CAICT 中国信通院　中国通信标准化协会 China Communications Standards Association

广东移动基于零信任DevOps远程研发实践探索之路

曾海剑

2021 可信云大会
2021 TRUSTED CLOUD SUMMIT
数字裂变　可信发展

自我介绍

曾海剑

- 现担任广东移动DevOps云原生体系实施总架构师，负责持续交付平台以及云原生基础设施的架构设计、部署实施与运营支撑，指导并支撑广东移动十多个合作商、八十多个项目向DevOps云原生成功转型。
- 多年云原生架构、微服务架构、持续交付架构实战经验，GOPS全球运维大会金牌讲师。

主题

- 远程研发面临的痛点
- 远程研发方案探索
- 基于SDP的远程研发安全接入方案实践
- 基于微隔离的安全隔离方案探索

研发外包模式的痛点

以瀑布模式进行开发管理，以“交钥匙”模式定期交付软件，交付周期长，应变需求难，开发返工多。

交付慢

质量低

软件质量低，长期通过升级硬件来弥补软件质量的缺陷。运维质量低，救火式抢通故障，熬夜式工程割接。

关注需求和验收结果，忽视开发过程管理，软件代码变成黑盒子。拥有代码产权，却无法消化代码产权。

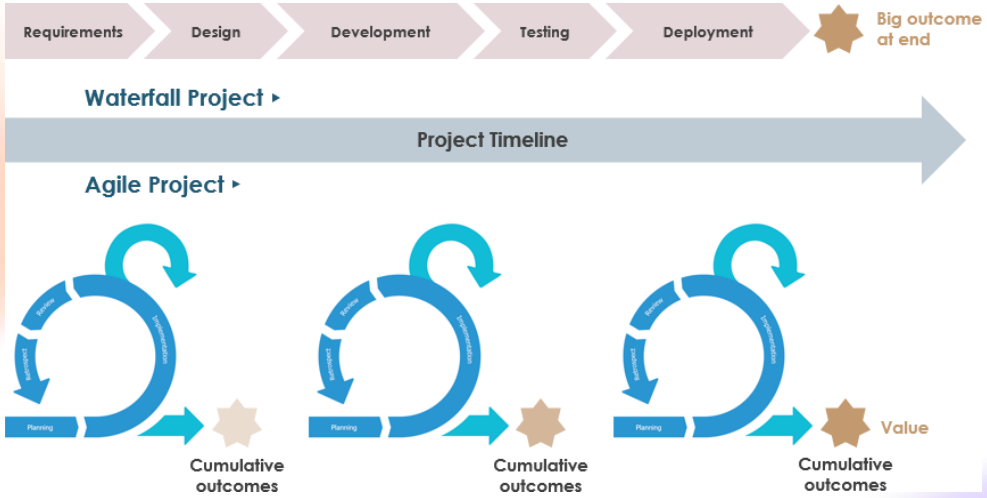
被牵制

空心化

自有员工侧重于包工头式项目管理，培养和提升了开发商的业务知识和技术能力，而自有员工离前沿技术越来越远。

引入DevOps云原生

DevOps



研发过程核心痛点 ——**浪费、质量**

云原生

应用迁移变得异常简单

应用横向扩展
故障迁移
负载均衡
服务发现
多租户资源隔离
……

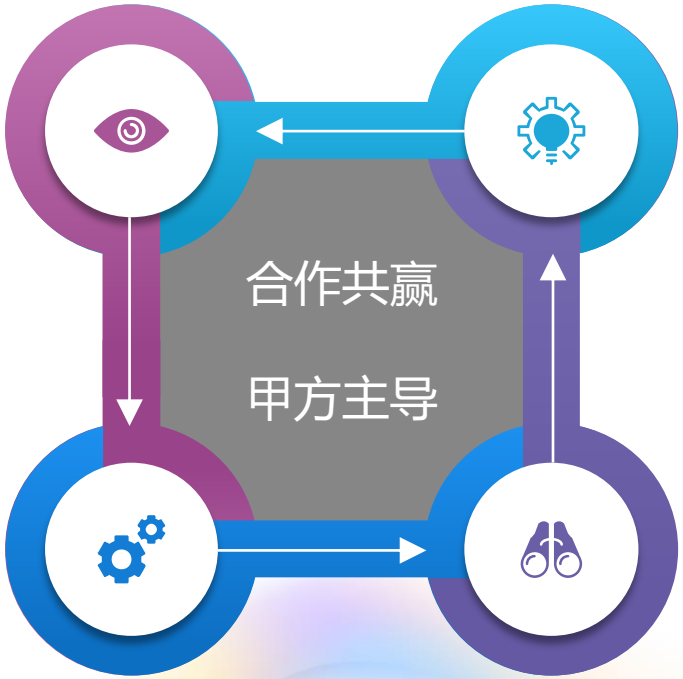
应用运维变得异常简单

转型目标与方法论

解决谁的问题？

- 快速应变
- 持续交付

交付慢



质量低

- 关注过程
- 内建质量

- **消化产权**
- **自主可控**

被牵制

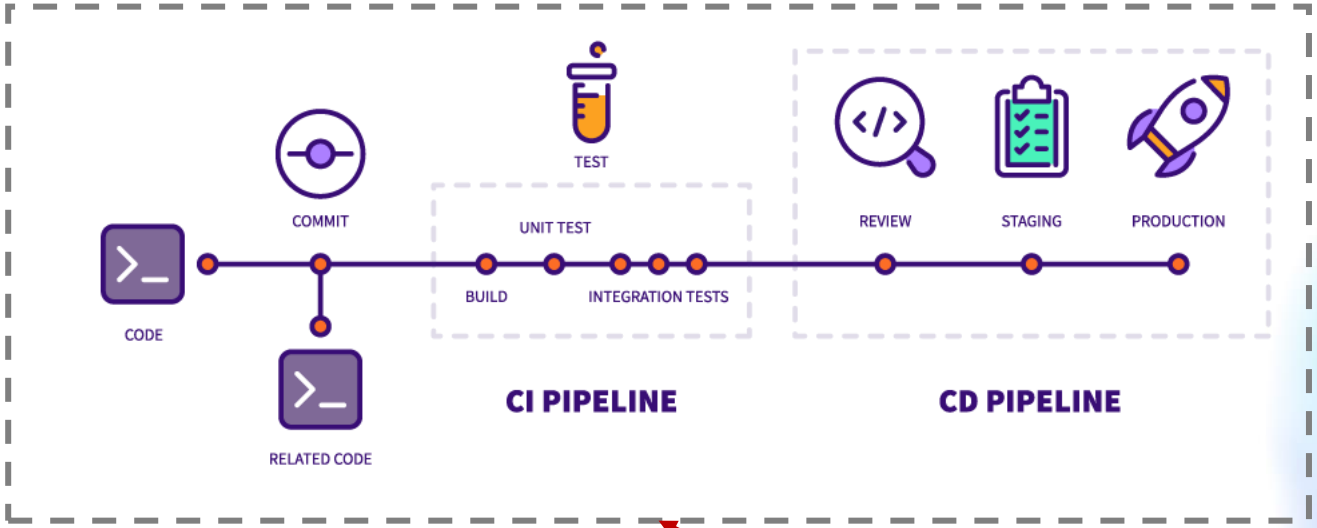
空心化

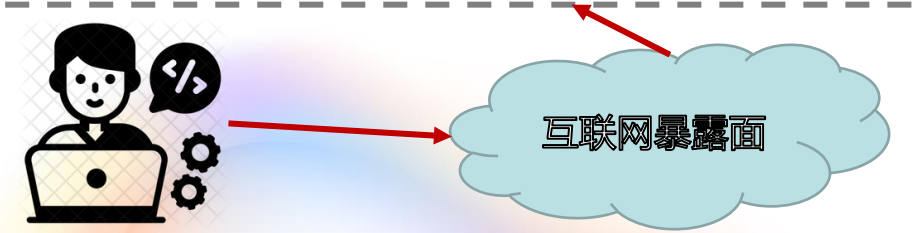
- 培养团队
- 自建自维

谁主导转型？

转型的关键要素

代码 + 研发过程 + 交付过程





远程研发的痛点

互联网暴露面

安全合规

甲方

便利高效

乙方

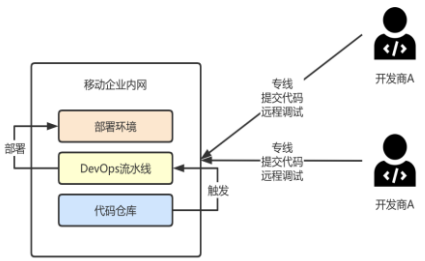
主题

- 远程研发面临的痛点
- **远程研发方案探索**
- 基于SDP的远程研发安全接入方案实践
- 基于微隔离的安全隔离方案探索

早期方案探索

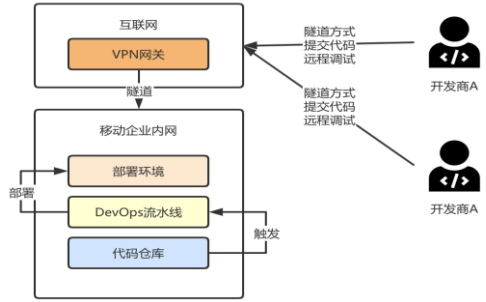
直连

专线



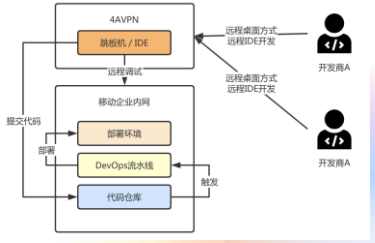
隧道

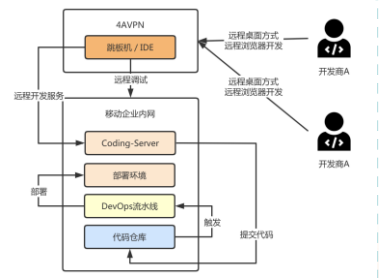
VPN方式



远程桌面

远程桌面IDE /WebIDE方式





专线方式

- 开发商各自申请移动专线，开发人员在开发商公司内能够通过专线接入访问移动企业内网。
- 开发人员通过本地IDE开发源代码，实现专线提交代码，安全性低、效率高、成本高。

安全分析	效率分析	成本分析
✓ 准入机制高，免公网暴露	✓ 本地开发	× 专线费用高
× 丧失安全管控权限	✓ 直连高效	× 管理成本高

有战略合作的大型开发商适用本方案

远程桌面方式

开发人员通过远程桌面连接跳板机，在跳板机上使用IDE或通过浏览器使用WebIDE进行远程开发和调试。本地不保存任何代码，提高了安全性，但过于依赖4AVPN稳定性效率较低，且需要为所有开发人员提供独立跳板机和IDE环境，成本高昂。

远程桌面	安全	效率	成本
WebIDE	高 ★★★★	低 ★	较高 ★★
IDE	高 ★★★★	较低 ★★	高 ★

隧道方式

- 开发人员通过本地IDE开发代码，使用个人VPN账号和VPN软件，通过隧道方式打通本机与移动企业内网的网络。
- 这种隧道方式提交代码及远程调试，效率较高，安全性一般，且需要支付维护开源VPN或采购商用VPN的成本。

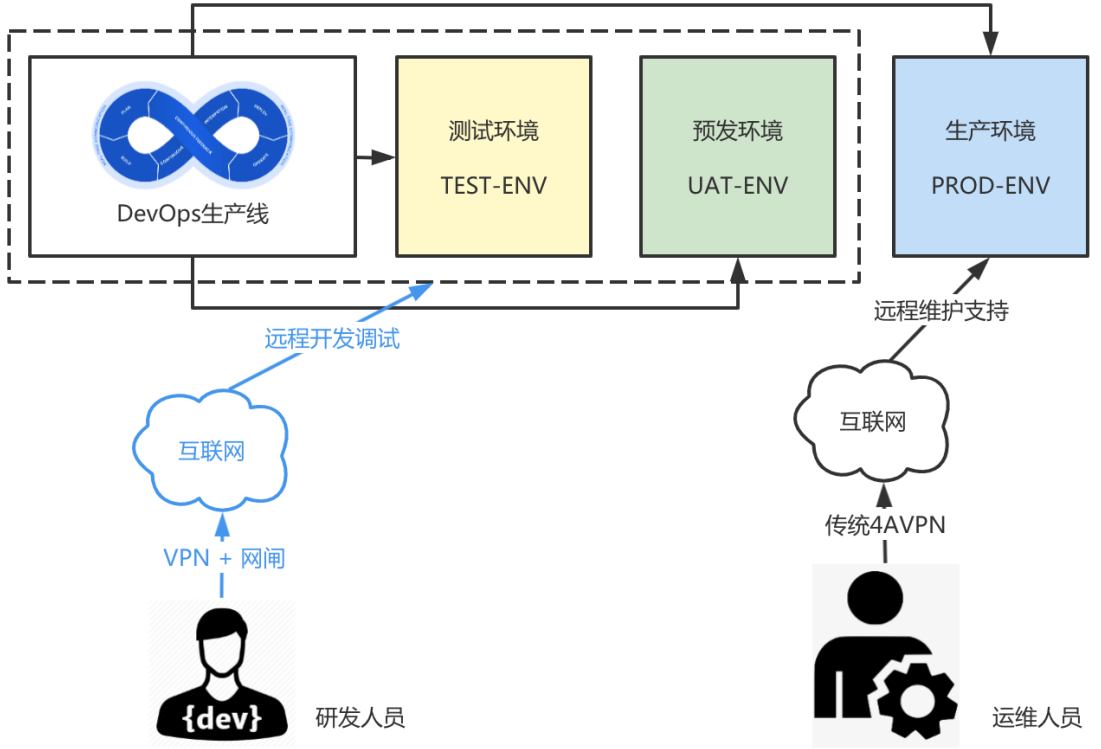
风险点分析	效率分析	成本分析
✓ 访问权限限制	✓ 本地开发高效	✓ 迁移成本低
✓ 证书账号定期更新	✓ 远程调试方便	× 维护成本较高
× 访问范围不可控		

开发商普遍适用本方案

早期方案实践

- 特点：
  - 研发、运维独立接入。
  - 登录证书密钥定期自动更新。
  - VPN+网闸双重认证。
  - 不同环境互相隔离。

- 痛点：
  - VPN授权通过内网全通。
  - 远程运维跳板机多开发商共用，运维隔离性差。
  - **HW等于DW。**

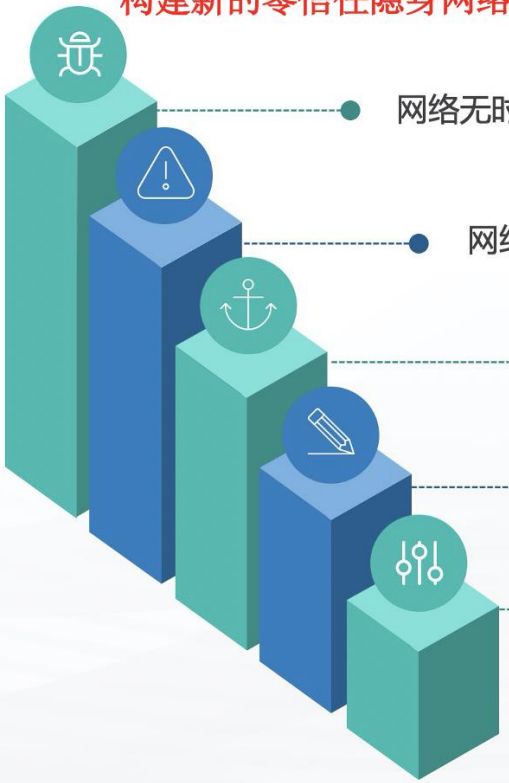


主题

- 远程研发面临的痛点
- 远程研发方案探索
- **基于SDP的远程研发安全接入方案实践**
- 基于微隔离的安全隔离方案探索

零信任的理念

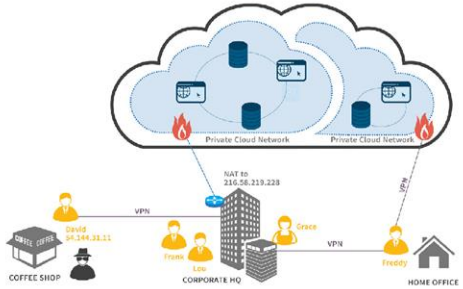
构建新的零信任隐身网络，基于动态、按需的及应用级访问控制，保障用户及数据访问安全



- 网络无时无刻不处于危险的环境中
- 网络中自始至终存在外部或内部威胁
- 网络的位置不足以决定网络的可信程度
- 所有的设备、用户和网络流量都应当经过认证和授权
- 安全策略必须是动态的，并基于尽可能多的数据源计算而来

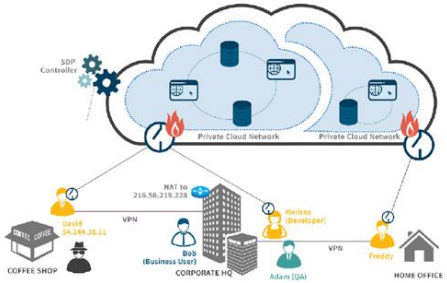
VPN vs SDP

安全边界模型



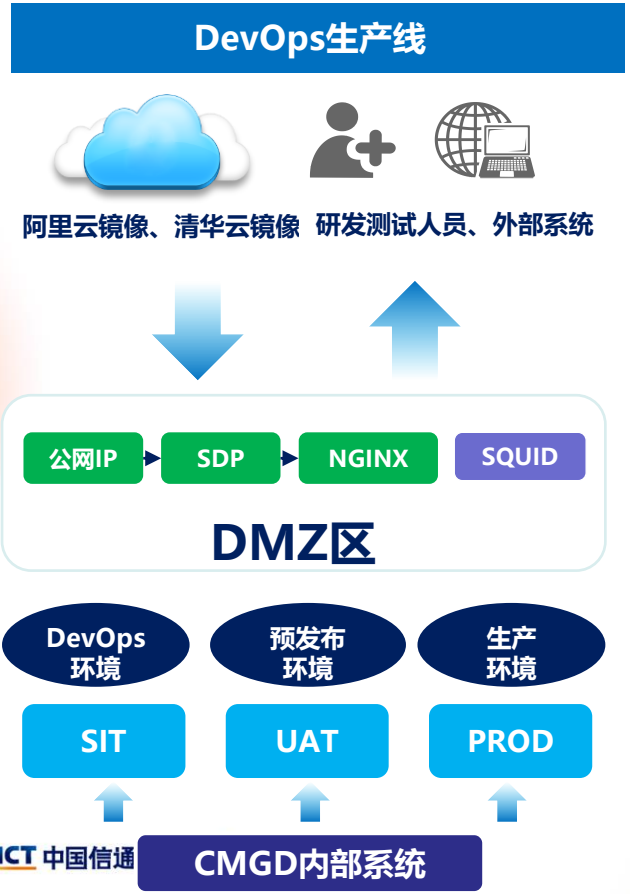
CyberEX 赛讯信息

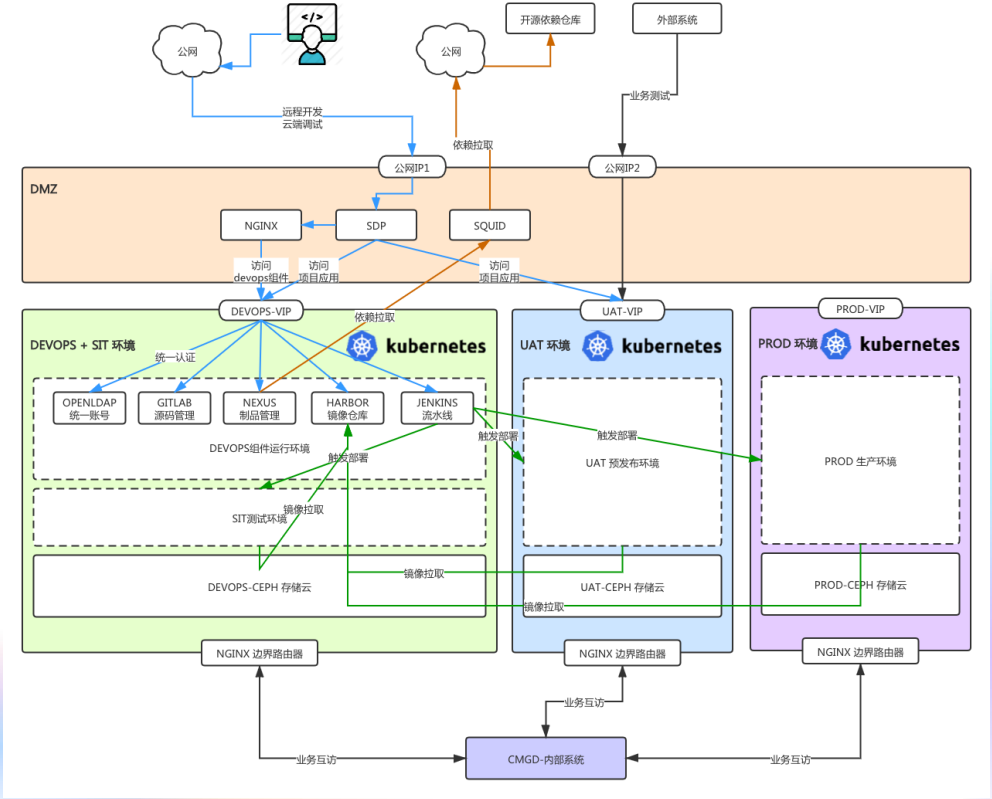
零信任模型



VPN	对比项	SDP
“一次验证”	核心	“永远验证”
基于TCP，可嗅探	网络隐身	基于UDP，反嗅探
各网络/系统出口等	部署位置	用户终端与应用系统之间，应用系统与用户数据服务之间等
无（通过防火墙实现来源约束）	来源鉴权	来源地点、设备指纹、访问时间段、请求报文……
IP地址+服务端口	目标策略	IP地址+服务端口、服务接口、服务标签……
无	行为审计	指令级、接口级行为审计能力
基于角色粗放授权	控制粒度	精细化最小授权，来源地址、访问设备、时间段
中	安全性	高

基于SDP的零信任远程研发方案 – 南北向安全（狭义零信任）





SDP方式

- 开发人员通过本地IDE开发代码，使用个人SDP账号和SDP软件，通过隧道方式打通本机与移动企业内网的网络。
- 开发人员只能在列入白名单的设备、时间、地点上访问特定的网络资源和网络服务，具有高安全性高效率的优点。

- ✓ 限制用户访问特定资源
- ✓ 反嗅探，HW不DW
- ✓ 访问审计
- ✓ 更细粒度准入控制

- ✓ 本地开发高效
- ✓ 远程调试方便
- ✓ 自动化程度高

- ✓ 迁移成本低
- ✓ 维护成本低
- × 一定的建设成本

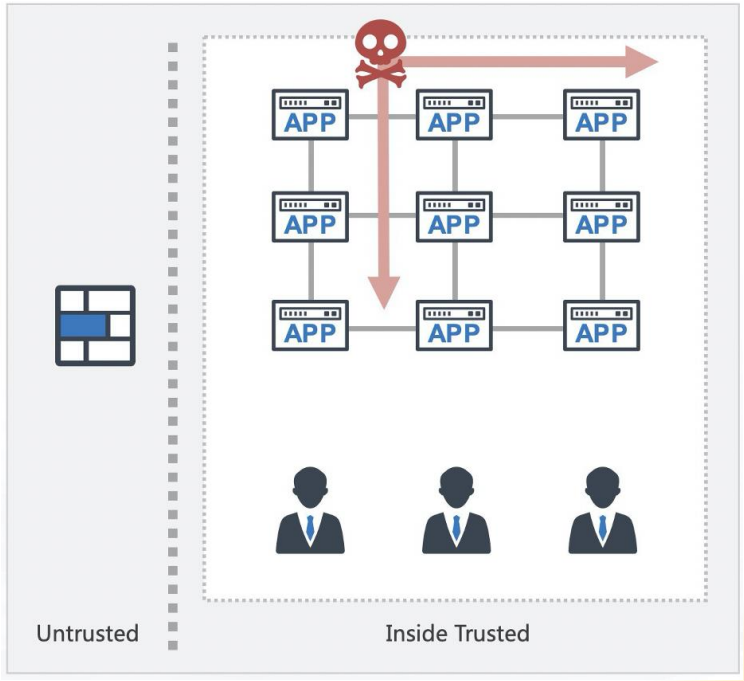
开发商普遍适用本方案

主题

- 远程研发面临的痛点
- 远程研发方案探索
- 基于SDP的远程研发安全接入方案实践
- **基于微隔离的安全隔离方案探索**

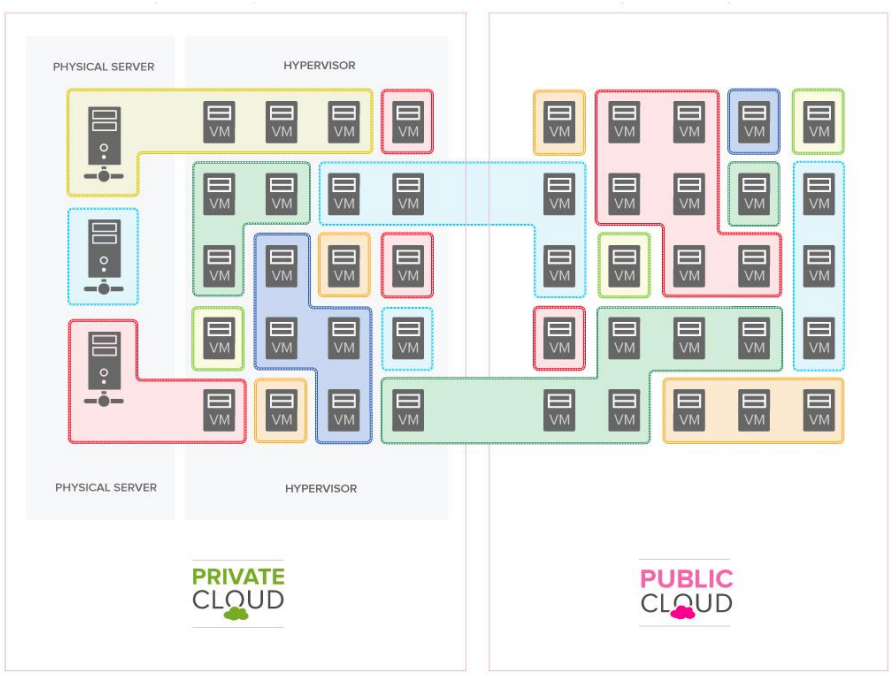
微隔离 - 东西向安全（广义零信任）

以网络为中心

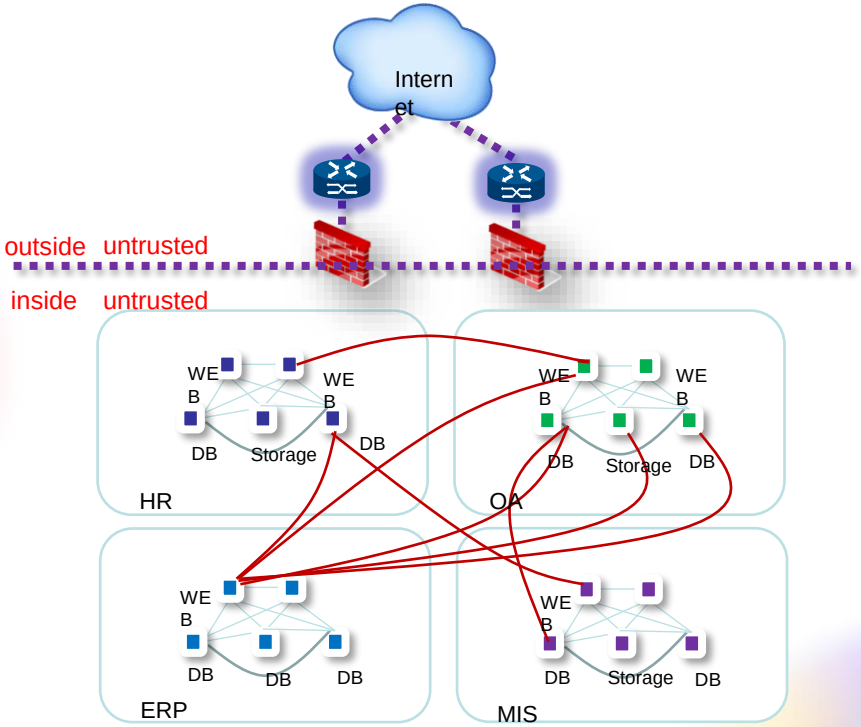


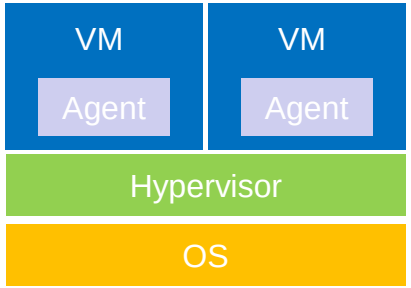
VS

以用户为中心（微隔离）



微隔离 – 主机模式（主机级）





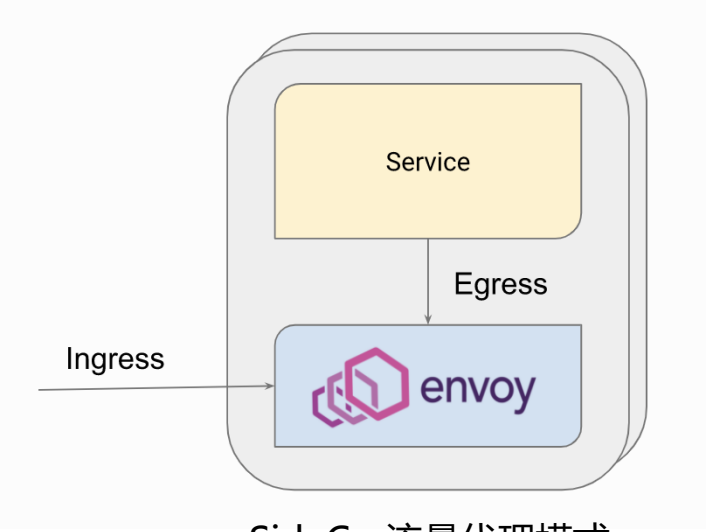
Agent流量代理模式

零信任	外网、内网都需要采用零信任安全模型
最小化	每个应用、服务器之间最小化互访原则
防扩散	避免病毒、APT、黑客横向扩展与渗透
自动化	简化大量且复杂安全策略配置，化繁为简

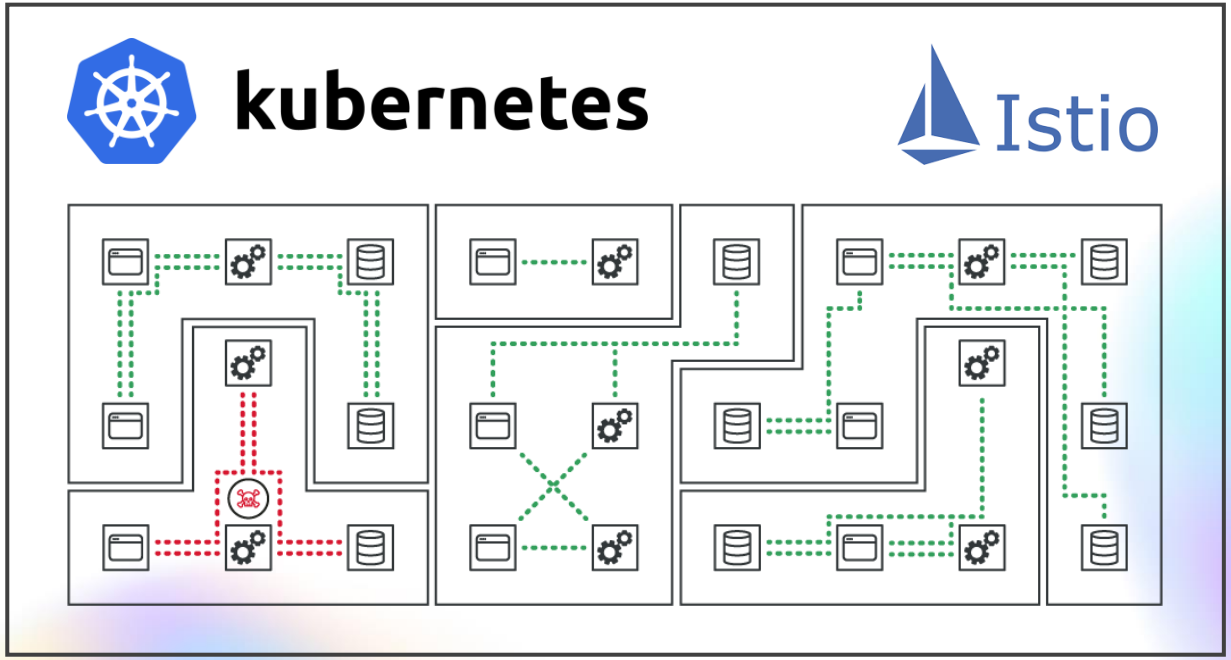
Zero Trusted Mode & Micro Segmentation

微隔离 – 云原生模式（容器级）

零信任 —— 流量治理



SideCar流量代理模式



欢迎来撩

Q & A

以码会友： https://github.com/cookeem

专注： DevOps、云原生、微服务、开源、智能化

THANKS!

2021
TRUSTED CLOUD
SUMMIT