

ACSC 2018 Conference

Effective Container Security

Delivered by Murray Goldschmidt, COO

12 April 2018

Sense of Security Pty Ltd

Sydney

Level 8, 66 King Street
Sydney NSW 2000
Australia

Melbourne

Level 15, 401 Docklands Drv
Docklands VIC 3008
Australia

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455

info@senseofsecurity.com.au
www.senseofsecurity.com.au
ABN: 14 098 237 908

App Virtualisation vs
VirtualMachines

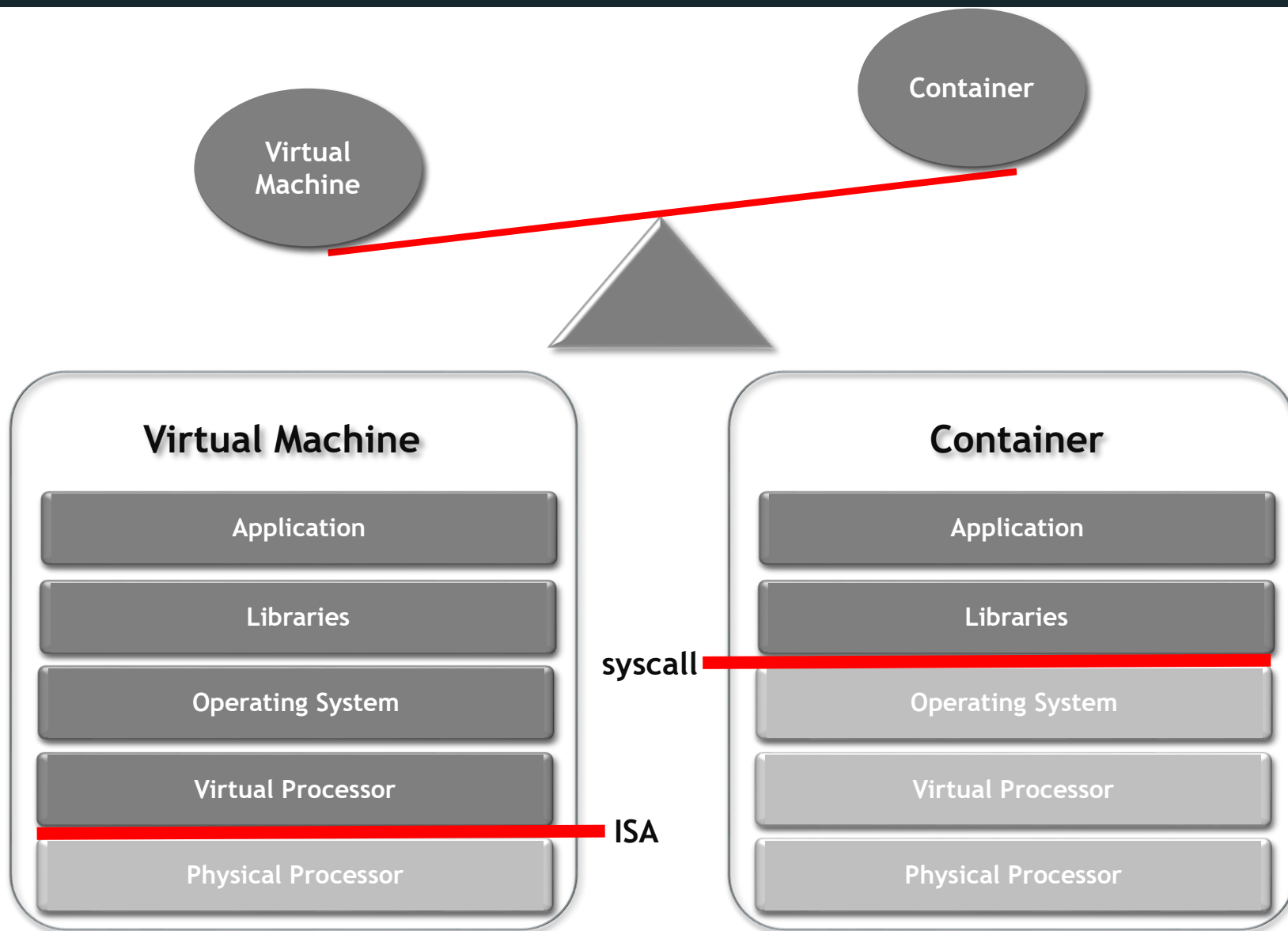
Why Containerised Apps?

Key Steps to Container Security

Vuln Mgt, Risk Mgt & Compliance

- ❖ Control Groups(cgroups)
- ❖ Namespaces
- ❖ Capabilities
- ❖ Seccomp
- ❖ Linux Security Mechanisms
- ❖ The Docker daemon

VM's < -- > Containers

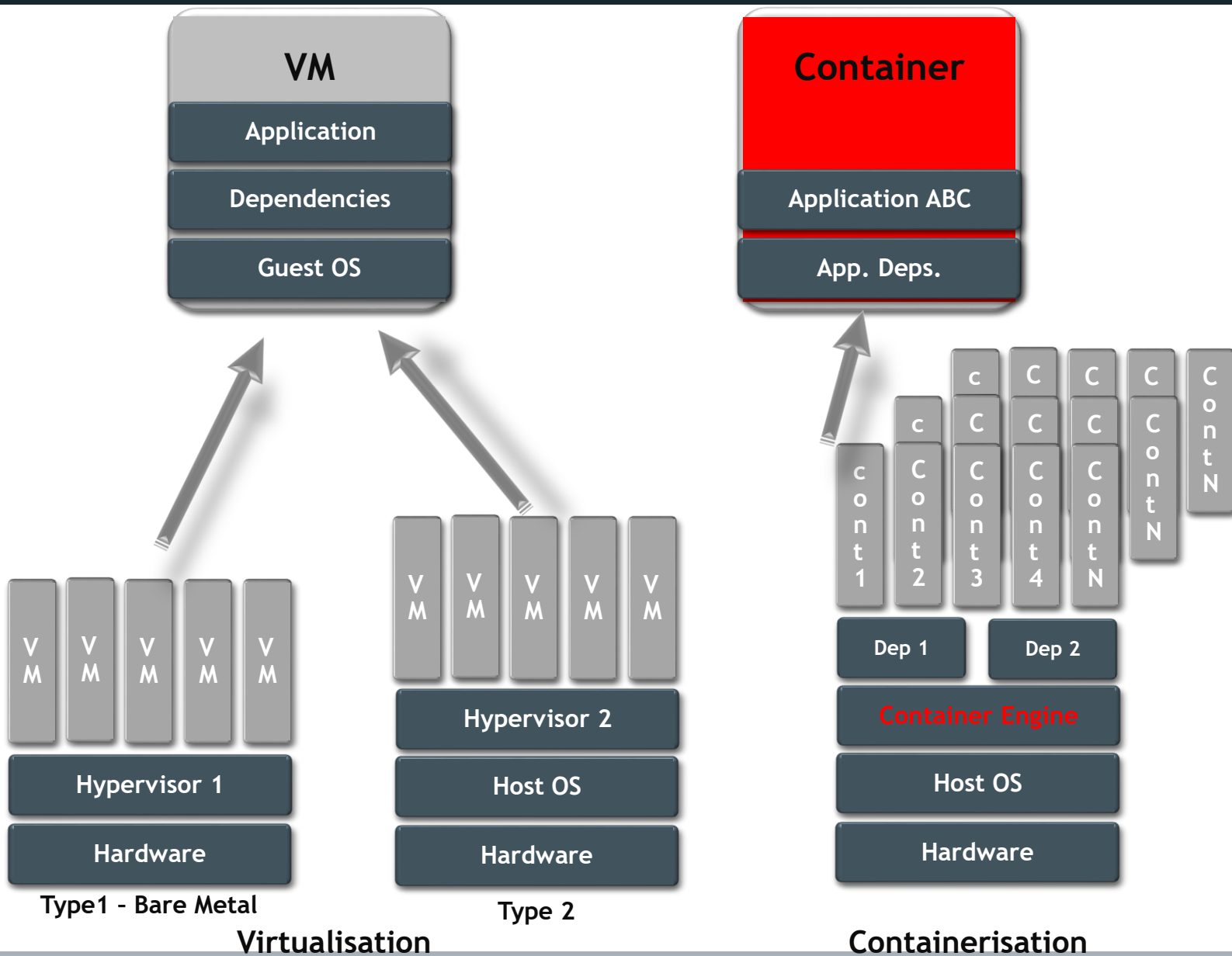


From: <http://www.weblaminar.com/index.php/technologies/docker-container>

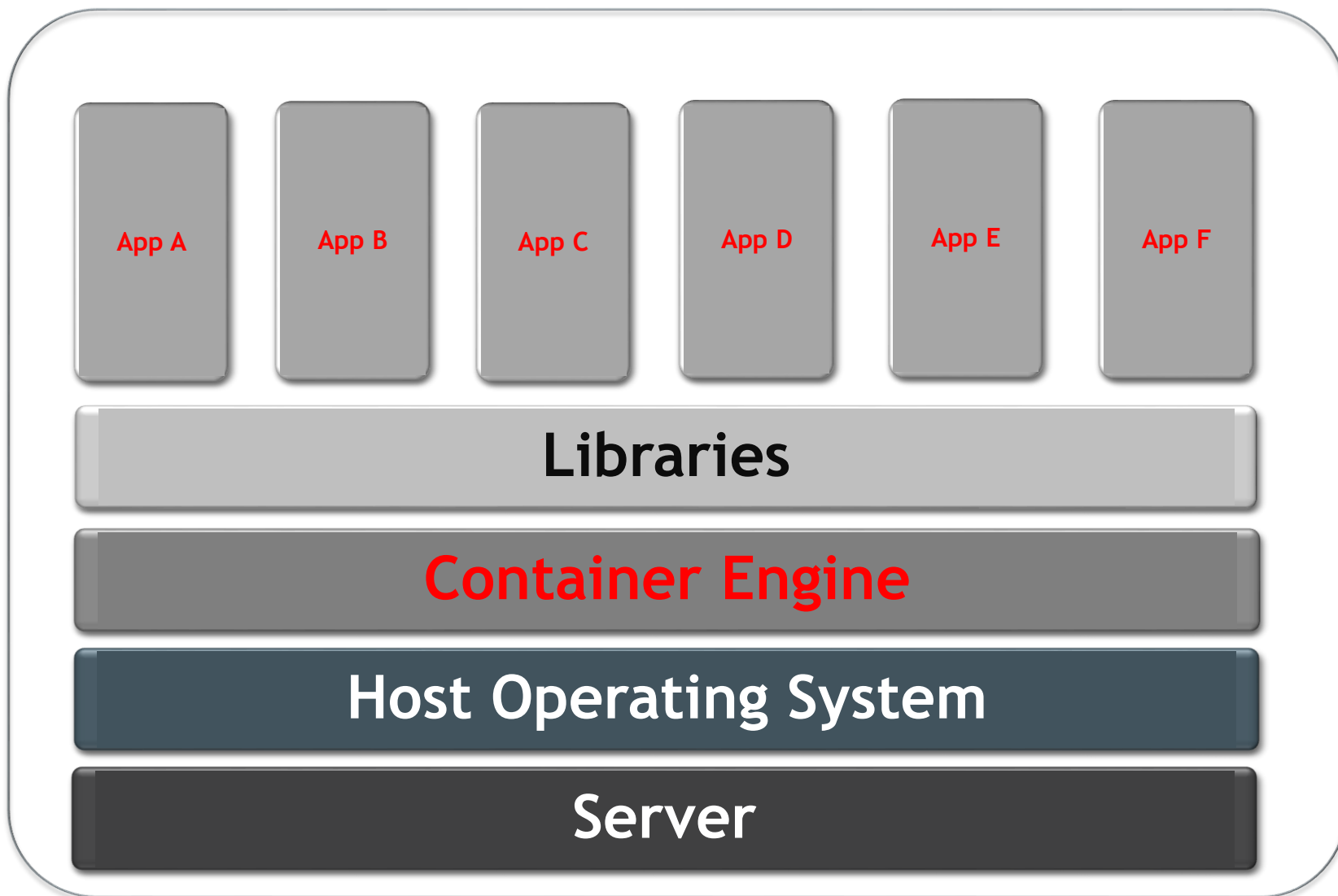
Why App Containers?

Speed	System Kernel is common Very fast to load and operate
Contained & Repeatable	All dependencies mounted ->Repeatable Separate Execution Environment for Multiple containers on single OS
Attack Surface Reduction	Lightweight Incorporate only parts you need
Control	Finer-grained execution environments
Lifecycle	Ease of integration into DevOps SDL Multiple Orchestration Platforms
Support	All Major OS's All Major Hosting Providers

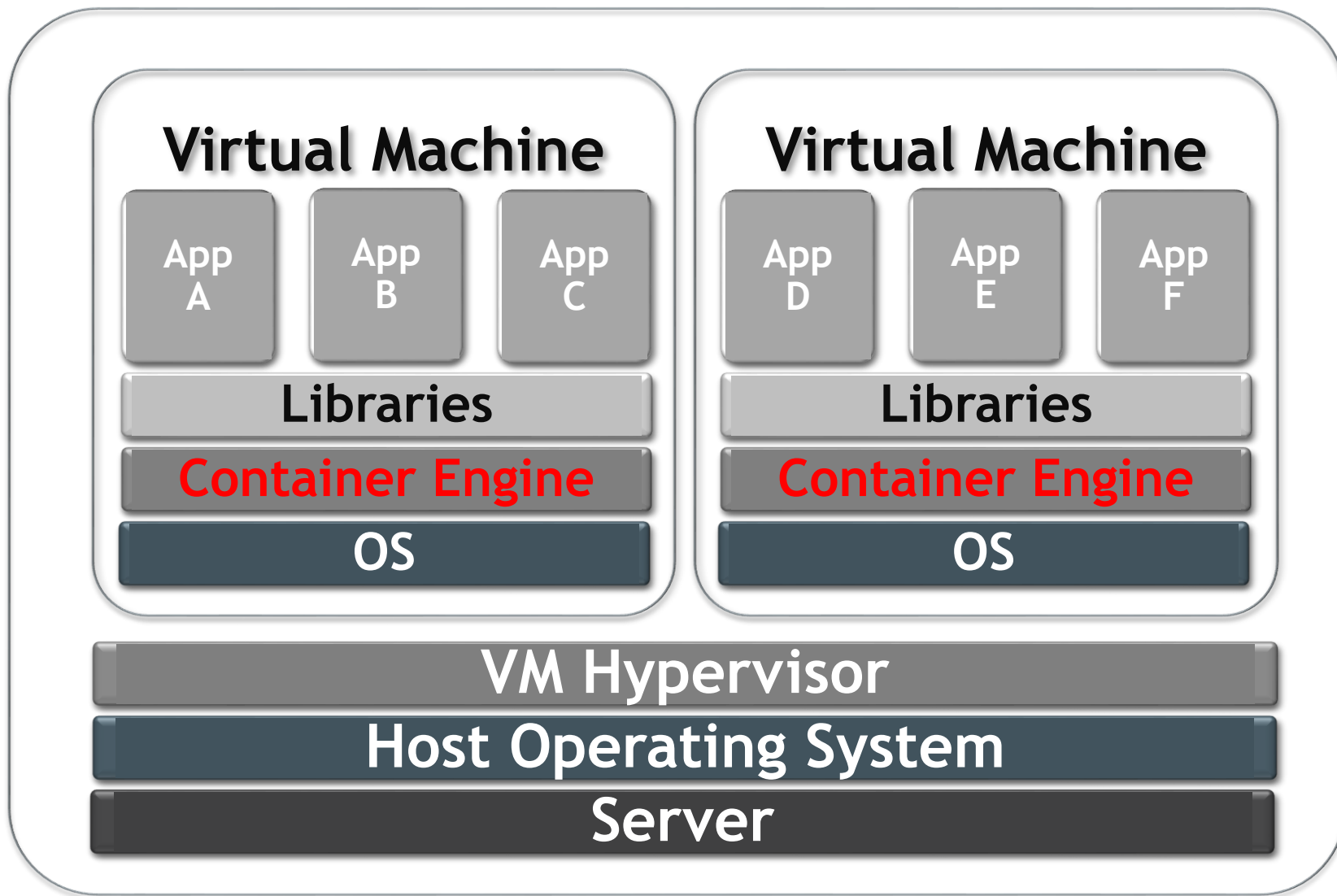
VM vs. Containers



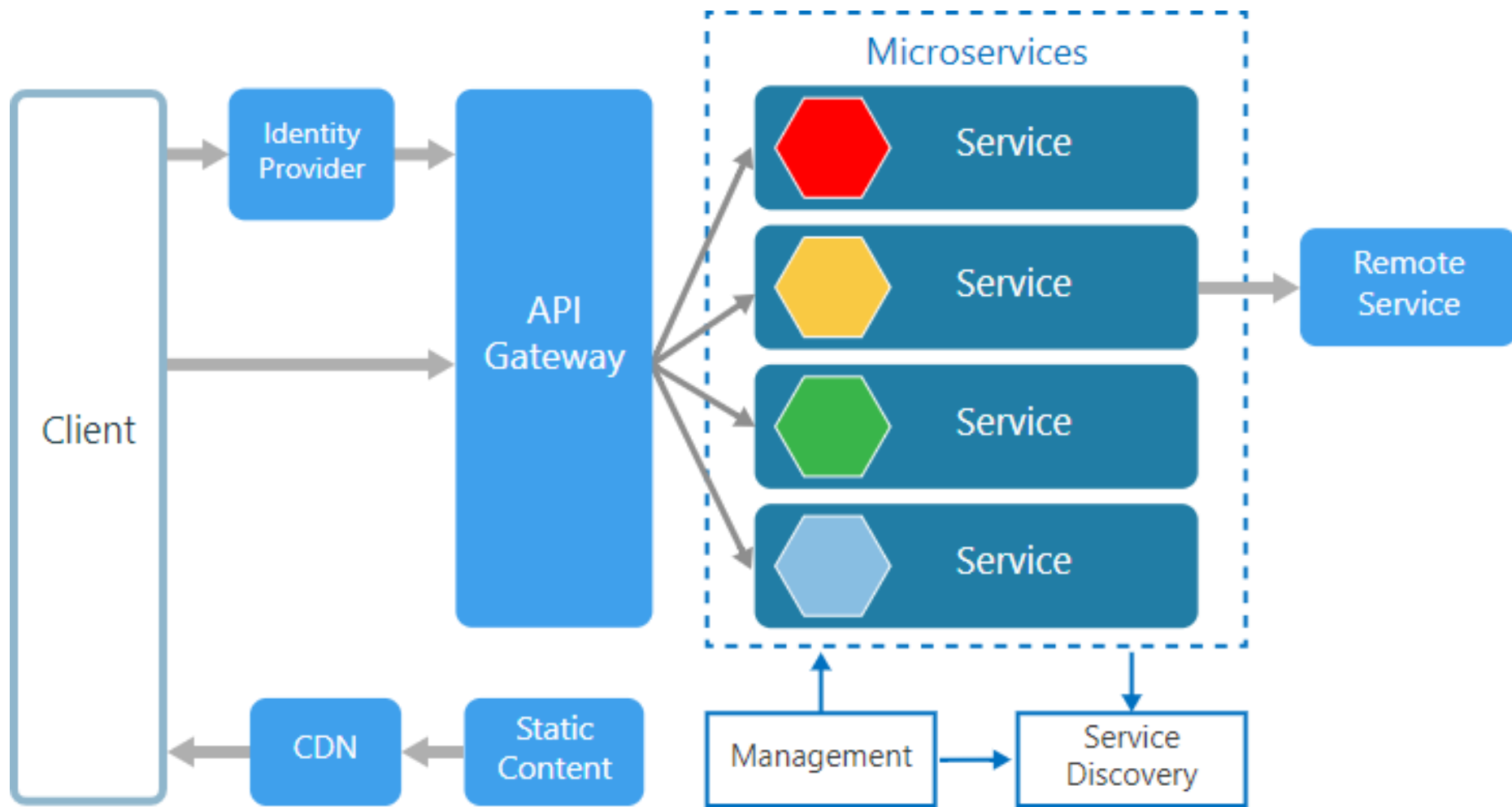
Containers On Bare Metal Server



Containers on VM's or Instances



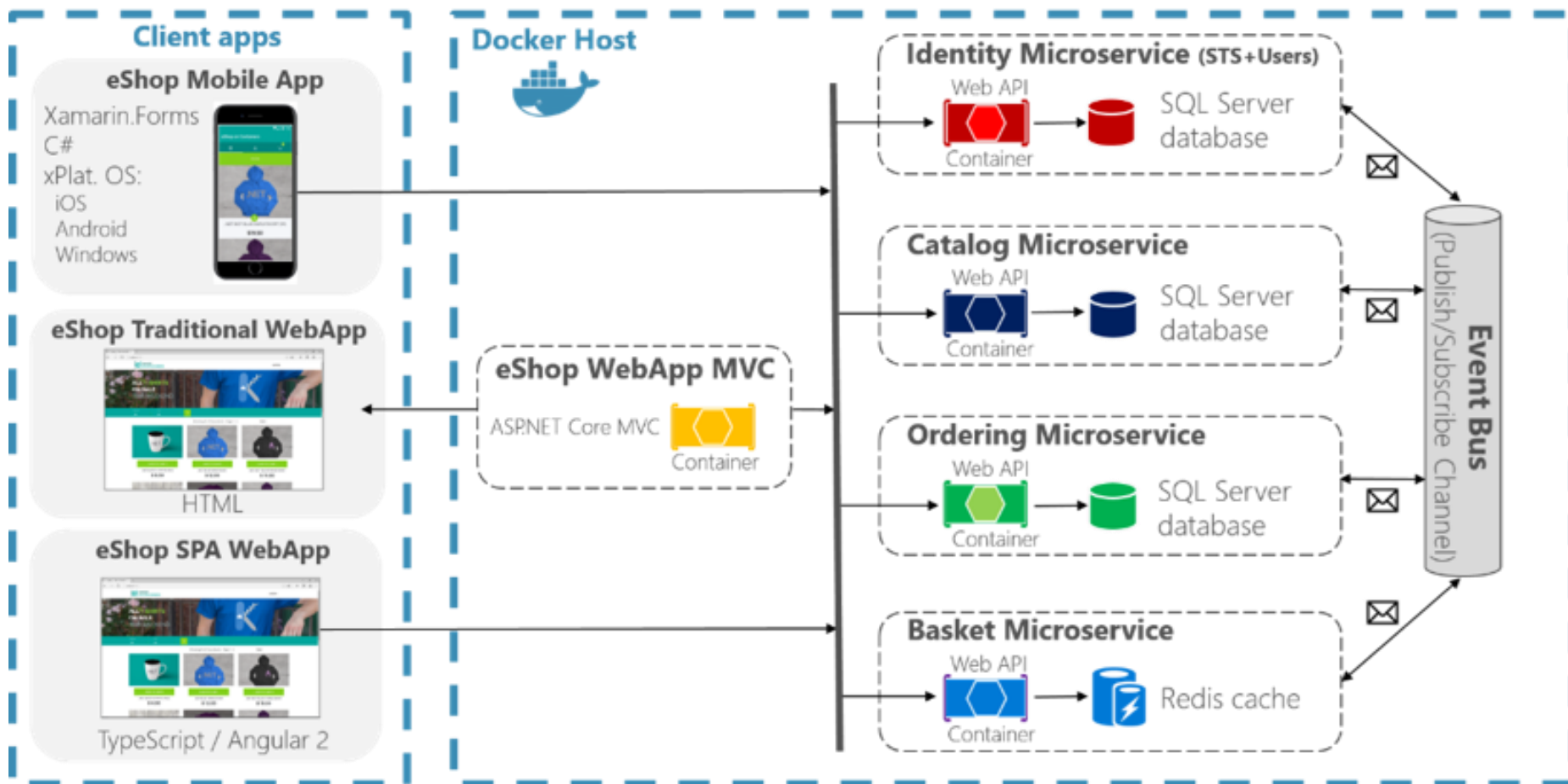
Microservices Architecture



<https://docs.microsoft.com/en-us/azure/architecture/guide/architecture-styles/microservices>

“eShopOnContainers” Reference Application

Microservices Architecture



IaaS	CaaS	PaaS	FaaS	
Functions	Functions	Functions	Functions	Customer Managed
Application	Application	Application	Application	Customer Managed Unit of Scale
Runtime	Runtime	Runtime	Runtime	Abstracted by Vendor
Container (Optional)	Container	Container	Container	
Operating System	Operating System	Operating System	Operating System	
Virtualization	Virtualization	Virtualization	Virtualization	
Hardware	Hardware	Hardware	Hardware	

<https://qph.ec.quoracdn.net/main-qimg-73dd2f0d9438e512525fc1608224dc79>

CaaS

Functions

Application

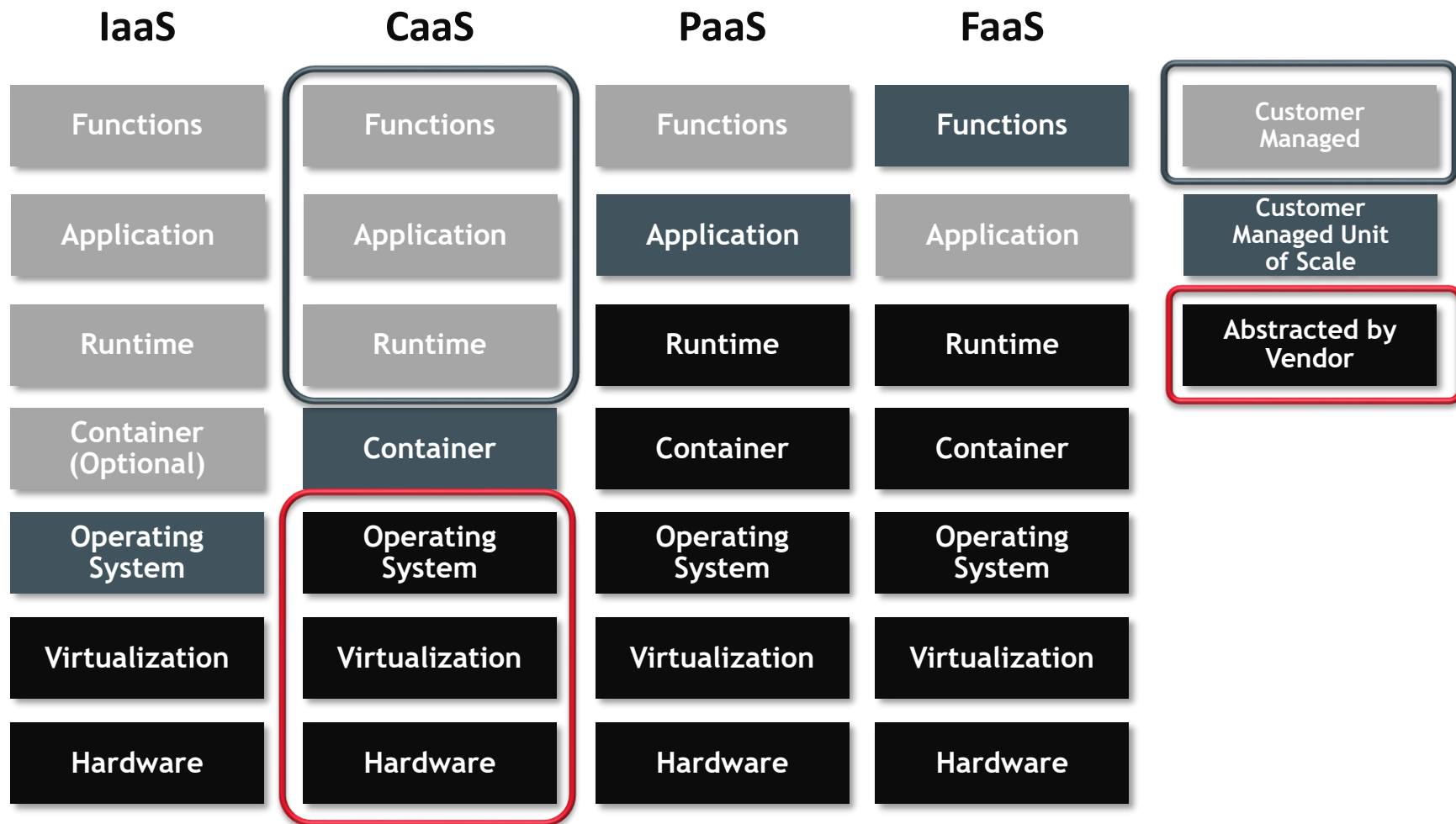
Runtime

Container

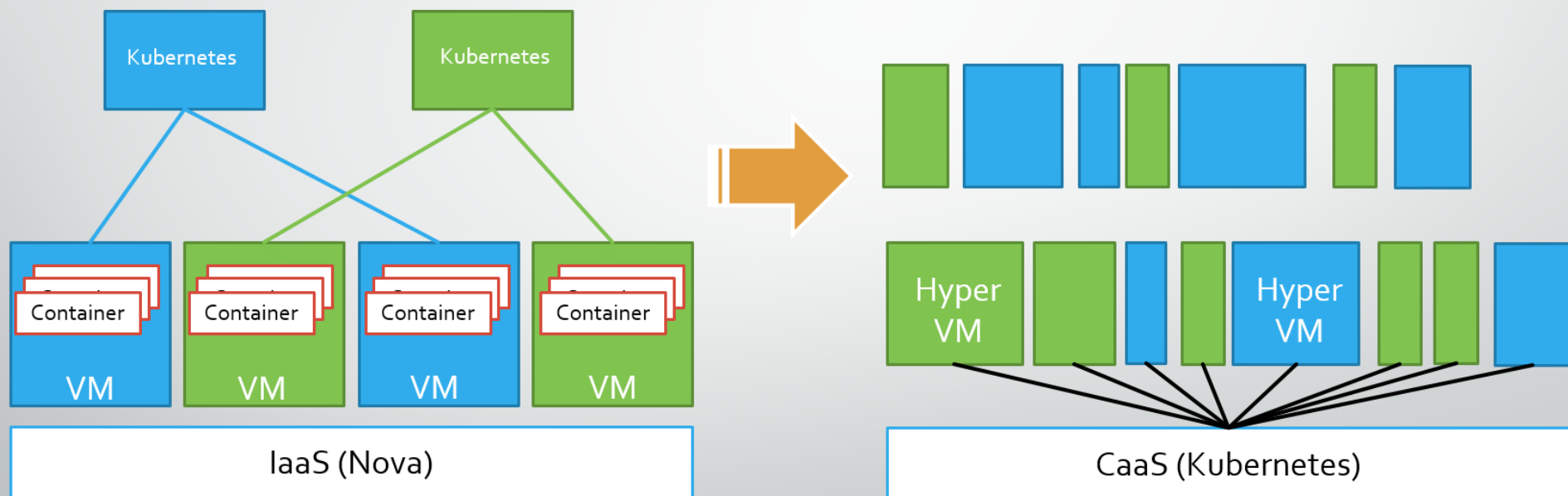
Operating System

Virtualization

Hardware



Hypernetes: Multi-tenant Container-as-a-Service



What Hypernetes does?

Hypernetes envisions a future of ******"Container-as-a-Service without IaaS"******. The idea is to combine the orchestration power in Kubernetes and the **runtime isolation in Hyper** to build the truly secure multi-tenant CaaS platform.

What is Hypernetes?

Hypernetes is a secure, multi-tenant [Kubernetes](#) distro. Simply put,

Hypernetes = Bare-metal + [Hyper](#) + Kubernetes + [KeyStone](#) + [Cinder](#) + [Neutron](#).

[Hyper.sh](#) is a secure container hosting service. '

ON-DEMAND CONTAINER. PER-SECOND BILLING

OpenStack Keystone

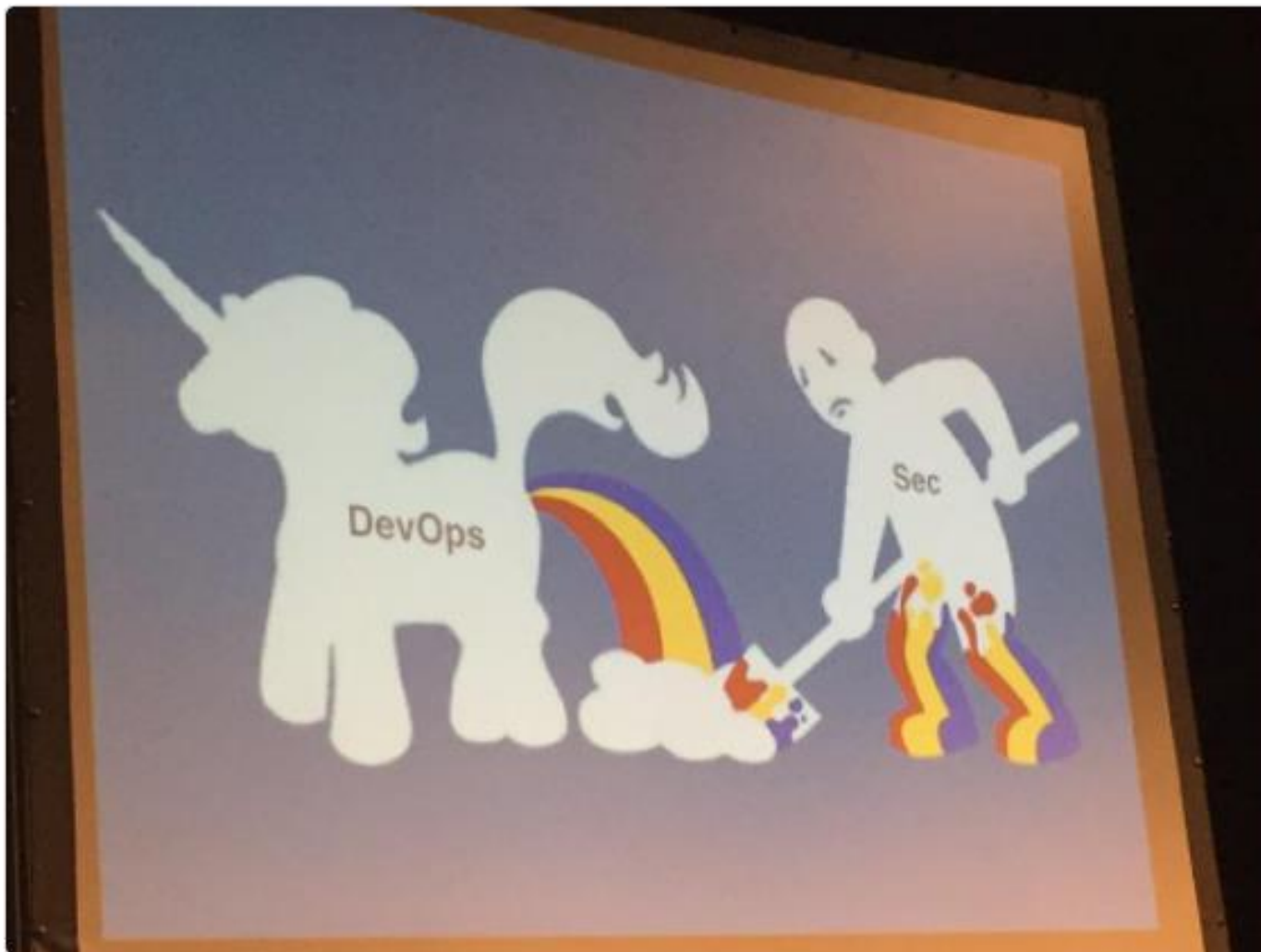
Keystone provides authentication, authorization and service discovery mechanisms via HTTP primarily for use by projects in the OpenStack family. It is most commonly deployed as an HTTP interface to existing identity systems, such as LDAP.

What Hypernetes does?

Hypernetes envisions a future of ****"Container-as-a-Service without IaaS"****. The idea is to combine the orchestration power in Kubernetes and [the runtime isolation in Hyper](#) to build the truly secure multi-tenant CaaS platform.

Containers Solve Everything?

Pete [@petecheslock](#) just won the internet with this. [#devopsdays](#)



DevOps is Agile

So we need to address

End-to-End Security

Security @ Source (Static)

&

Run Time Security (Dynamic)

1	End-to-End Vulnerability Management
2	Container Attack Surface Reduction
3	User Access Control
4	Hardening the Host OS & the Container
5	SDLC Automation (DevOps)

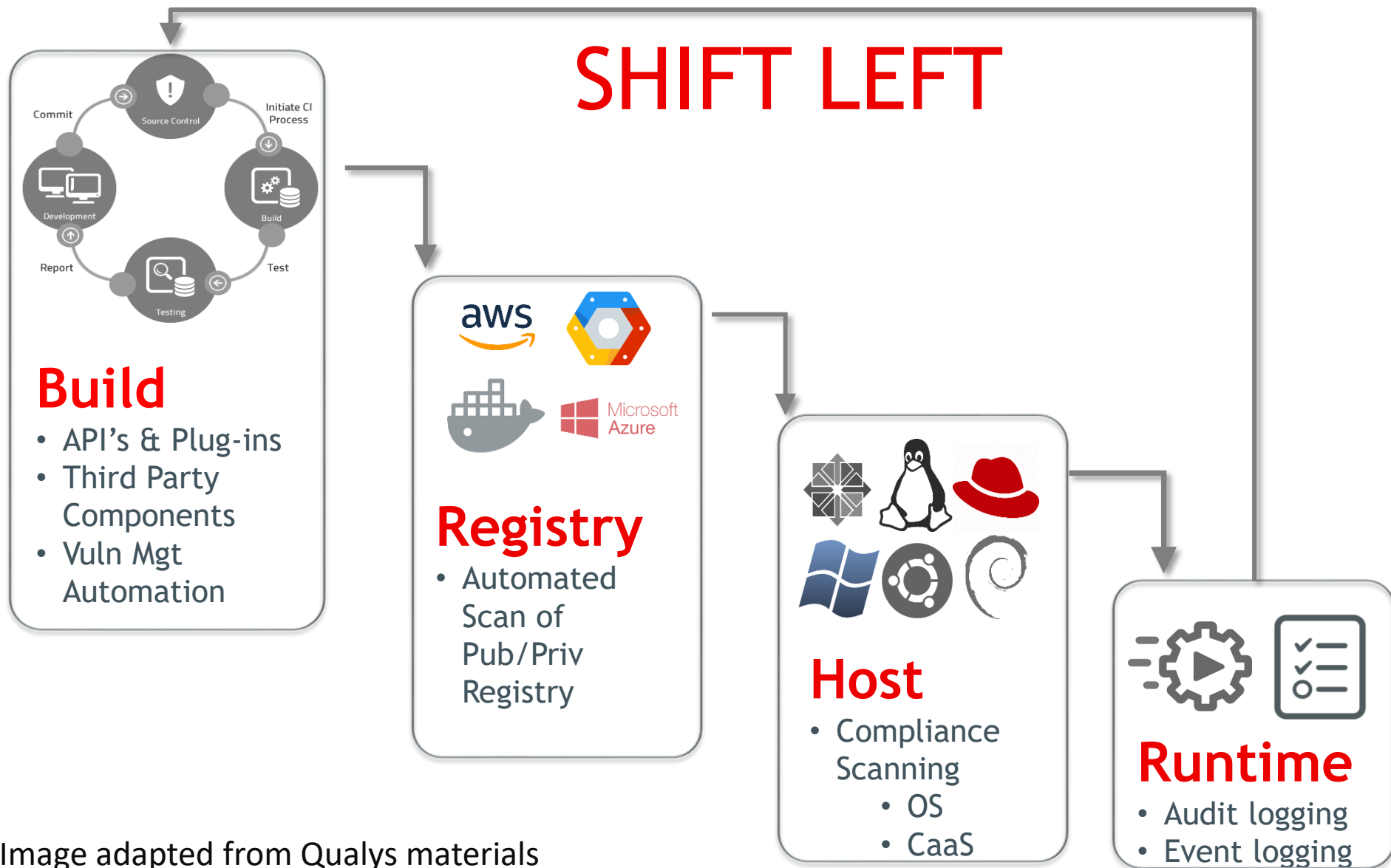


Image adapted from Qualys materials

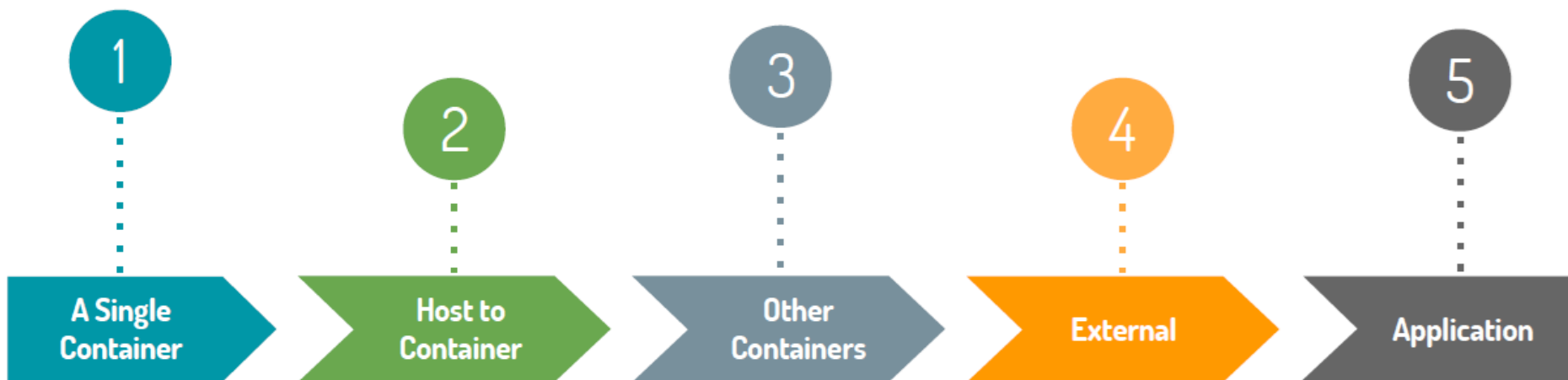
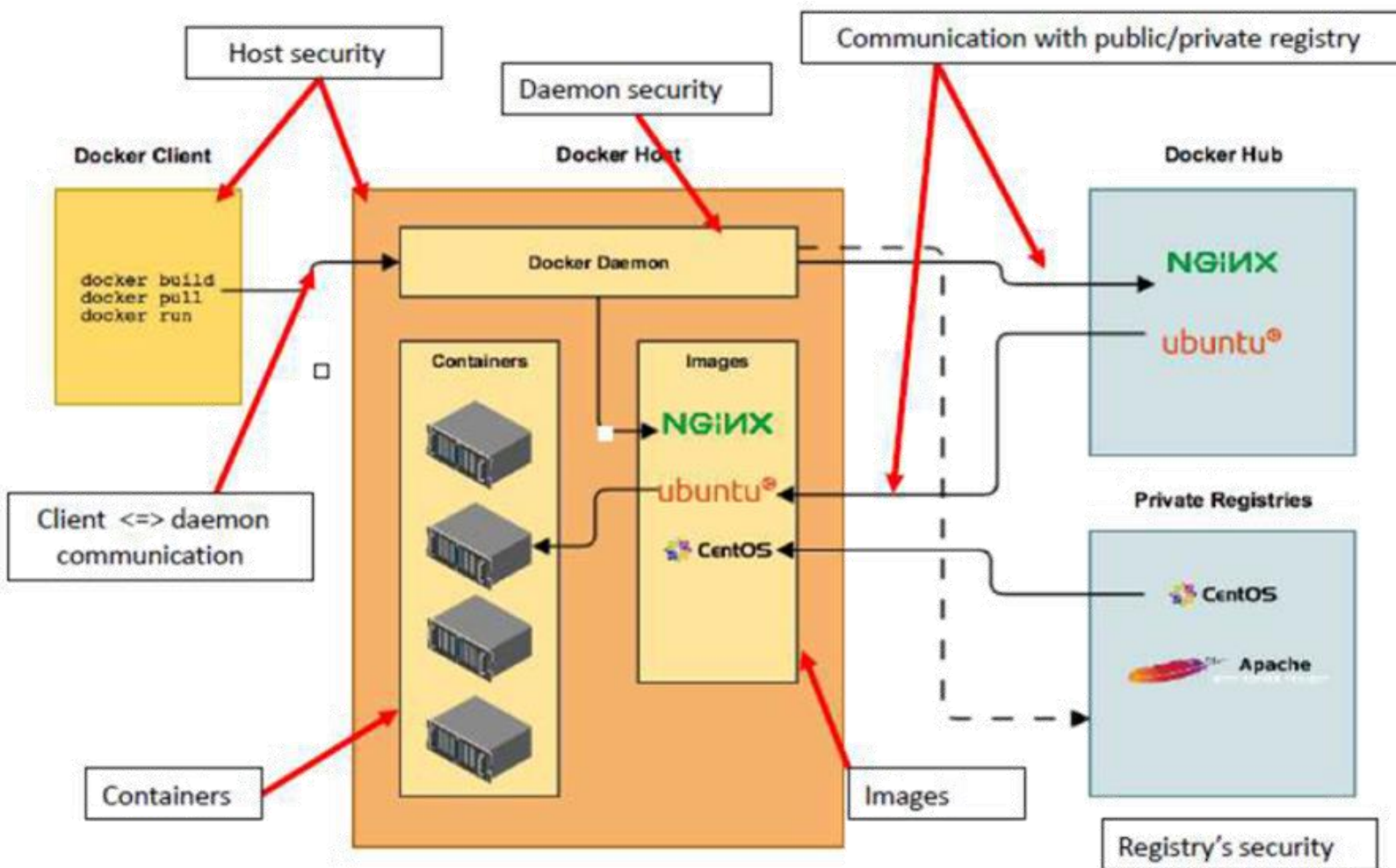



Image by: Phil Estes, Container Security, Everything You Probably Should Know, Docker London 2016

Sec/Vuln Injection Points



Container Security Goals




Discovery & tracking across scale and sprawl



Effective vulnerability management and container-native intrusion detection program



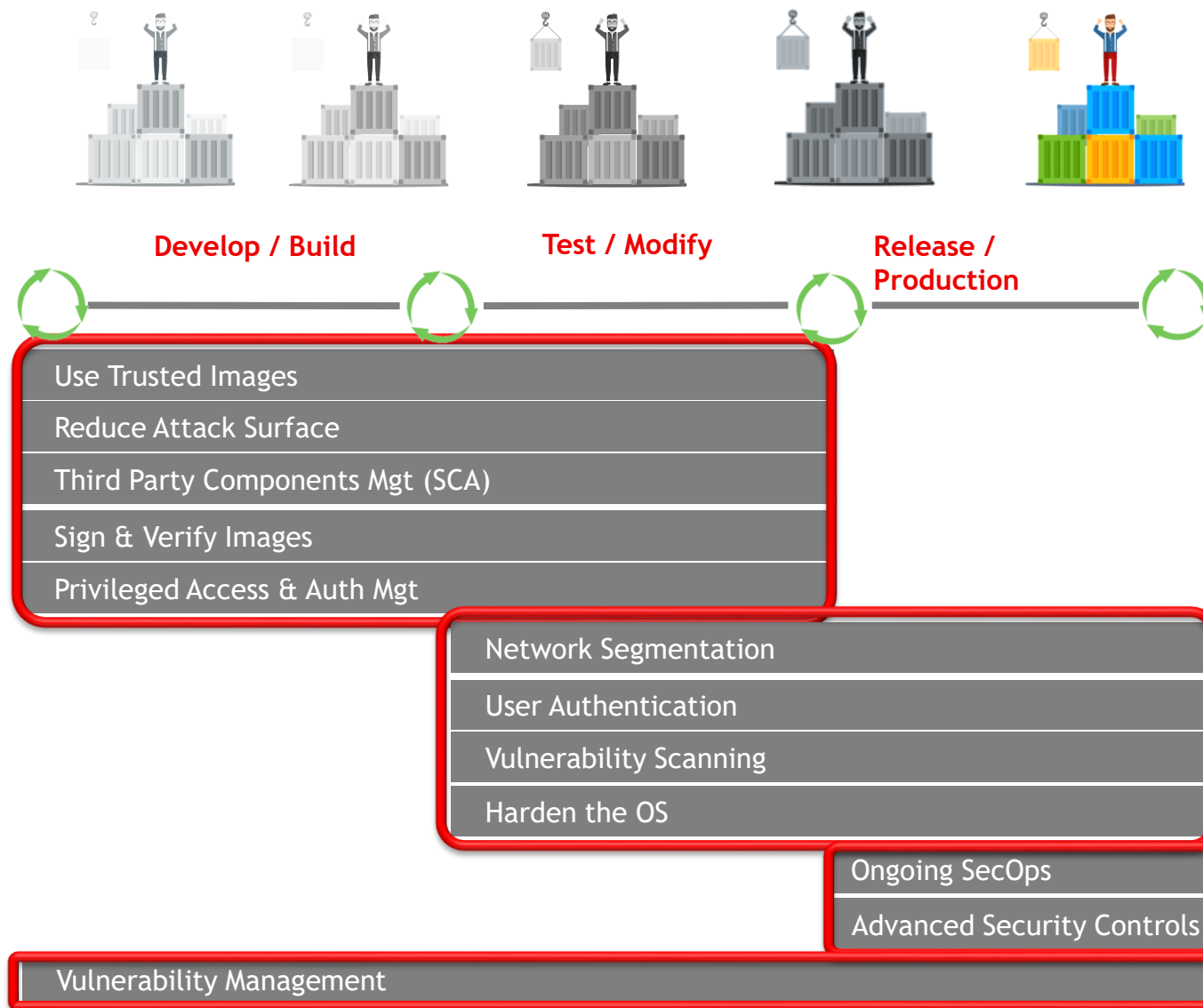
Adaptive security that integrates into modern practices and platforms (DevSecOps)



Update Operational Monitoring, Patching and Incident Response Runbooks

<https://www.qualys.com/apps/container-security/>

Container Security Lifecycle Management & Compliance Summary



Thank you

Head office is level 8, 66 King Street, Sydney, NSW 2000, Australia. Owner of trademark and all copyright is Sense of Security Pty Ltd. Neither text or images can be reproduced without written permission.

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455
info@senseofsecurity.com.au
www.senseofsecurity.com.au