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

云原生安全的全景和架构

构建以应用为中心的安全体系

CAICT 中国信通院

总括

01 云原生对安全带来的挑战

02 云原生安全的整体建设思路

03 云原生安全展望

01

云原生对安全带来的挑战

云原生对云生态带来的整体变革：三大统一

统一基础平台

- 容器作为标准的应用发布和运行格式
- Kubernetes作为标准的应用运行平台

统一软件架构

- 云原生的核心价值是——加速业务应用进化
- 微服务是加速业务应用进化的手段
- 微服务架构成为云原生时代的标准应用架构

统一开发流程

- 从资源 到 应用开发 到 应用运维一体化流程拉通
- 贯穿软件全生命周期的自动化文化

云原生时代下的安全变革因素

云原生时代下的安全变革因素

应用运行环境
边界模糊化

应用内生性安全
要求凸显

应用内安全
监测及管控
能力的不足

数据访问安全
及数据保护

机械化的应用
安全管控与自
动化软件开发
流程的矛盾

02

云原生安全的整体建设思路

以应用为中心

云原生安全的整体建设思路：**以应用为中心**

应用的四个范畴

应用运行平台　应用架构　应用开发流程　应用管理

应用运行平台安全

容器层安全

- docker镜像安全
- 容器运行时安全
- 安全容器技术

Kubernetes安全

- 节点
- 命名空间
- 配置和Secret
- 网络策略
- RBAC

基础Linux安全

- 账户安全加固
- 文件权限加固
- Iptables与seLinux
- 自动化漏洞补丁升级
- 全网实施情报驱动的自动化响应

应用架构安全

1 微服务与Web层架构安全

- 网站请求伪造
- 防止点击劫持
- Iframe风险应对
- 跨站脚本攻击

2 应用中间件安全

- Redis缓存
- 消息中间件
- 网关
- 其他中间件

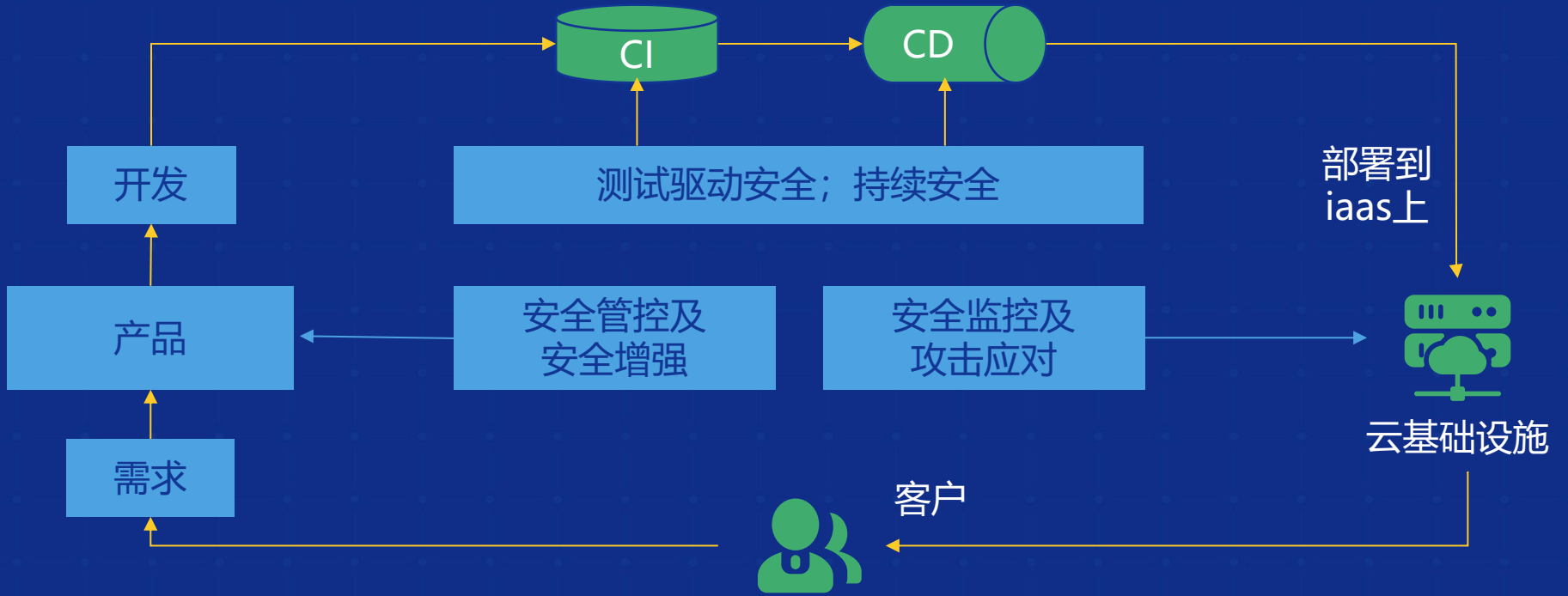
3 微服务间的通信安全

- 微服务流量限制
- 微服务间访问控制
- HTTPS通信加密及证书管理

4 ServiceMesh与应用服务安全

- 流量动态可视化
- 流量精细调整
- 流量可追踪（染色技术）

应用开发流程安全增强机制-DevSecOps



应用安全管理

应用安全审计

业务操作日志记录
从系统及应用中收集日志
基于日志分析的入侵检测

应用配置和密钥安全

应用配置中心安全防护
应用密钥安全保障

应用数据安全

数据安全的三个要素
数据加密技术
数据脱敏技术
数据访问身份认证

微服务应用业务出口安全

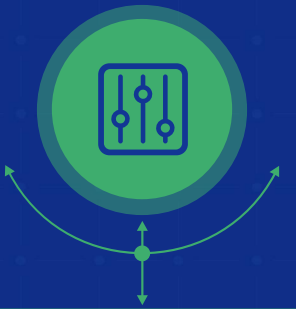
ID授权管理及统一认证
访问策略、流控策略
应用访问监控

03 云原生安全展望

云原生安全展望

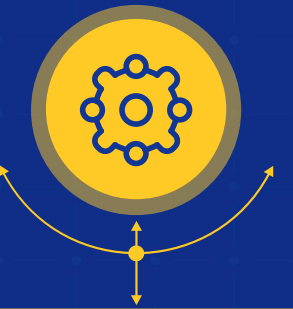
新身份认证技术

随着云原生技术的发展，云网融合后的边界变化带来新的身份认证挑战。身份认证从传统的人-机关系信息模型，转变为人与人之间、人-机之间、机与机之间的多维护信任关系。多元化、细粒度、普适性的新身份认证技术含苞待放。



向以数据为中心的安全体系进化

数据成为新经济的核心驱动力，数据的广泛流动和数据价值的增长，促进从网络为中心的安全体系演变为以应用为中心的安全体系，最后逐渐进化为面向数据保护、数据访问保护的 以数据为中心的安全体系。



多云协同的综合性安全治理模式

云间情报共享，公有云、私有云、混合云等云架构场景下，多云中的联邦安全治理模式是一个趋势。

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