GOTC

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

OPEN SOURCE , OPEN WORLD

「LF 开源教育及人才培养高峰会」专场

本期议题：容器应用的一体化全流程安全防护实践

叶剑宏 2021年08月01日

云原生人才培养计划 2.0 发布！

- **强强联手，打造最懂开发者的云原生人才课程**

Linux 基金会开源软件学园、阿里云、马哥教育联合出品，从理论基础，到开源实践，再到企业真实落地，各路专家打造最懂开发者需要的云原生人才课程体系

- **由浅入深，引导最适合开发者的云原生学习路径**

遵循云原生人才学习路径及人才发展不同阶段搭建课程体系框架，由浅入深，第一期将帮助云原生人才学习 Kubernetes 完整技术栈内容

- **一课双证，打通云原生人才专业技能认证快速通道**

贯穿理论、实践、体验，为广大云原生领域人才完成 CKA、CKAD、ACA、ACP 等专业认证提供积累专业技能的基础环境，以及相关资格考试优惠福利

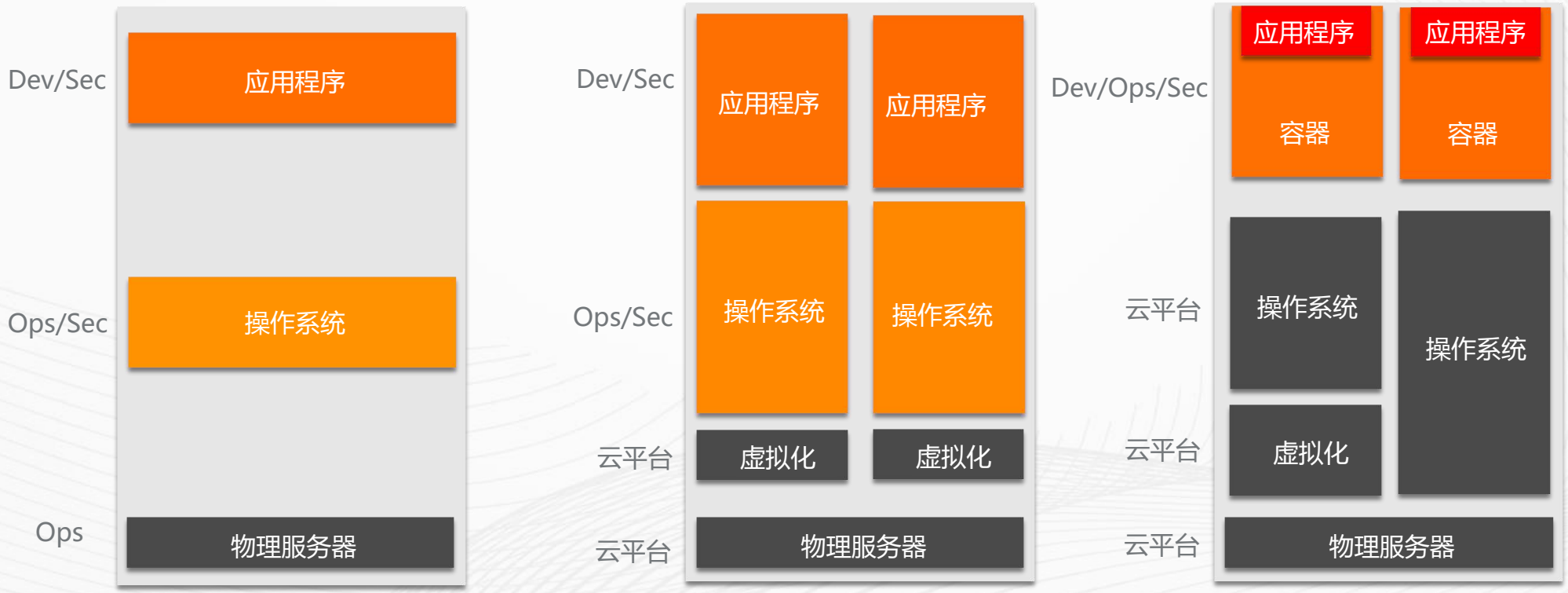
THE LINUX FOUNDATION 开源软件学园 | 阿里云 | 马哥教育

容器对IT基础设施的影响

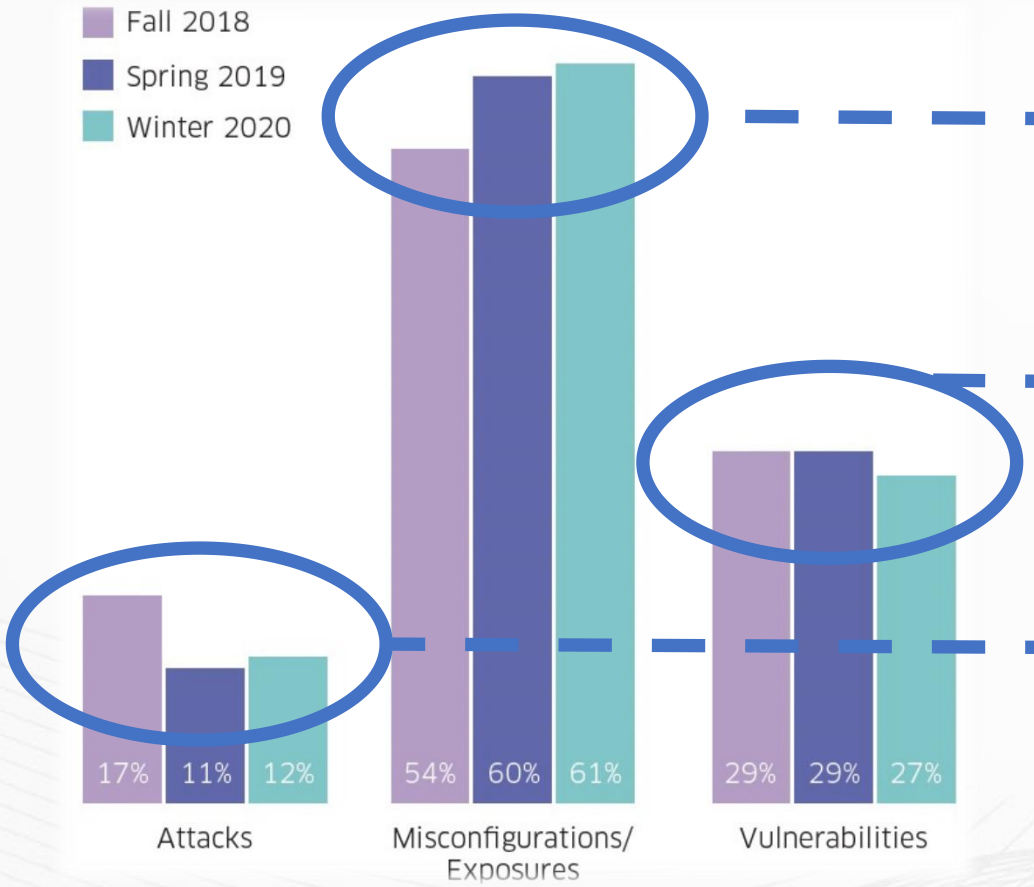
容器环境下IT架构的变化

基础架构

IT架构



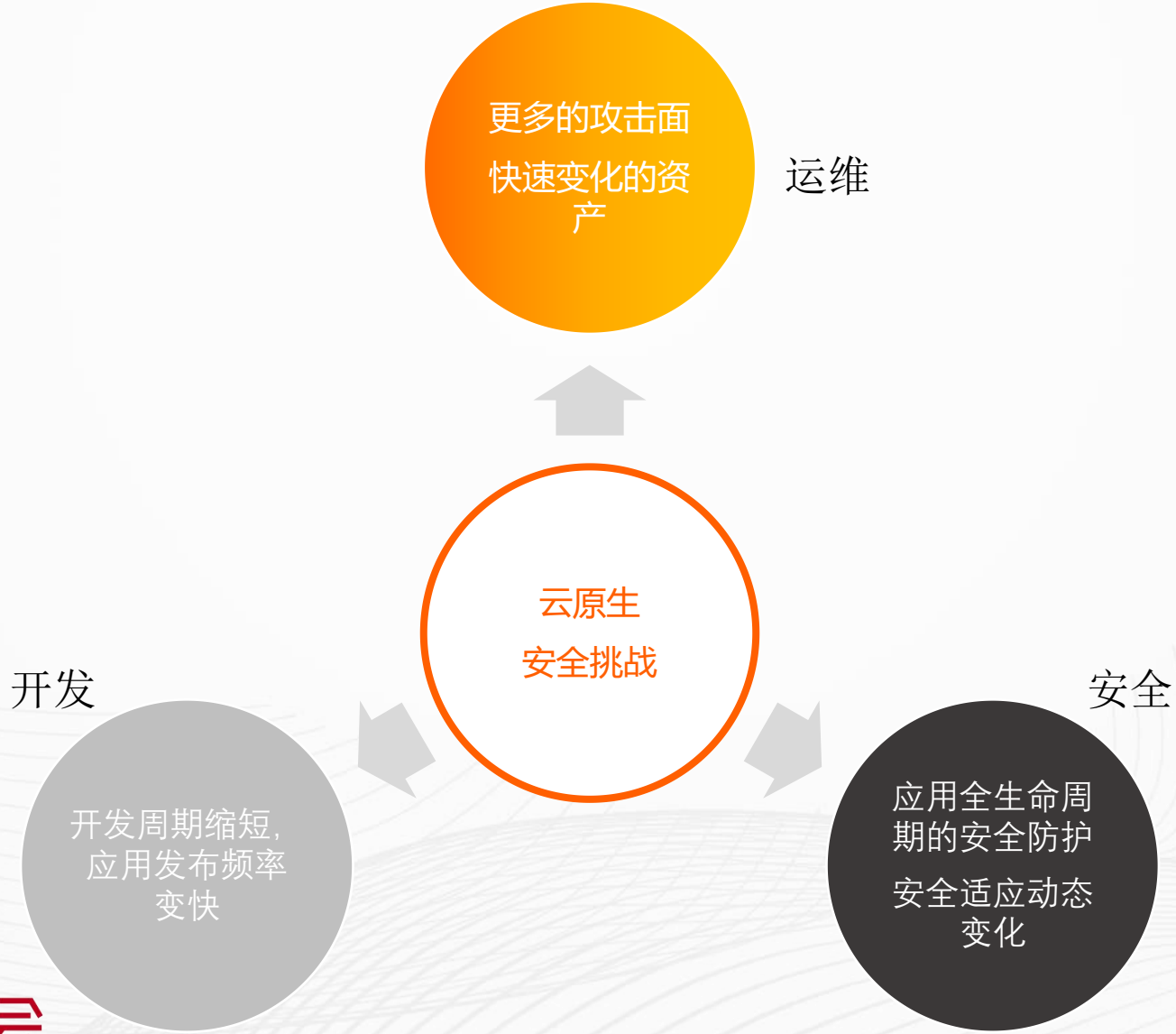
企业面临的容器安全风险



主要风险	威胁举例
配置安全	Docker.sock暴露到公网 容器挂载宿主机敏感目录 K8s API Server未授权访问
镜像安全	黑客上传恶意镜像 存在安全漏洞的系统和软件 中间人攻击篡改镜像
运行安全	特权漏洞导致的权限提升漏洞 恶意特权容器的启动

《The State of Container and Kubernetes Security》
——2020 Winter StackRox

云原生容器对开发者、运维、安全的挑战



端到端的云原生容器安全架构

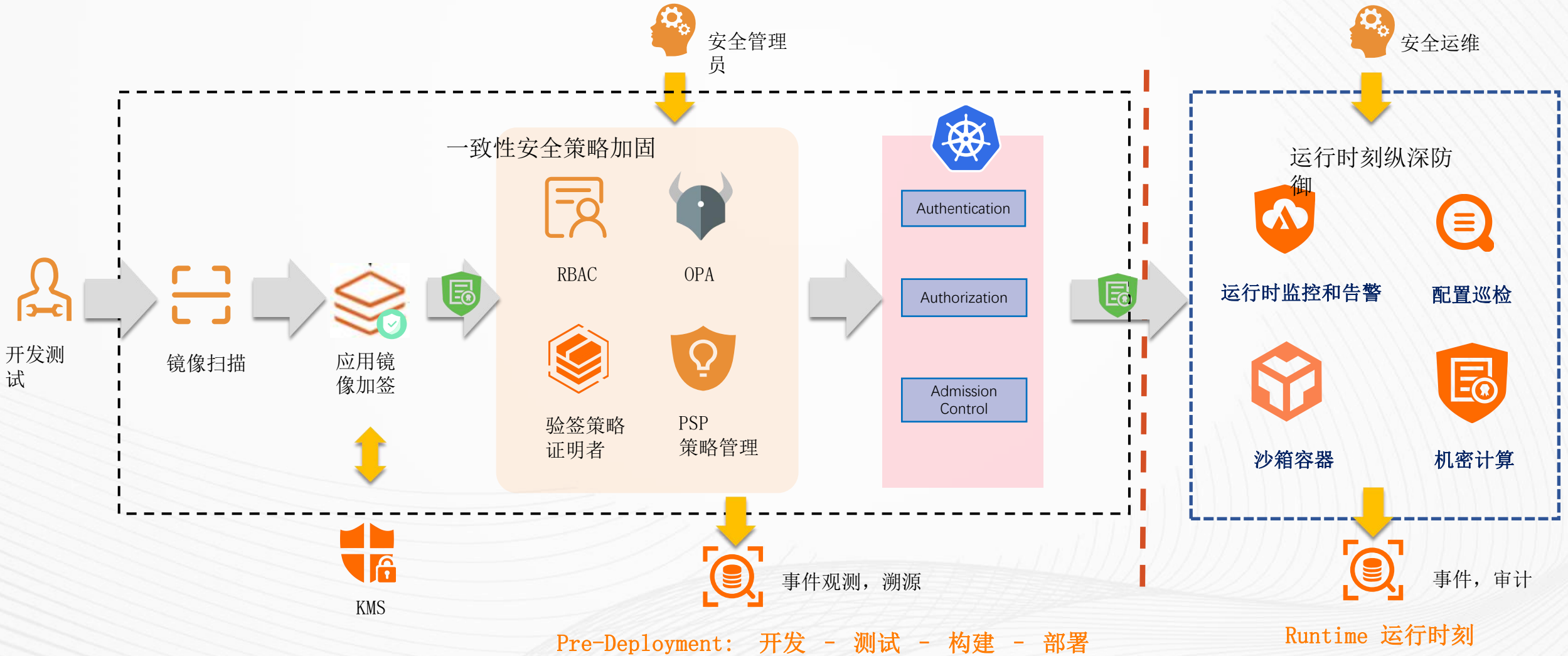
纵深防御

构建从供应链到运行时的一体化安全流程

最小化攻击面

安全稳定的容器基础设施平台

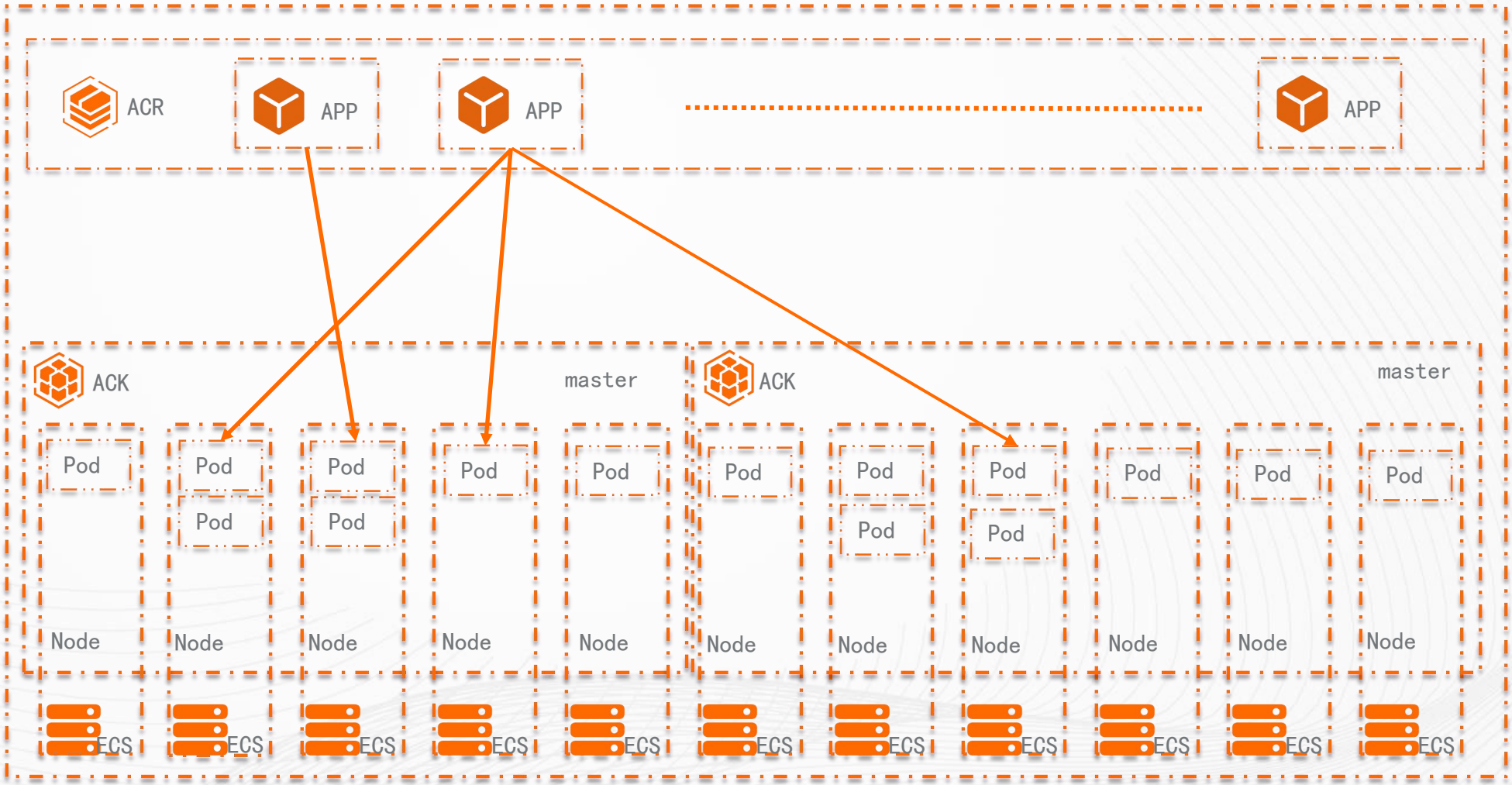
云原生应用生命周期安全能力



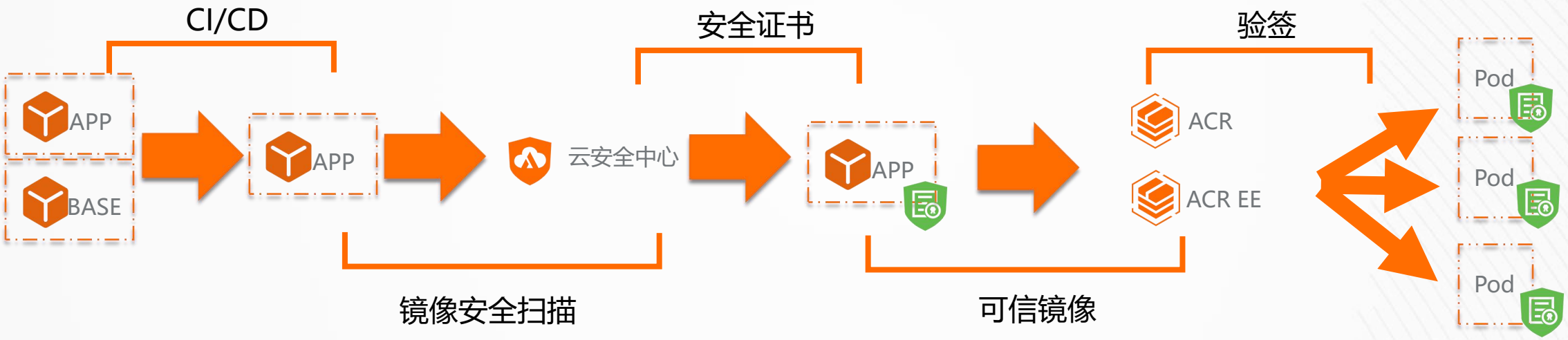
容器资产识别与关联

GOTC

- 镜像监控
- 容器集群弹性监控
- 宿主主机监控
- 识别与关联



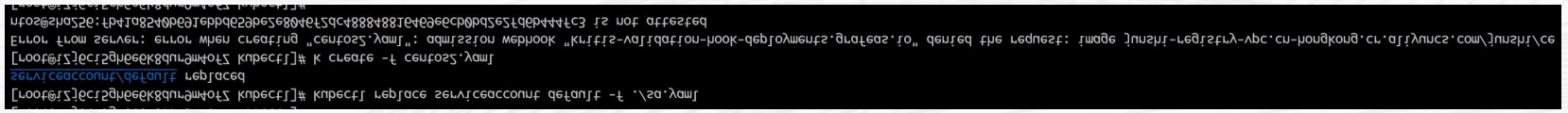
镜像安全



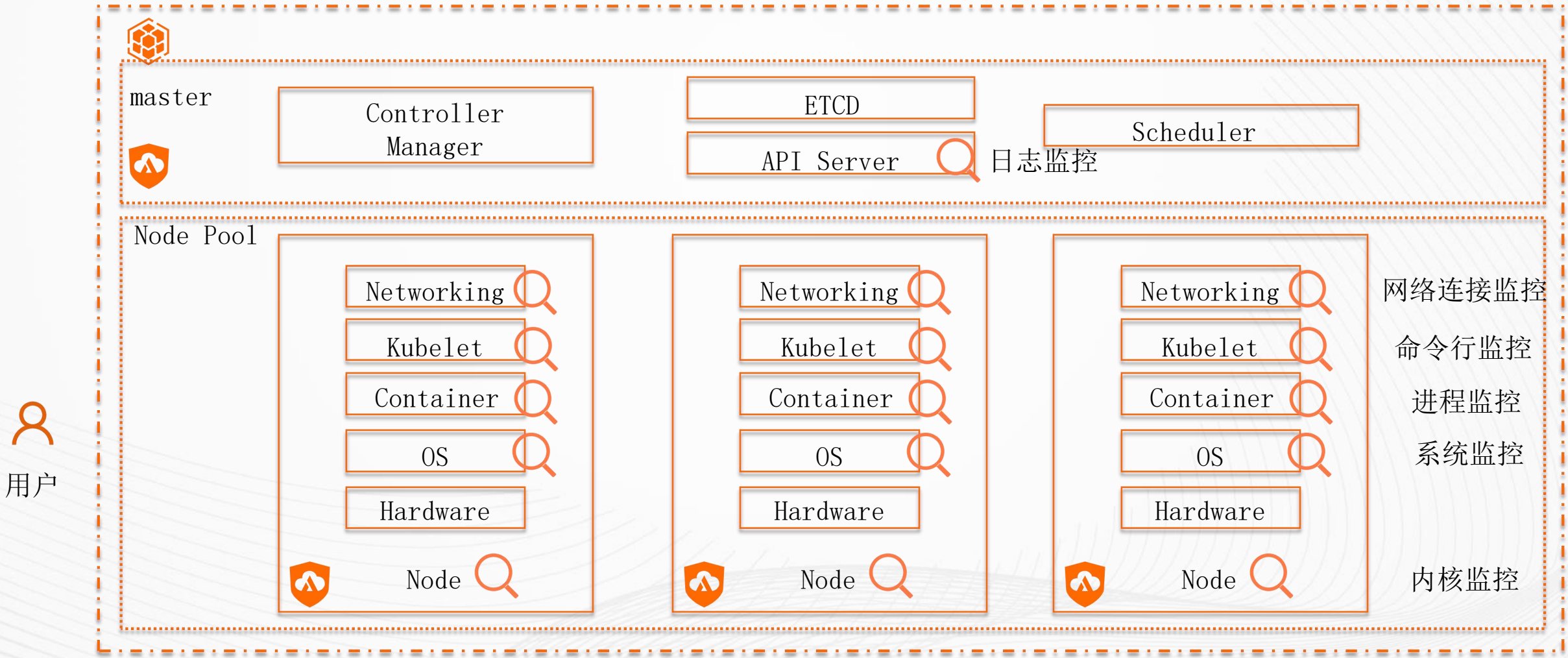
镜像版本

刷新

版本	镜像ID	状态	Digest	镜像大小	加签状态	最后更新时间	操作
0.5	8c8dc9786b05...	正常	fb41a8540b691ebbd659be2e8046f2dc488848816469e6cb0bd2e2fd6b444fc3	72.368 MB		2020-06-10 16:57:12	安全扫描 | 层信息 | 删除
0.4	fc700e555576...	正常	c7e8fc6c11b0b8d9ff37ee1d3bb57a682ac3ba683e2dd68ad30246b4cb41a00f	72.368 MB		2020-06-10 16:45:20	安全扫描 | 层信息 | 删除



运行时安全


master
Controller Manager
ETCD
API Server
Scheduler
日志监控
Node Pool
Networking
Kubelet
Container
OS
Hardware
Node
网络连接监控
命令行监控
进程监控
系统监控
内核监控
用户

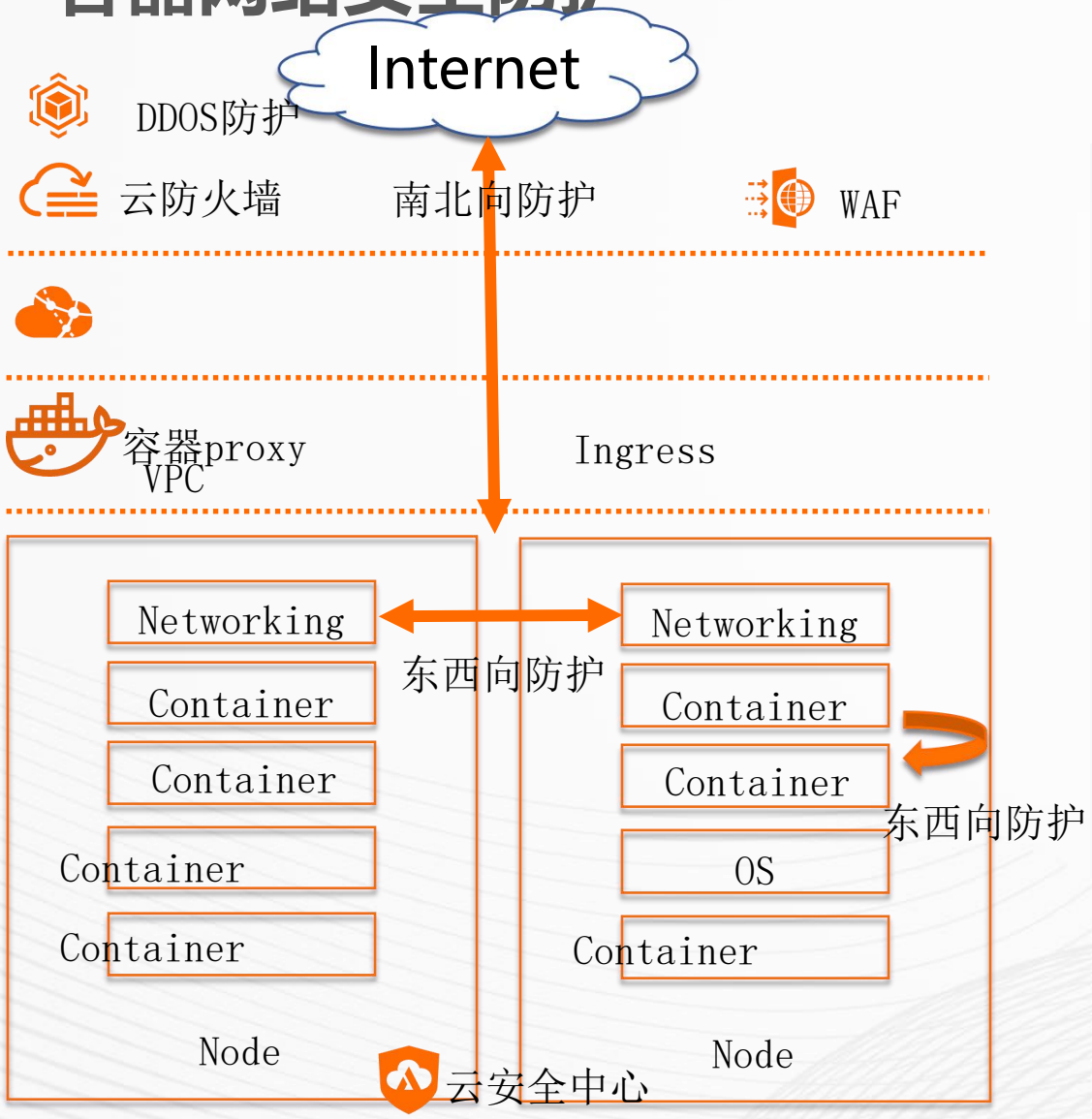
容器运行时防护路径

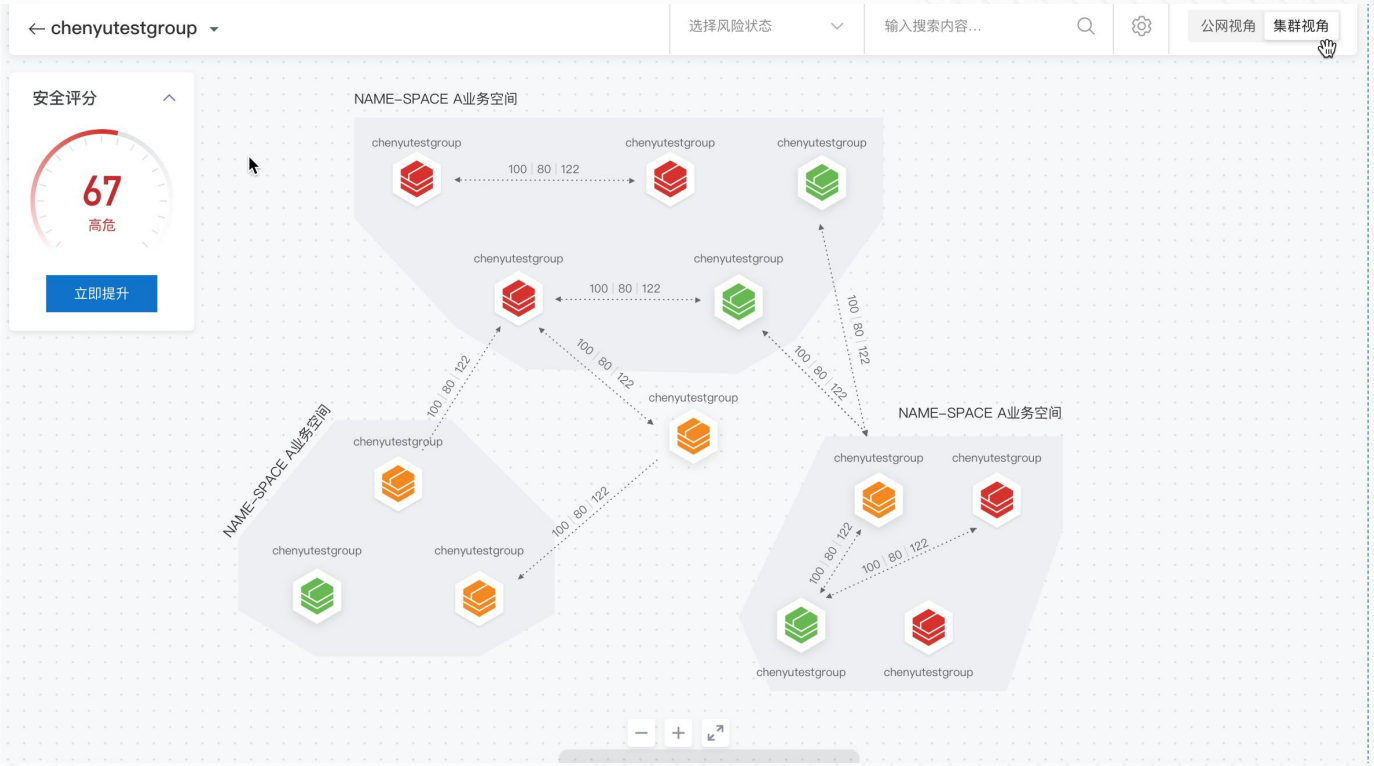
攻击者

开发
运维

初始入侵	下发指令	持久控制	权限提升	躲避防御	窃取凭证	探测信息	横向攻击	达成目标
云账号AK泄露	通过kubectl 进入容器	部署远控容器	利用特权容器逃逸	容器及宿主机 日志清理	K8s Secret泄露	访问K8s API Server	窃取凭证 攻击云服务	破坏系统及数据
使用恶意镜像	创建后门容器	通过挂载目录 向宿主机写文件	K8s Rolebinding添加用户权限	K8s Audit 日志清理	云产品AK泄露	访问Kublet API	窃取凭证 攻击其他应用	劫持资源
K8s API Server 未授权访问	通过K8s控制器 部署后门容器	K8s cronjob 持久化	利用挂载目录逃逸	利用系统Pod伪装	K8s Service Account凭证泄露	Cluster内网扫描	通过Service Account访问K8s API	DDoS
K8s configfile 泄露	利用Service Account连接API Server执行指令	在私有镜像库 的镜像中植入后门	通过Linux内核 漏洞逃逸	通过代理或匿名 网络访问K8s API Server	应用层API 凭证泄露	访问K8s Dashboard 所在Pod	Cluster内网渗透	加密勒索
docker daemon公网暴露	带有SSH服务 的容器		通过Docker漏洞 逃逸	清理安全 产品Agent		访问私有镜像库	通过挂载目录 逃逸到宿主机	
容器内应用 漏洞入侵	通过云厂商 CloudShell 下发指令		利用K8s漏洞 进行提权			访问云厂商 服务接口	访问K8s Dashboard	
Master节点SSH 登录凭证泄露			容器内访问 docker.sock逃逸			通过NodePort 访问Service	攻击第三方 K8s插件	
私有镜像库暴露			利用Linux Capabilities逃逸					

容器网络安全防护



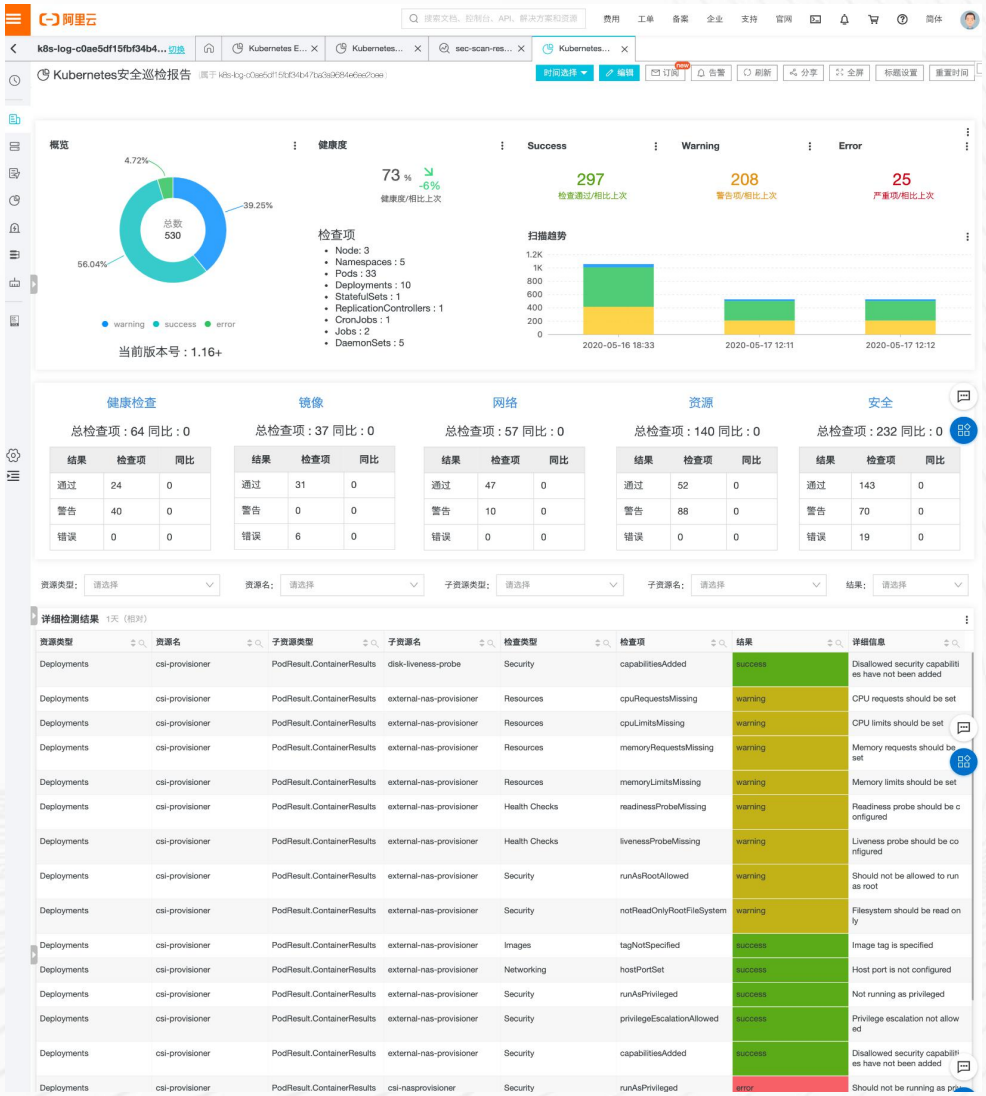


基于大数据的自动拓扑
智能算法策略推荐

一致性安全策略管理

基于容器安全最佳实践，一键化免费检查集群应用配置安全：

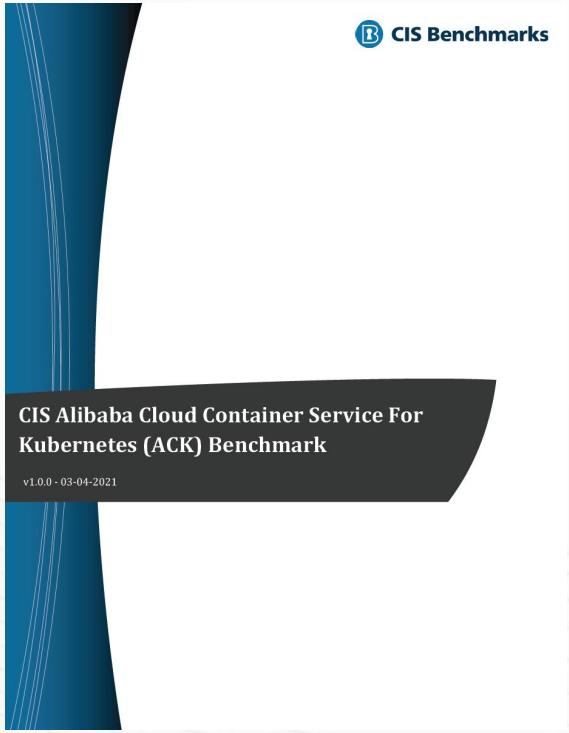
- 健康检查配置校验
- 资源限制配置校验
- 网络安全参数校验
- 镜像拉取安全校验
- 安全参数配置校验



CIS Kubernetes Benchmark for ACK

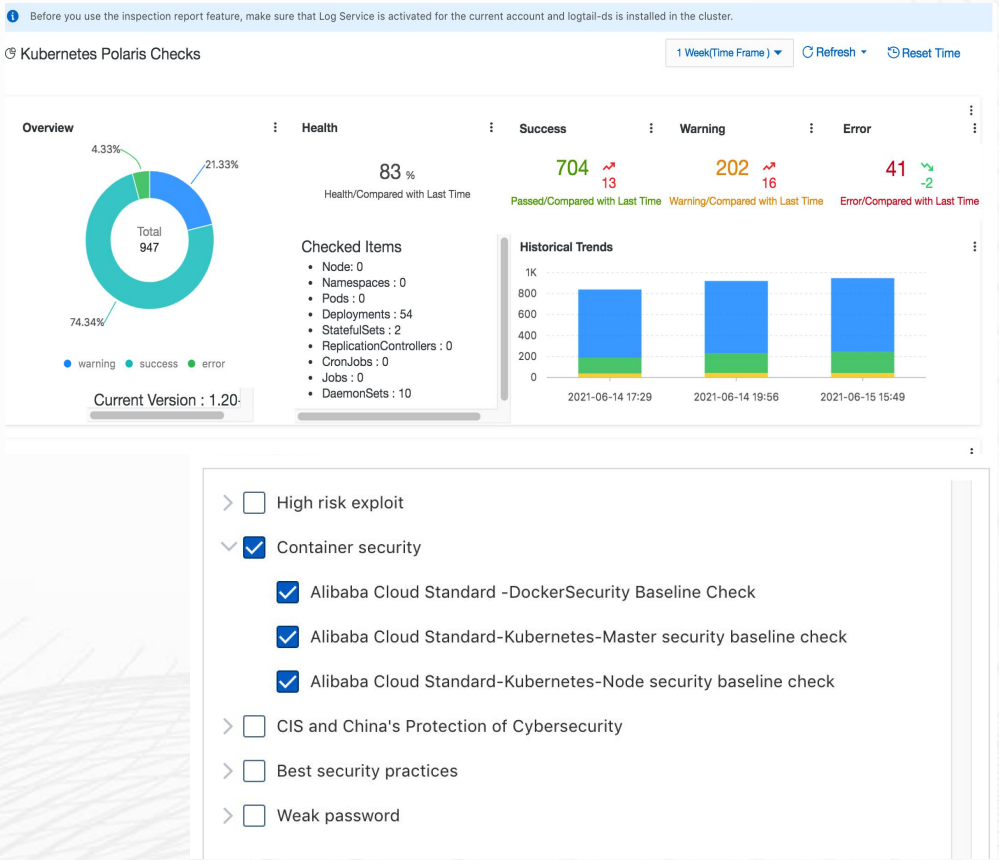
GOTC

CIS Kubernetes Benchmark for ACK

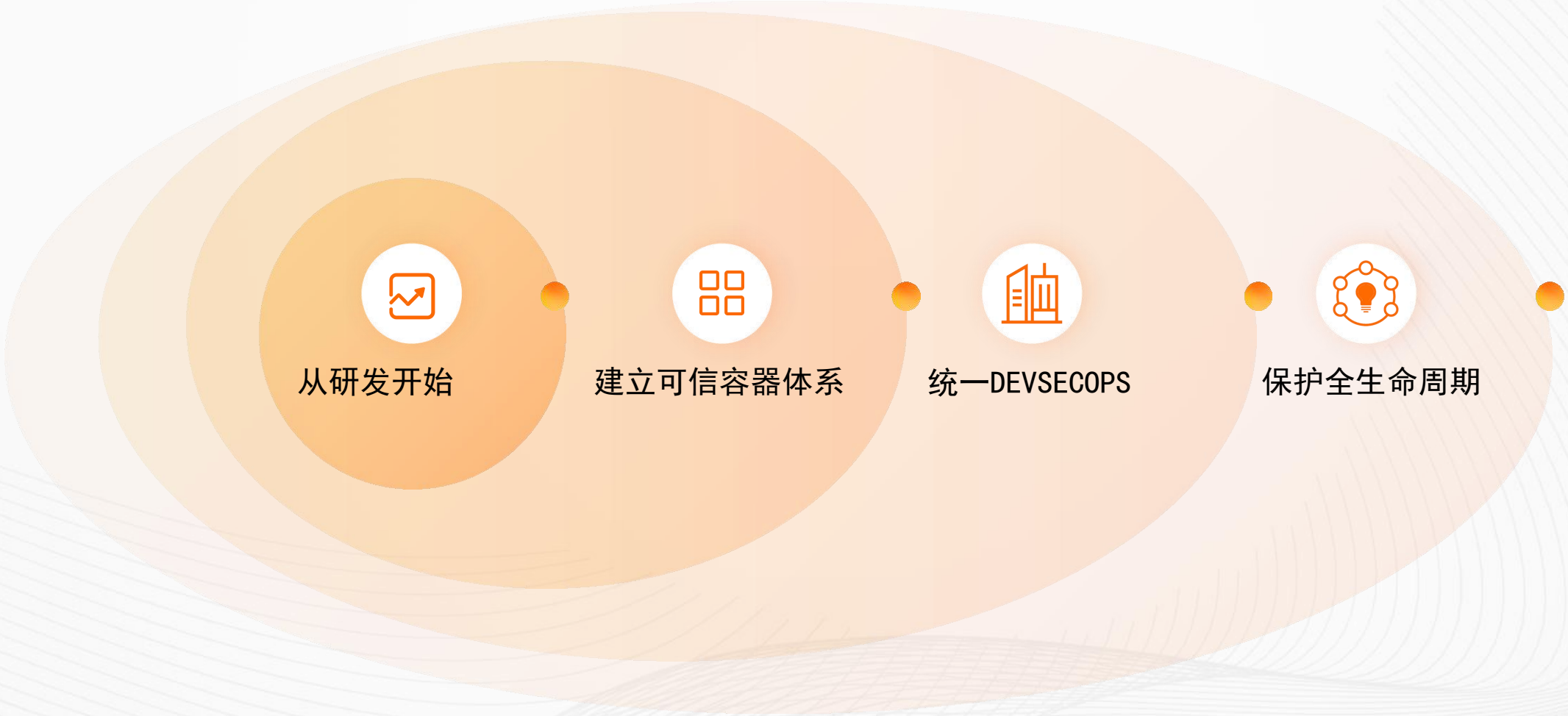


https://www.cisecurity.org/benchmark/kubernetes/

Security Inspection Report



打造一体化云原生安全

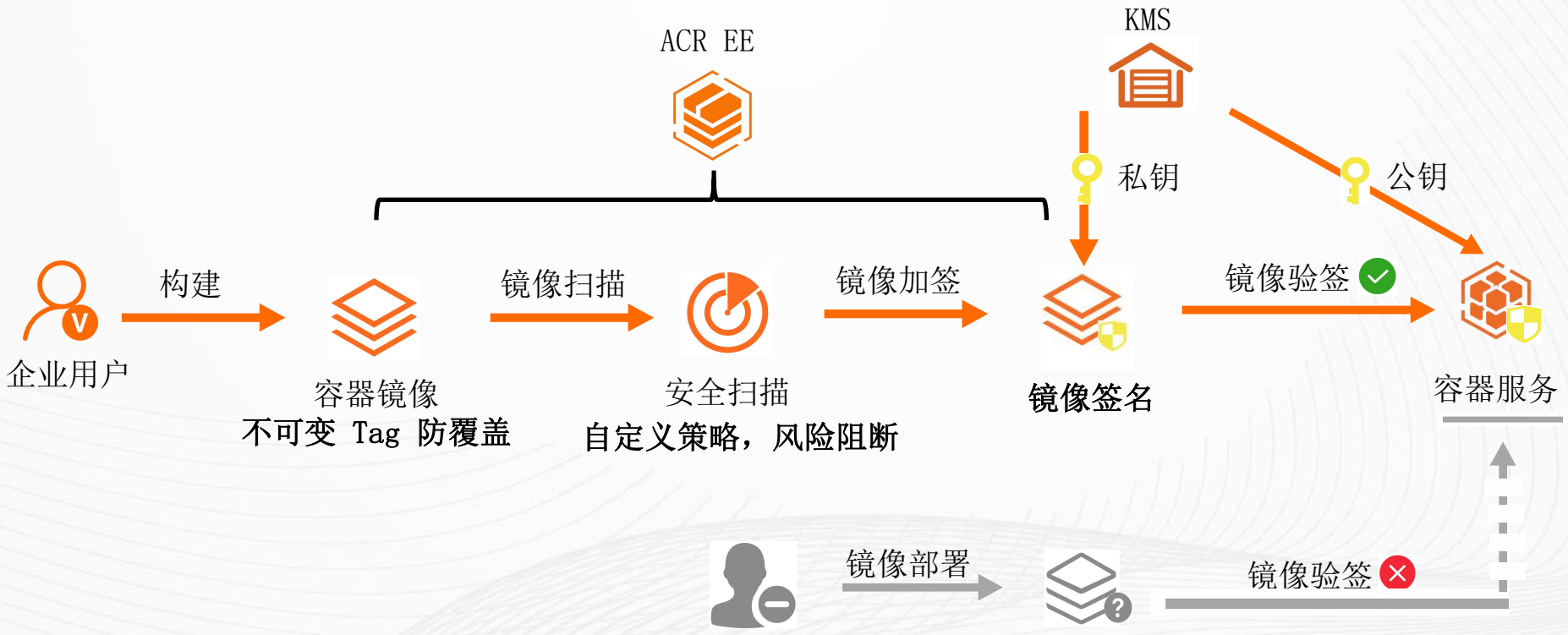


ACR EE DevSecOps 端到端安全

GOTC

云原生应用交付链，支持**多安全扫描引擎**、**镜像加签**配置，全链路可观测、可追踪、可自定义安全策略。

将 DevOps 全面升级 DevSecOps，保障制品更加安全、高效交付上线。



GOTC

THANKS

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE