BuildPacks

Kubernetes OCI Images

29 June, 2023

Viktor Bonev

01

What is OCI?

Quick summary of container runtime interfaces and process & resource isolation

02

BuildPacks

Historical overview of the process before and what has changed?

03

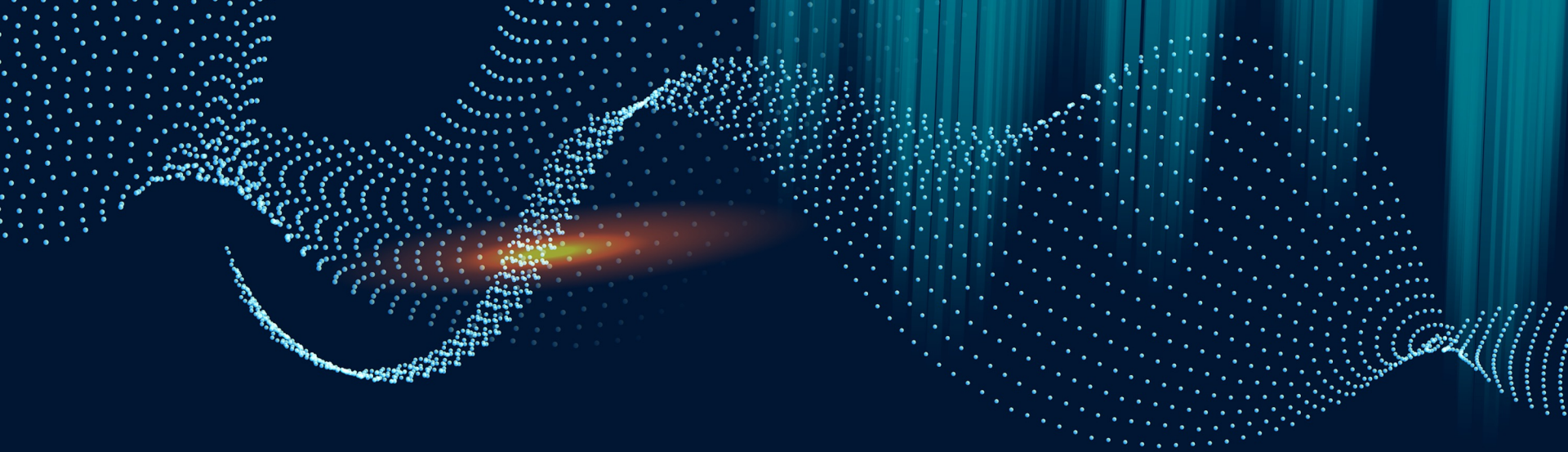
k8s workloads

Efficiently provision a strategy to handle hundred of thousands of k8s workloads

$ whois 127.0.0.1

Senior Member of Technical Staff

vmware® Carbon Black



01 What is OCI?

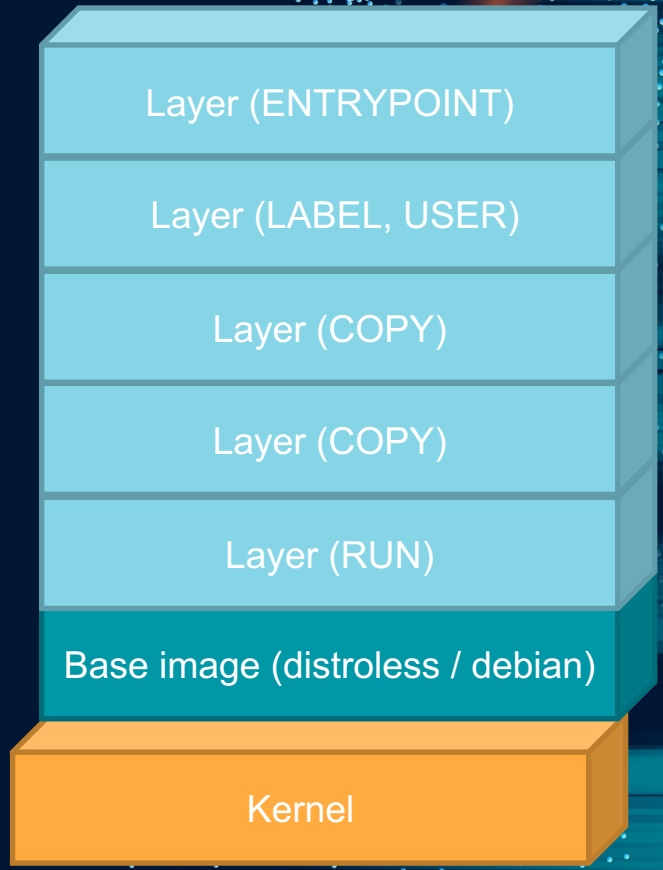
Summary of a container
concept key components

What makes a container – container?

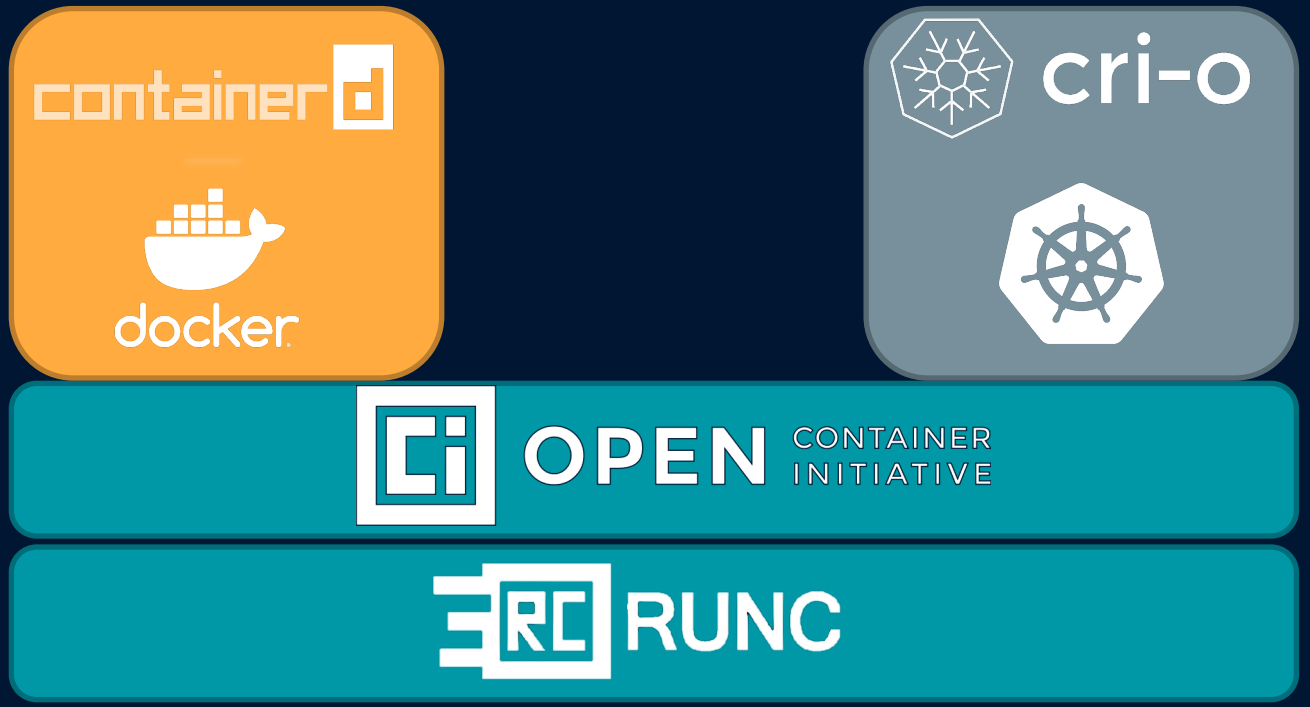
It is an isolated process by design, who can control and spawn other isolated processes. All processes controlled by container runtime interface are communicated through native kernel features

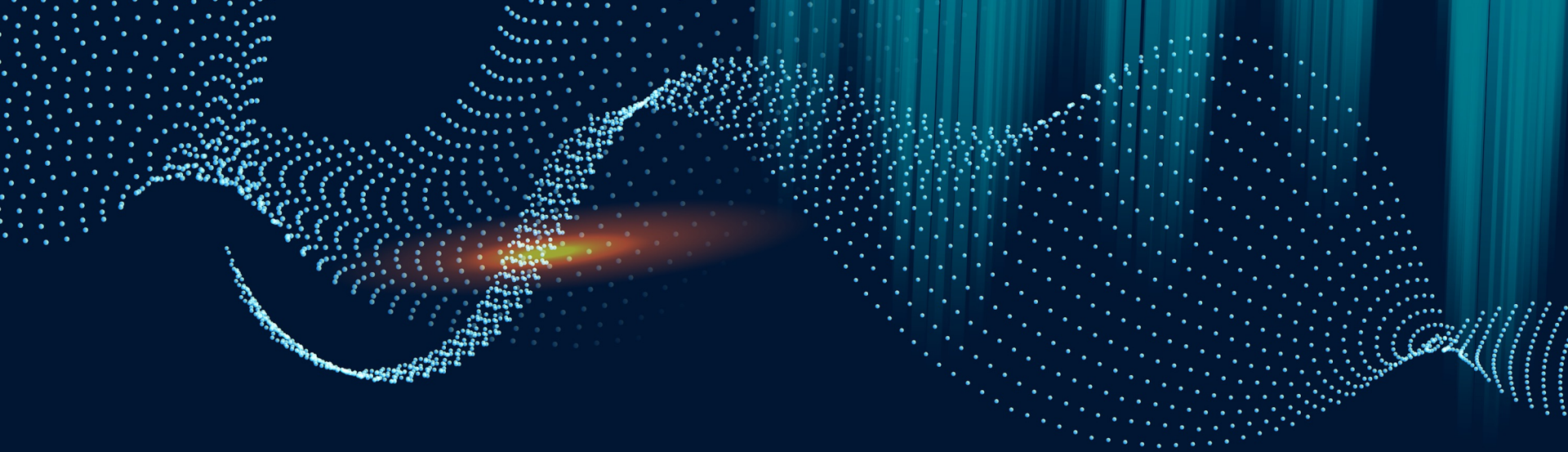
- **namespaces** – limit what you can see
  - → *pid, net, mnt, uts, ipc, user*
- **cgroups** – limit what you can use
  - → *memory, cpu, block IO, network (via iptables/nftables)*
- **chroot** – limit root directory FS

In fact, you can create manually a container and ‘simulate’ the work of CRI (container runtime interface)



Different CRI (Container Runtime Interface)

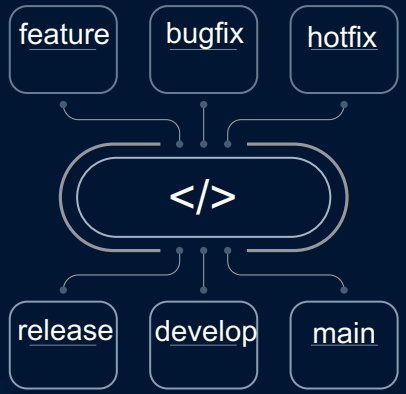


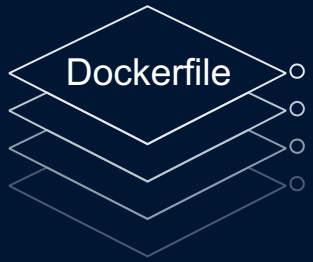


02 BuildPacks

Why bother?

Casual approach





DoD build image

Huge collection of dockerfiles

Image tag process

Push OCI artifact

Pull …

Image size is quite often neglected :-(

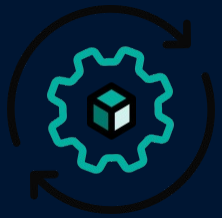
buildah

BuildKit

Buildpacks.io

FACT

You do need Docker to build images

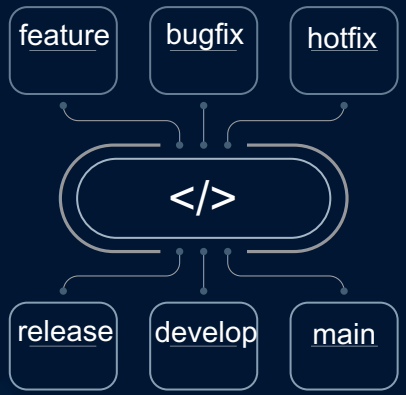


kpack

Kaniko

podman

BuildPacks 101 Part I

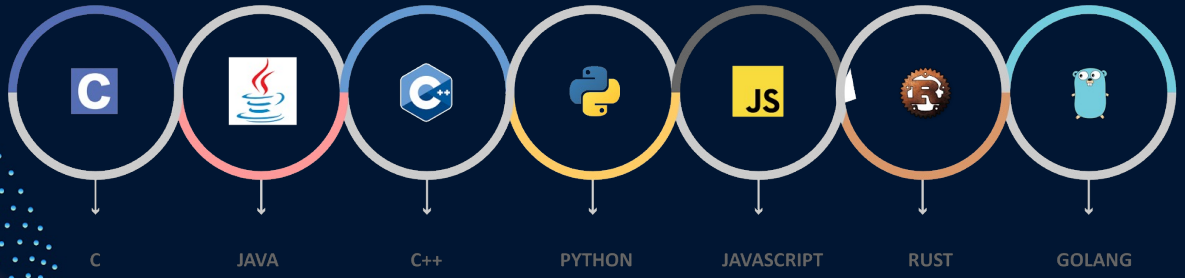


builder.toml

Paketo Builder

Paketo Buildpacks

Paketo Stack

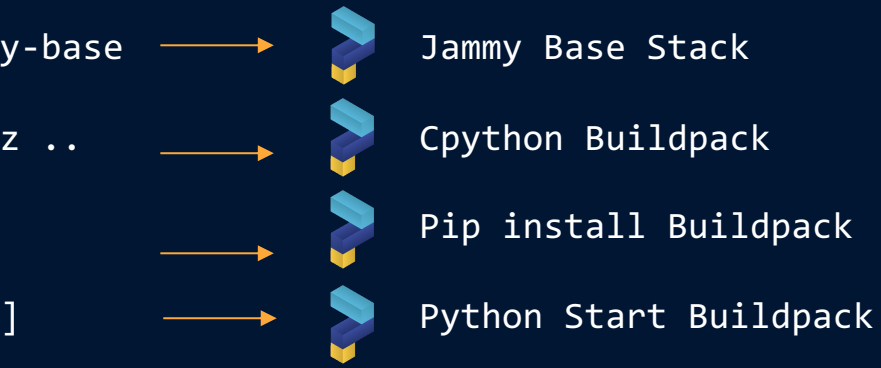


BuildPacks 101 Part II

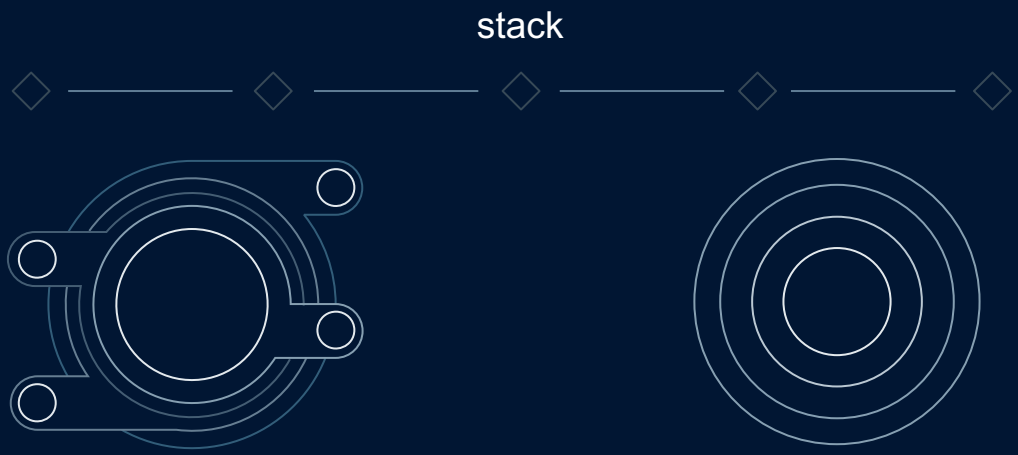
```
FROM paketobuildpacks/build-jammy-base

RUN curl –sSLo /layers/python.tgz ..
ENV PYTHONPATH=/layers/python

RUN pip install …
ENTRYPOINT[“python”, “server.py”]
```



Stack tooling via jam



Build Image

Contains:

- Base OS
- Packages

Run Image

Contains:

- Base OS
- App dependencies

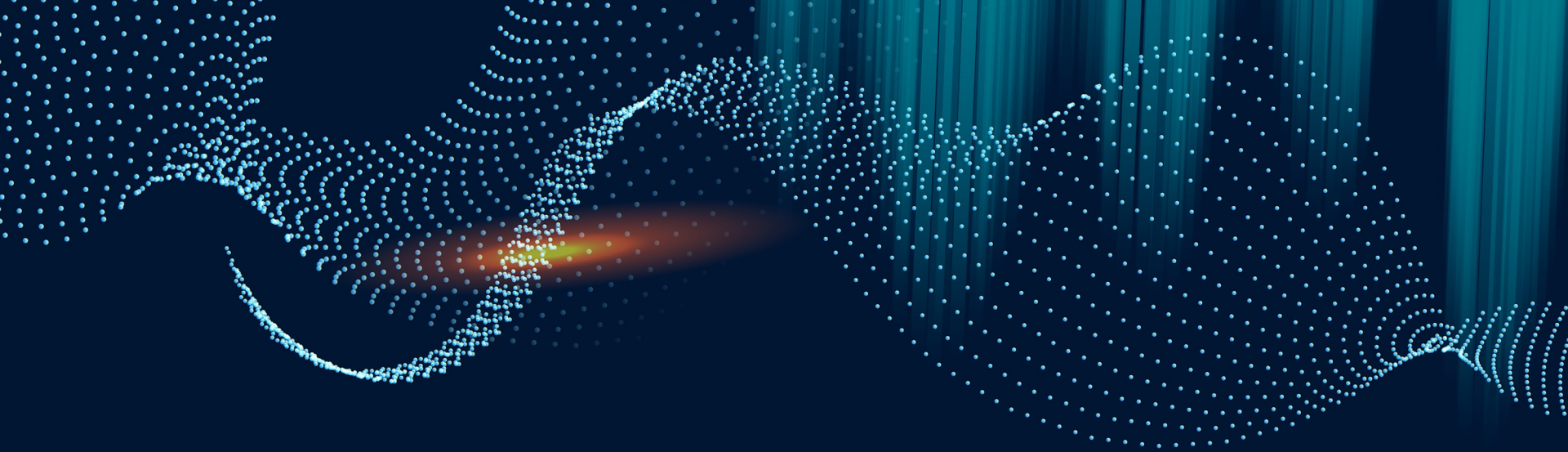
kpack
Buildpacks for Kubernetes

Same as pack but for k8s obj definitions

A stack provides the buildpack lifecycle with build-time and run-time environments in the form of images.

A **builder** is an image that bundles all the bits and information on how to build your apps, like

Demo
Go application



03 k8s workloads

Creating the perfect harmony

Key points k8s OCI

Size

Network traffic, agility, Cost of Operations

Debt

Build error free compact stacks quick

Redudancy

Add only the things you need – smart layers

Security

Limit pkg usage – scan and address CVEs before deploy

Sign

Preferably use cosign or notary to sign OCI artifacts

Network

Design intelligent k8s via network provider (calico, flannel)

Results

15%

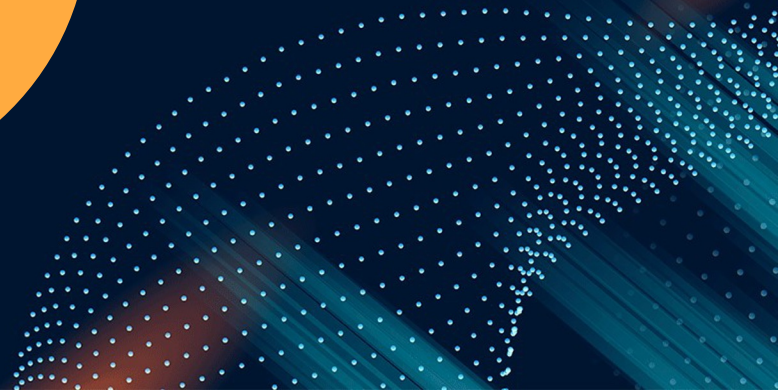
Cloud instance type optimization

91%

Size OCI image decrease

21%

Less traffic cost*



THANKS!

vbonev@vmware.com

Viktor Bonev