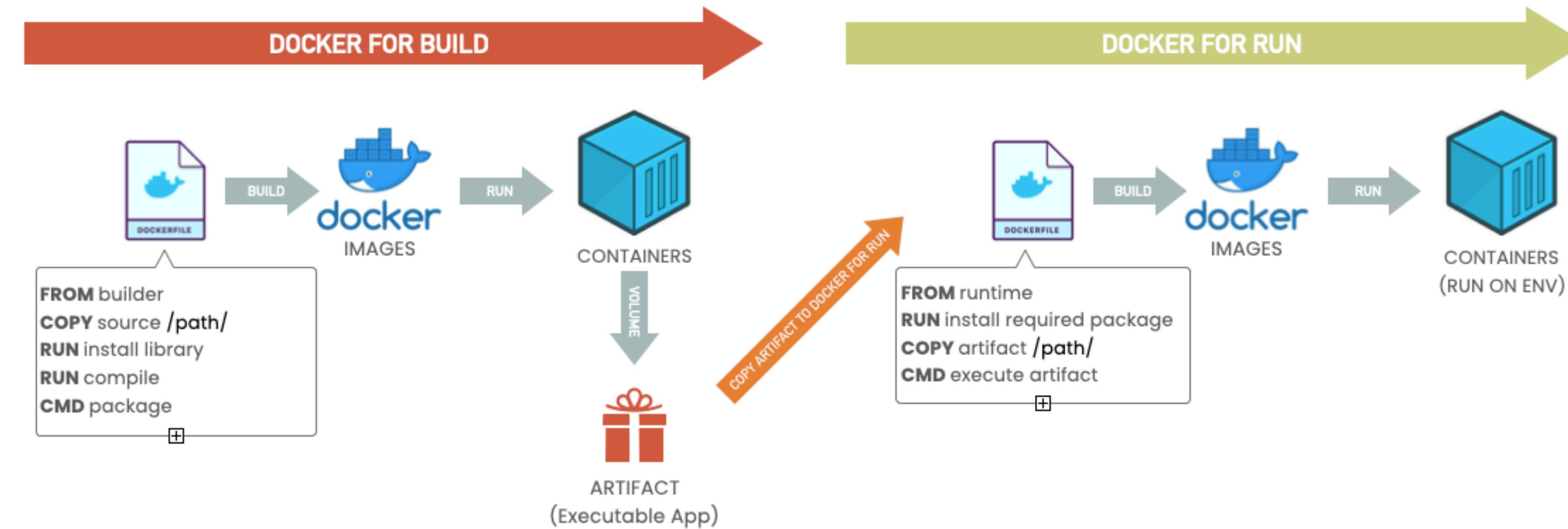
Dockerfile.build

```
# 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

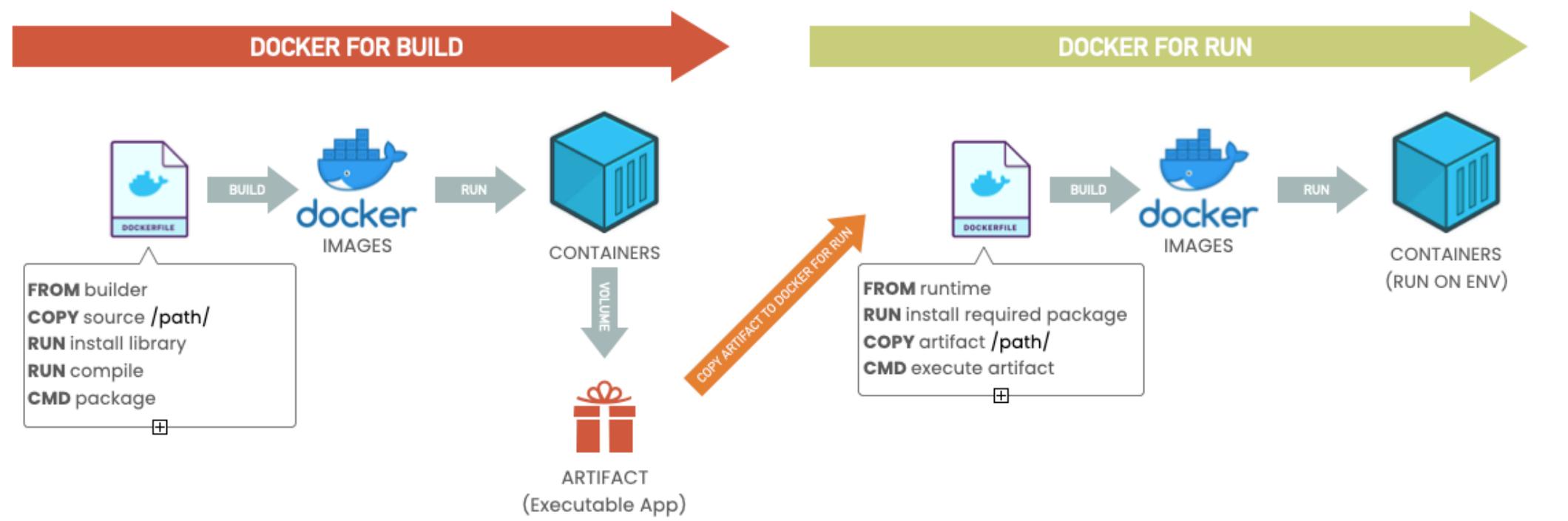
```
# syntax=docker/dockerfile:1
FROM alpine:latest
RUN apk --no-cache add ca-certificates
WORKDIR /root/
COPY app .
CMD ["./app"]
```

# USE MULTI-STAGES BUILD

---

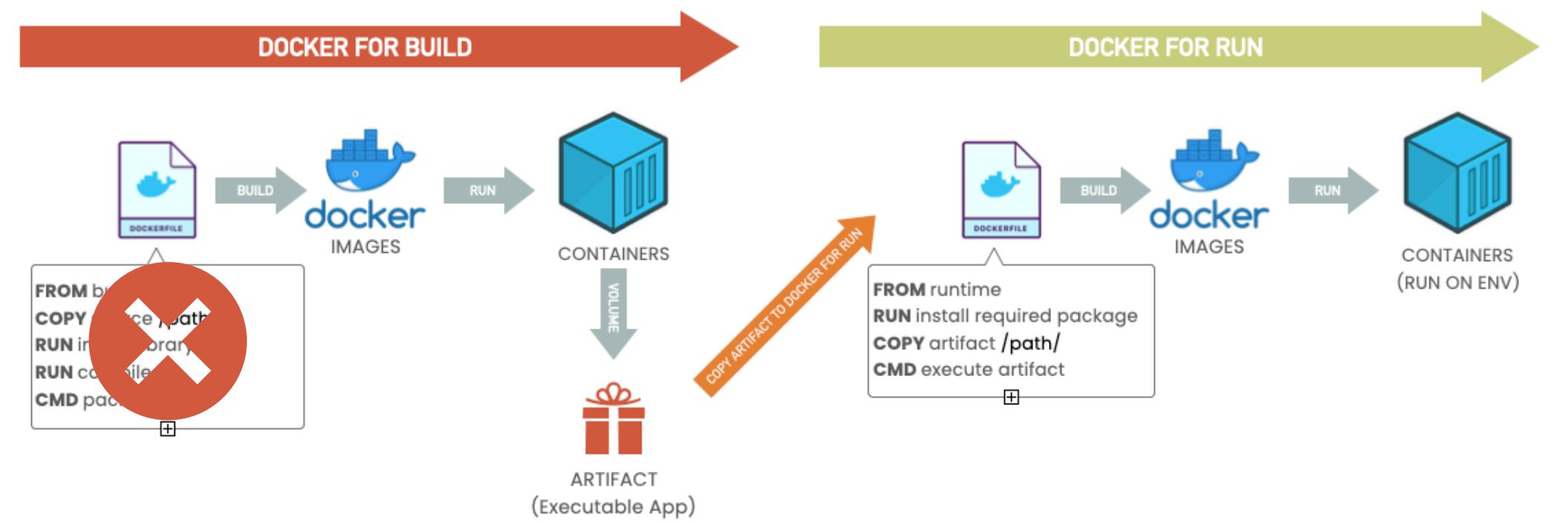
Use multiple **FROM**

# USE MULTI-STAGES BUILD



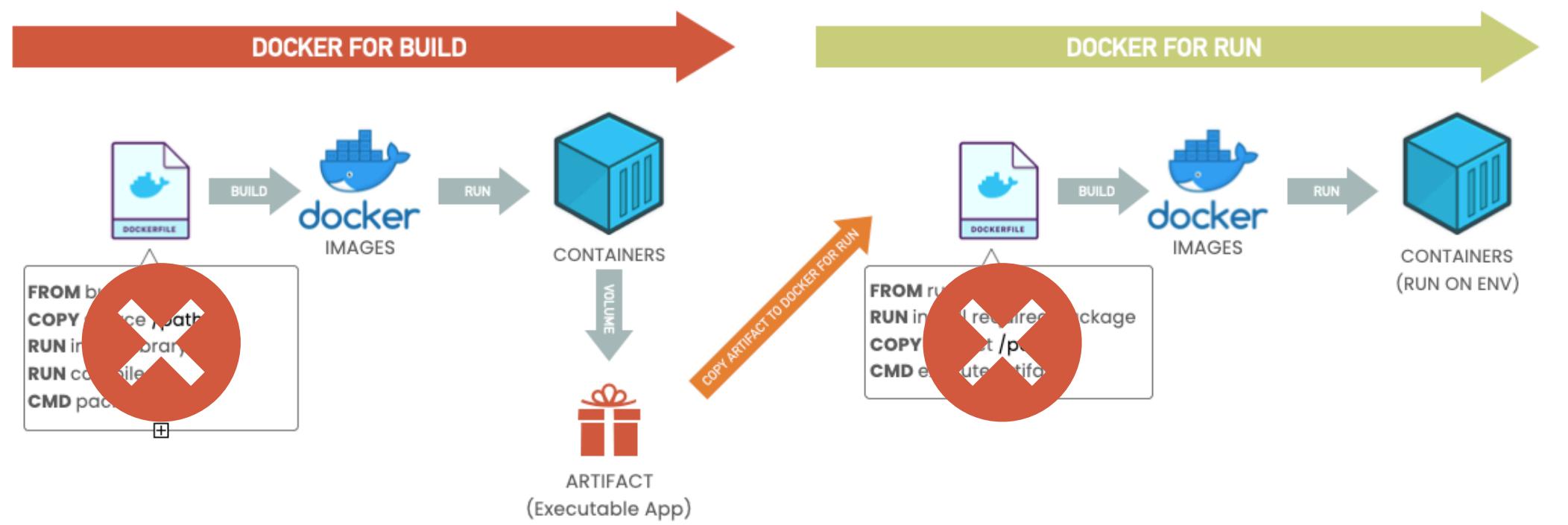
Use multiple **FROM**

# USE MULTI-STAGES BUILD



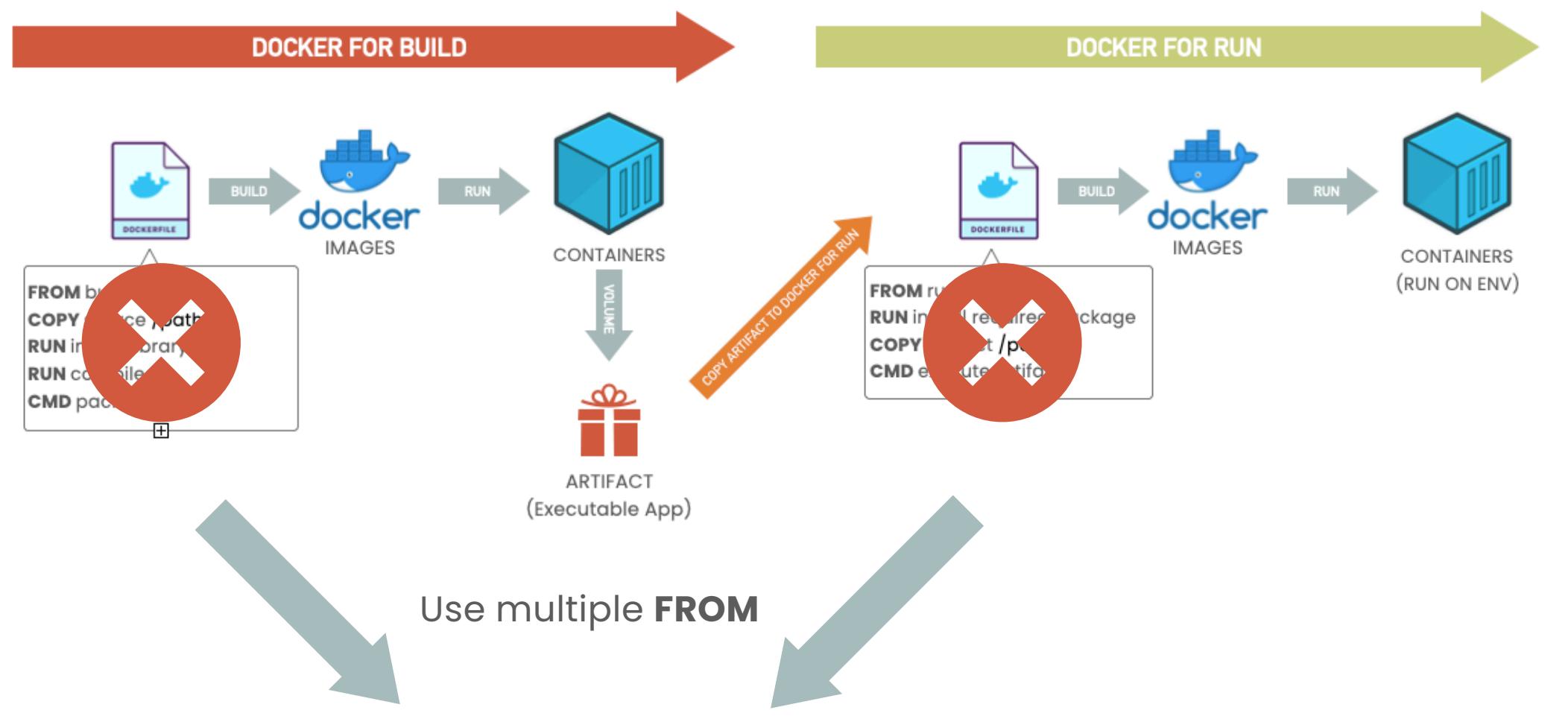
Use multiple **FROM**

# USE MULTI-STAGES BUILD

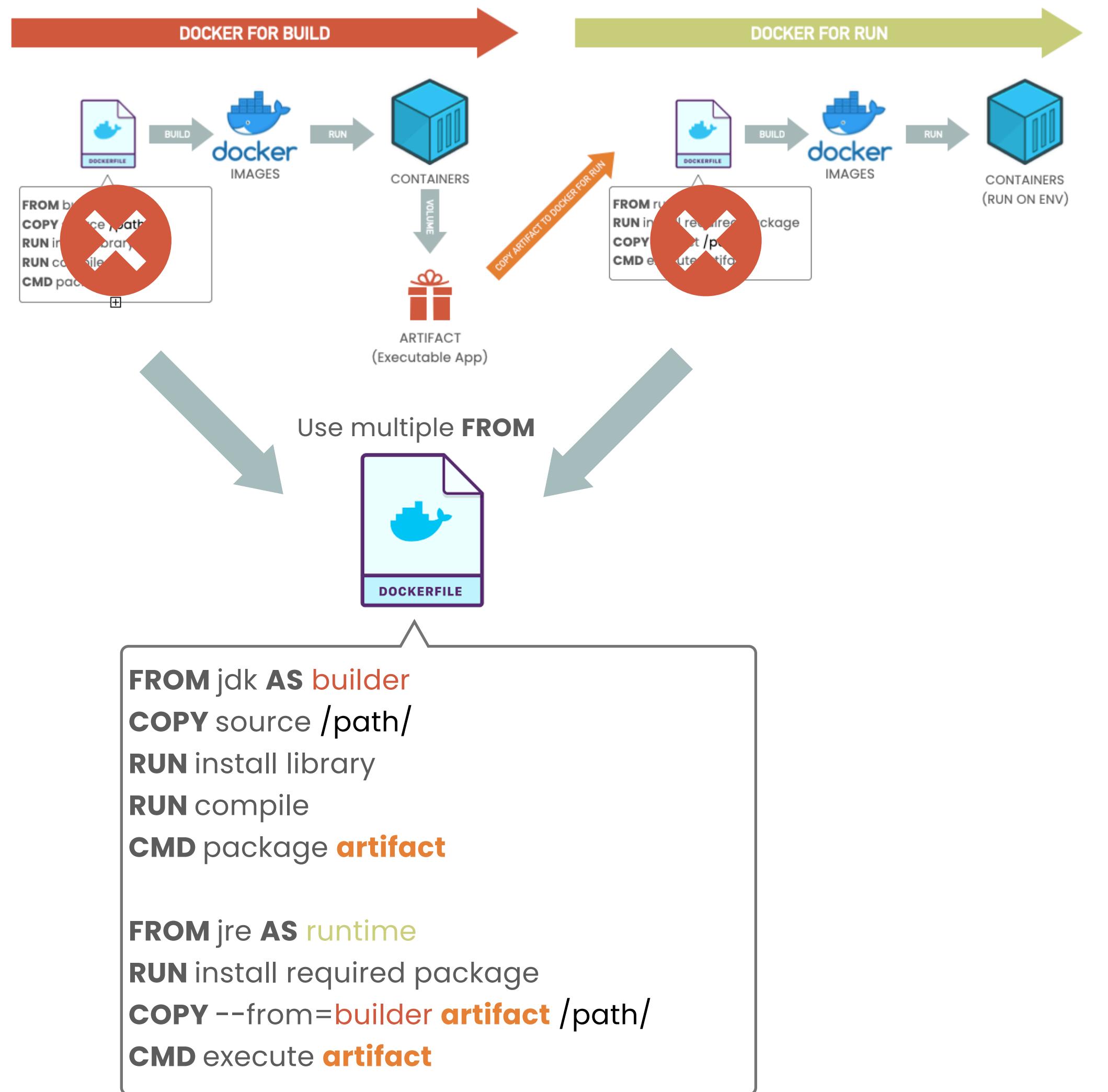


Use multiple **FROM**

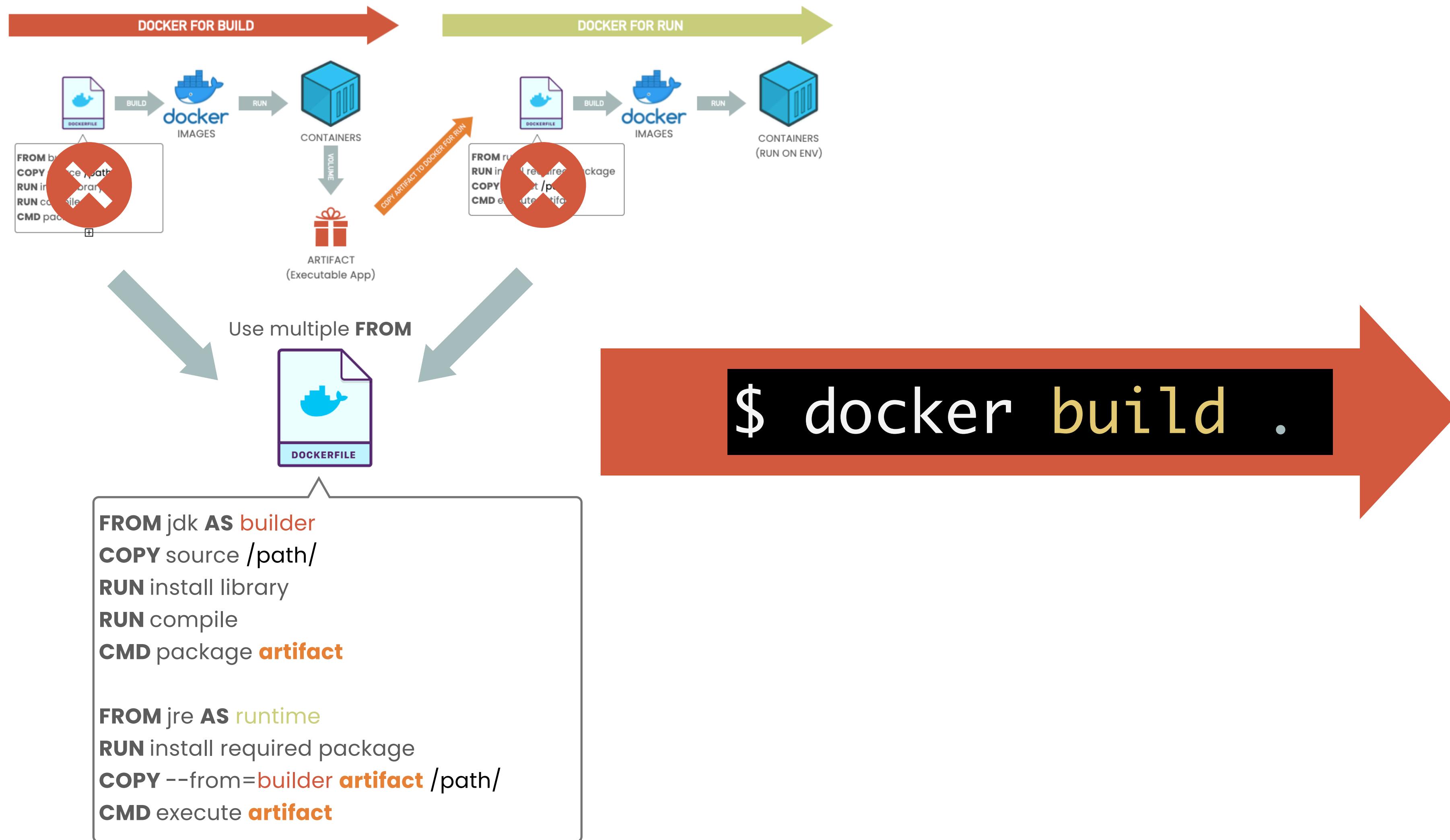
# USE MULTI-STAGES BUILD



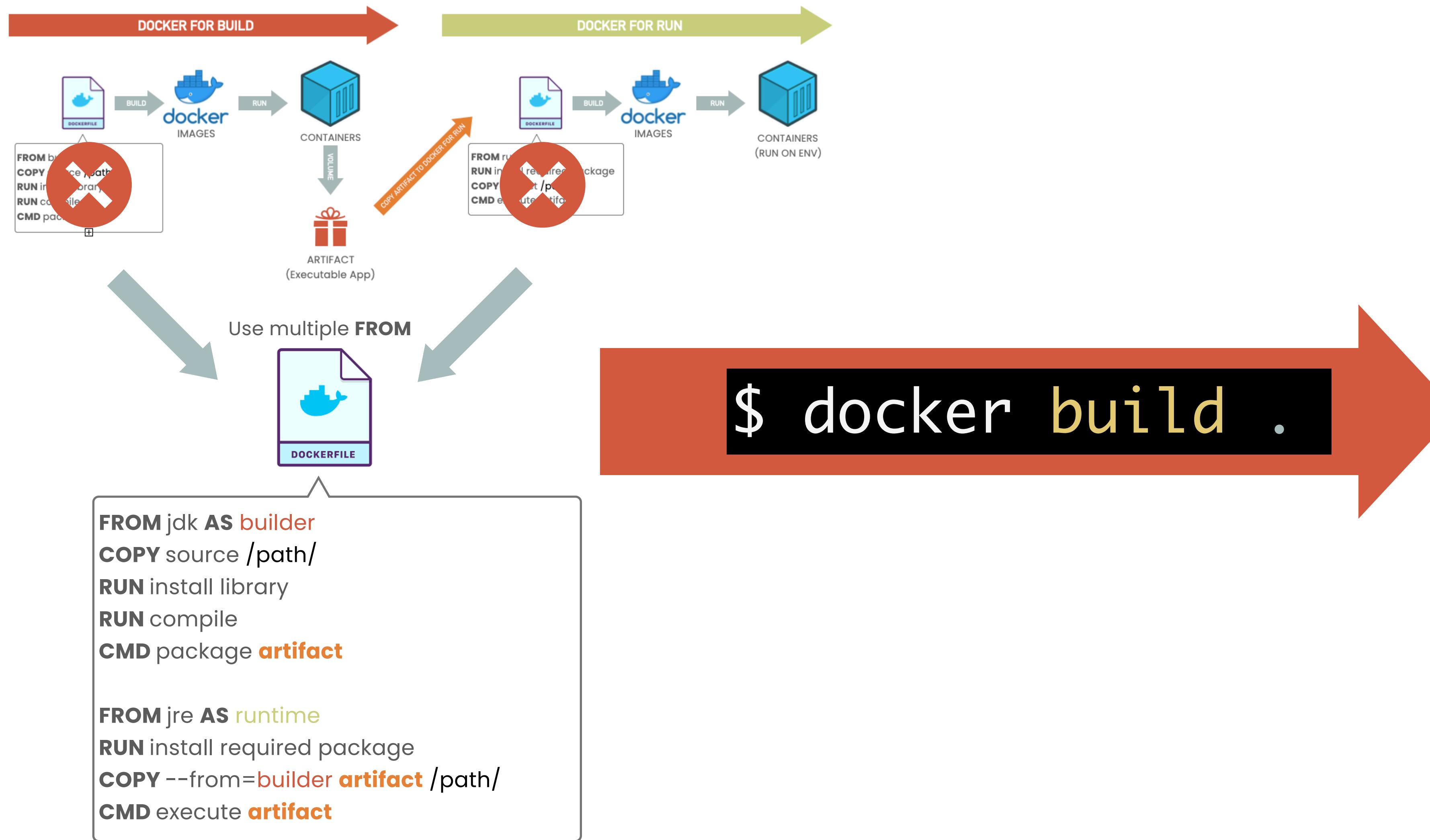
# USE MULTI-STAGES BUILD



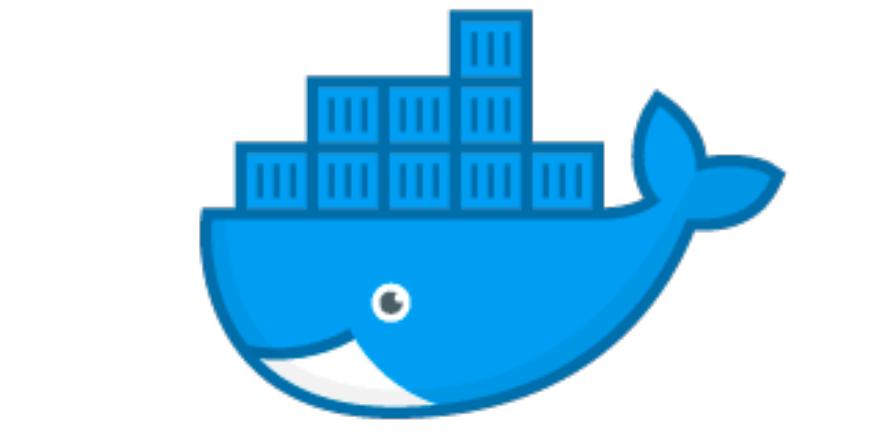
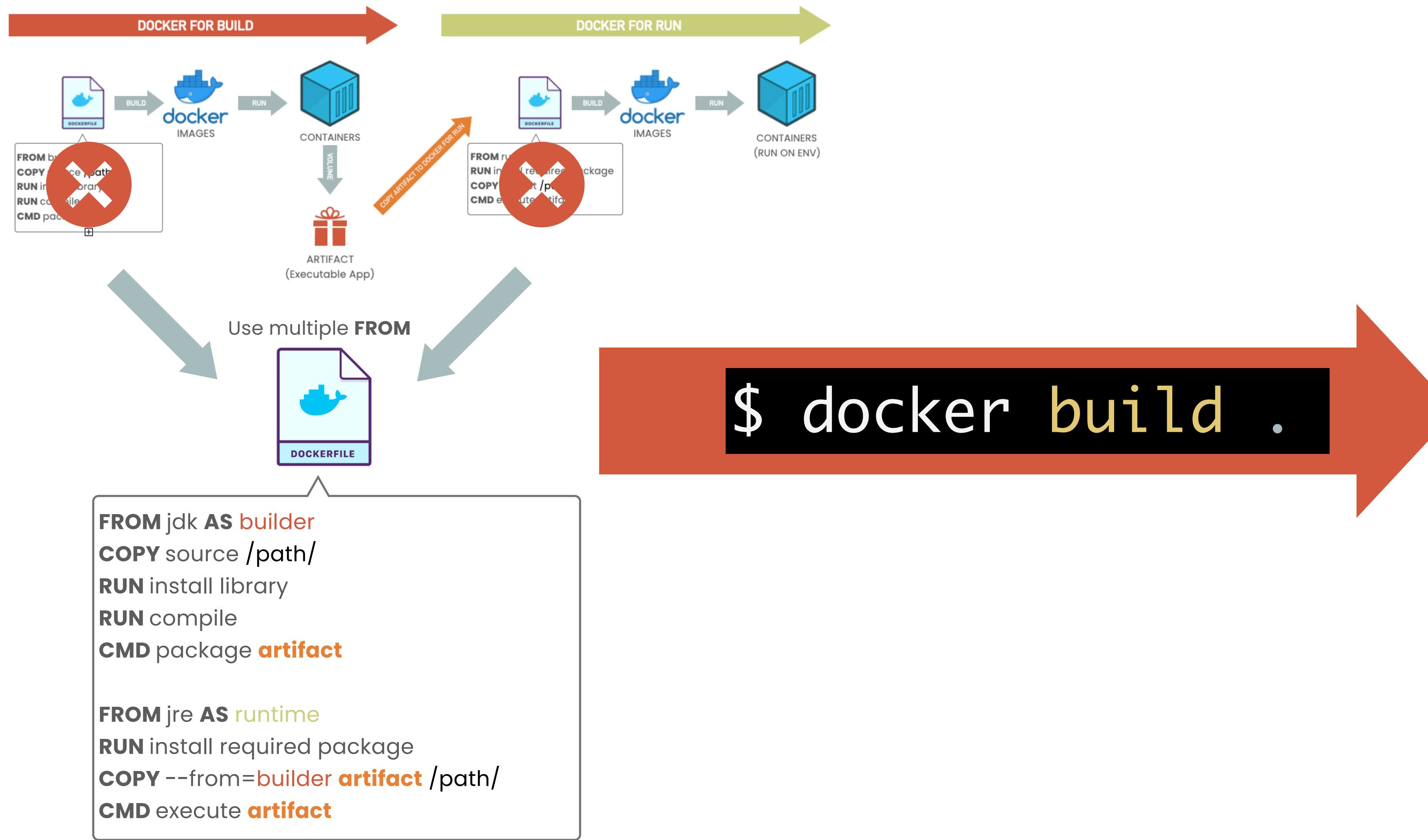
# USE MULTI-STAGES BUILD



# USE MULTI-STAGES BUILD



# USE MULTI-STAGES BUILD



**docker**  
IMAGES

jre image  
~70MB

alpine image  
~3MB

# DOCKER (SECURITY) SCAN

---

# DOCKER IMAGE SCAN COMMAND

---

# DOCKER IMAGE SCAN COMMAND

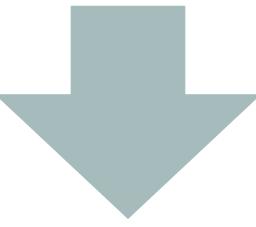
---

```
$ 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...

x 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...

x 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)
```

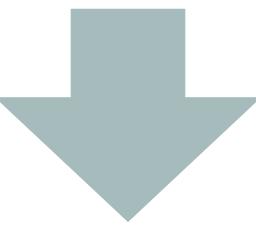
```
y  
Testing ubuntu...  
  
x Low severity vulnerability found in util-linux/libblkid1  
  Description: Integer Overflow or Wraparound  
  Info: https://snyk.io/vuln/SNYK-UBUNTU2004-UTILLINUX-1534917  
  Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, e2fsprogs@1.45.5-2ubuntu1, util-linux/mount@2.34-0.1ubuntu9.1,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

```
x 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...
```

```
x 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:
```

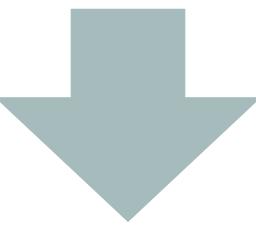
Major upgrades	Vulnerabilities	Severity
ubuntu:impish-20211015	20	0 critical, 0 high, 8 medium, 12 low

```
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...
```

```
x 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...
```

```
x 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

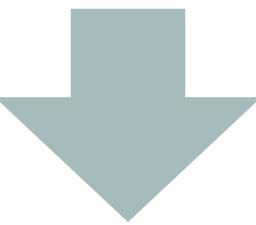
```
Recommendations for base image upgrade:
```

Major upgrades	Vulnerabilities	Severity
Base Image	20	0 critical, 0 high, 8 medium, 12 low
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...
x 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...
x 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

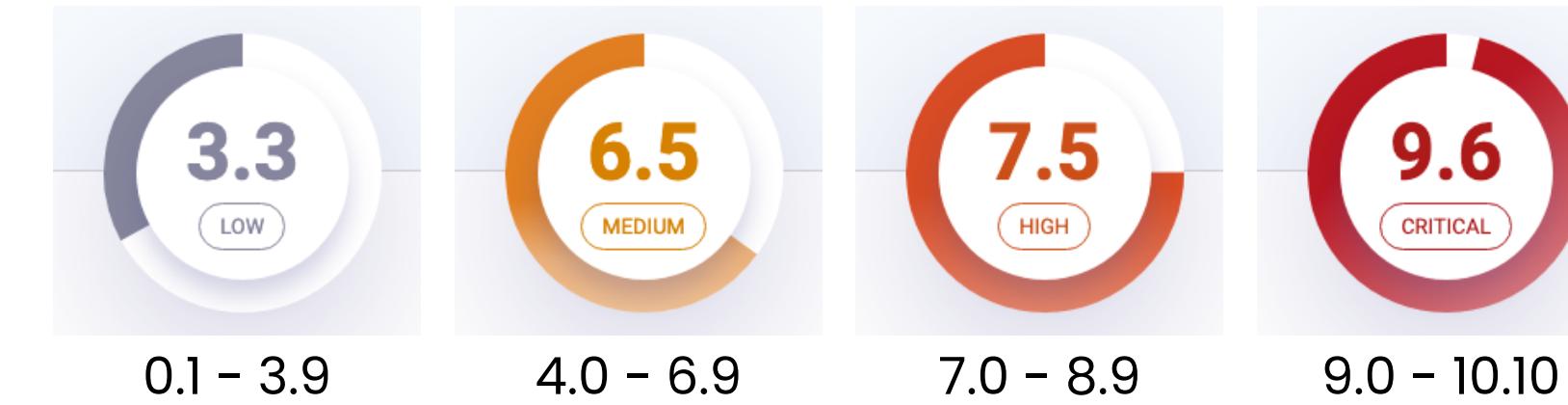
For more free scans that keep your images secure, sign up to Snyk at https://dockr.ly/3ePqVcp
```

# IMAGE VULNERABILITY DB (WITH CVSS V3 RATING)

---

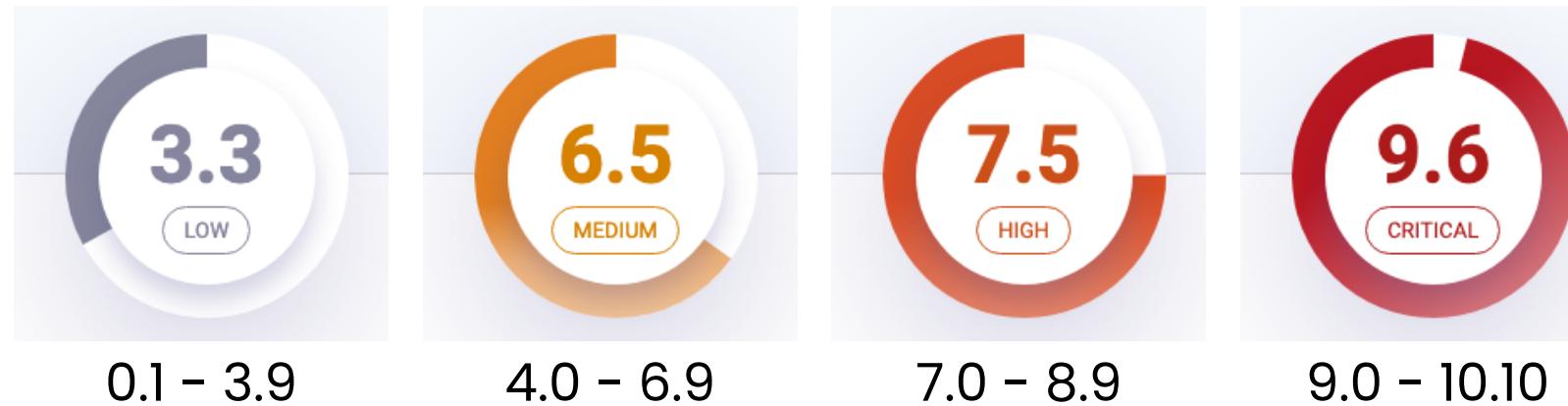
# IMAGE VULNERABILITY DB (WITH CVSS V3 RATING)

---



# IMAGE VULNERABILITY DB (WITH CVSS V3 RATING)

---



- x Low severity vulnerability found in [util-linux/libblkid1](#)

Description: Integer Overflow or Wraparound

Info: <https://snyk.io/vuln/SNYK-UBUNTU2004-UTILINUX-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...

- x Medium severity vulnerability found in [util-linux/libblkid1](#)

Description: CVE-2021-3996

Info: <https://snyk.io/vuln/SNYK-UBUNTU2004-UTILINUX-2387723>

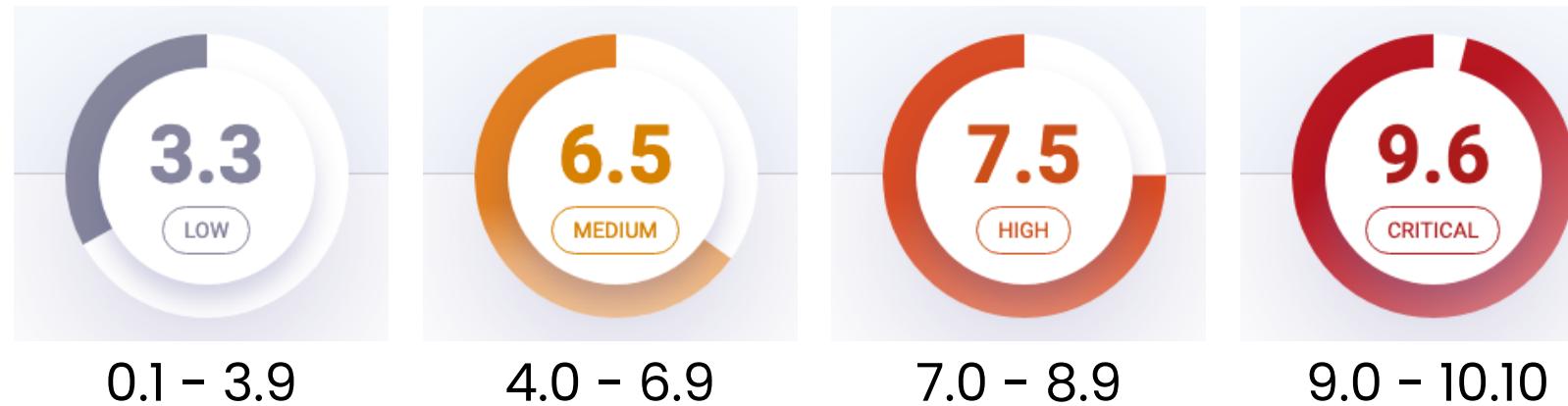
Introduced through: util-linux/libblkid1@2.34-0.1ubuntu9.1, ...

From: util-linux/libblkid1@2.34-0.1ubuntu9.1

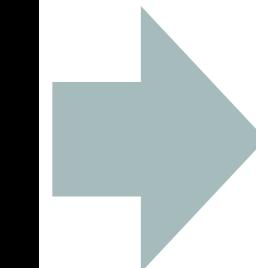
From: e2fsprogs@1.45.5-2ubuntu1 > util-linux/libblkid1@2.34-0.1ubuntu9.1

From: util-linux/mount@2.34-0.1ubuntu9.1 > util-linux/libblkid1@2.34-0.1ubuntu9.1  
and 23 more...

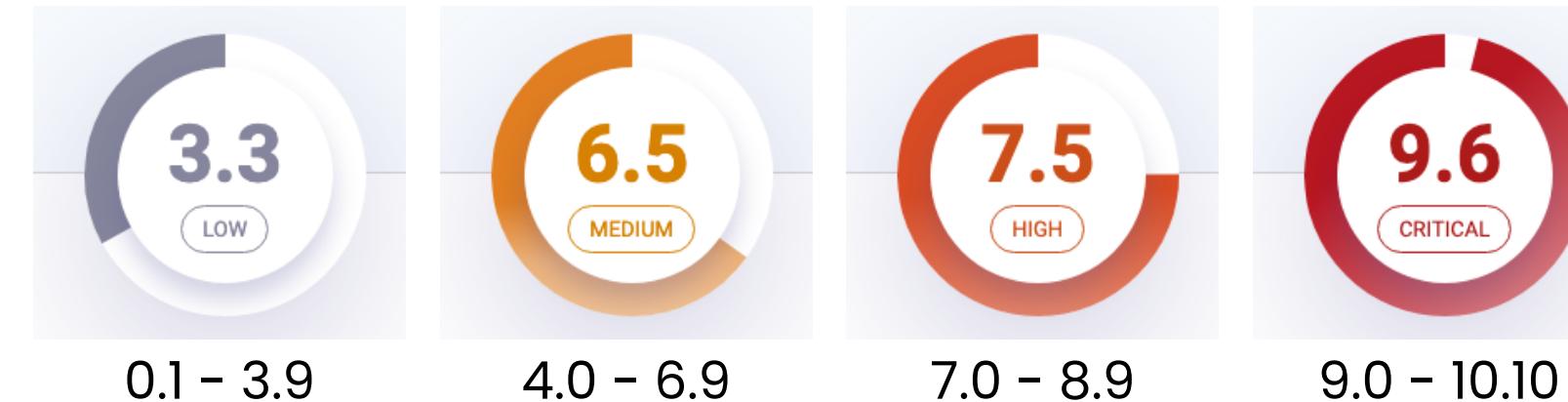
# IMAGE VULNERABILITY DB (WITH CVSS V3 RATING)



- x Low severity vulnerability found in [util-linux/libblkid1](#)  
Description: Integer Overflow or Wraparound  
Info: <https://snyk.io/vuln/SNYK-UBUNTU2004-UTILINUX-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...
- x Medium severity vulnerability found in [util-linux/libblkid1](#)  
Description: CVE-2021-3996  
Info: <https://snyk.io/vuln/SNYK-UBUNTU2004-UTILINUX-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)



- x 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...
- x 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...

**snyk** Vulnerability DB

About Snyk

Snyk Vulnerability Database > Linux > ubuntu:20.04 > util-linux

Search vulnerabilities

## CVE-2021-3996

Affecting [util-linux](#) package, versions \*

INTRODUCED: 29 JAN 2022 NEW CVE-2021-3996

Share

### How to fix?

There is no fixed version for [Ubuntu:20.04 util-linux](#).

[Sign up to Snyk](#) for more details.



NVD CVSS Score is not yet available. When available we recommend using the distro's own rating score.

### NVD Description

Note: Versions mentioned in the description apply to the upstream [util-linux](#) package.  
[Unauthorized umount in util-linux's libmount]

### References

- [ADVISORY](#)

### Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

# 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

---

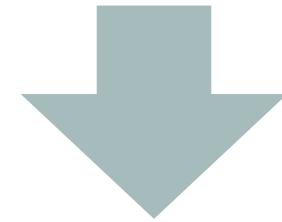
```
$ docker scan --json ubuntu:latest
```



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

Back To Project      Back To Reports

[Back to Project](#)      [Back To Reports](#)

[Status](#)

[Changes](#)

[Console Output](#)

[Edit Build Information](#)

[Delete build '#64'](#)

[Snyk Security Report](#)

[Open Blue Ocean](#)

[Restart from Stage](#)

[Replay](#)

[Pipeline Steps](#)

[Workspaces](#)

[Previous Build](#)

**snyk**

**Snyk test report**

July 1st 2021, 2:36:14 pm

Scanned the following path:

- /home/jenkins/work/workspace/my\_pipeline (npm)

1 known vulnerabilities | 1 vulnerable dependency paths | 1 dependencies

**Project** testproj1  
**Path** /home/jenkins/work/workspace/my\_pipeline  
**Package Manager** npm  
**Manifest** package-lock.json

**CRITICAL SEVERITY**

**Prototype Pollution**

• Package Manager: npm  
• Vulnerable module: lodash

[Back To Reports](#)

# MORE FOR IMAGE SCAN (--HELP)

---

## MORE FOR IMAGE SCAN (--HELP)

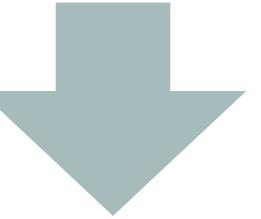
---

```
$ 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](https://hub.docker.com))**

---

# DOCKER REGISTRY ([HUB.DOCKER.COM](https://hub.docker.com))

---



**Docker Registry**

# DOCKER REGISTRY ([HUB.DOCKER.COM](https://hub.docker.com))



Docker Registry

The screenshot shows the Docker Hub sign-up page. At the top, there's a navigation bar with the Docker Hub logo, a search bar, and links for Explore, Pricing, Sign In, and Sign Up. The main heading is "Build and Ship any Application Anywhere". Below it, a sub-headline reads: "Docker Hub is the world's easiest way to create, manage, and deliver your teams' container applications." To the right, a "Get Started Today for Free" section contains fields for Docker ID, Email, and Password, along with checkboxes for receiving updates and agreeing to terms. A reCAPTCHA box is also present. A prominent blue "Sign Up" button is at the bottom.

# DOCKER REGISTRY ([HUB.DOCKER.COM](https://hub.docker.com))



Docker Registry

The screenshot shows the Docker Hub sign-up interface. At the top, there's a navigation bar with the Docker Hub logo, a search bar, and links for 'Explore', 'Pricing', 'Sign In', and a prominent 'Sign Up' button. The main area features a large blue background graphic with a white frog and shipping containers. Text on the page reads: 'Build and Ship any Application Anywhere' and 'Docker Hub is the world's easiest way to create, manage, and deliver your teams' container applications.' A 'Get Started Today for Free' section includes fields for 'Docker ID', 'Email', and 'Password', along with checkboxes for accepting terms and conditions and a reCAPTCHA field. A final 'Sign Up' button is at the bottom.



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

# DOCKER REGISTRY ([HUB.DOCKER.COM](https://hub.docker.com))



Docker Registry

The screenshot shows the Docker Hub sign-up interface. At the top, there's a navigation bar with 'docker hub' (with a logo), a search bar ('Search for great content'), and links for 'Explore', 'Pricing', 'Sign In', and 'Sign Up'. The main heading is 'Build and Ship any Application Anywhere'. Below it, a sub-headline reads: 'Docker Hub is the world's easiest way to create, manage, and deliver your teams' container applications.' A large orange 'Get Started Today for Free' button is prominent. To its left is a 'Sign In' link. The sign-up form consists of three input fields: 'Docker ID', 'Email', and 'Password'. Below these are two checkboxes: 'Send me occasional product updates and announcements.' and 'I agree to the [Subscription Service Agreement](#), [Privacy Policy](#), and [Data Processing Terms](#)'. There's also a reCAPTCHA field with text in Thai: 'ฉันไม่ใช่หุ่นยนต์' and 'reCAPTCHA'. At the bottom is a large blue 'Sign Up' button.



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



Amazon ECR



Azure  
Container  
Registry



Google Container Registry

# DOCKER REGISTRY ([HUB.DOCKER.COM](https://hub.docker.com))



Docker Registry

The screenshot shows the Docker Hub sign-up interface. At the top, there's a navigation bar with 'docker hub' (with a logo), a search bar ('Search for great content'), and links for 'Explore', 'Pricing', 'Sign In', and 'Sign Up'. The main heading is 'Build and Ship any Application Anywhere'. Below it, a sub-headline reads: 'Docker Hub is the world's easiest way to create, manage, and deliver your teams' container applications.' A large orange 'Get Started Today for Free' button is prominent. To its left is a smaller 'Sign In' button. The sign-up form includes fields for 'Docker ID', 'Email', and 'Password', each with a placeholder and a password strength indicator icon. There are also two checkboxes: one for receiving product updates and another for agreeing to the 'Subscription Service Agreement', 'Privacy Policy', and 'Data Processing Terms'. A reCAPTCHA checkbox is present, followed by a 'Sign Up' button.



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



Amazon ECR



Azure  
Container  
Registry



Google Container Registry



[goharbor.io](https://goharbor.io)



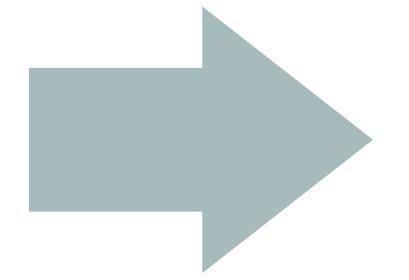
JFrog Artifactory

SIGN UP ON [HUB.DOCKER.COM](https://hub.docker.com)

---

# SIGN UP ON HUB.DOCKER.COM

The Docker Hub sign-up page features a blue header with the Docker logo and navigation links for Explore, Pricing, Sign In, and Sign Up. The main content area has a large blue banner with the text "Build and Ship any Application Anywhere" and a subtext: "Docker Hub is the world's easiest way to create, manage, and deliver your teams' container applications." Below the banner is a "Get Started Today for Free" section with fields for Docker ID, Email, and Password, along with checkboxes for receiving updates and agreeing to terms. A reCAPTCHA field is at the bottom, followed by a blue "Sign Up" button.

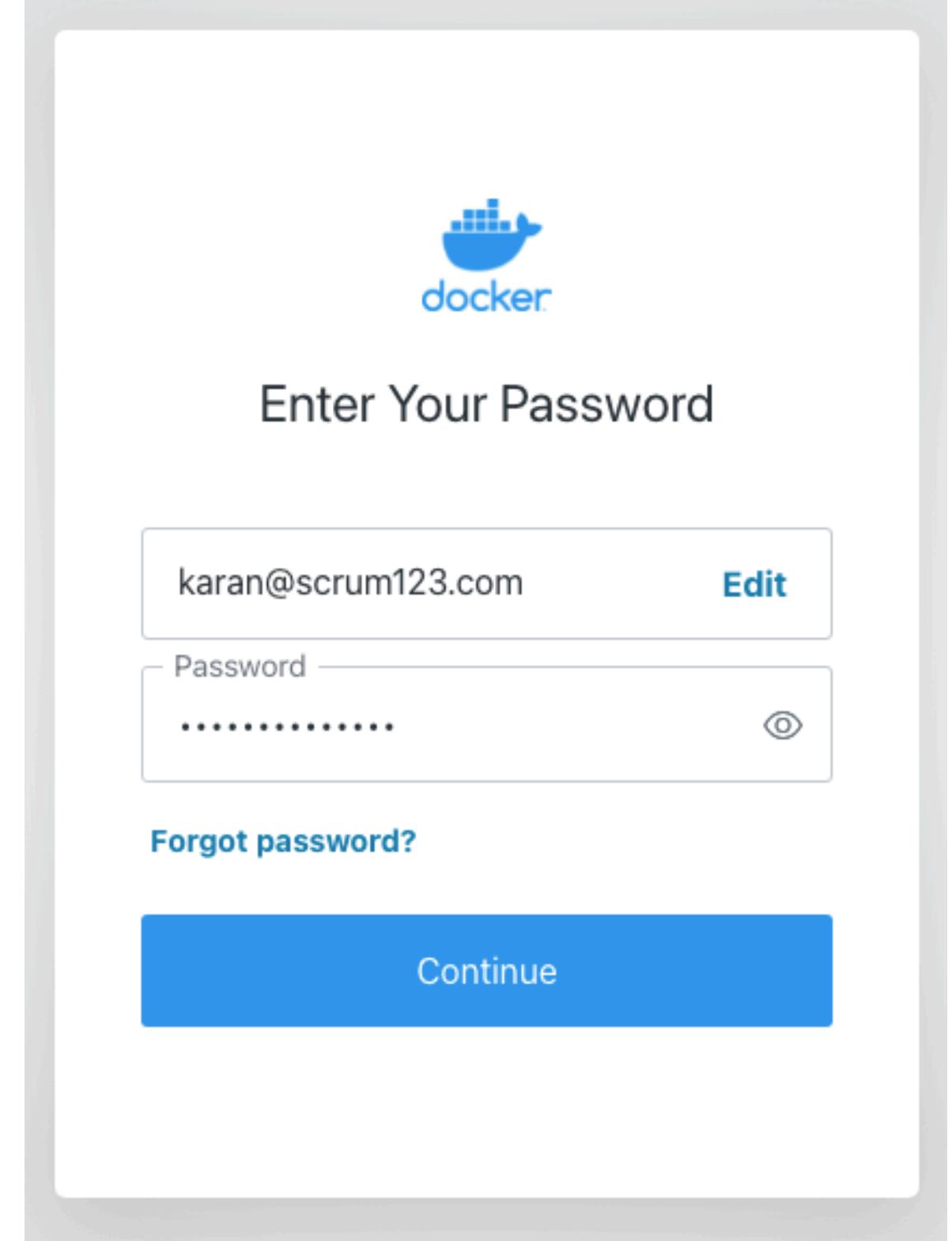
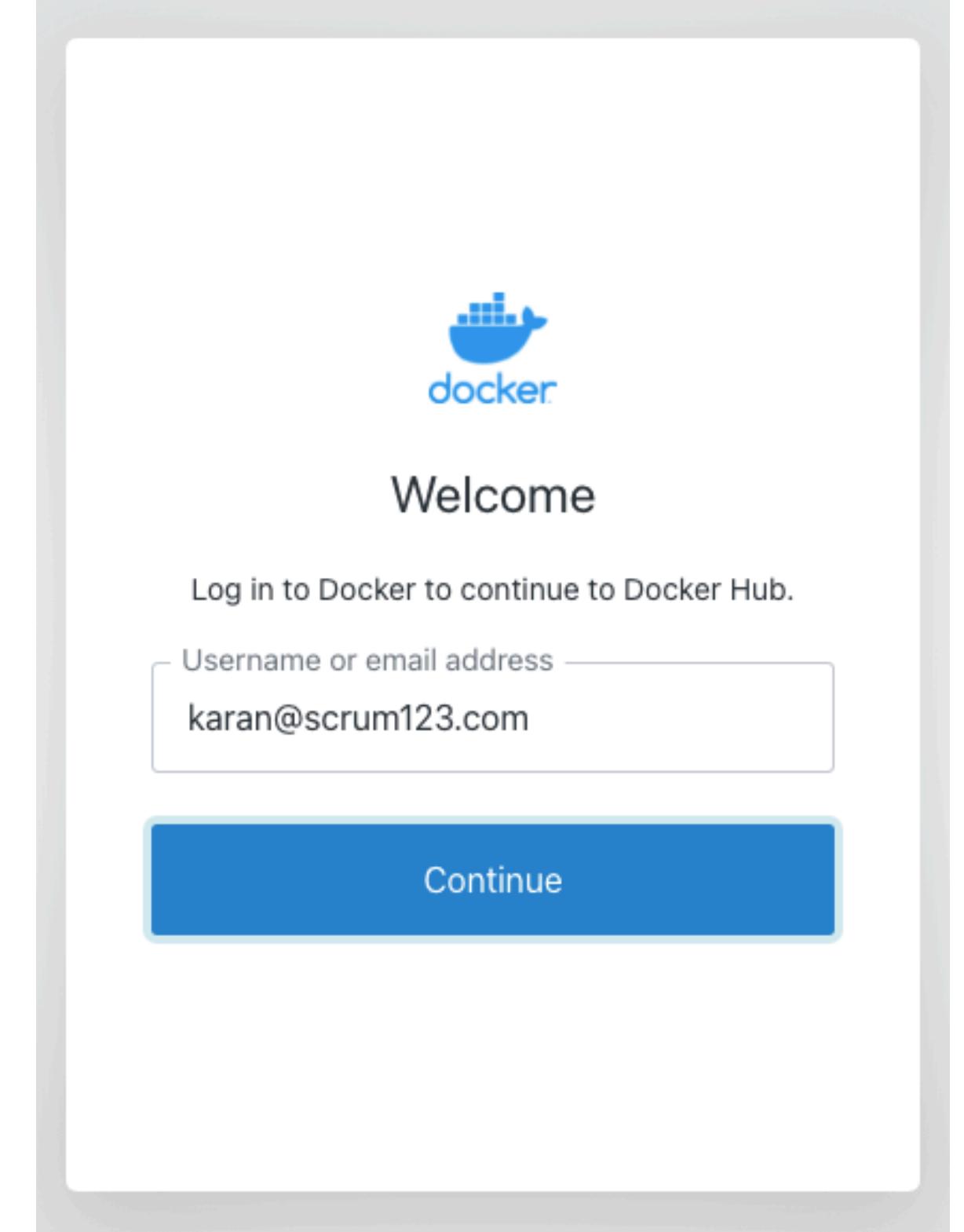
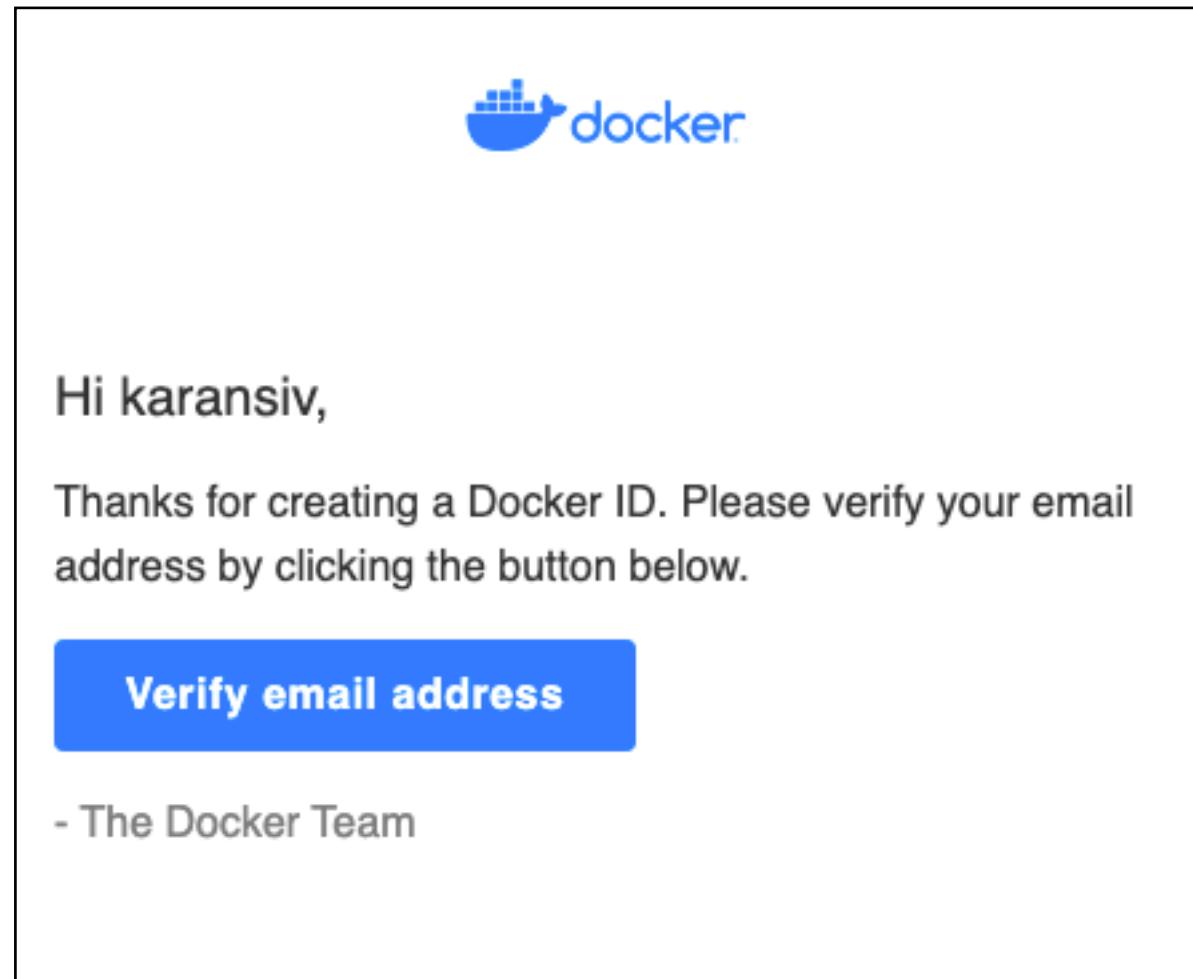


The confirmation page for creating a Docker ID. It shows the Docker logo at the top. The main section is titled "Create a Docker ID." and includes a "Sign In" link. It displays the entered information: "karansiv" for Docker ID, "karan@scrum123.com" for Email, and a masked password. Below this are checkboxes for receiving updates and agreeing to terms. The "I agree to the terms" checkbox is checked. A reCAPTCHA field is present at the bottom, followed by a blue "Sign Up" button.

**SIGN UP ON HUB.DOCKER.COM**

---

# SIGN UP ON HUB.DOCKER.COM



SIGN UP ON [HUB.DOCKER.COM](https://hub.docker.com)

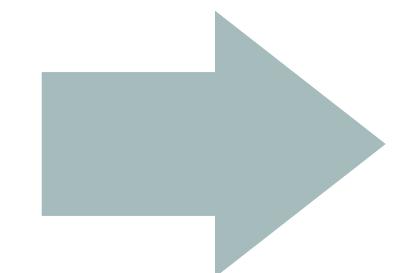
---

# SIGN UP ON HUB.DOCKER.COM

The screenshot shows the Docker Hub 'Choose a Plan' page. At the top, it says 'Choose a Plan' and 'Select a plan to get started with Docker'. Below are three plan options:

- Personal** (\$0): Includes Docker essentials and is ideal for individual developers, education, open source communities, and small businesses.
- Pro** (\$5/month): Extends Docker capabilities and includes pro tools for individual developers who want to accelerate their productivity.
- Team** (\$7/month minimum 5 seats): Ideal for teams and includes capabilities for enhanced collaboration, productivity and security. It lists additional features: Docker Desktop, Unlimited private repositories, Docker Engine + Kubernetes, 5,000 image pulls per day, 5 concurrent builds, Unlimited image scans, Unlimited scoped tokens, Role-based access control, and Audit log.

Buttons at the bottom include 'Continue with Free' for Personal and 'Buy Now' for Pro and Team.



The screenshot shows the Docker Hub 'Download the desktop application' page. At the top, it says 'Welcome to Docker' and 'Download the desktop application'. It offers 'Mac with Intel chip' and 'Mac with Apple chip' options, with a note that it's 'MOST COMMON'. It also mentions 'Also available for Windows and Linux'. Below are three guides: 'Create a Repository', 'Docker Hub Basics', and 'Language-Specific Guides'. A large grey arrow points down to the 'Access the world's largest library of container images' section.

Access the world's largest library of container images

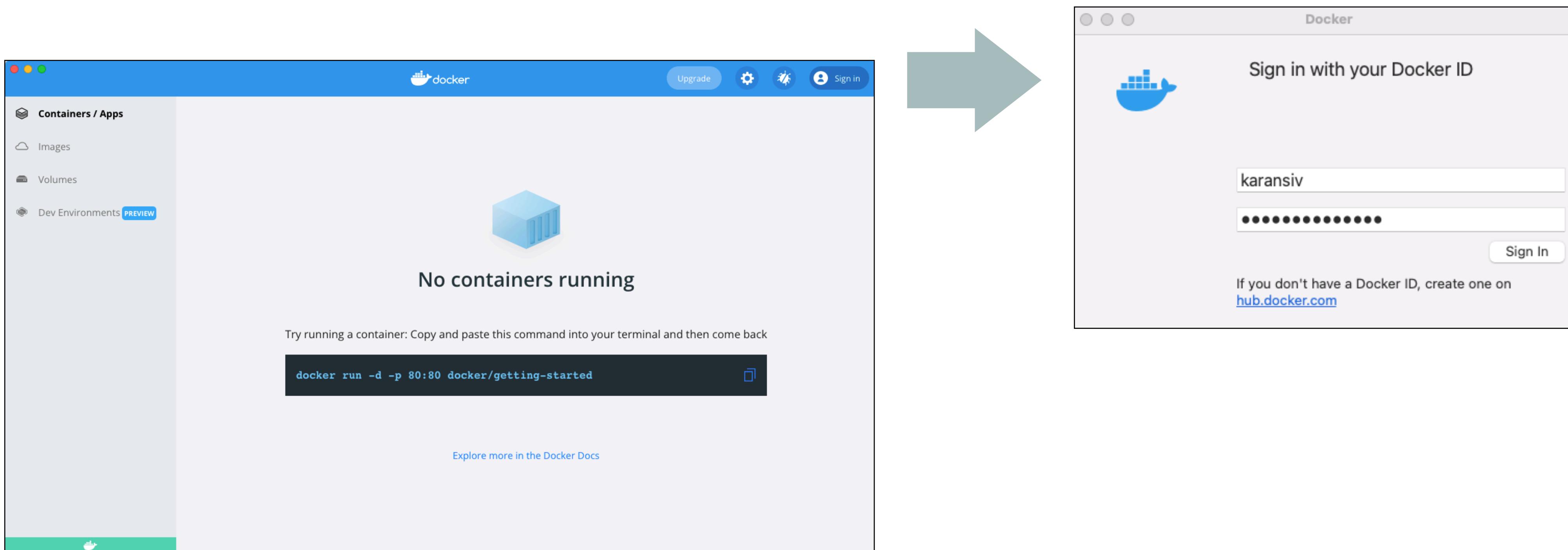
Official Images



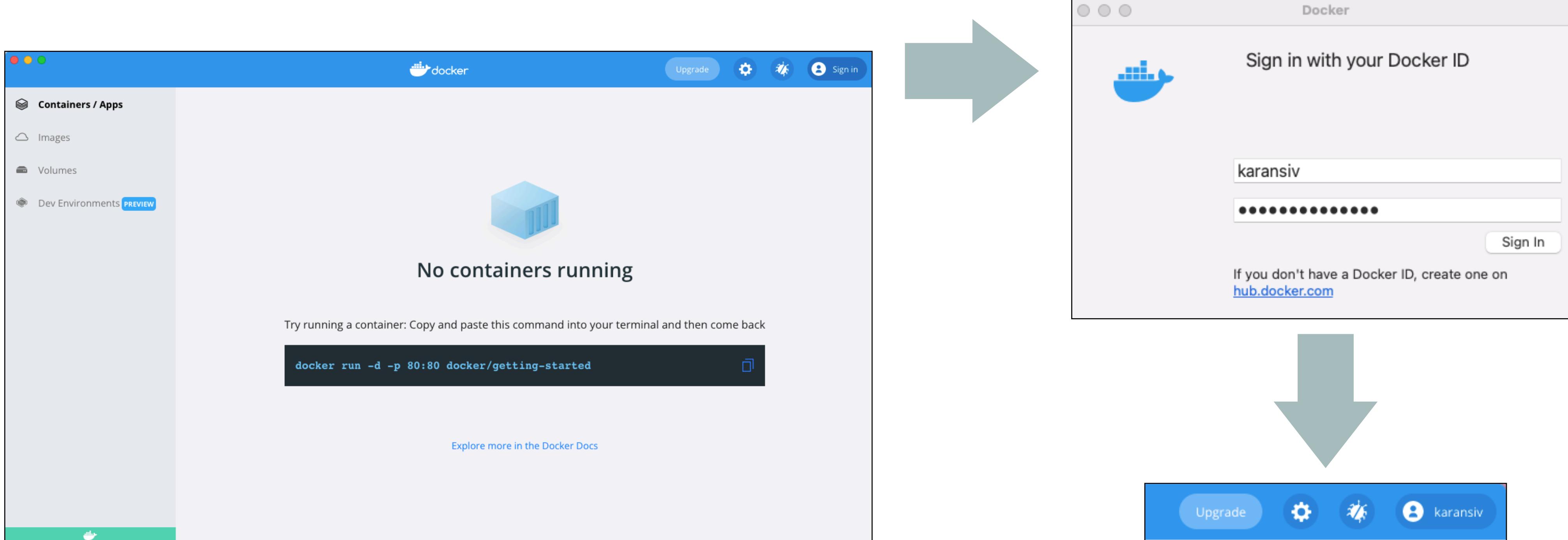
# SIGN IN DOCKER DESTOP

---

# 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
```

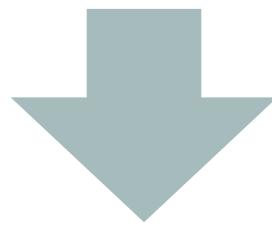
# DOCKER PUSH COMMAND

---

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

*Example :*

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



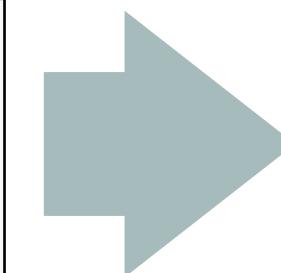
```
The push refers to repository [docker.io/karansiv/application]
57cf4935a684: Pushed
b79069e91828: Pushed
0eba131dff0: Mounted from library/ubuntu
0.0.1: digest:
sha256:2e64722cdb0275c0068d7786755b7a0e179410796bf2484a890c3f879aefb6b7 size: 952
```

**DOCKER REMOTE REPOSITORY ([HUB.DOCKER.COM](https://hub.docker.com))**

---

# DOCKER REMOTE REPOSITORY ([HUB.DOCKER.COM](https://hub.docker.com))

The screenshot shows the Docker Hub search interface. At the top, there's a search bar with the placeholder "Search for great content". Below it, a navigation bar includes "Explore", "Repositories", "Organizations", "Help", and a yellow "Upgrade" button. A dropdown menu shows the user "karansiv". A search bar below the main one has the text "Search by repository name". A blue "Create Repository" button is visible. In the main area, a repository card for "karansiv / application" is shown, which was updated 7 minutes ago. It has a status of "Not Scanned", 0 stars, 5 downloads, and is marked as "Public".

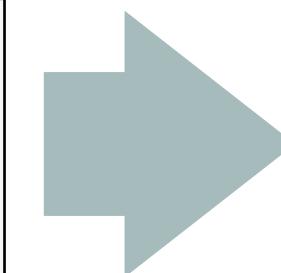


The screenshot shows the Docker Hub repository details page for "karansiv / application". The top navigation bar includes "Explore", "Repositories", "Organizations", "Help", and an "Upgrade" button. The user "karansiv" is logged in. The repository "application" is selected. The page displays the "General" tab. An "Advanced Image Management" section is present, with a note about viewing images and tags, available with Pro, Team, and Business subscriptions. The repository card for "karansiv / application" shows it does not have a description, was last pushed 5 minutes ago, and has 1 tag. The "Docker commands" section contains the command "docker push karansiv/application:tagname". The "Tags and Scans" section lists 1 tag: "0.0.1" (PULLED 5 minutes ago, PUSHED 5 minutes ago). The "VULNERABILITY SCANNING - DISABLED" status is shown with an "Enable" link. The "Automated Builds" section explains how to connect GitHub or Bitbucket for automated builds. The "Readme" section indicates the repository description is empty.

# DOCKER REMOTE REPOSITORY ([HUB.DOCKER.COM](https://hub.docker.com))

The screenshot shows the Docker Hub homepage. At the top, there is a search bar labeled "Search for great content". Below it, a navigation bar includes "Explore", "Repositories", "Organizations", "Help", and a yellow "Upgrade" button. A dropdown menu for the user "karansiv" is open, showing "karansiv" and a "Create Repository" button. Below the navigation, a list of repositories is shown, with "karansiv / application" being the active one. This repository has 0 stars, 5 downloads, and is public. It was last updated 7 minutes ago and has not been scanned.

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.



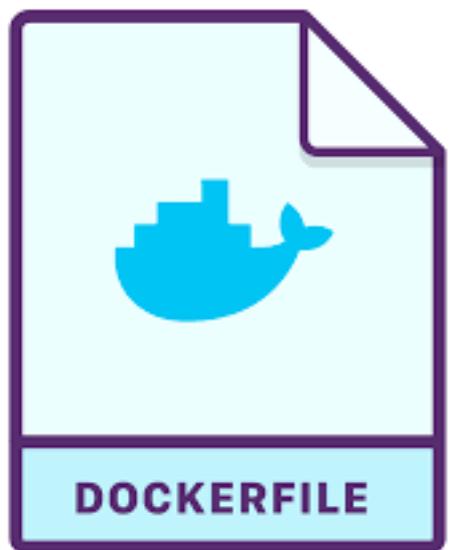
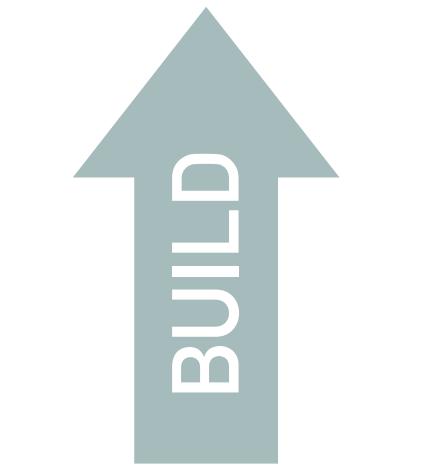
The screenshot shows the detailed view of the "karansiv / application" repository. The top navigation bar includes "Explore", "Repositories", "Organizations", "Help", and an "Upgrade" button. The user "karansiv" is logged in, indicated by the profile icon and name in the top right. The repository "application" is selected in the breadcrumb navigation. The main content area starts with an "Advanced Image Management" section, which is currently unavailable. Below this, the repository name "karansiv / application" is displayed, along with a "Docker commands" section containing the command "docker push karansiv/application:tagname". The repository has no description and was last pushed 5 minutes ago. The "Tags and Scans" section shows 1 tag (0.0.1) and vulnerability scanning disabled. The "Automated Builds" section explains how to automatically build images. The "Readme" section indicates the repository description is empty.

# DEVELOPMENT WORKFLOW WITH DOCKER

---

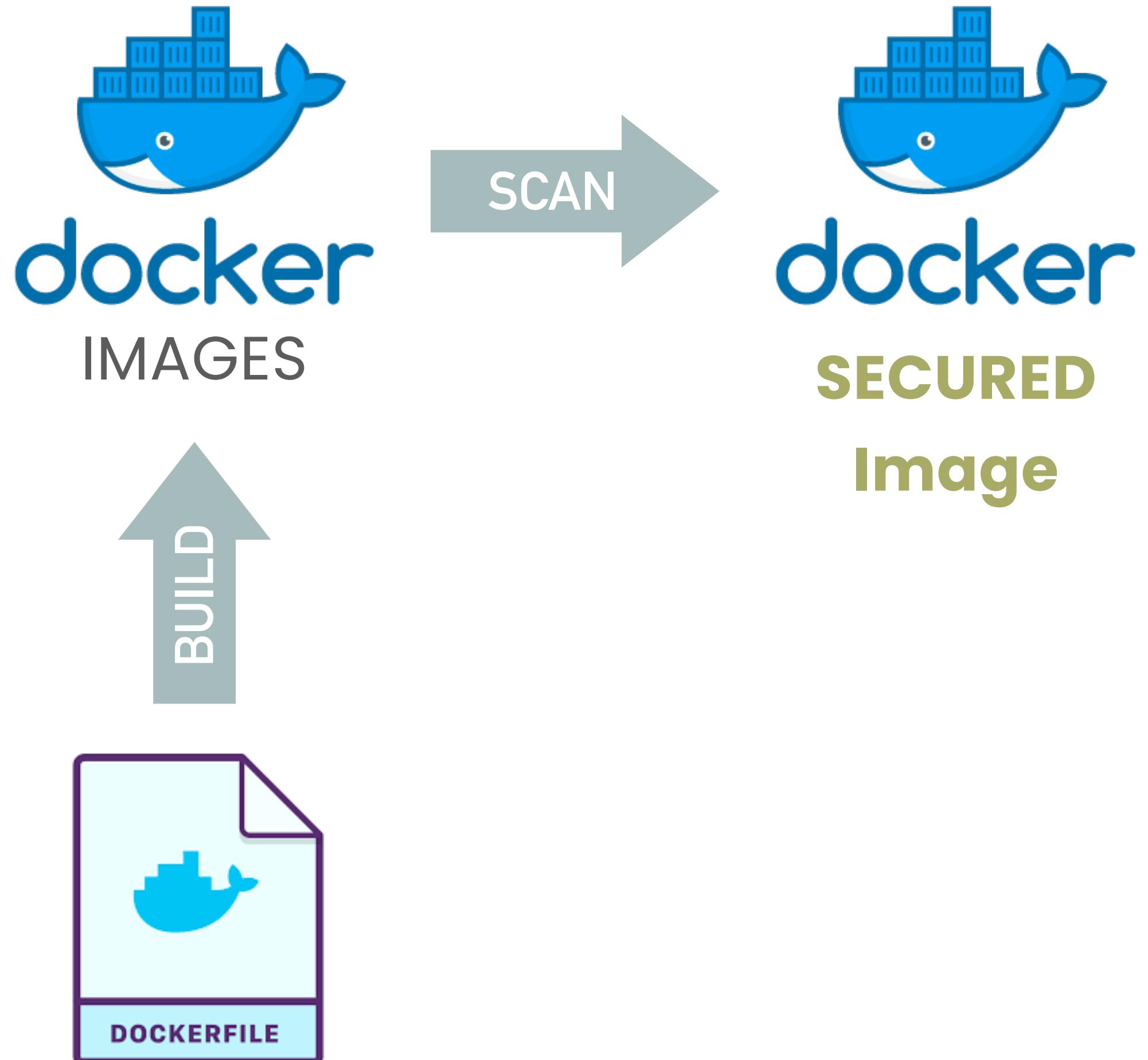
# DEVELOPMENT WORKFLOW WITH DOCKER

---



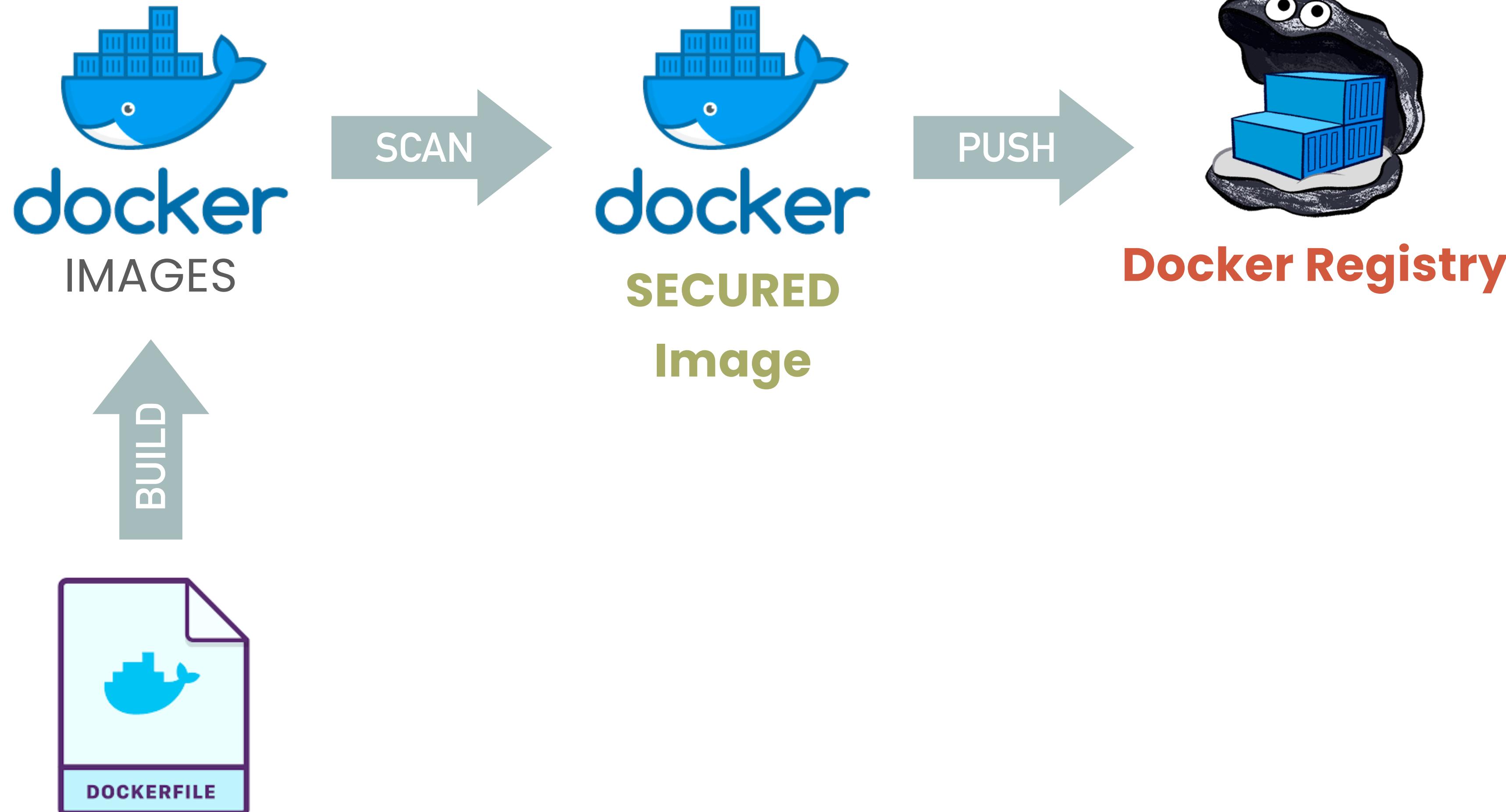
# DEVELOPMENT WORKFLOW WITH DOCKER

---

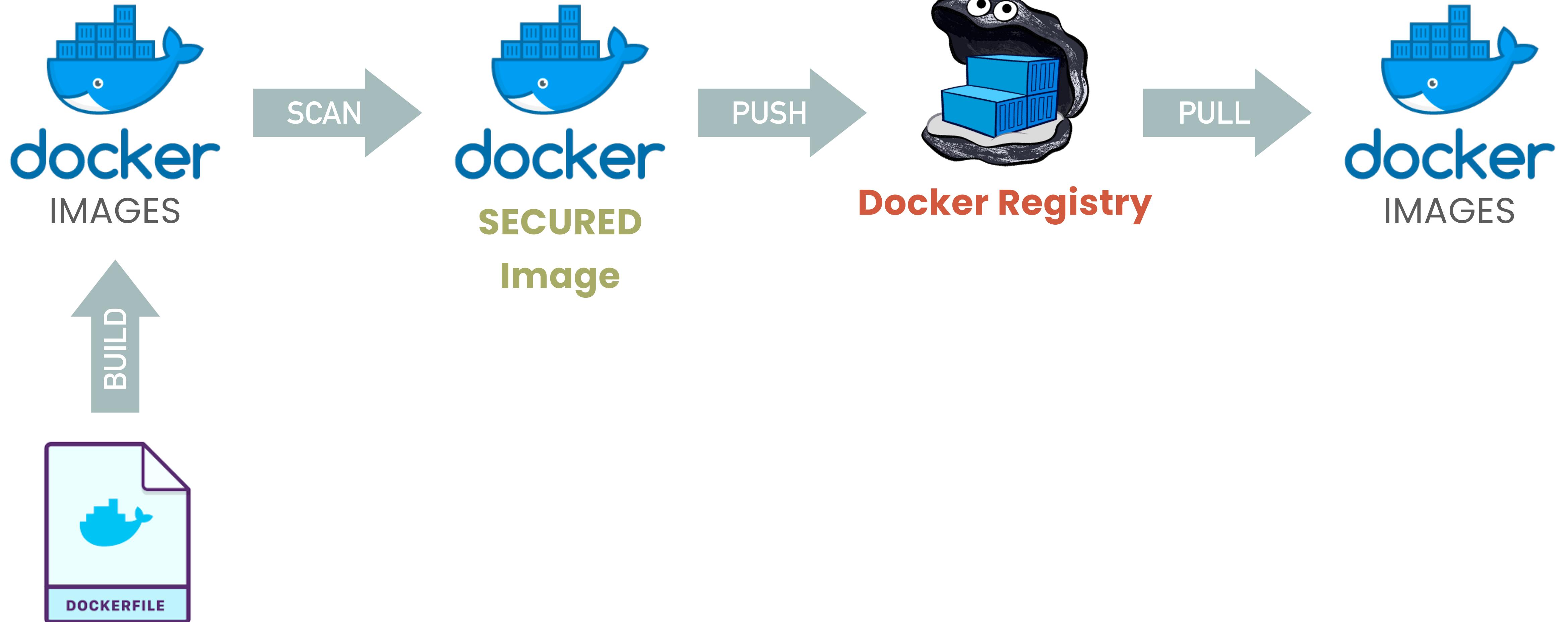


# DEVELOPMENT WORKFLOW WITH DOCKER

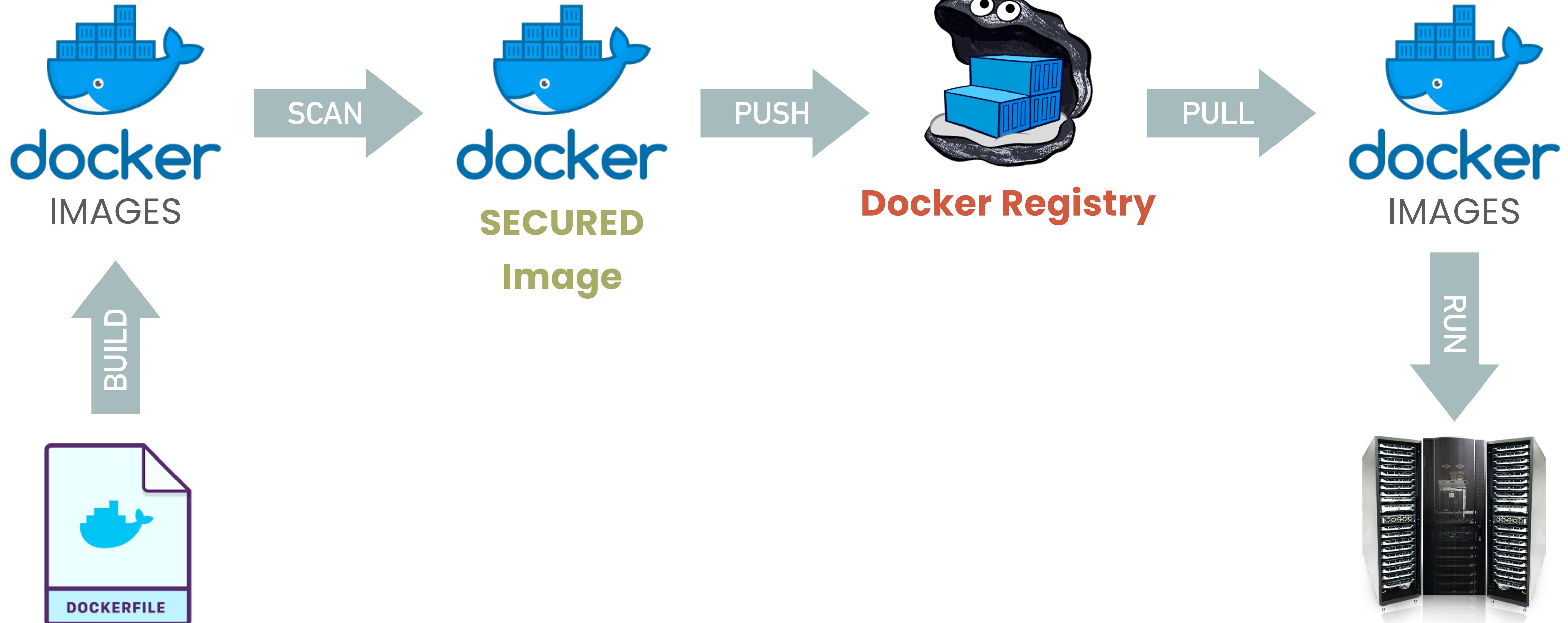
---



# DEVELOPMENT WORKFLOW WITH DOCKER



# DEVELOPMENT WORKFLOW WITH DOCKER



**THANK YOU**