Alibaba Group 阿里巴巴集团 | APSARA CONFERENCE 云栖大会

安全容器的发展与思考

刘奖

阿里云智能资深技术专家

王旭

蚂蚁金服资深技术专家

Kata Containers Arch Committee

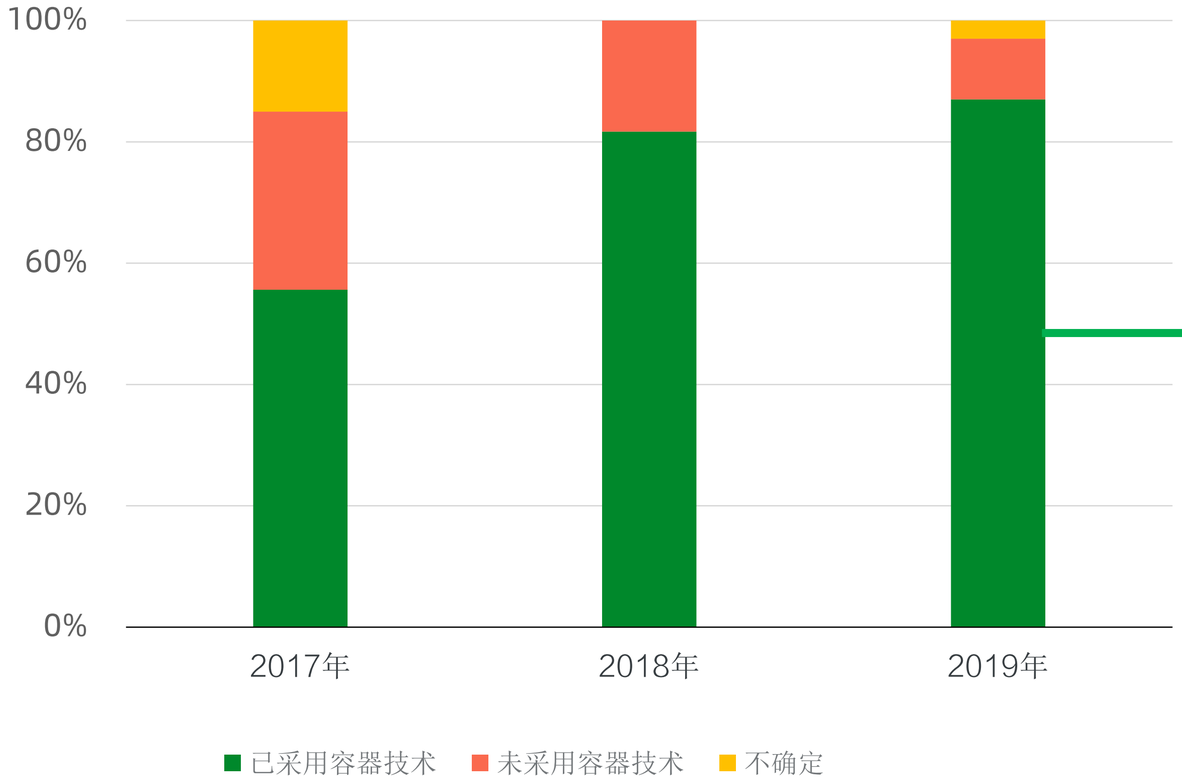
关注“阿里巴巴云原生”公众号
获取第一手技术资料

Contents

目录

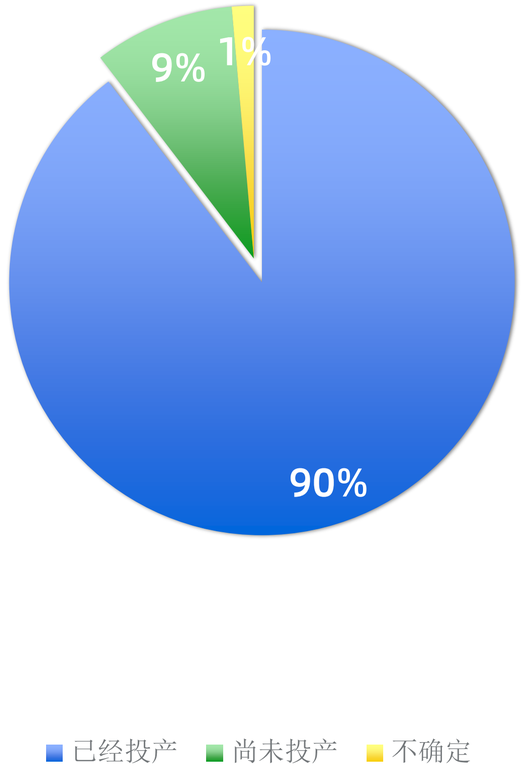
容器技术日渐普及，并快速进入企业生产系统

您的企业是否已经采纳容器技术？



87%

是否已经在生产系统中采用容器技术？

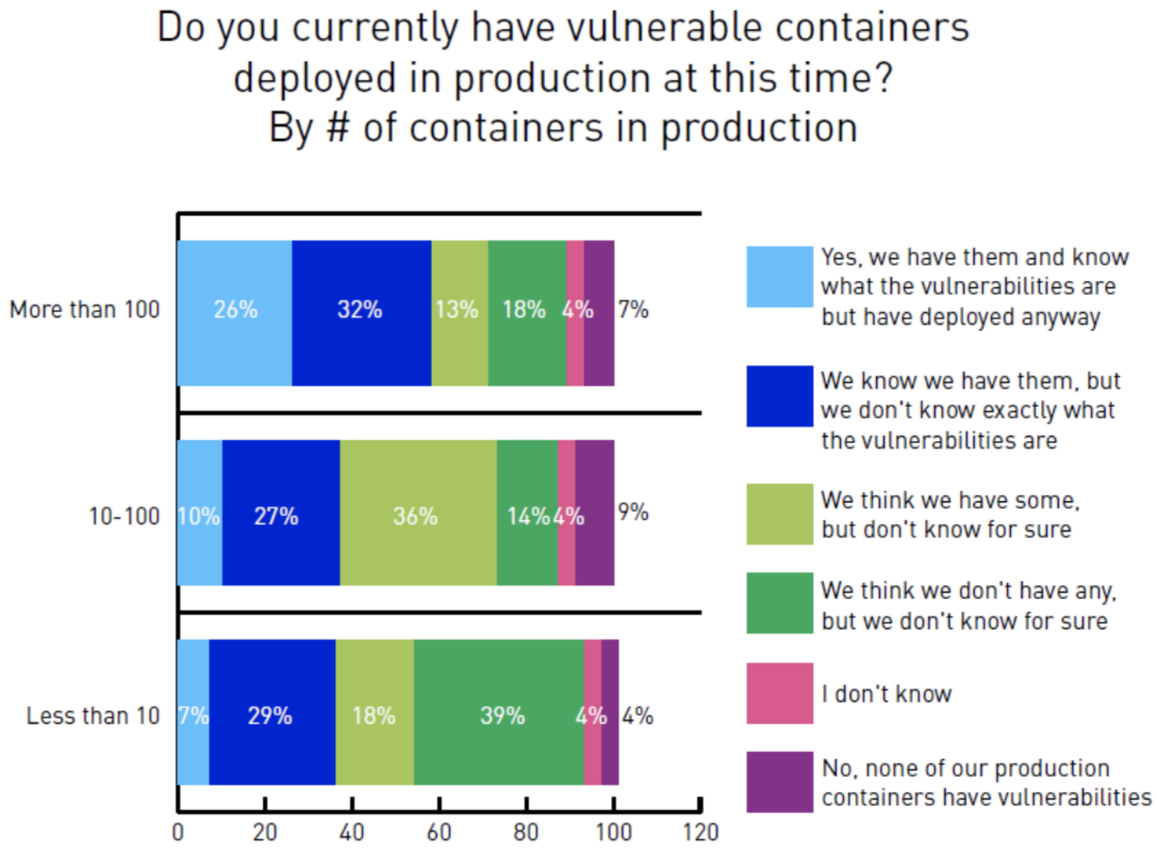


数据源：2019 Container Adoption Survey，Portworx and Aqua Security

企业采用容器技术依然面临安全挑战

42 percent of respondents said that their company has delayed or limited container adoption because of security concerns.

Of the 266 that have containers in production, 47 percent said the containers had vulnerabilities, with that figure rising to 58 percent for those with more than 100 containers in production. The percentage of those that “don’t know” if there are vulnerabilities declines as the number of containers running increases.



https://thenewstack.io/security-worries-rise-as-container-adoption-increases/

端到端的安全容器服务

容器供应链安全

Container Supply Chain Security

基础设施安全

Infrastructure Security

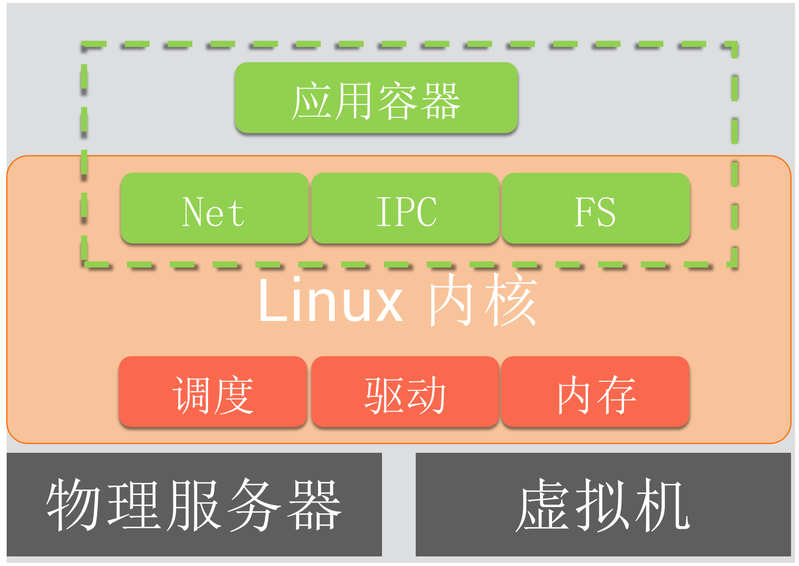
容器运行时安全

Container Runtime Security

Contents

目录

基于Linux共享内核的容器引擎



成也萧何：

方便易用
高性能
低开销

败也萧何：

安全隔离性 不够健壮
性能隔离性 不够健壮
故障隔离域 过大

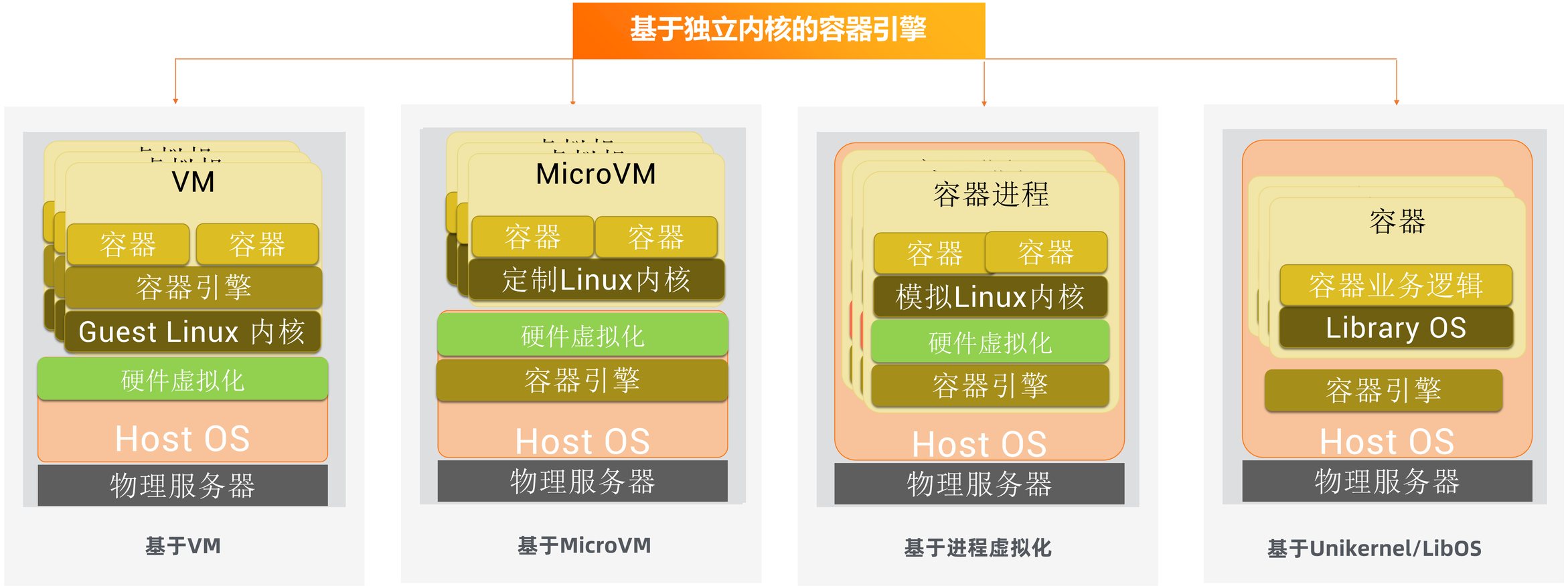
?

行业需要 **高效、安全、稳定、低开销、生态兼容** 的容器引擎

*"The only real **solution to security** is to admit that bugs happen, and then mitigate them by having multiple layers."*

---Linus Torvalds (LinuxCon NA 2015, Seattle)

基于独立内核构建安全的容器引擎



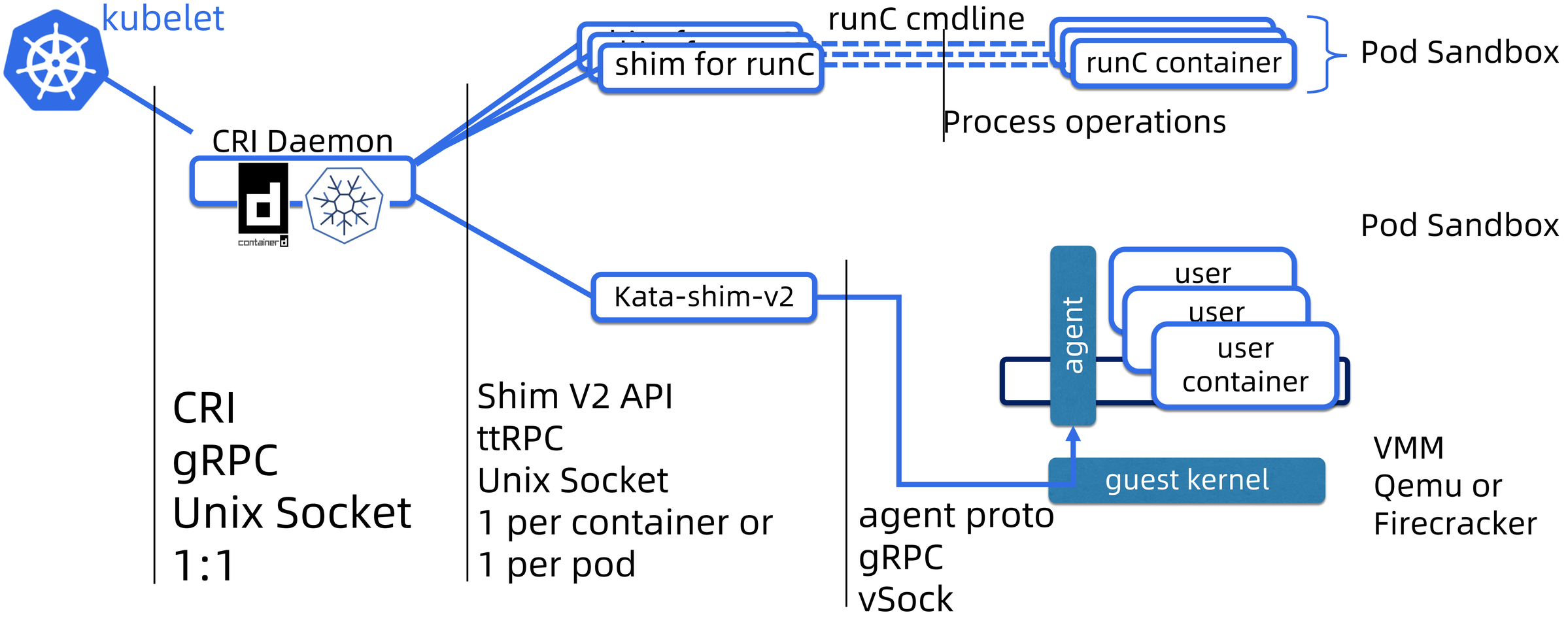
Kata Containers 项目简介

Kata Containers is an open source community working to

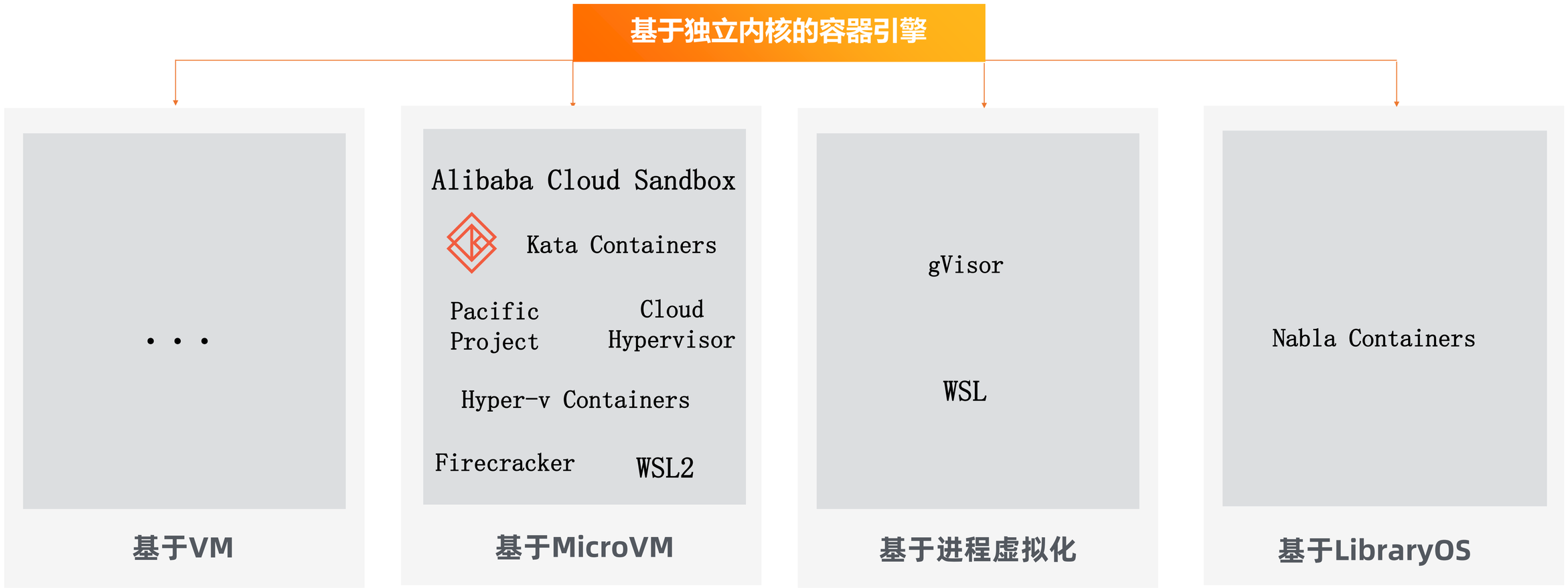
- build a secure container runtime
- with lightweight virtual machines
- that feel and perform like containers,
- but provide stronger workload isolation
- using hardware virtualization technology as a second layer of defense.

OpenStack Foundation旗下的顶级开放基础设施项目；发布于2017年，主要社区贡献者来自于Intel，蚂蚁金服和阿里云，IBM，华为，ARM等

Kata Containers 架构



基于独立内核的安全容器技术方案



阿里云内外安全容器发展历程

2015

播种

开始研发vLinux，利用VM技术运行容器服务

Hyper.sh 创立；runV 开源
Intel 发布 Clear Containers

2016

生根

MaxCompute商用vLinux技术

Hyper.sh 发布基于runV的容器云服务
Kubernetes 引入CRI

2017

萌芽

研发基于VM的安全容器

Azure发布ACI服务
Hyper.sh 与 Intel 宣布 Kata Containers项目

2018

成长

商用基于VM的安全容器
研发Alibaba Cloud Sandbox

Google开源gVisor
AWS开源Firecracker

2019

开花

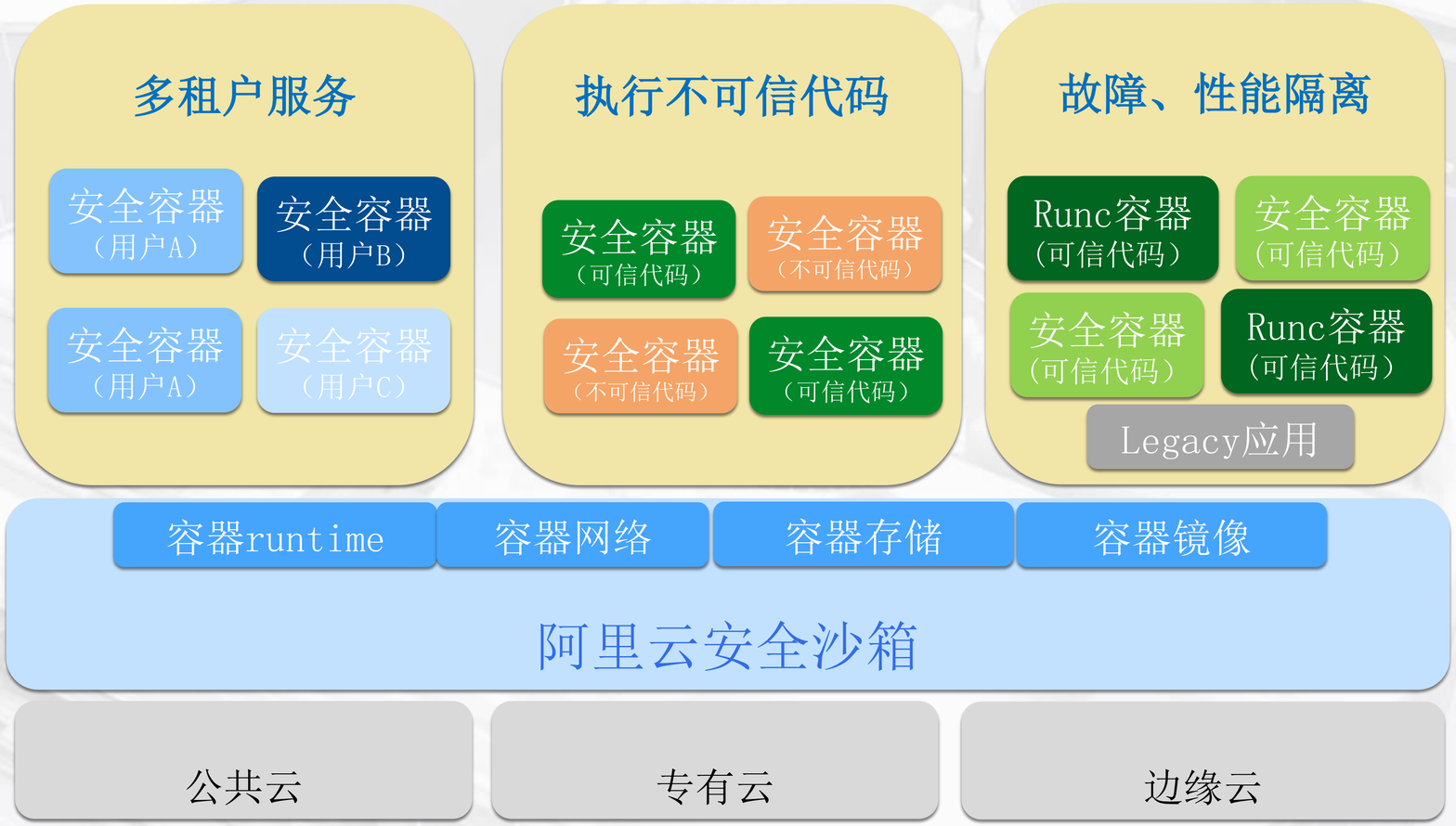
Alibaba Cloud Sandbox商用支持ECI、ACK、SAE、边缘计算等服务

Hyper.sh团队加入蚂蚁金服，和阿里的容器团队一起推进安全容器技术发展

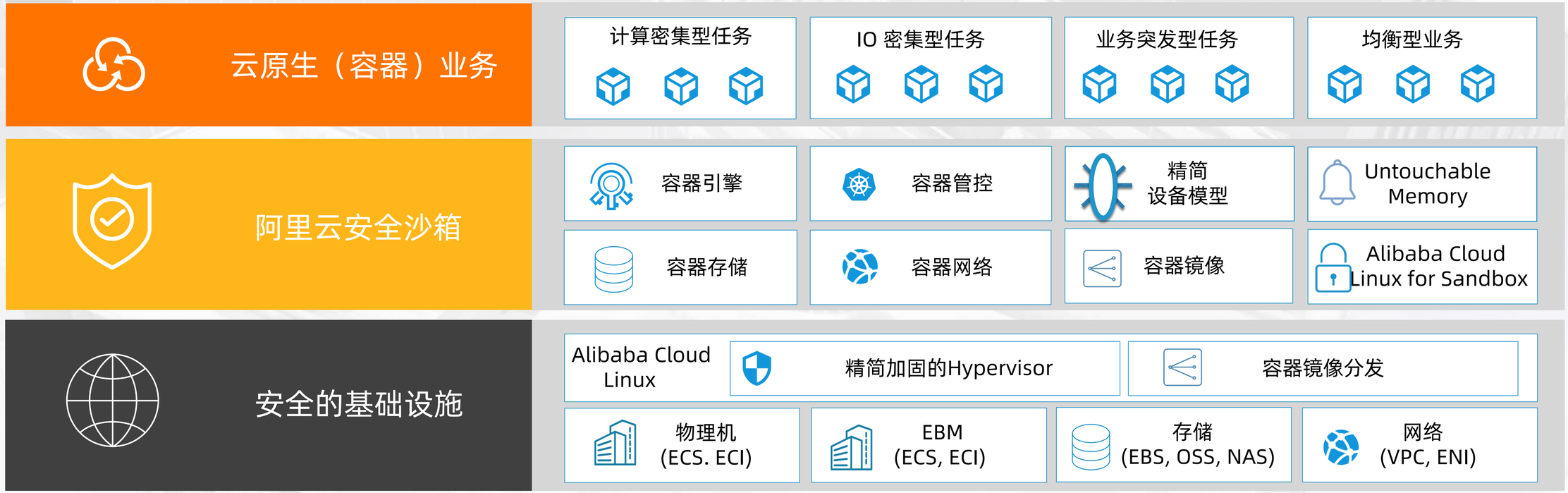
Contents

目录

阿里云安全沙箱支持丰富的业务场景



阿里云安全沙箱软件架构



阿里云安全沙箱技术指标

<500ms

沙箱启动时间

>200/s

并发创建能力

<2.5M

内存开销

Contents

目录

构建理想的安全容器引擎

超越虚拟机的安全性

云服务的多租户

金融服务的强隔离

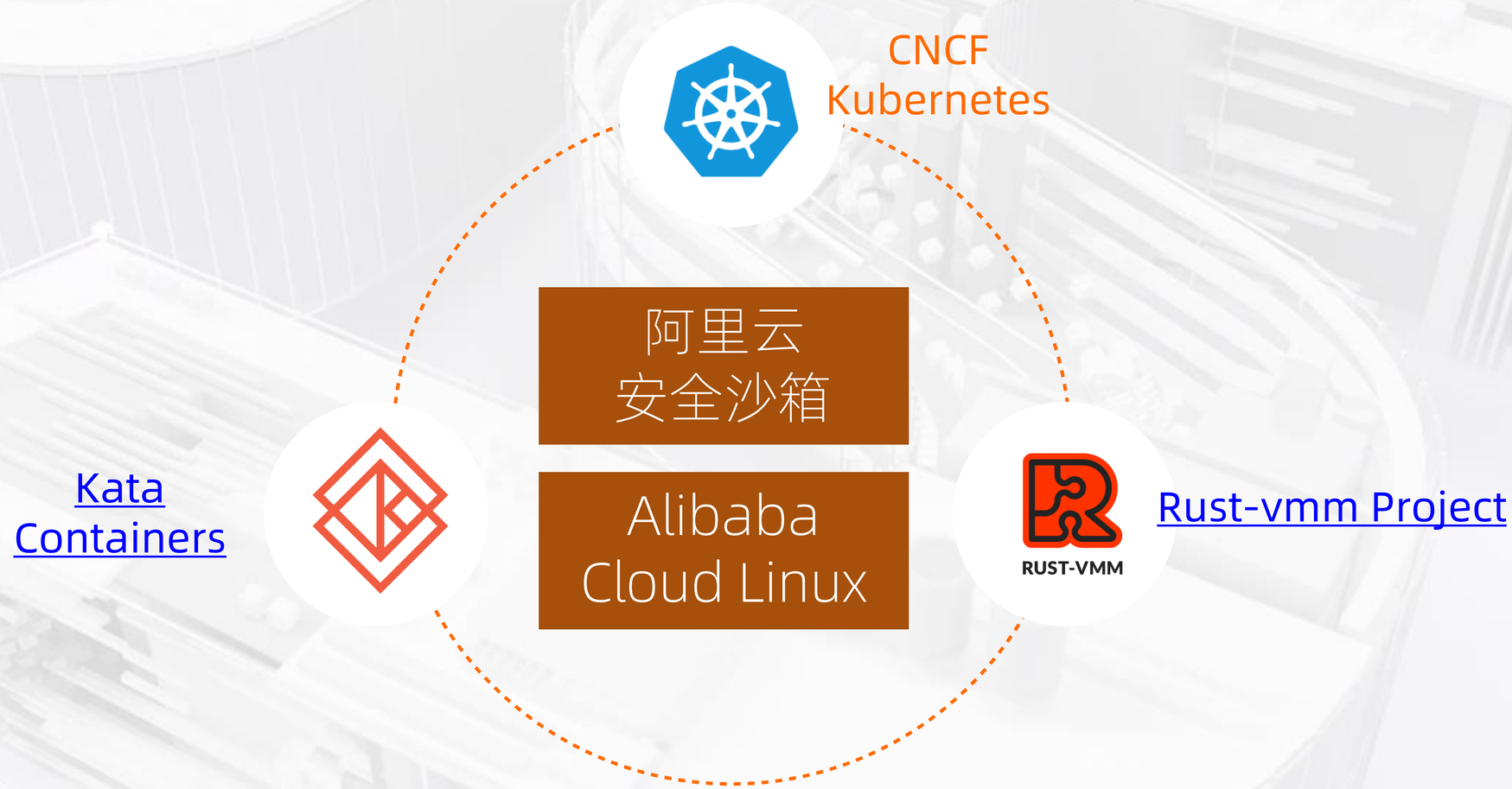
持平runc的性能

全栈优化

无缝对接生态

源于开源、融入开源、贡献开源

合作共建，开放共赢


CNCF
Kubernetes
阿里云
安全沙箱
Alibaba
Cloud Linux
Kata
Containers
RUST-VMM
Rust-vmm Project

Alibaba Group 阿里巴巴集团 | APSARA CONFERENCE 云栖大会

谢谢！

关注“阿里巴巴云原生”公众号
获取第一手技术资料