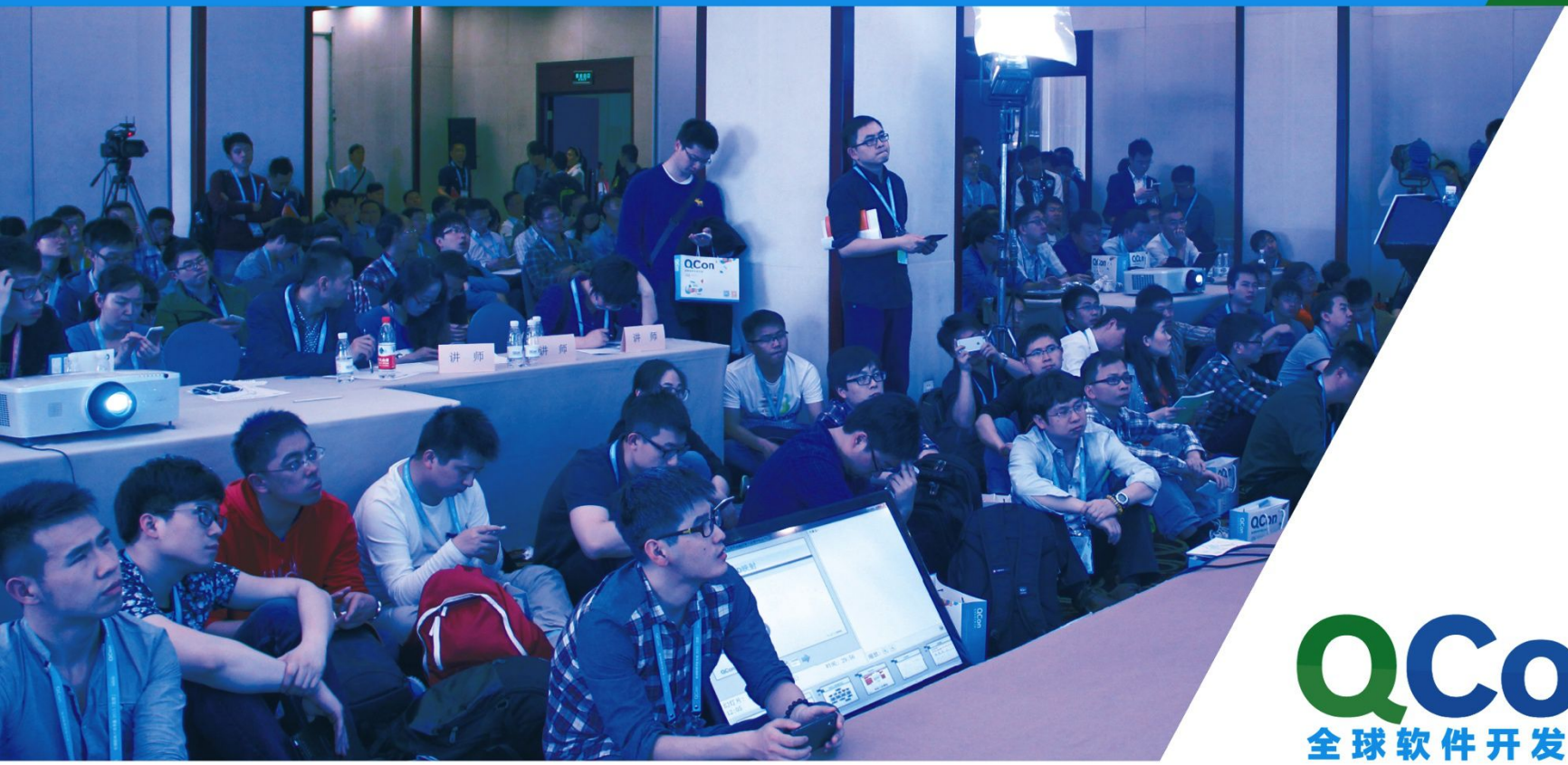
QCon全球软件开发大会

International Software Development Conference



QCon
全球软件开发大会

云原生应用平台架构解析

张海宁 (Henry Zhang)
云应用平台资深架构师
VMware中国研发中心

About Me

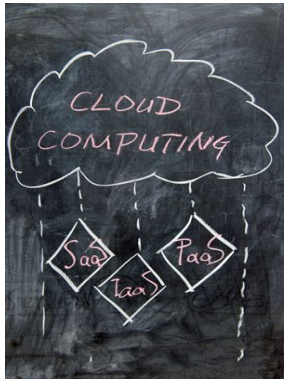
- Lead Architect in China R&D for Cloud Native App Solutions
- One of the first China evangelists of Cloud Foundry
- Full stack engineer
  - Cloud architect – PaaS, IaaS
  - iOS developer – top free app and top 10 paid apps in China App Store
  - Operator of 10M PV web sites
- 10 years experience on containers

Agenda

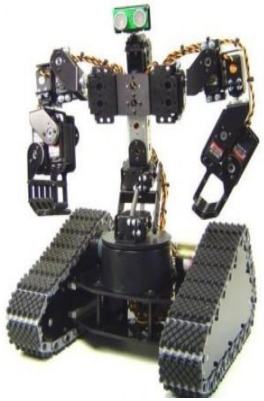
1	The Rise of Cloud Native Applications
2	Cloud Native Key Technologies
2.1	Container optimized Linux
2.2	Developer Tooling
2.3	Secure Container Runtime
2.4	Microservices governance

Mobile-Cloud Era = Increased Customer Expectations

Everything On-Demand



Fully Functional, All the Time

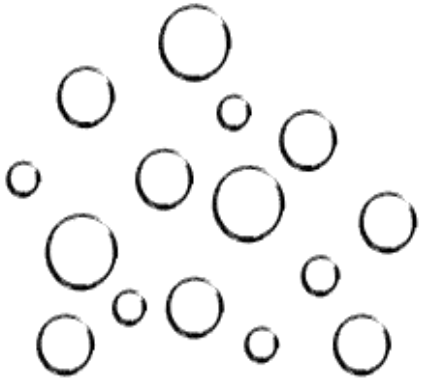


Accessible Everywhere

Applications must be more resilient than ever!

Market Expectations drive Operational Changes for Customers

IT decisions moving to LOB and application developers

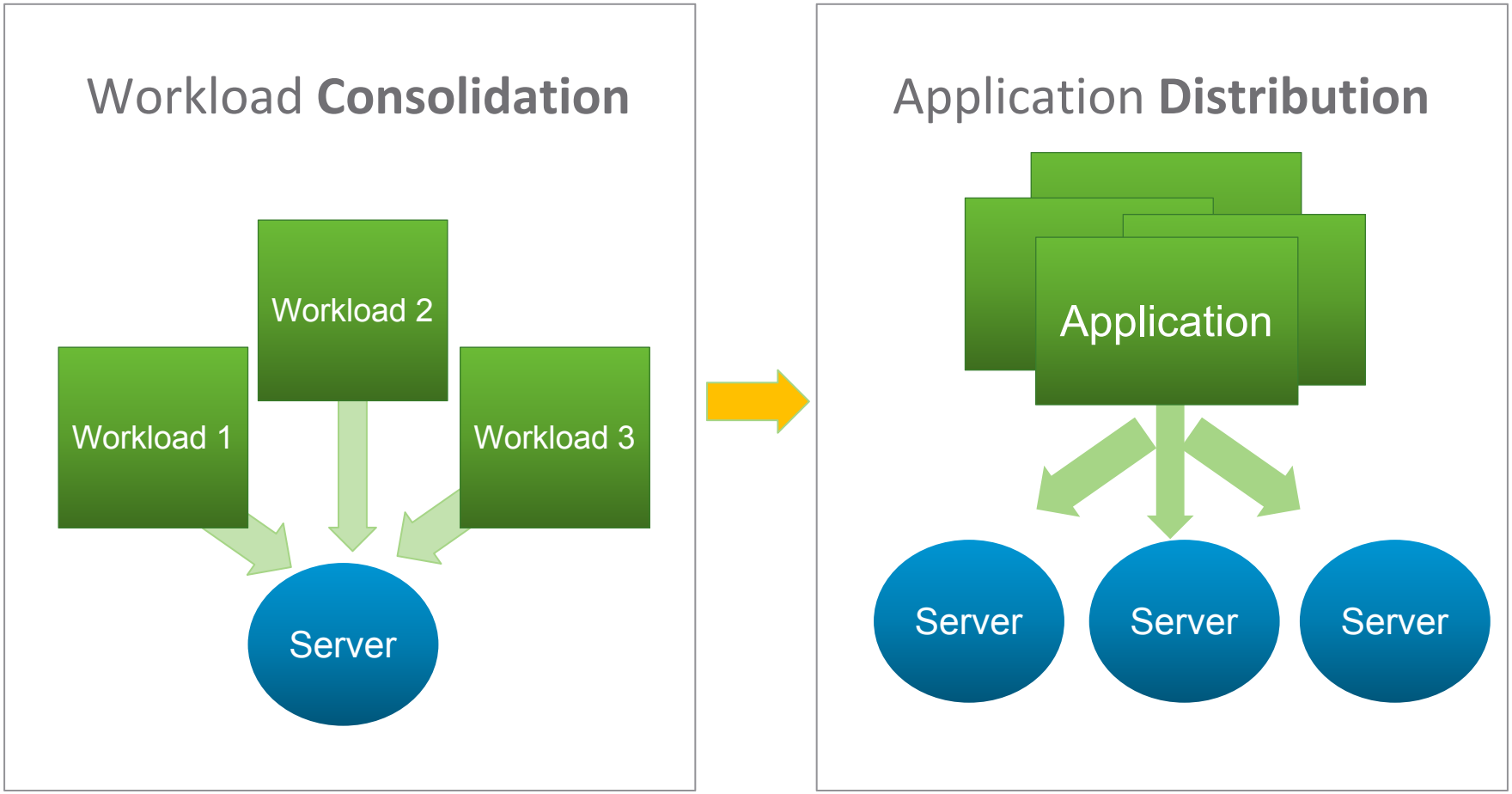


Applications broken into microservices

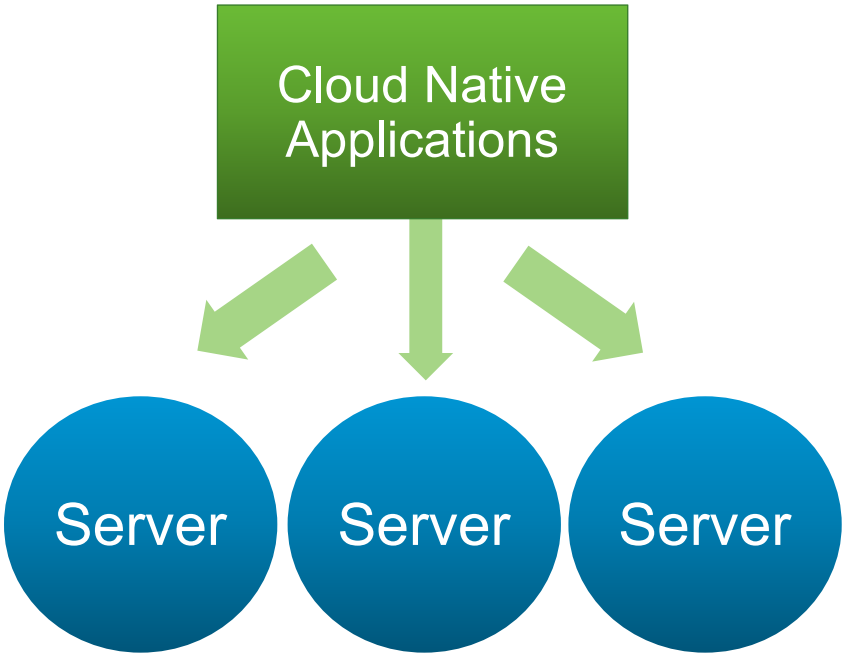
Continuous Delivery Several times a day

Do everything faster

Changing Infrastructure Needs



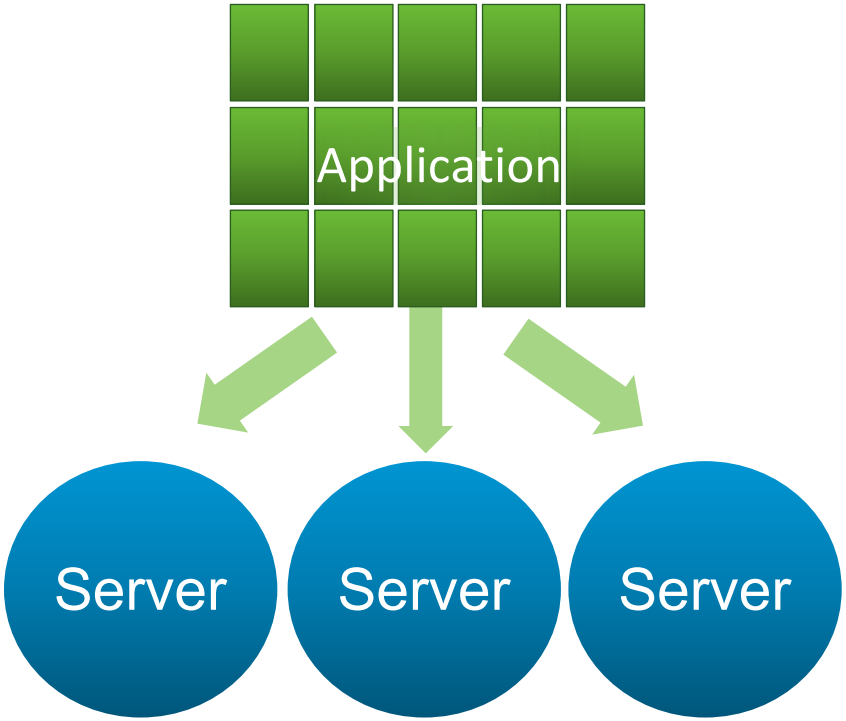
The Cloud Native Application



Leverage elastic infrastructure to

- Provision instances of itself
- Scale up and down
- Detect and work around failures

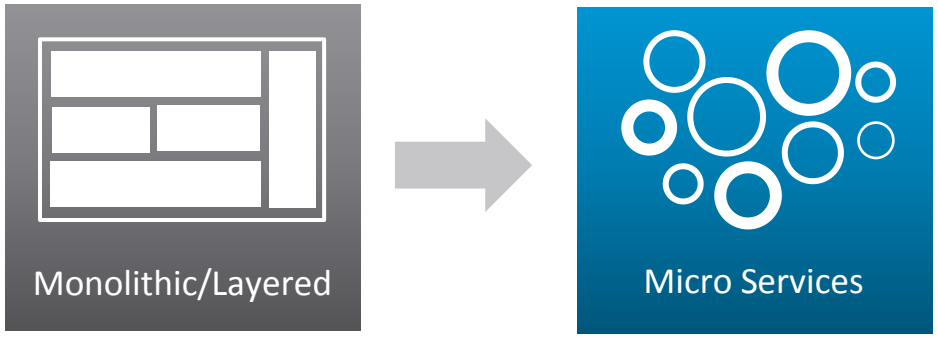
Cloud Native Application Characteristics



Distributed and Scale-out

- Microservices oriented
- Container packaged
- Dynamically managed

A New Application Architecture is Emerging



Properties of a Microservice

Small code base

Easy to scale, deploy and throw away

Autonomous

Resilient

Benefits of a microservices architecture

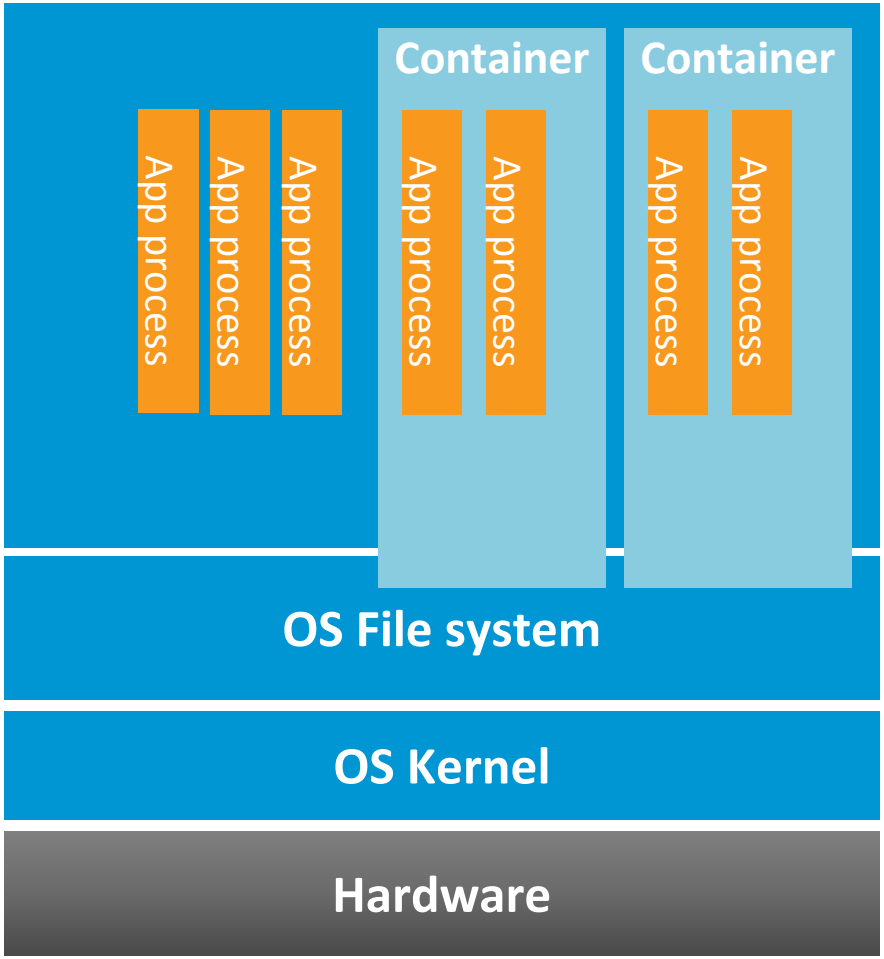
A highly resilient, scalable and resource efficient application

Enables smaller development teams

Teams free to use the right languages and tools for the job

Rapid application development

Microservices with Containers



Conatiners Exist for Many Years

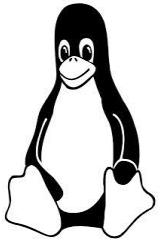
- Solaris Zones, FreeBSD Jails, OpenVZ, LXC

Why Containers?

- Process isolation with good performance isolation
- Reproducible environment
- Enables management at scale

It's a Challenging Jump to Cloud Native Application

Ecosystems to be harmonized



Containers **DO NOT** provide:

Security isolation

Data Persistence

Guaranteed Resources

Overcommit and rebalancing

Hidden Costs

- Management overheads
- Container sprawl
- Governance challenges

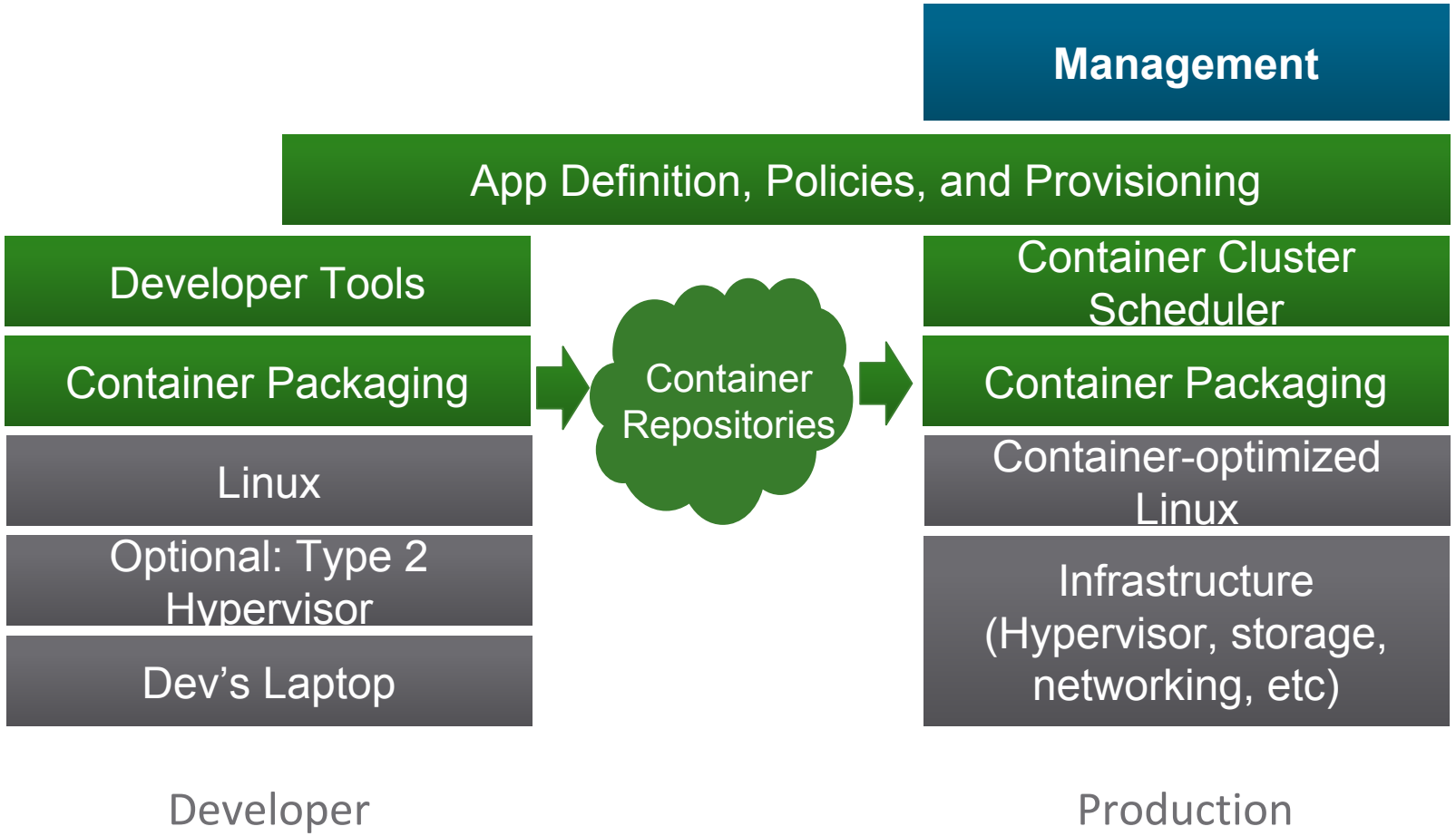
Agenda

1	The Rise of Cloud Native Applications
2	Cloud Native Key Technologies
2.1	Container optimized Linux
2.2	Developer Tooling
2.3	Secure Container Runtime
2.4	Microservices governance

Developer is a First-Class User of the Cloud

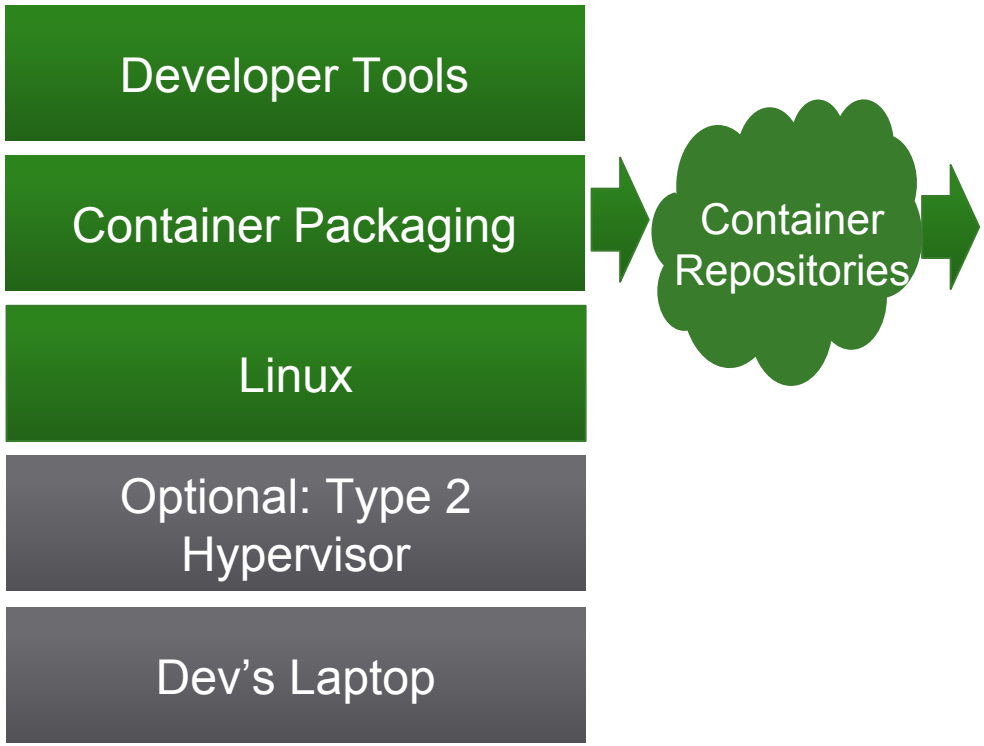
- Build technologies that **span the app lifecycle**
- **Empower operations teams** to manage Cloud-Native applications
- Build to and support **open systems and standards**

Cloud Native Platform
– *Dev & Production Stack, DevOps Process*

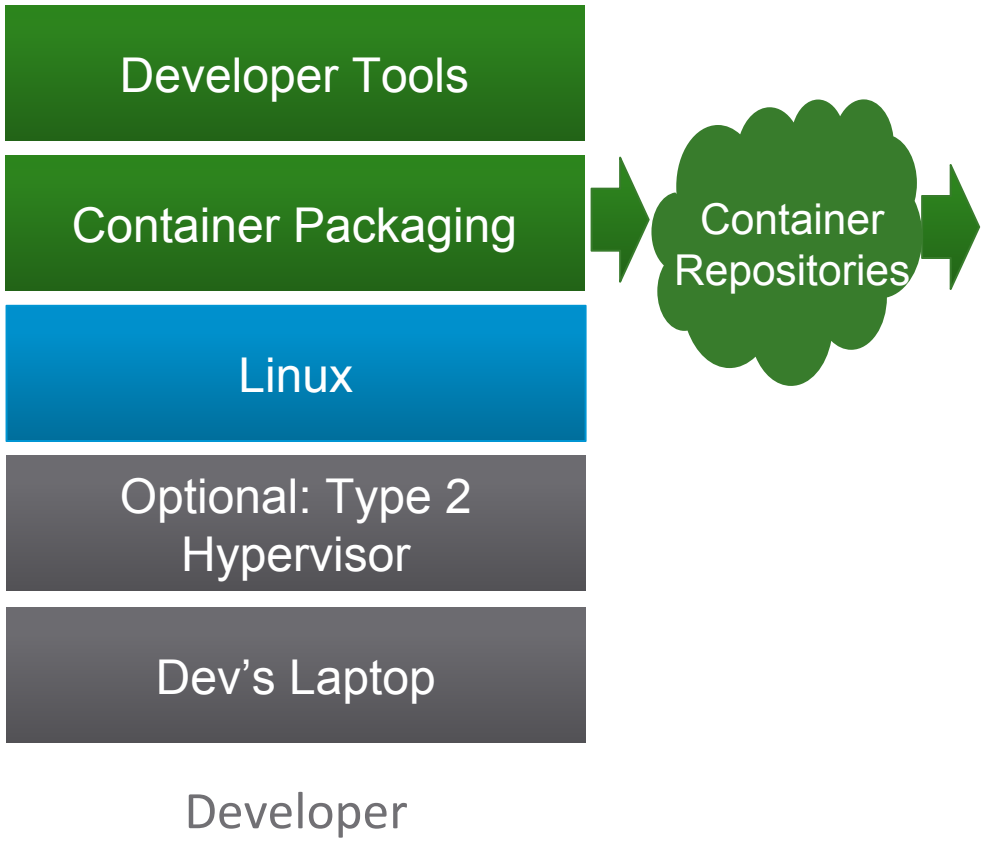


Agenda

Container Developer Stack



Container Developer Stack – Container Runtime



Photon OS - Secure & Optimized Container Runtime

Container Optimized Linux OS

Docker, rkt and Garden (Pivotal) support

Minimal footprint to run containers

vSphere Integration

Part of your vSphere install

Hypervisor-optimized container runtime

Updates from VMware

Enterprise support

Security and update patches from VMware

Open Source

GPL v2 License

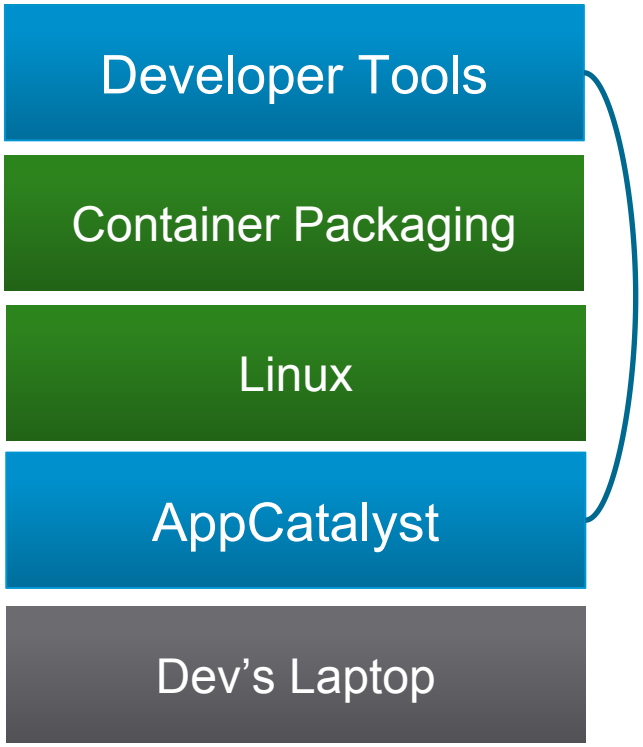
Photon OS Directions

- Hypervisor-optimized container host
  - Guest customization support – improved vSphere and vCloud Air compatibility
  - Shared folders for Workstation & Fusion – streamline developer to production pipeline
  - Lightwave integration – single identity across all infrastructure
  - Software Defined Datacenter for Containers – single operational model for all workloads
  - Performance and packaging optimizations – faster boot, smaller footprint
- Secure container stack
  - Signed packages – ensures trust of VMware packages
  - Lightwave integration – extends trust to containers and container authors
  - Secure boot and attestation – creates a chain of trust from the hardware, through the hypervisor, to the container

Agenda

1	The Rise of Cloud Native Applications
2	Cloud Native Key Technologies
2.1	Container optimized Linux
2.2	Developer Tooling
2.3	Secure Container Runtime
2.4	Microservices governance

Container Developer Stack – Dev Tooling

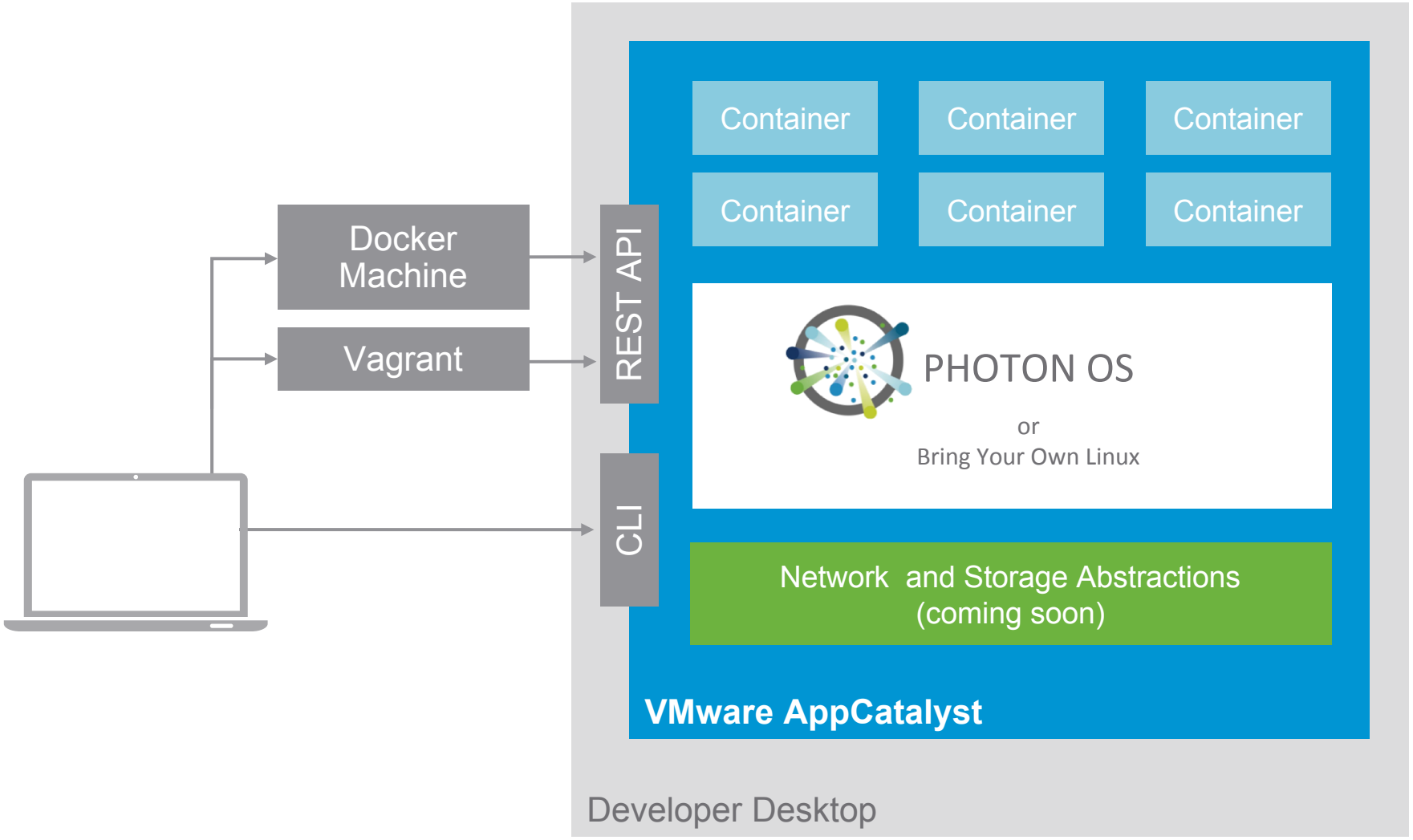


Developer

Integrated with Docker Machine and Vagrant

An alternative to VirtualBox

AppCatalyst - The Hypervisor for Container Developer



AppCatalyst - Hypervisor to Speed up Development

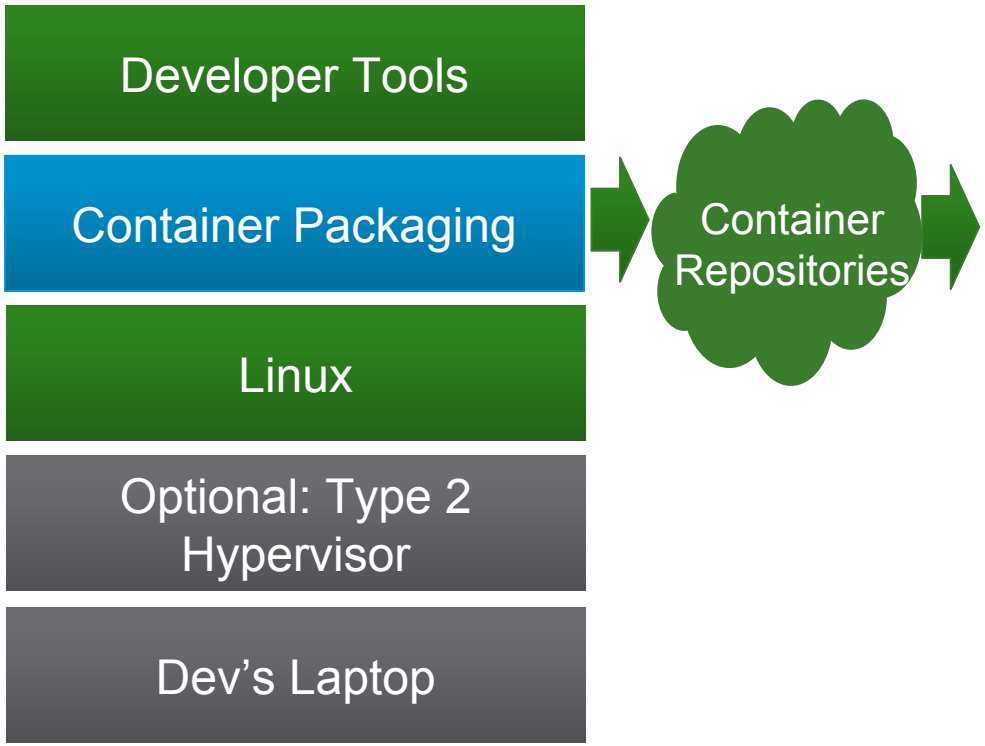
Datacenter-in-a-laptop, model production deployments on your laptop

- Same battle-tested virtualization engine as Fusion and Workstation
- Drop-in replacement for Virtualbox in Docker Machine and Vagrant

Developer-Friendly

- Optimized to support developer workflows
- Exposes REST API with command-line interface
- No UI to mess with, built to run fast and mean

Container Developer Stack



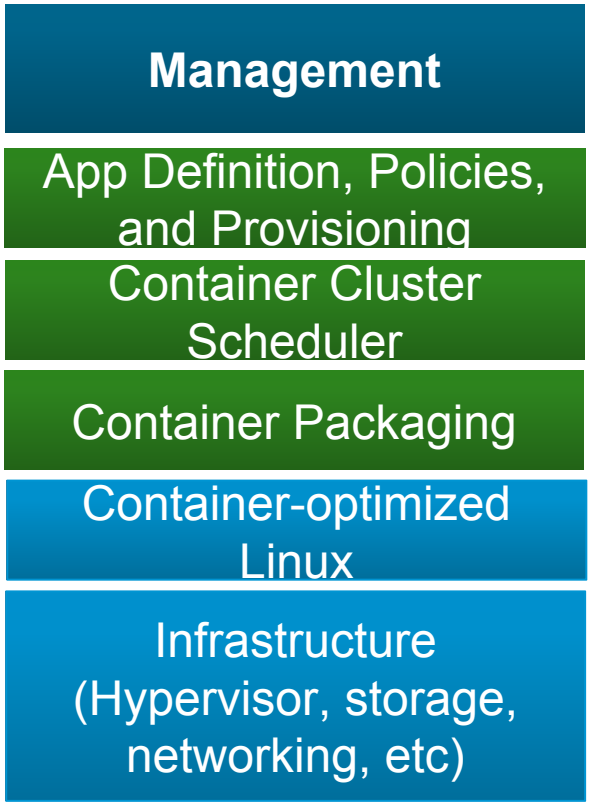
OCF:

- Standard operations
- Content-agnostic
- Infrastructure-agnostic
- Designed for automation
- Industrial-grade delivery

Agenda

1	The Rise of Cloud Native Applications
2	Cloud Native Key Technologies
2.1	Container optimized Linux
2.2	Developer Tooling
2.3	Secure Container Runtime
2.4	Microservices governance

Cloud Native Platform – Production Stack



e.g. Photon OS, CoreOS, Atomic

e.g. vSphere Integrated Container, VSAN, NSX, KVM,

Production

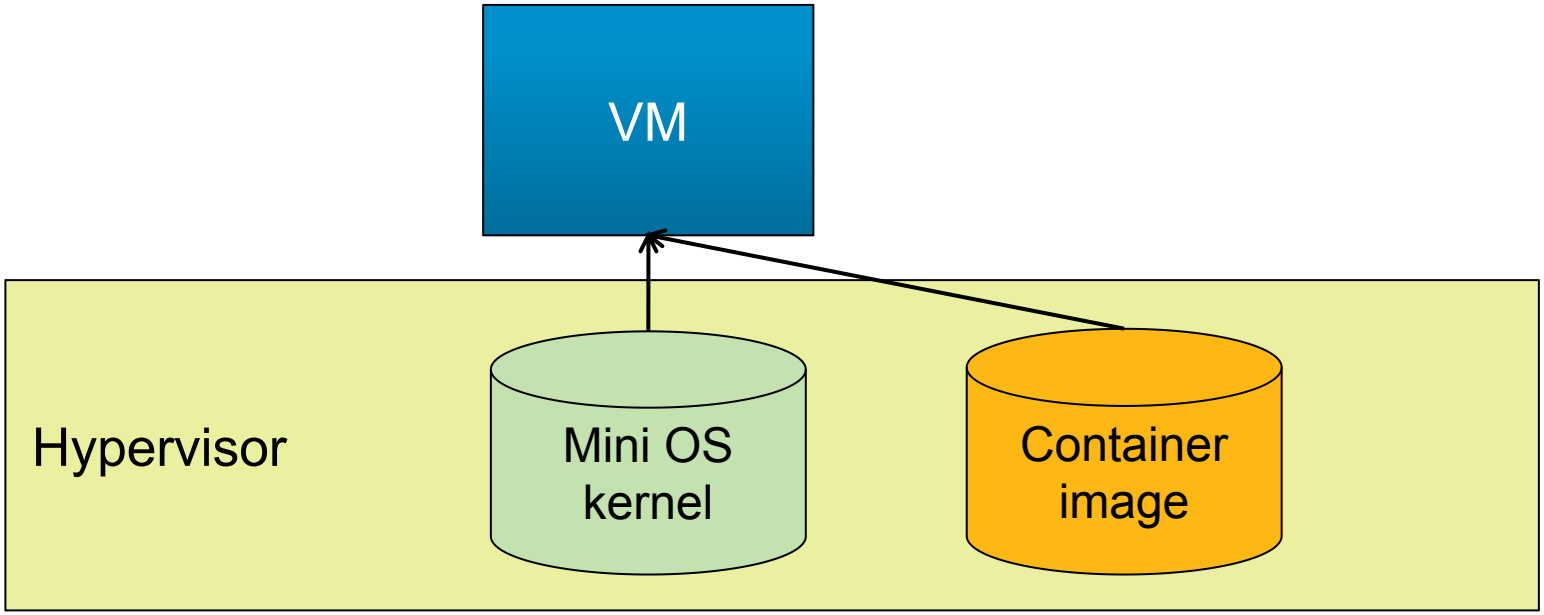
The Debate: Container vs VM

VS

- Portable packaging
- Small footprint
- Performance

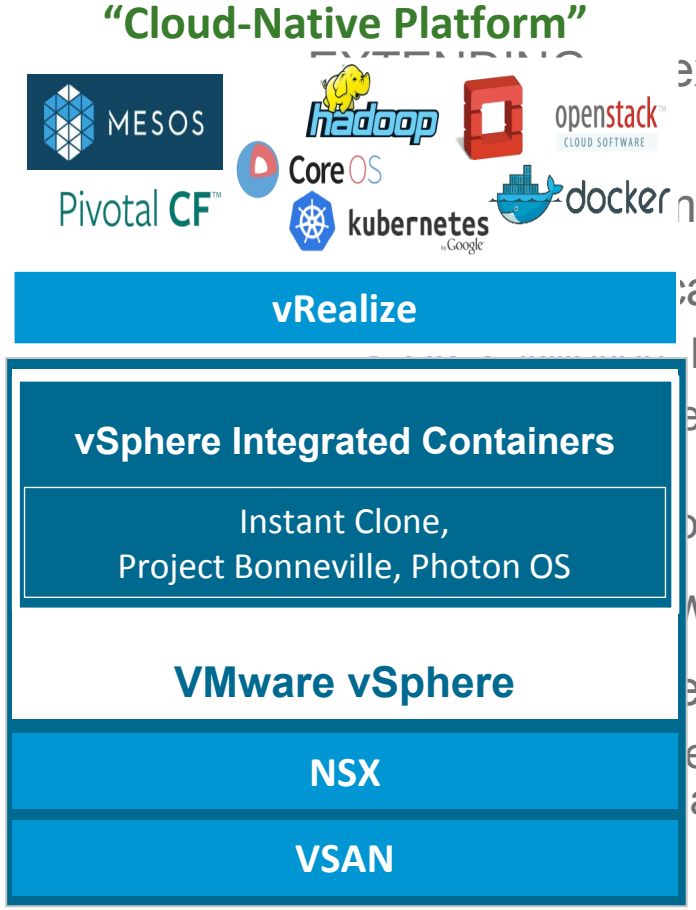
- Secure
- Isolation
- Mature

Combining the best of both Container & VM



- Mini OS kernel enables fast startup time
- Mounting container image to start the bundled application
- Achieve strong isolation as VM

vSphere Integrated Containers (VIC)



existing vSphere

ne a first-class citizen

capabilities

HA/DR

etwork Integration (VSAN and

or re-architecture required

with existing tools

em

eveloper tools, application

ardware platforms

Leverage Your Existing Investments and Enable On-Ramp To Cloud-Native

vSphere Integrated Containers – Combine the best of both worlds

The convenience of Docker containers with the management and security of vSphere

Docker containers encapsulated as virtual machines

- Everything in ESX becomes a well-isolated VM “container”
- Customers can move containers in and out of vSphere seamlessly

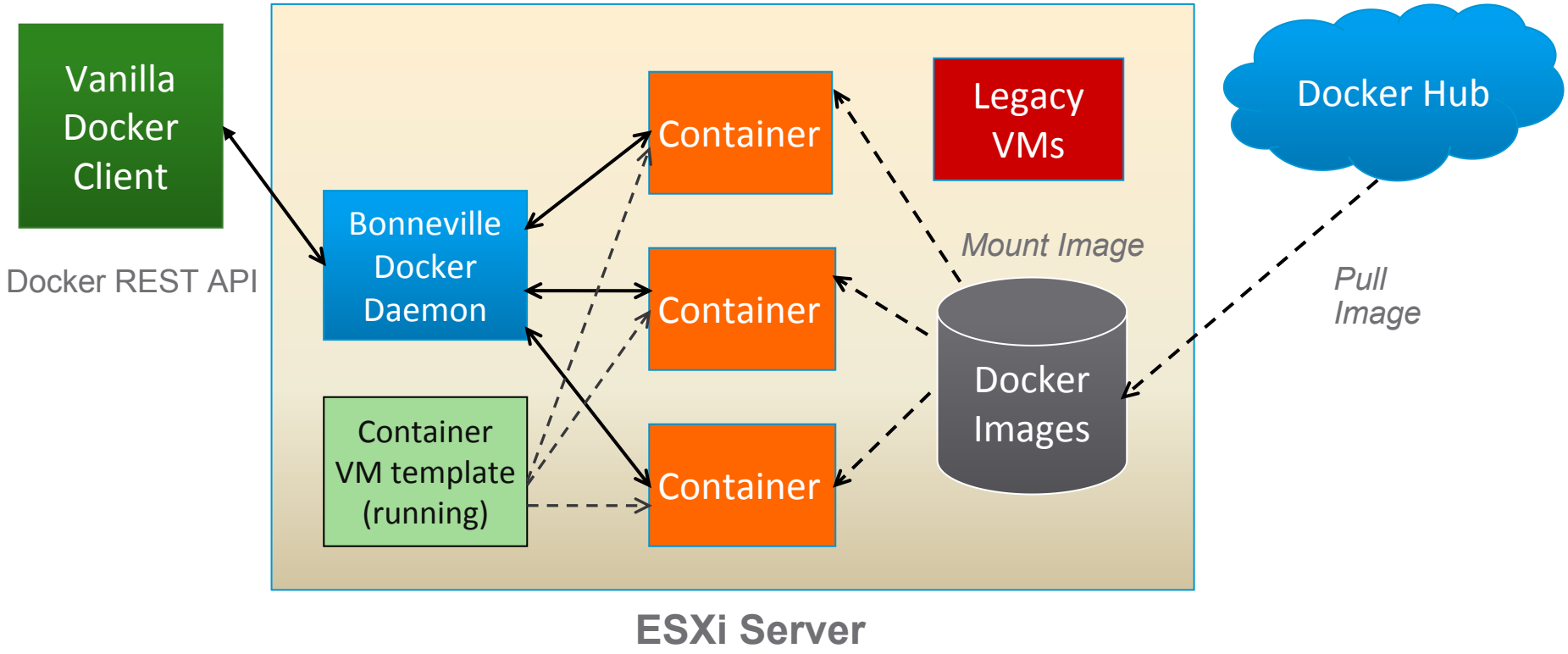
Complete API compatibility with Docker

- Containers visible to IT administrators when running on ESX
- Works with full ecosystem of Docker clients

Greater security and resource efficiency

- No container host operating system to maintain.
- ESX clustering allows for more efficient multi-tenant access

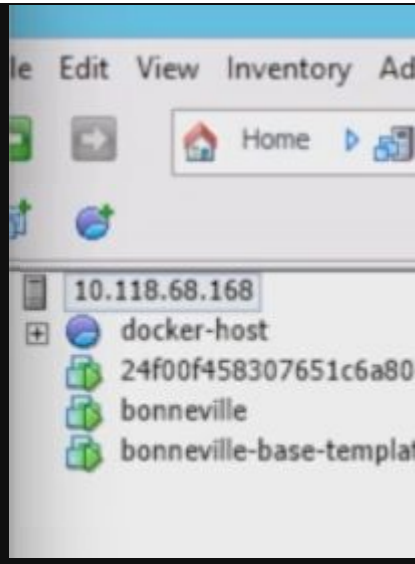
vSphere Integrated Containers Architecture



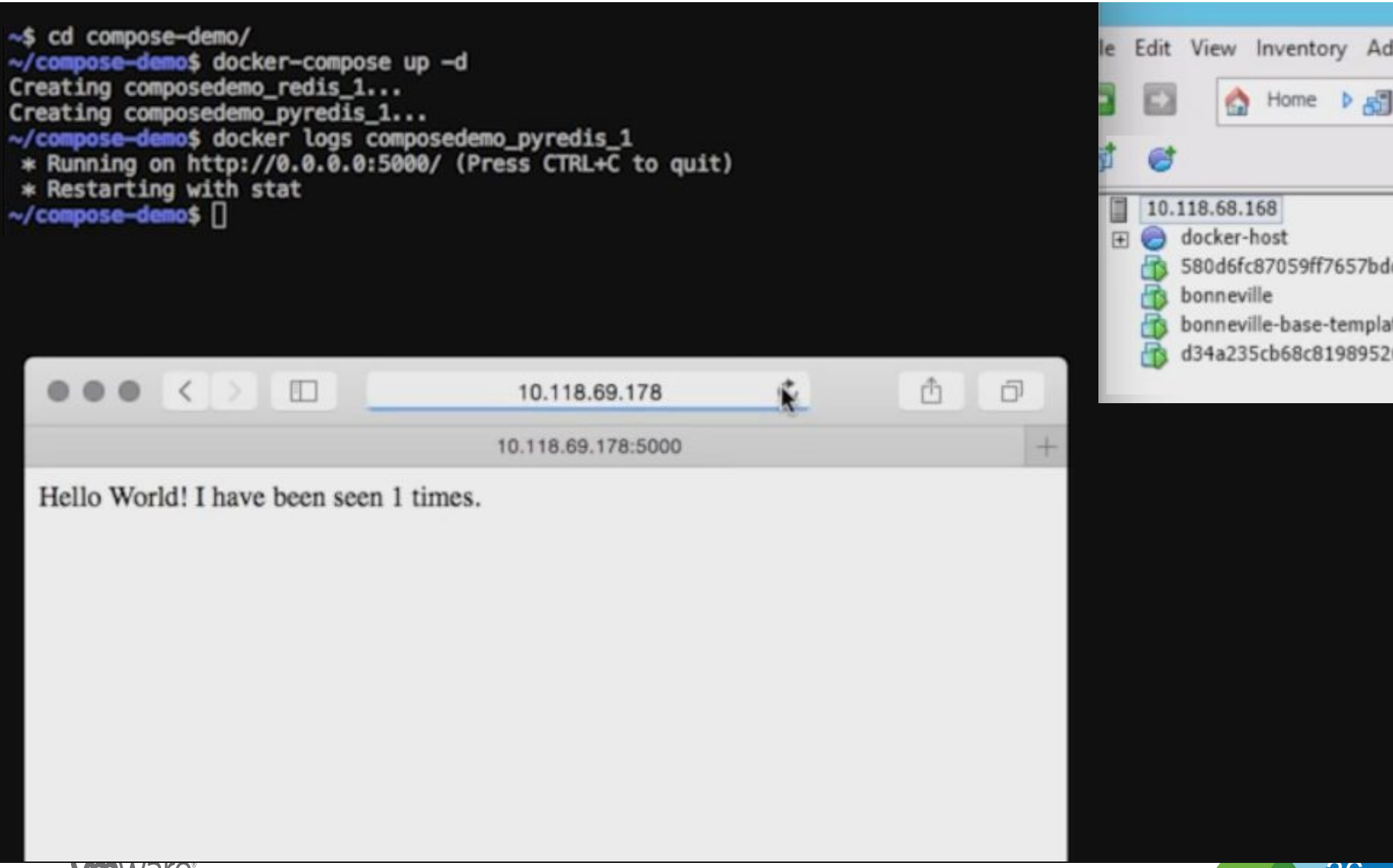
- Containers are first-class citizens on the hypervisor
- No need for a separately managed Linux container host, ESX is the container host
- Virtualization brings many benefits: Security, Isolation and multiple-OS support, migration, HA

Demo: Containers integrated with VMs on ESX

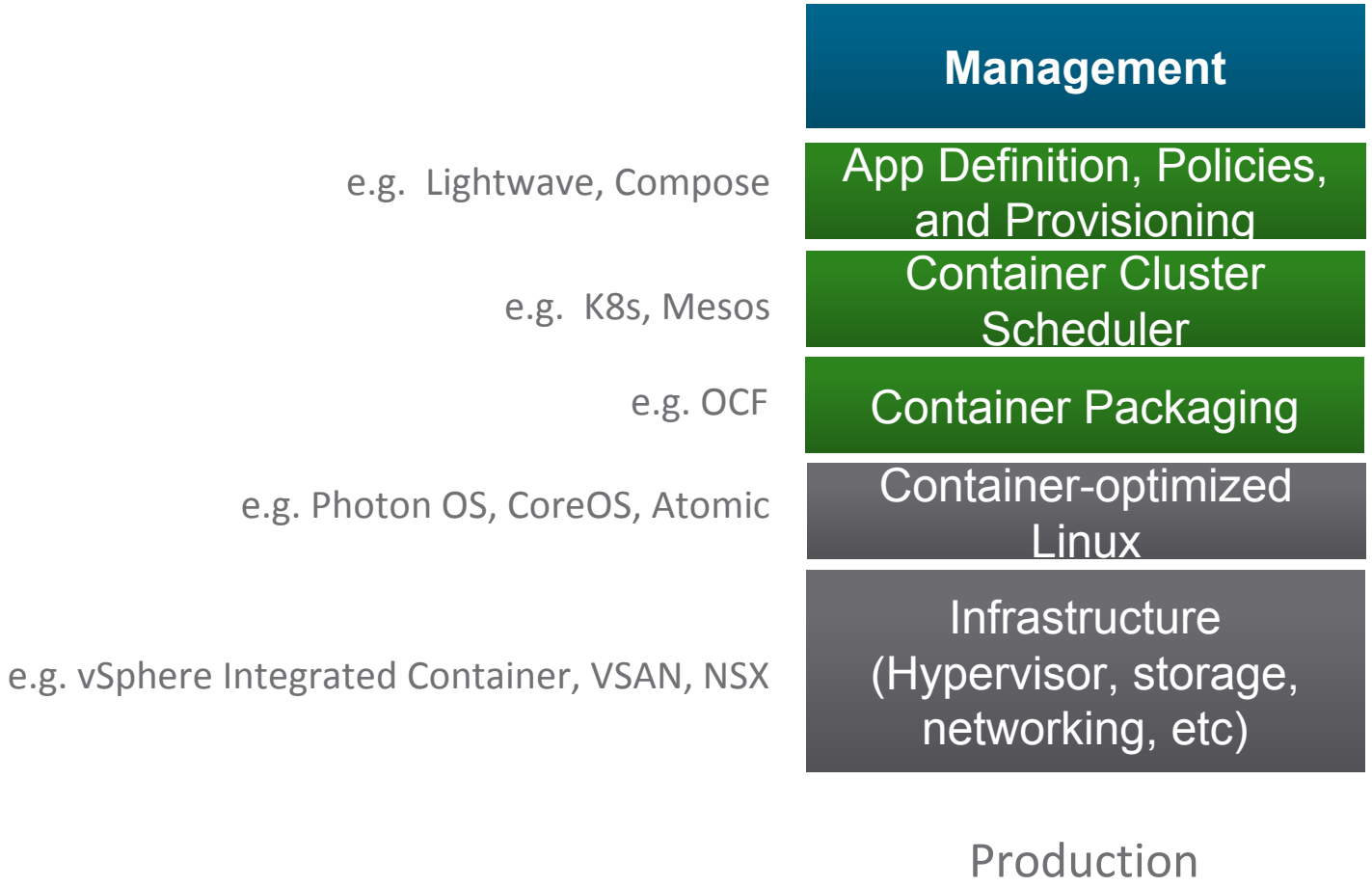
```
~$ docker -v
Docker version 1.6.2, build 7c8fca2
~$
~$ docker pull ubuntu
latest: Pulling from ubuntu
e118faab2e16: Already exists
7e2c5c55ef2c: Already exists
e04c66a223c4: Already exists
fa81ed084842: Already exists
Digest: sha256:738edd684282277c07f23277718e43562daf2ee210f7aca9a13fae65f0159ddd
Status: Image is up to date for ubuntu:latest
~$ docker pull redis
latest: Pulling from redis
b5edc072cfec: Already exists
41eb1212d9f4: Already exists
2c010358721d: Already exists
fb83dcd979bd: Already exists
a1811b7b024f: Already exists
05a396cb49e2: Already exists
361283d1af1a: Already exists
de77586468a2: Already exists
0f3059144681: Already exists
Digest: sha256:45ea798b819b69f3eb4d856d53154afd008b7aaae9280fcfeac26321dfcfd7a1
Status: Image is up to date for redis:latest
~$
~$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             VIRTUAL SIZE
pyredis             latest              1530d4760567        5 minutes ago       755.7 MB
python              2.7                 1ab93ac449ed        28 hours ago        748.2 MB
redis               latest              0f3059144681        6 days ago          111 MB
ubuntu              latest              fa81ed084842        10 days ago         188.3 MB
~$
~$ docker run -it ubuntu sh -ic "apt-get update -qq  && apt-get install cmatrix && cmatrix"
```



Demo: Containers integrated with VMs on ESX



Cloud Native Platform – Production Stack

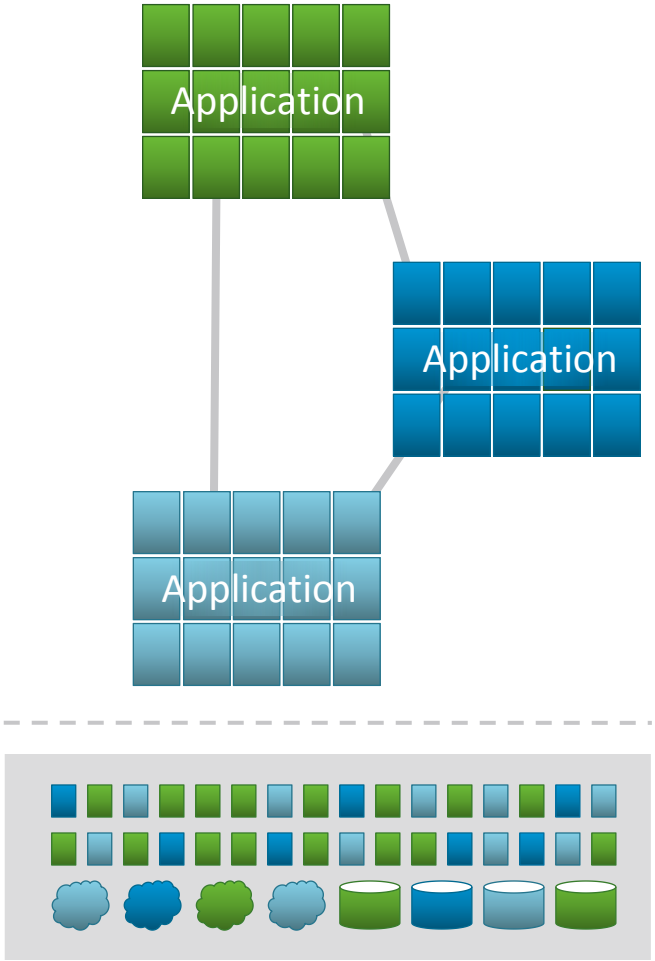


Production

Agenda

1	The Rise of Cloud Native Applications
2	Cloud Native Key Technologies
2.1	Container optimized Linux
2.2	Developer Tooling
2.3	Secure Container Runtime
2.4	Microservices governance

How Will We Secure Cloud-Native Applications?



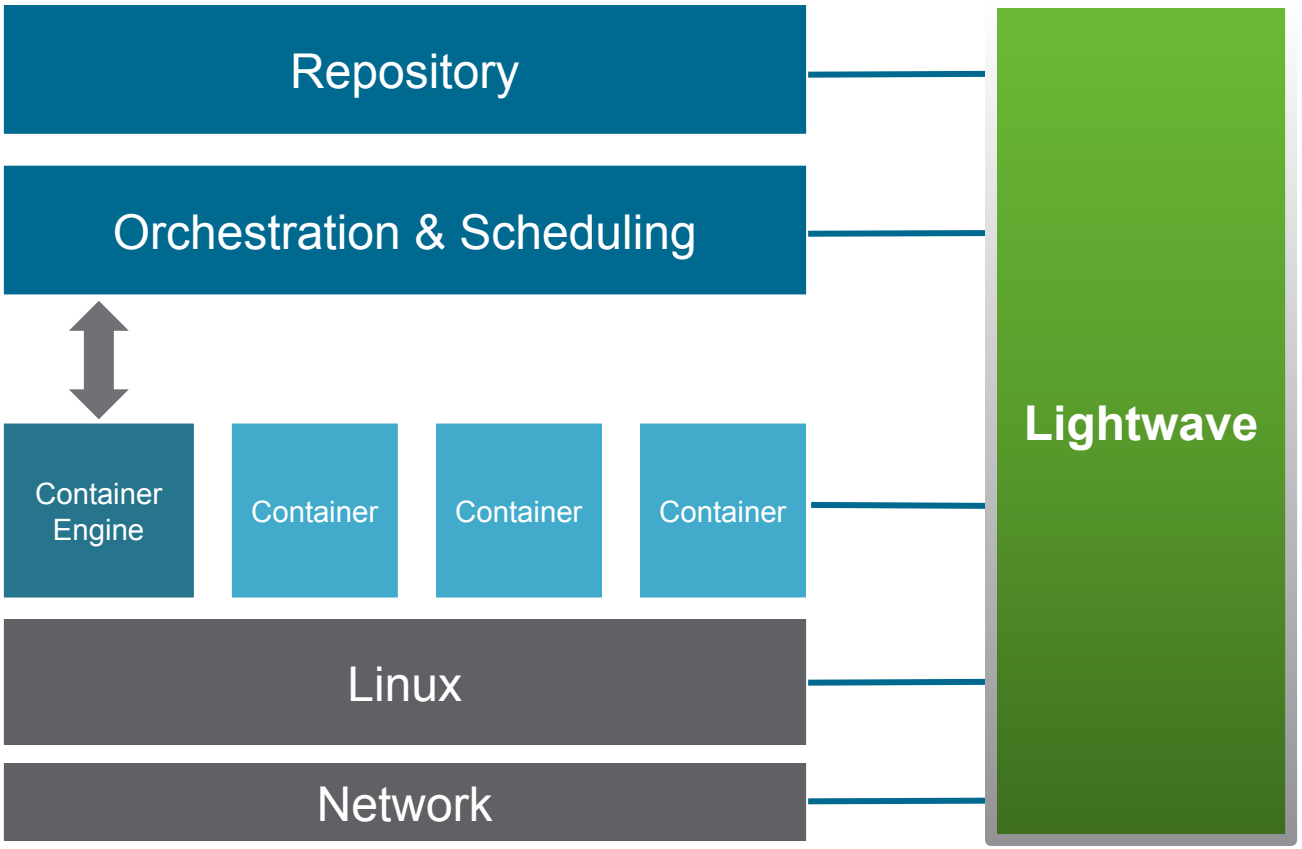
Challenges

- Complex networks of microservices
- Services themselves are complex distributed systems
- Many points of attack

Needs

- Scalable identity infrastructure
- Network isolation
- Trusted compute runtime

Cloud-Native Security Solution



vmware

Cloud-Native Identity & Access Management

Identity, Authentication and Authorization Server

LDAP, Kerberos, SAML, OAuth2.0, x.509

Scalable Architecture

Multi-master state-based replication

Multi-data center replication

Multi-Tenant

Multiple independent forests

Open Source

Apache 2.0

We Are Hiring

- Engineers for Cool Projects on Containers

resume-china@vmware.com

注明: 容器方向

THANKS