云原生安全在中国移动磐基（PaaS）平台的安全防护实践

王庆栋

中国移动信息技术中心
研发创新中心（平台能力共享中心）

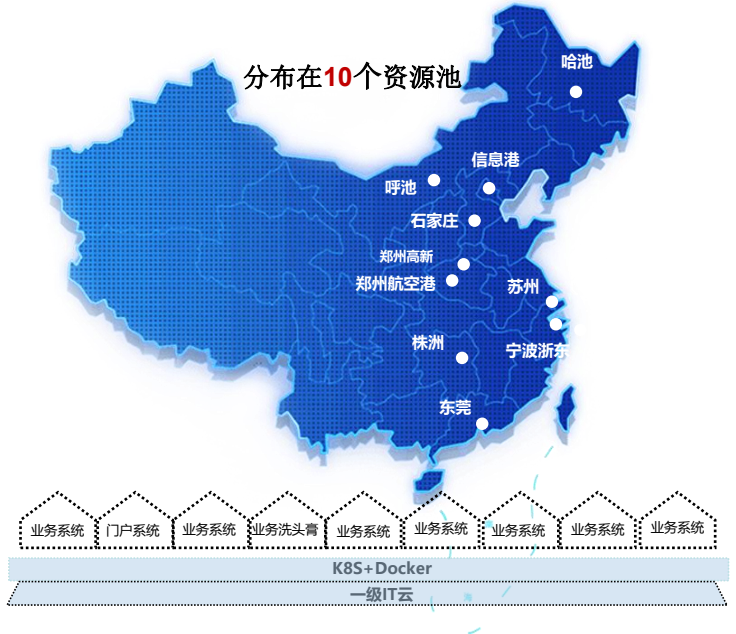
目录

磐基PaaS平台运营现状

- 磐基PaaS平台采用容器、微服务治理以及K8S调度技术，打造自主的技术底座，为上层业务系统提供了容器云平台资源管理与供给、容器应用运行环境、技术组件服务、CI/CD开发部署以及平台研发、运营维护等服务。提供了资源管理与供给、容器引用运行环境、丰富的技术组件服务、运营维护等服务。
- 磐舟一体化交付平台基于DevOps理念构建了需求、开发、测试、部署、运维一体的生产流水线，应用开发遵循中国移动标准的云原生开发规范，一键上磐基PaaS，真正实现乘舟上云，稳如磐基。实现了规模化应用。

30%+	无感知	分钟级	秒级
利用率提升	应用发布	容灾切换	弹性伸缩

100%	统一	敏捷
技术沉淀	架构管控	开发过程



CNCF、可信云认证

磐基平台
China Mobile CMIT PaaS

可信云
容器解决方案

先进级

磐基PaaS平台面临的安全风险

中国移动 China Mobile

基础设施安全风险

- 基础设施的安全是PaaS安全的基础
- 基础设施安全风险关注：计算安全、网络安全、存储安全。

编排组件与镜像安全风险

- 编排工具自身如果存在漏洞，则可能导致非法提权和逃逸攻击。
- 业务应用镜像的构建、提交、拉取部署整个流水线过程中，如果权限设置不当、传输通信不加密、账号管理不足、应用存在被利用的漏洞等，可能形成镜像漏洞、过期镜像及恶意镜像。

容器运行时风险

- 无法有效识别来在各方的攻击行为是容器运行时的主要风险点，如：端口扫描、暴力破解、容器逃逸攻击等
- 容器网络与传统物理网络不同，访问控制手段缺失会增加横向攻击风险造成威胁蔓延，及时有效应对入侵行为响应风险。

微服务风险

- 微服务架构的采用意味着微服务数量的增多，和暴露的端口数量的急剧增加，进而导致攻击面扩大。另外，微服务间的网络流量多为东西向流量，传统网络安全设备难以防护。

多租户多集群场景

- 磐基PaaS平台环境中，跨多个数据中心，多集群，多个租户。该场景下对安全运营提出了更高的要求，增加了安全运营的复杂度。

5G++

磐基PaaS安全防护体系建设方案

- 打造完善的磐基PaaS安全防护体系，为租户提供安全工具和安全服务能力；
- 从基础设施安全、软件工具链安全、漏洞管理和修复、运行时安全、安全量化模型等六个方面，加强安全服务能力输出
- 基于磐舟平台从源头进行安全加固：包括代码安全扫描、代码质量扫描、开源漏洞扫描、开源协议扫描、镜像安全扫描，安全防护左移，提前预防安全风险。

运行时安全

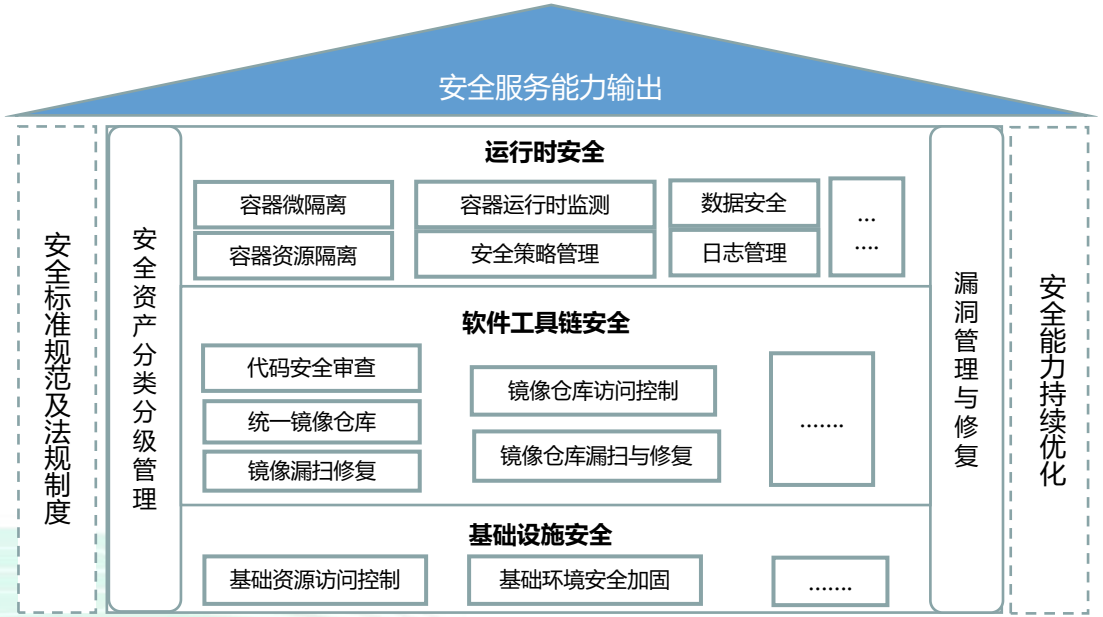
通过**容器安全与微隔离**软件对容器运行实时监测

软件工具链安全

代码安全：devops+上线前实现代码安全审查自服务
统一镜像仓库：构建一二级镜像仓库的统一管理
镜像漏扫：上云+devops+已上云镜像的漏扫与修复

基础设施安全

访问控制：借助外部资源
安全加固：借助外部工具漏扫，内部团队及时修复加固



漏洞管理与修复

漏洞修复：建立漏洞台账，按照系统漏洞、镜像漏洞、组件漏洞、应用漏洞分类管理，明确责任人，推进漏洞修复

安全能力持续优化

构建安全量化模型：15项量化数据监测推进安全监测、修复与加固，提升安全能力
合理使用安全力量：

- 运行时安全做到**实时监测**
- 供应链安全做到**自服务+按需响应**
- 常规安全实现**定期漏扫**（系统漏扫每月一次，渗透测试每季度一次）

目录

跨数据中心多集群的安全防护

中国移动 China Mobile

统一纳管

磐基PaaS内的容器集群，每个集群部署一个代理服务器，统一收集安全状态信息上报至容器安全数据库。代理服务器与容器安全管理平台和数据库之间网络可达即可，与物理位置无关。

统一展示

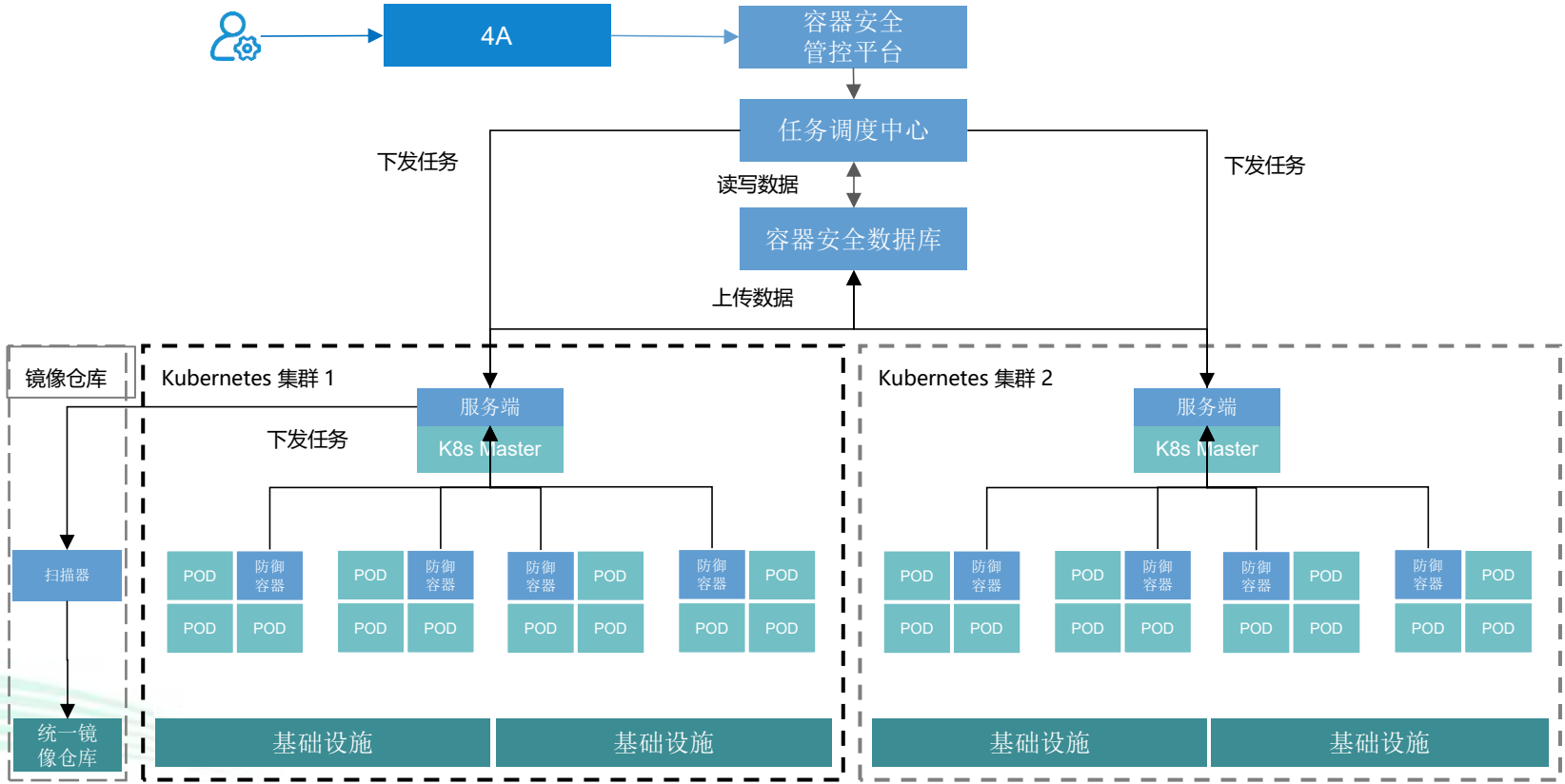
数据汇总至容器安全数据库，由容器安全管控平台对数据进行抽取、转换、分析、聚合，统一展示资产视图与风险视图。

统一运营

安全策略管理员配置策略，设定任务，由任务调度中心统一通知各对应容器集群。一键下发，全局生效。

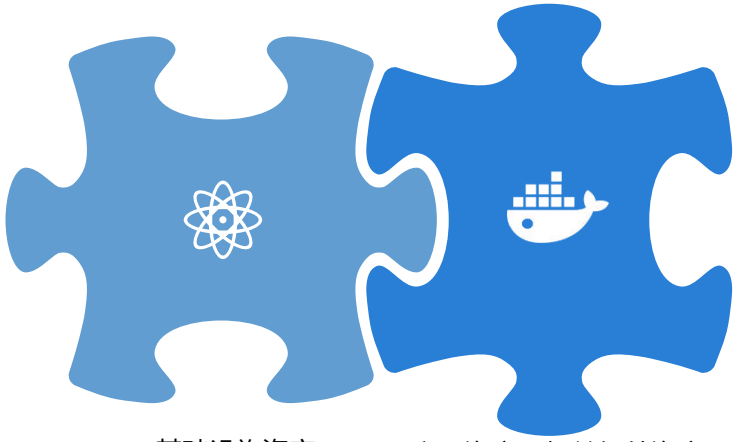
统一账号

与4A相结合，打通各平台统一账号体系。并按照集群内namespace与租户的映射关系，容器安全管理平台支持分权分域，提供平台角色视角、租户角色视角。



协同合作共筑基础设施安全

将基础设施资产与容器资产进行关联分析，分类分级，覆盖基础设施与容器平台的完备台账。容器运行所在宿主机及宿主机自身信息均可快速获取，从而使安全运营有的放矢，以及更快响应各类问题处理。



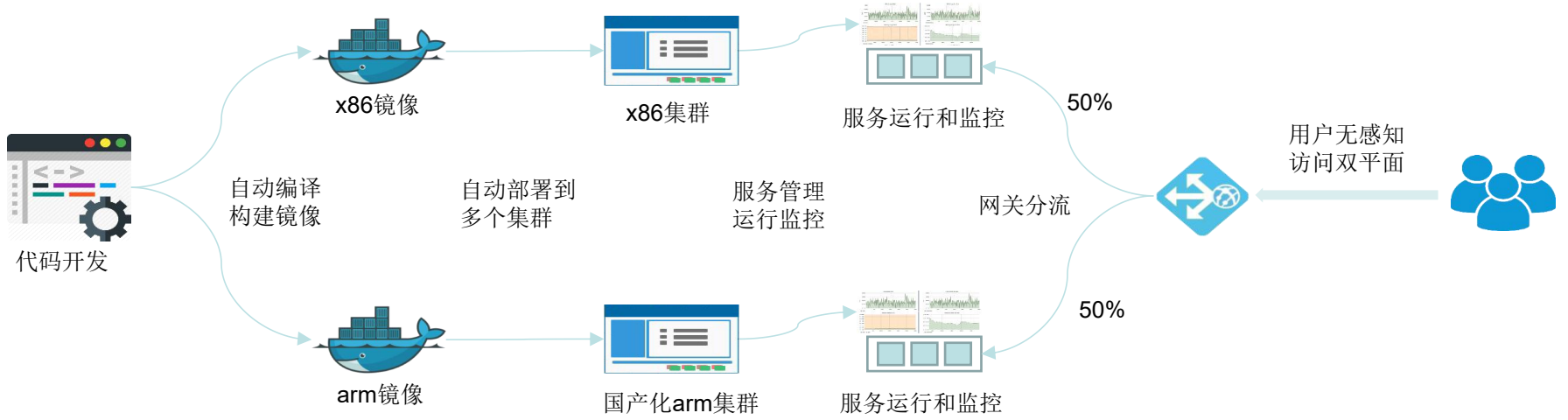
基础设施资产　　容器资产及相关组件资产

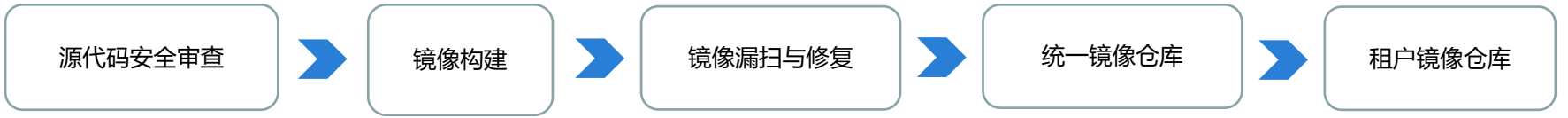
基于基础设施资产梳理，借助公司安全能力，重点建设了主机安全，包括主机漏扫、主机合规、对主机进行加固，以及主机层入侵监测。

- **主机漏扫**：对主机操作系统存在的软件漏洞、病毒木马进行实时扫描
- **主机合规**：根据相关合规标准对操作系统进行配置检查
- **系统加固**：对发现的漏洞及其他脆弱项进行加固
- **入侵检测**：对主机的文件、进程以及网络连接进行监控，发现病毒，发现针对于主机的入侵行为

除主机防护之外，其他相关的基础设施安全建设也均有投入，涉及存储安全、网络安全（抗DDOS）、全流量溯源取证、日志审计、数据库审计等等

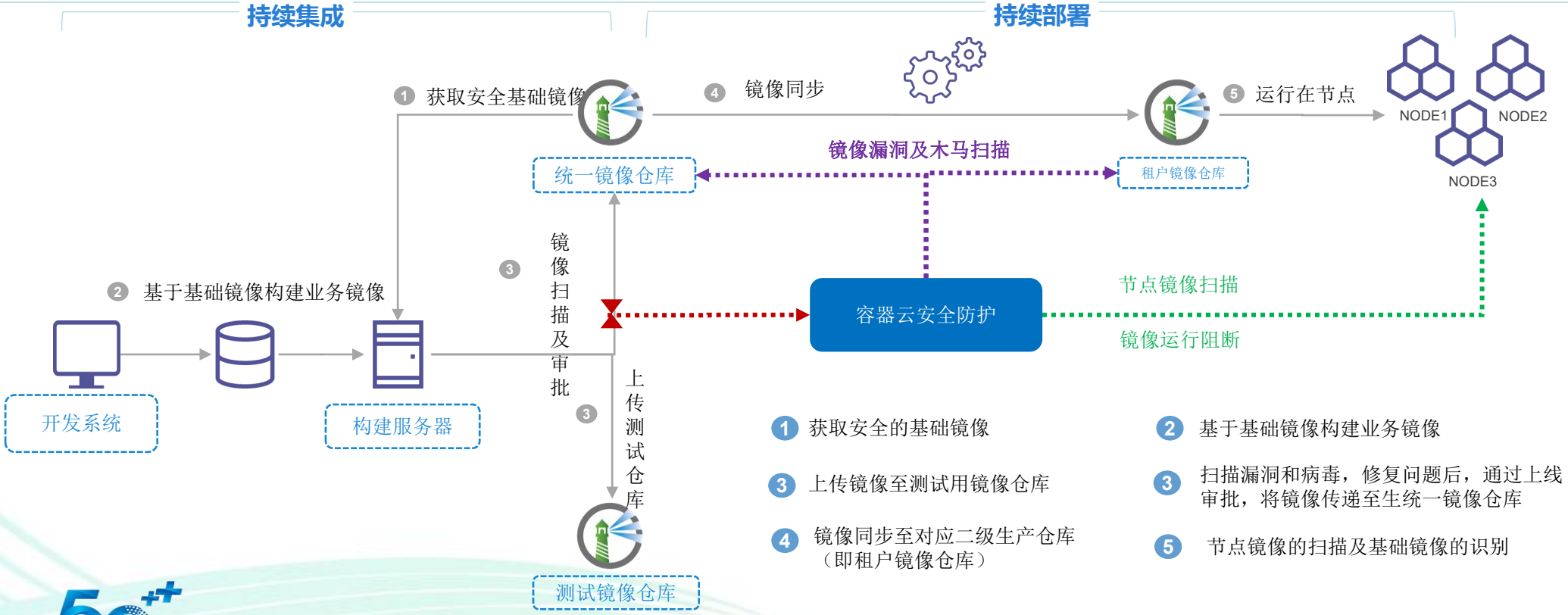
基于DevOps的软件工具链安全





为租户提供软件工具链安全，主要包含源代码安全审查、镜像构建、镜像漏扫与修复、统一镜像仓库管理、镜像传输安全等，对全流程研发过程进行安全防护，避免任何一点成为攻击目标。

基于统一镜像仓库的漏洞管理与修复



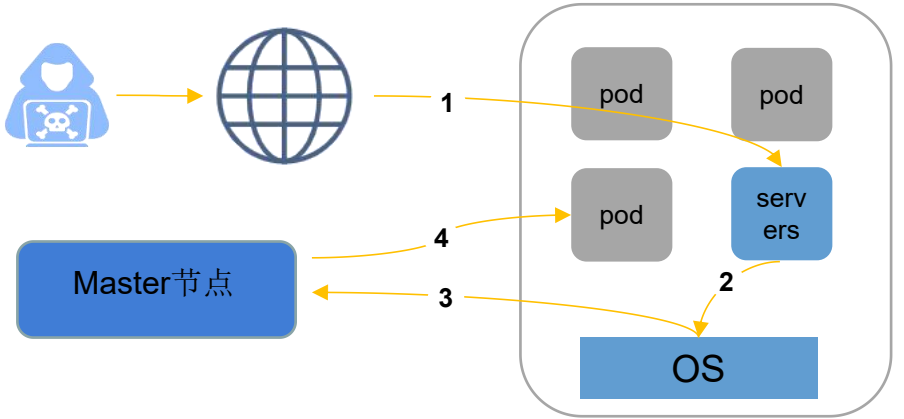
容器运行时安全监测

初始访问	执行	持久化	权限提升	防御绕过	凭证访问	发现	影响
攻击对外开放的服务	容器管理命令	外部远程服务	逃逸到宿主机	在宿主机构建镜像	暴力破解	容器和资源发现	端点拒绝服务
外部远程服务	部署容器	植入内部镜像	滥用提权	部署容器	不安全的凭证	网络服务发现	网络拒绝服务
可用账户	预定任务/作业	预定任务/作业	预定任务/作业	损害防御			资源劫持
	用户执行	可用账户	可用账户	宿主机指示器移除			
				伪装			
				可用账户			

- 端口扫描、暴力破解
- Webshell文件检测
- 反弹网络连接检测
- 挖矿行为检测
- 勒索病毒文件检测
- 敏感文件操作检测
- 危险命令检测
- 可疑进程检测

- Runc漏洞逃逸行为检测
- Docker-cp逃逸检测
- 脏牛漏洞逃逸检测
- Setuid逃逸检测

- 未授权访问ApiServer



集群节点一

① 攻击对外服务漏洞 → ② 尝试逃逸到宿主机 → ③ 攻击master节点，拿下集群控制权 → ④ 控制整个集群

容器运行时安全-微隔离

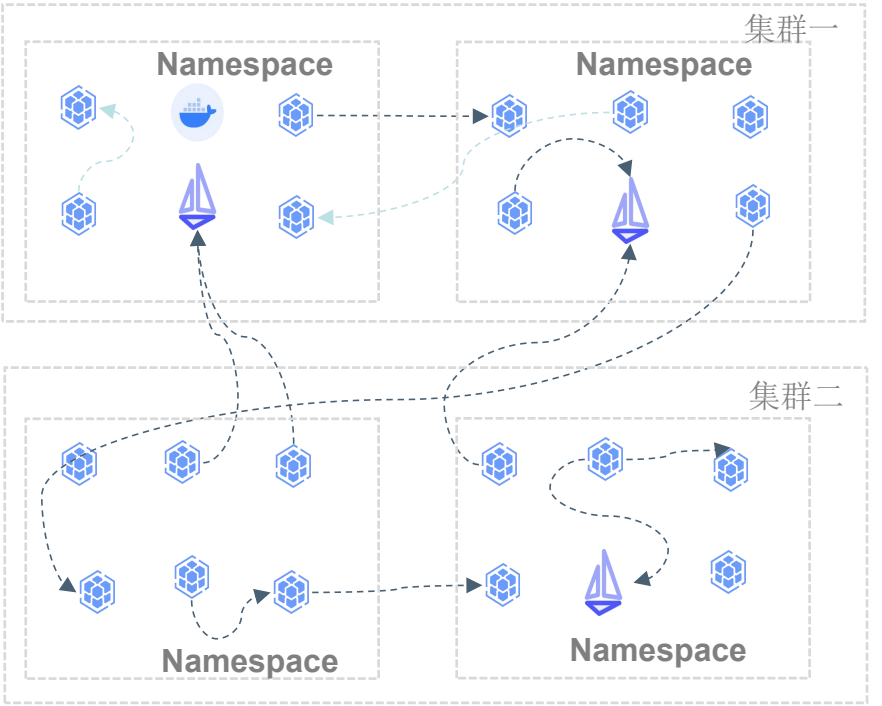
容器微隔离用于阻止容器间东西向攻击，减小攻击面，全自动构建和管理容器层的ACL隔离安全策略。主要通过双向控制、访问可视化、访问过程溯源的功能，对基于容器、容器组和业务视角进行超细粒度的双向网络访问控制，能够对非法访问的轨迹监控并溯源整个行为访问的过程。

01 **集群之间的隔离**
可以为不同集群之间设置访问控制策略

02 **Namespace之间的隔离**
可以为同一集群的不同Namespace之间设置访问控制策略

03 **POD之间的隔离**
可以为任一POD之间设置访问控制策略

04 **微服务访问控制**
可以对微服务的访问设置控制策略



微服务安全

微服务接口增多

微服务跨网络跨服务调度

微服务治理框架漏洞

攻击端口和攻击面增加

引入访问控制风险

引入应用风险

01 服务自动发现

自动发现云原生环境中存在的所有微服务

02 服务类型识别

识别服务的类型(如NodePort、ClusterIP等），并可进一步识别服务的应用类型（如Web、数据库等）

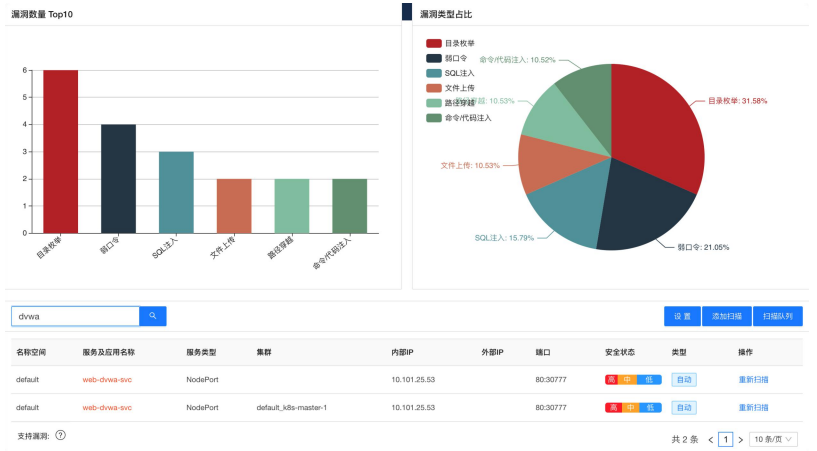
03 服务漏洞检测

扫描服务存在的安全漏洞，覆盖OWASP TOP10全部类型，以及暴露的API漏洞

微服务场景下，业务逻辑分散在很多的进程里。每一个进程都有自己的入口点，每一个入口点都可能成为一个攻击面。显著增加的服务接口数量，也更容易引入“无认证”、“弱口令”、“凭据泄露”、“越权”等风险。

容器网络间如果不对Pod间访问进行显式授权，一旦某一Pod失陷，将极速扩展至整个集群的Pod。

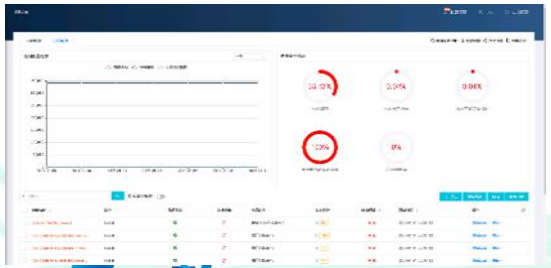
常用微服务治理框架例如Spring Cloud、Dubbo等基于社区的模式运作，其默认值通常并不安全，常常引入不可预料的漏洞，为微服务的开发和使用者带来安全隐患。

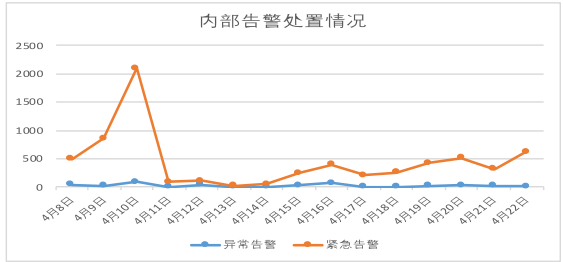


磐基PaaS平台安全量化模型

基于磐基PaaS安全管理平台的实践，对各类数据进行整理，形成安全量化模型，运行报告模板，助力安全运营工作。磐基PaaS平台安全量化模型包含以下15项重点数据，保证各业务系统7*24小时的稳定。

•工单	上线前安全加固									运行时保护	专项保障		运营审计	
•系统漏扫工单、镜像漏扫工单、基线检查工单	含恶意文件的镜像	不合规配置	•系统漏扫	镜像漏扫	基线检查	弱口令	组件修复	修复应用漏洞数量	组织应用渗透次数	处置的告警数量	•两部委和公司安全检查	春节、两会、元旦等重要节假日	•配合4A	配合和BOMC





目录

云原生安全防护未来规划

中国移动 China Mobile

方向一

容器安全能力对外输出

安全能力微服务化，通过API、微服务等形式对外开放输出。例如镜像漏扫，镜像阻断；

方向二

各项安全能力的融合

安全能力左移、生产融合安全能力全流程贯通、适配云原生的应用场景；

方向三

容器安全覆盖范围的规模扩大

扩大容器防护的规模，更多的集群节点、容器实例数量、容器镜像数量；

方向四

新技术探索

例如集群内东西向流量检测，servicemesh与安全的集成等；

5G++


CMIT云原生公众号
乘舟上云 稳如磐基！

云原生 产业大会
2021 CLOUD NATIVE INDUSTRY CONFERENCE
2021/05/26 × 中国 / 北京
原生蓄力 云领未来

THANKS !

CAICT 中国信通院