云时代企业安全建设

默安科技 云舒

2018.12

云是大方向

- 工信部要求
  - 2020年全国新增100万家企业上云
  - 建立100个标杆案例

- 银监会要求
  - 2020年，银行互联网业务100%上云
  - 非互联网业务，60%上云

- SaaS化的云业务广泛应用

两类企业安全

- 建云的企业，建设安全的云
- 不建云的企业，安全的使用云

自建云，建设安全的私有云、混合云

公有云安全

云平台和租户分担云计算安全的责任

IAAS云的三个角色

使用方

- 保护自身业务系统安全
- 保护自身数据安全

运营方

- 保证云平台全部租户业务和行为合法合规
- 保证基础IDC和云平台宏观安全状况可靠、可控

建设方

- 云平台自身安全如openstack安全、OVS安全
- 云平台提供基本的安全功能如VPC、安全组

公有云安全责任共担模型

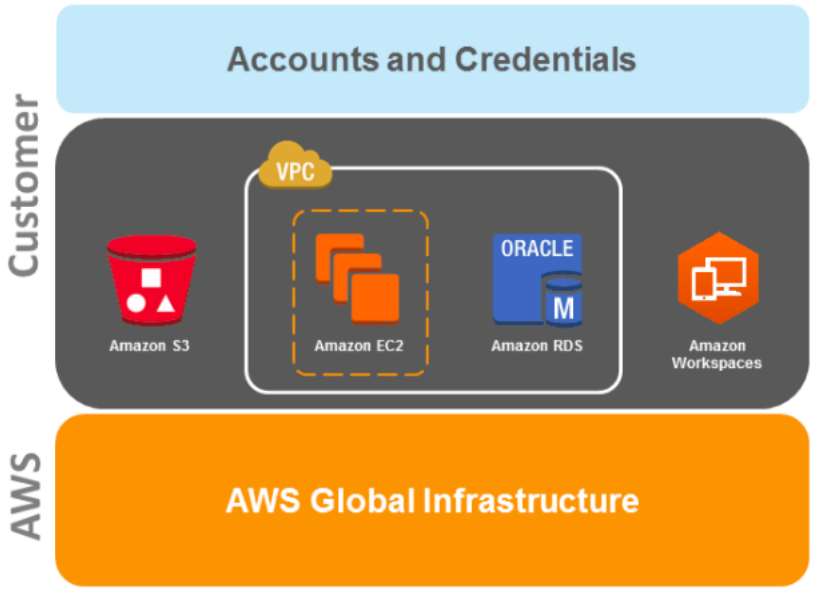


Figure 1: AWS Shared Security Responsibility Model

企业：公有云安全等于使用方租户安全

- 云上安全
  - 云安全市场各种租户安全产品
  - 第三方安全公司独立提供的能在云里面部署的安全产品
  - 云WAF、DDoS防御、云主机安全agent、SaaS化的漏扫等等

- 上云前的安全检查
  - 自定义镜像的安全
    - 漏洞
    - 基线
  - 自己开发的应用系统安全扫描

私有云安全

自己承担一切

私有云安全怎么做?

三种角色：全部自己做！

私有云：建设方安全

- 第三方商业建云服务
  - SLA（服务等级协议）承诺云平台自身安全漏洞、服务相关条款
    - 漏洞信息同步
    - 漏洞补丁提供与升级
  - 提供VPC租户隔离、安全组、防火墙等基本安全功能

- 开源产品自建云
  - 部署漏洞扫描产品
  - 关注kvm、openvswitch、openstack等基础组件安全通告

私有云：运营方安全

- 传统IDC基础安全
  - 物理安全
  - 网络访问控制、网络入侵检测等
  - 主机漏洞管理、基线配置
  - 主机入侵检测、主机认证授权审计堡垒机等
  - ……

私有云：运营方安全

- 宏观的基础安全防护
  - 统一的DDoS保护
  - 统一的网络层异常攻击防护
  - 统一的网络日志留存分析，以符合网络安全法

私有云：运营方安全

- 云平台基本安全能力设置
  - 是否启用VPC功能，确保租户可以隔离到不同网络形成虚拟专用云
  - 是否启用安全组、防火墙等功能让租户自助配置

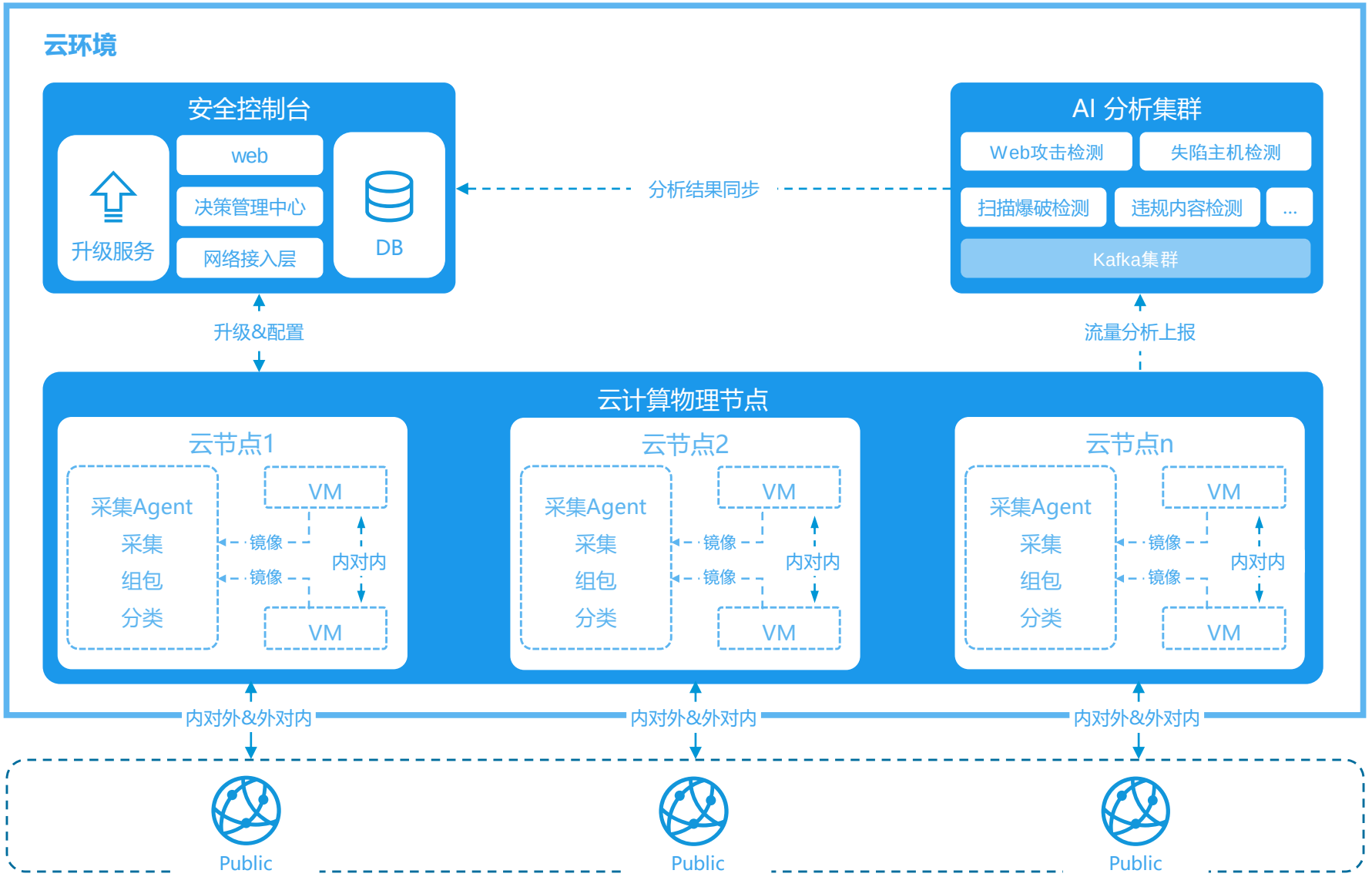
- 镜像安全管理
  - 镜像服务器安全管理：认证、授权、审计
  - 上传镜像自动化安全审计、批准流程：漏洞、基线等

私有云：租户安全

- 硬件安全资源池模式
  - 旁路部署、流量牵引
  - WAF、IPS、防火墙等等偏流量控制的安全产品

- 纯软件部署模式
  - 云主机本地检测agent部署模式
  - 漏扫类私有云SaaS部署模式

东西向攻击的问题！



- 与云平台WEB API整合，自动化分布式部署，随着云节点伸缩而伸缩。
- 与SDN接口对接，自动导入流量，自动下发拦截策略。
- 旁路部署模式，不对平台核心组件更改劫持，安全稳定。

混合云安全

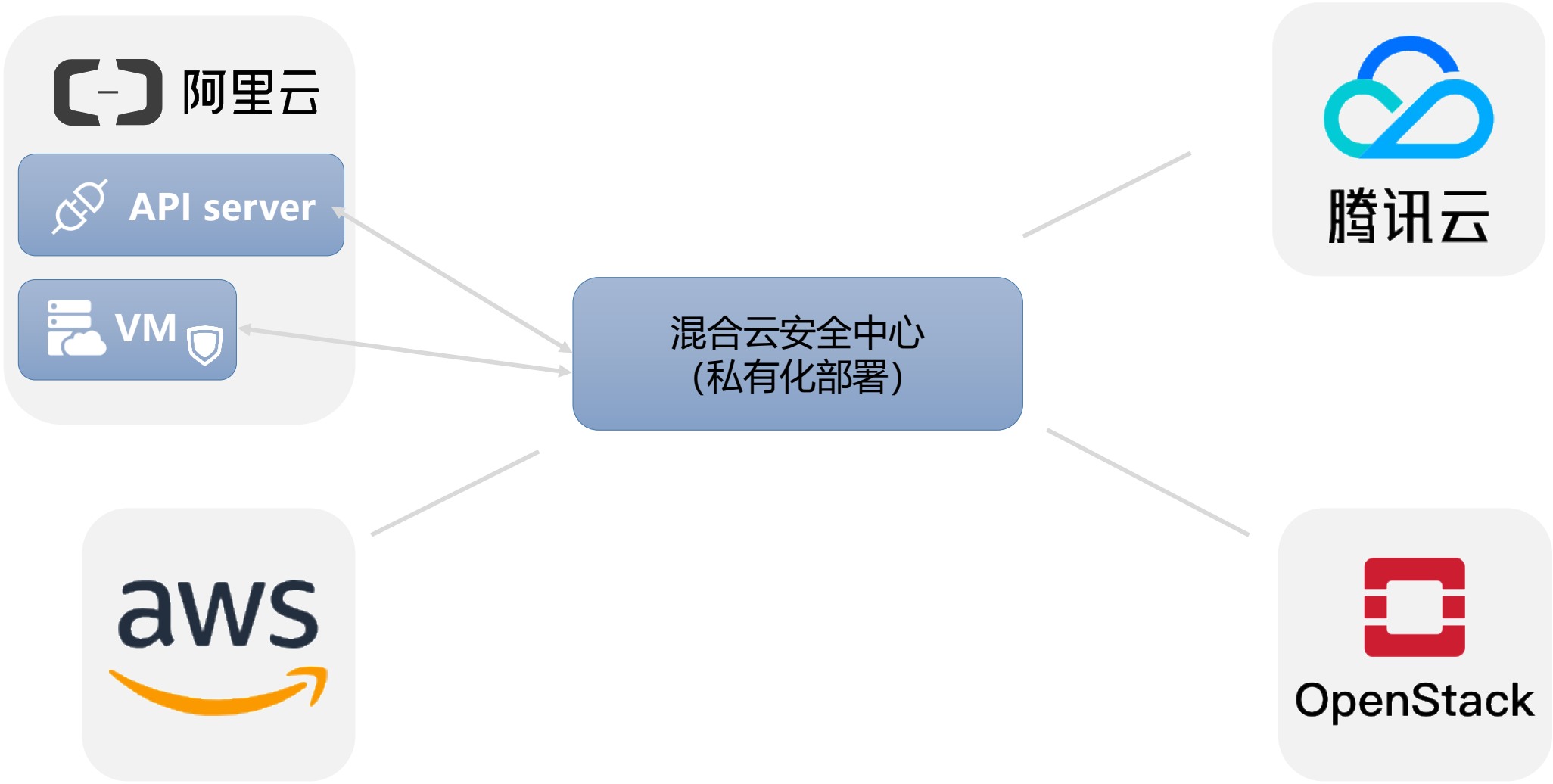
企业使用云，混合云是未来的方向

混合云是企业的方向

- 大中型企业私有云、公有云形成混合云
  - 前端业务部署到云获得云的弹性
  - 后端数据部署到私有云获得云的安全性
  - 跨越互联网打通VPC形成混合云
- 小企业异构公有云形成混合云
  - 阿里云、腾讯云等异构云容灾互备
  - 阿里云、AWS云兼顾国内外访问效率

混合云的安全挑战

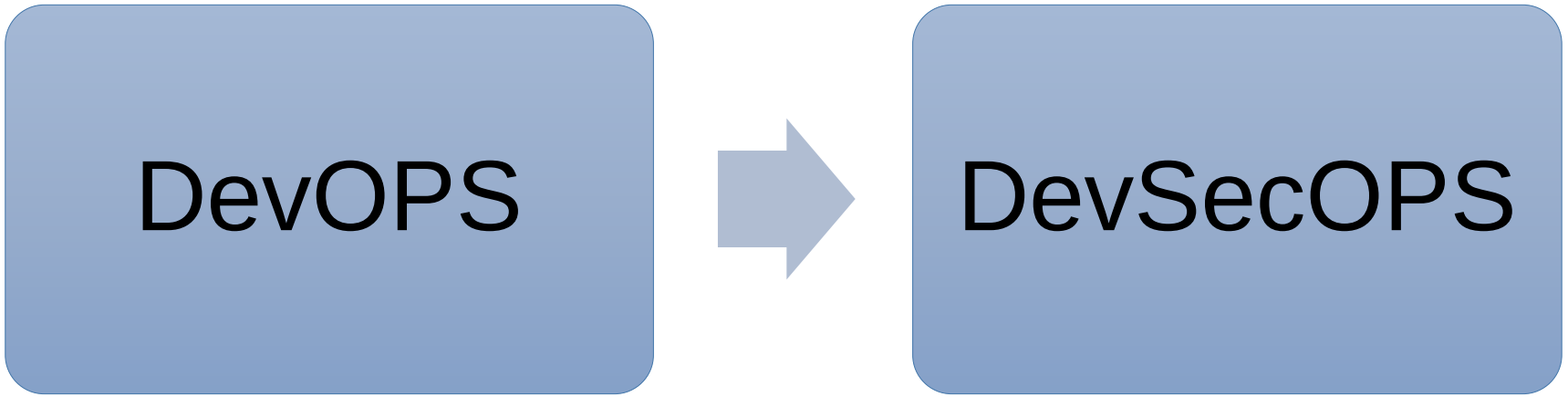
- 缺乏统一的安全管理平台
  - 无法实现统一的安全策略管理与分发
  - 无法实现统一的安全事件展示与处理
- 数据割裂无法进行统一的机器学习大数据分析
  - 数据存在于各个云的内部，只能独立分析
  - 网络五元组、系统日志、web日志、DNS日志……

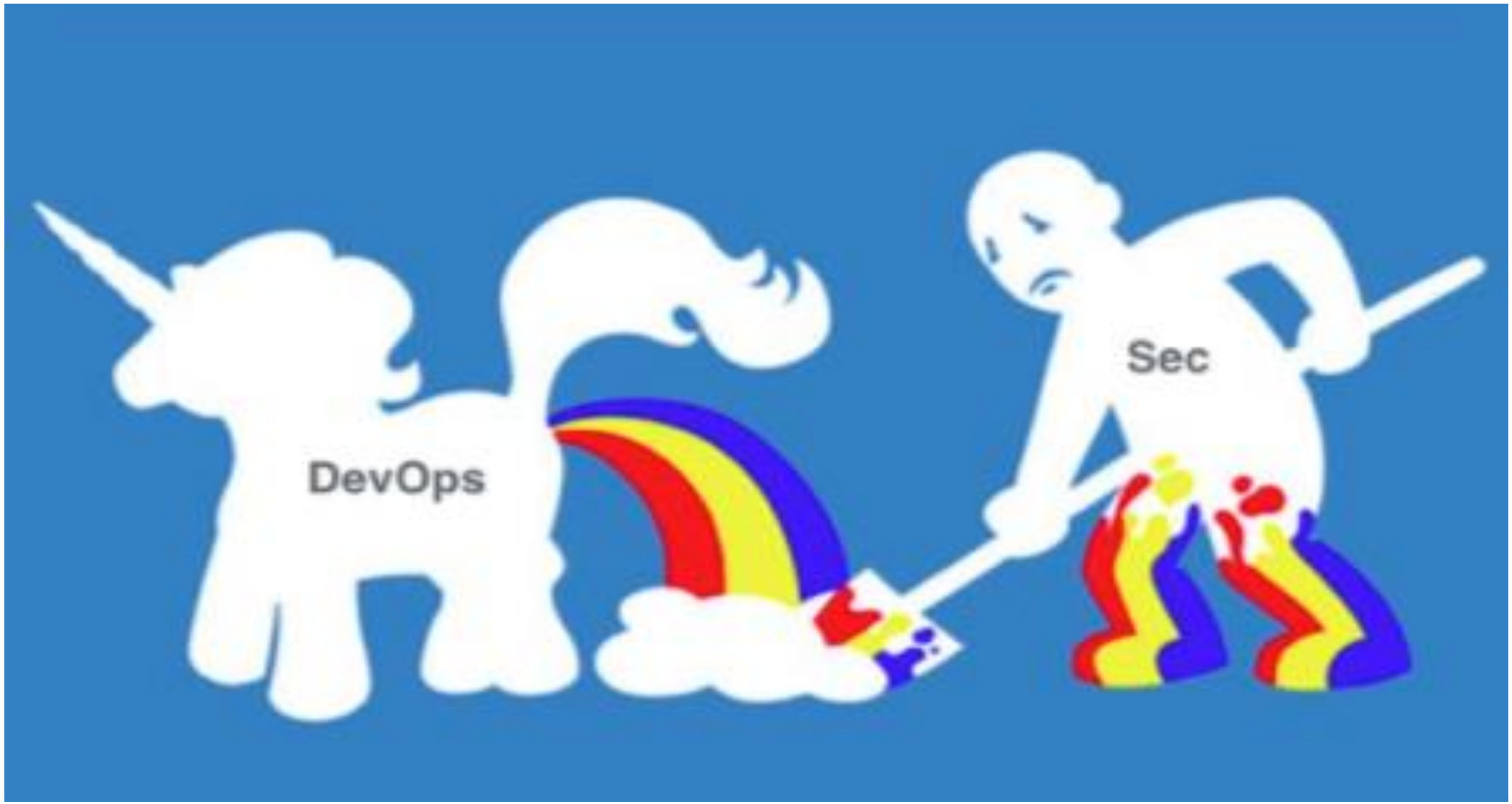

阿里云
API server
VM
混合云安全中心
（私有化部署）
腾讯云
aws
OpenStack

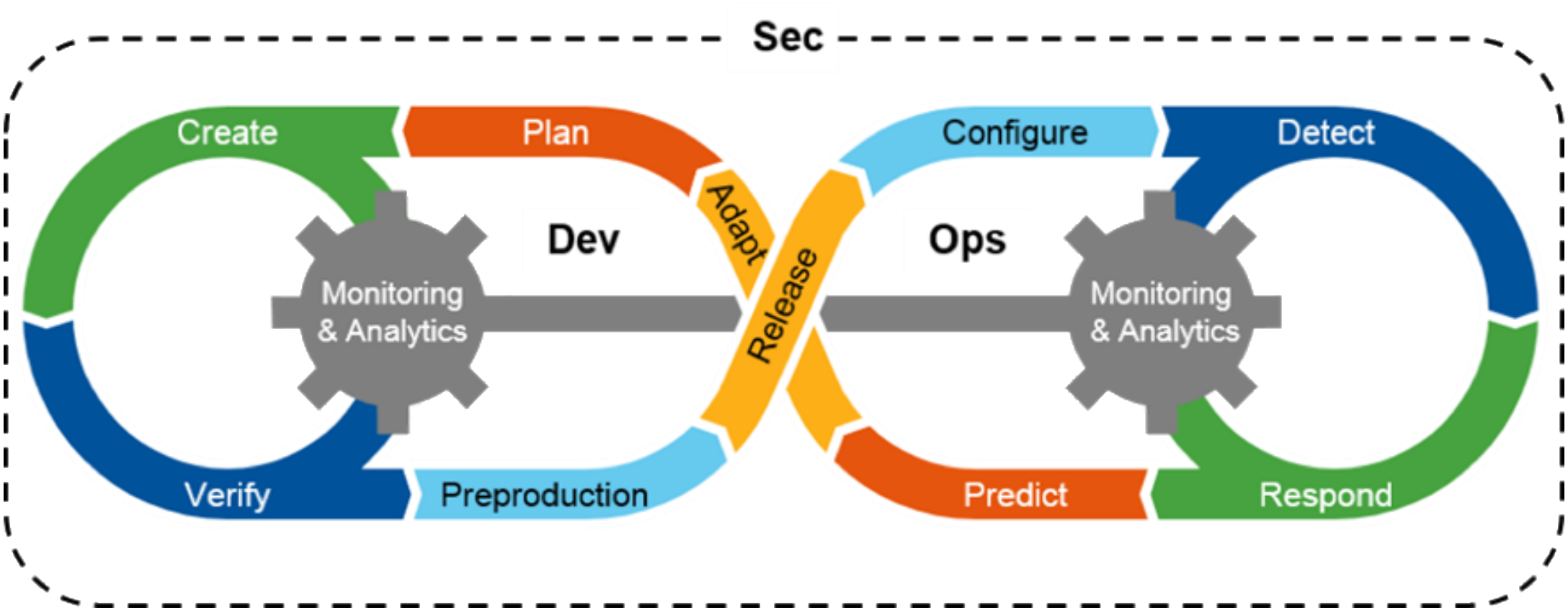
建云的安全问题基本解决

上云前的安全检查

从DevOPS到DevSecOPS，安全贯穿整个生命周期


DevOPS
DevSecOPS


DevOps
Sec


Sec
Create
Plan
Configure
Detect
Dev
Adapt
Release
Ops
Monitoring
& Analytics
Monitoring
& Analytics
Verify
Preproduction
Predict
Respond

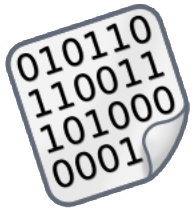
云时代，不建云的企业的安全重点

云一直在被使用，只是你不知道

据英国卫报报道，全球四大会计师事务所之一的德勤公司近日爆出公司史上最严重的黑客攻击事件，超过500万份内部邮件疑遭泄露，这些邮件中包含了大量德勤客户的敏感信息和知识产权。

颇为讽刺的是，德勤是世界最大的安全咨询公司，安全咨询服务是德勤公司的主要业务之一。


GitHub


010110
110011
101000
0001
PASTEBIN

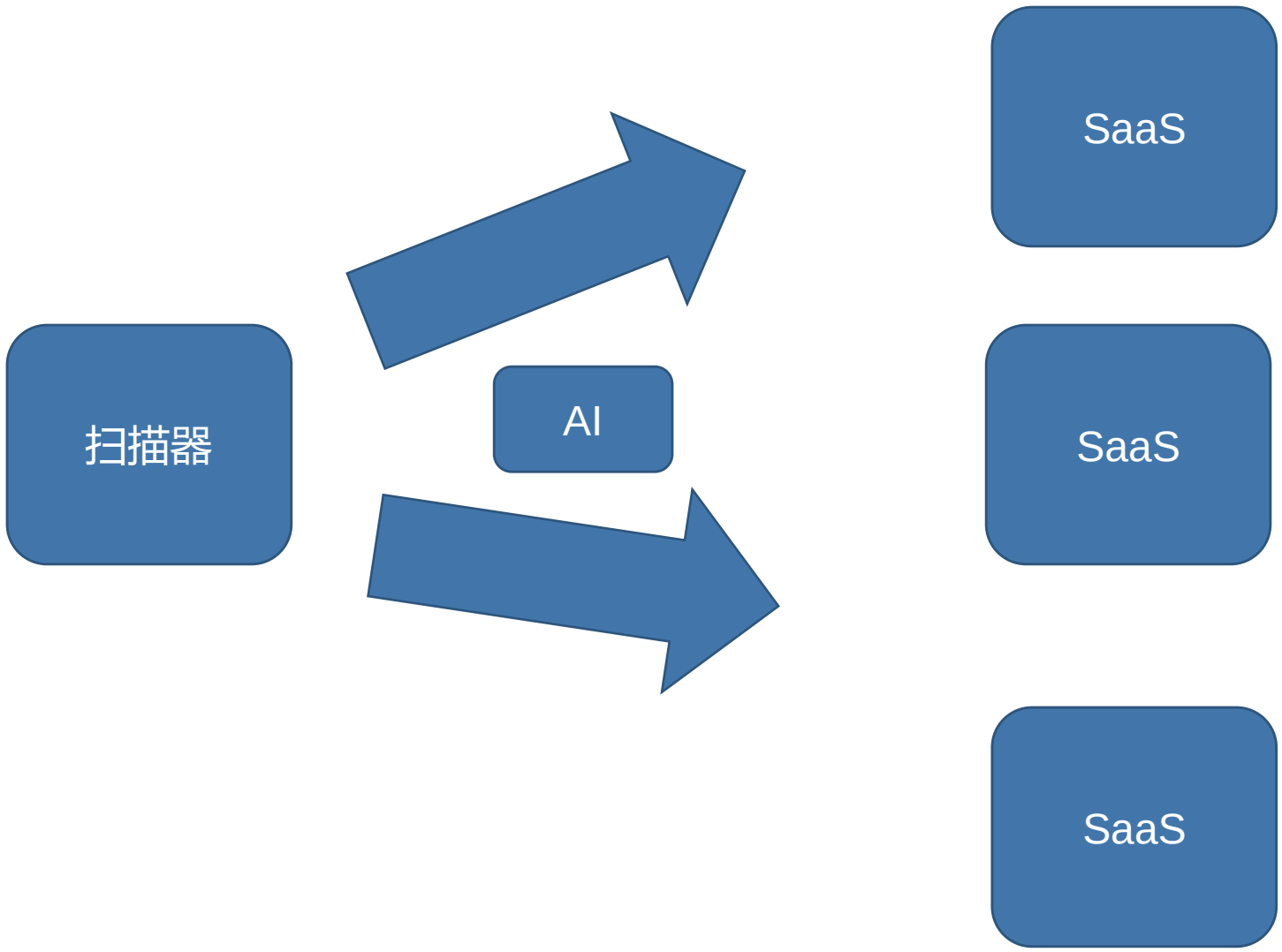

印象笔记™
EVERNOTE

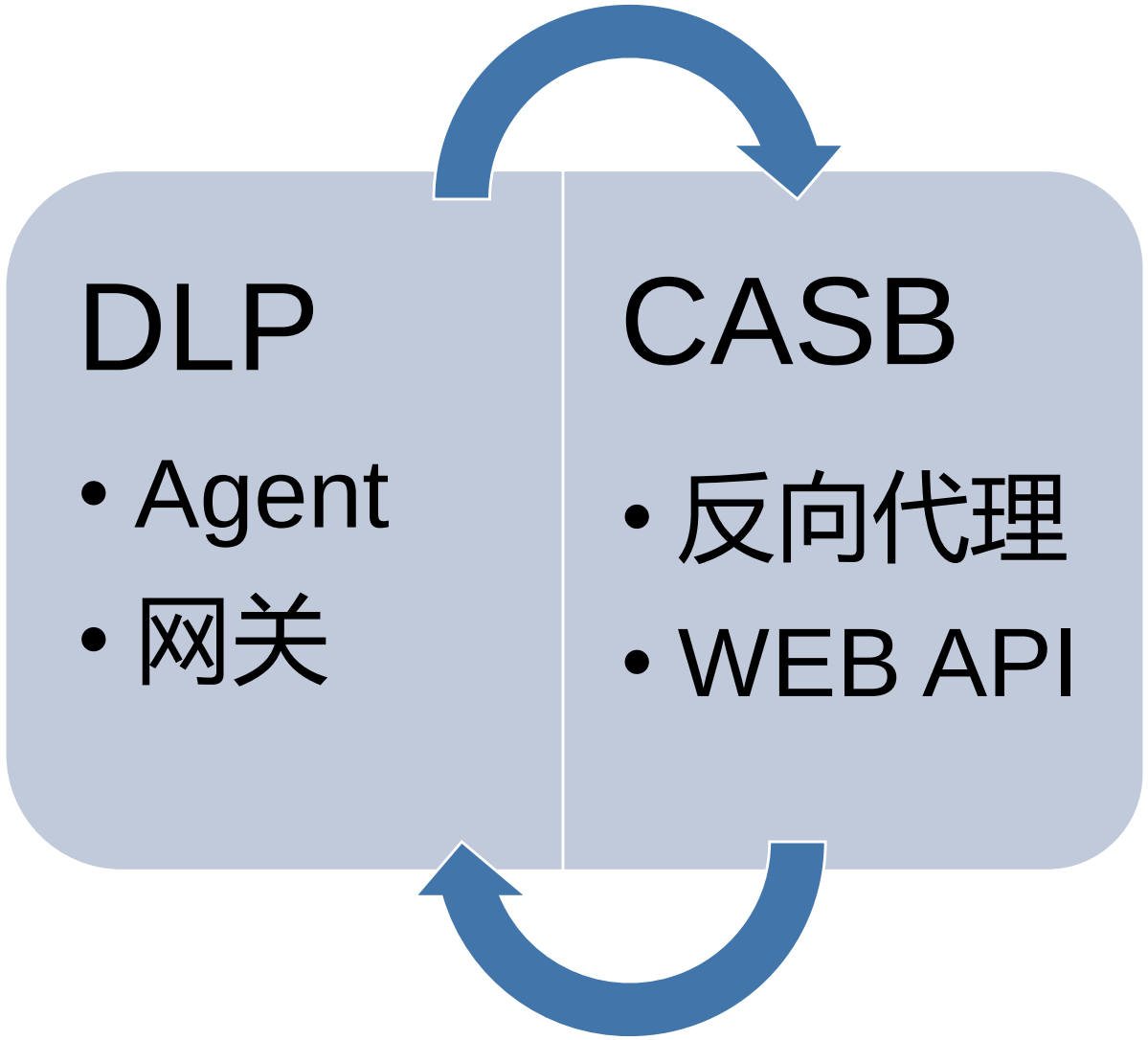

销售易
让销售更容易


百度云

数据泄漏保护

检测、防御敏感数据被员工不小心泄露到SaaS云服务里面

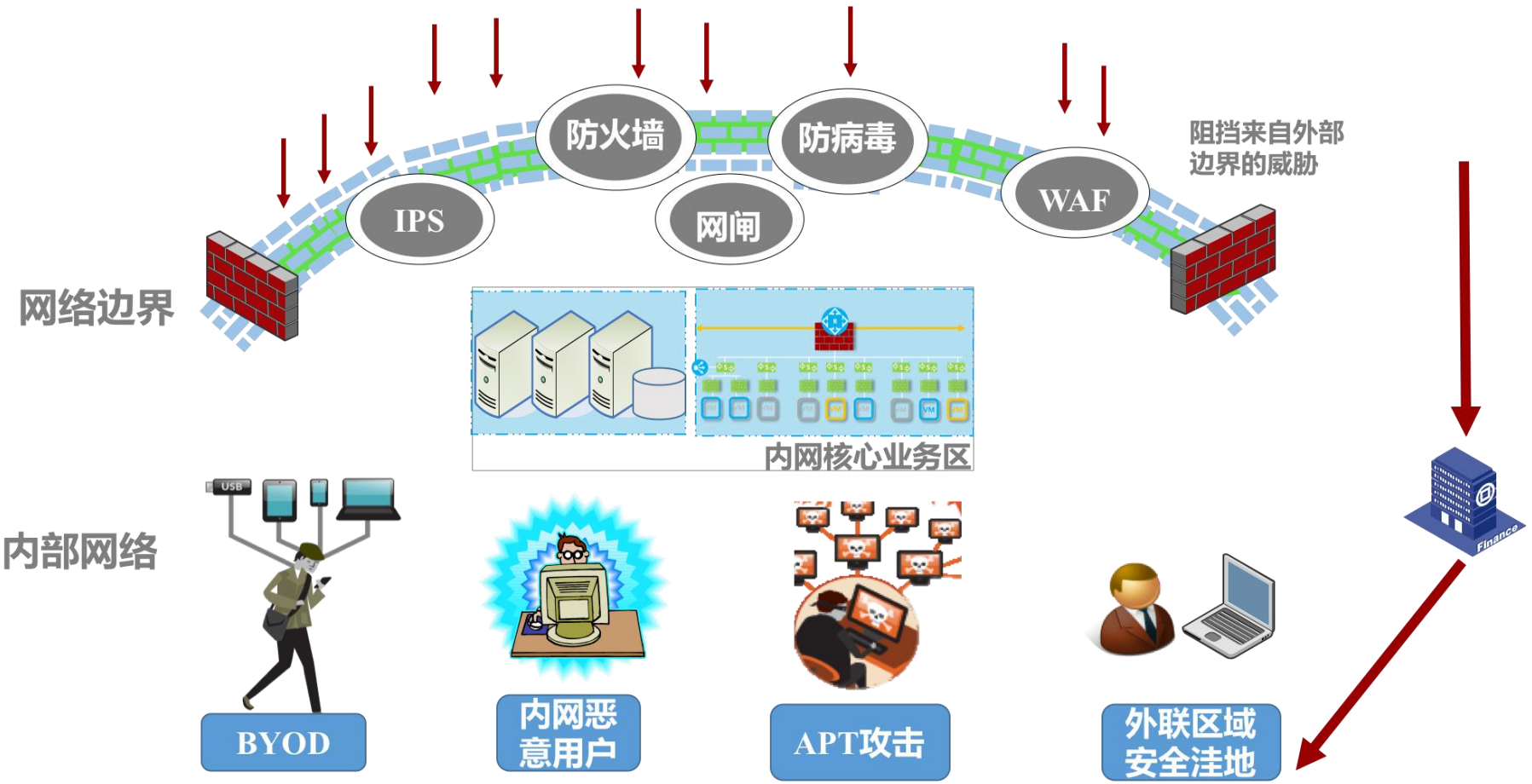

扫描器
AI
SaaS
SaaS
SaaS


DLP
• Agent
• 网关
CASB
• 反向代理
• WEB API

APT检测

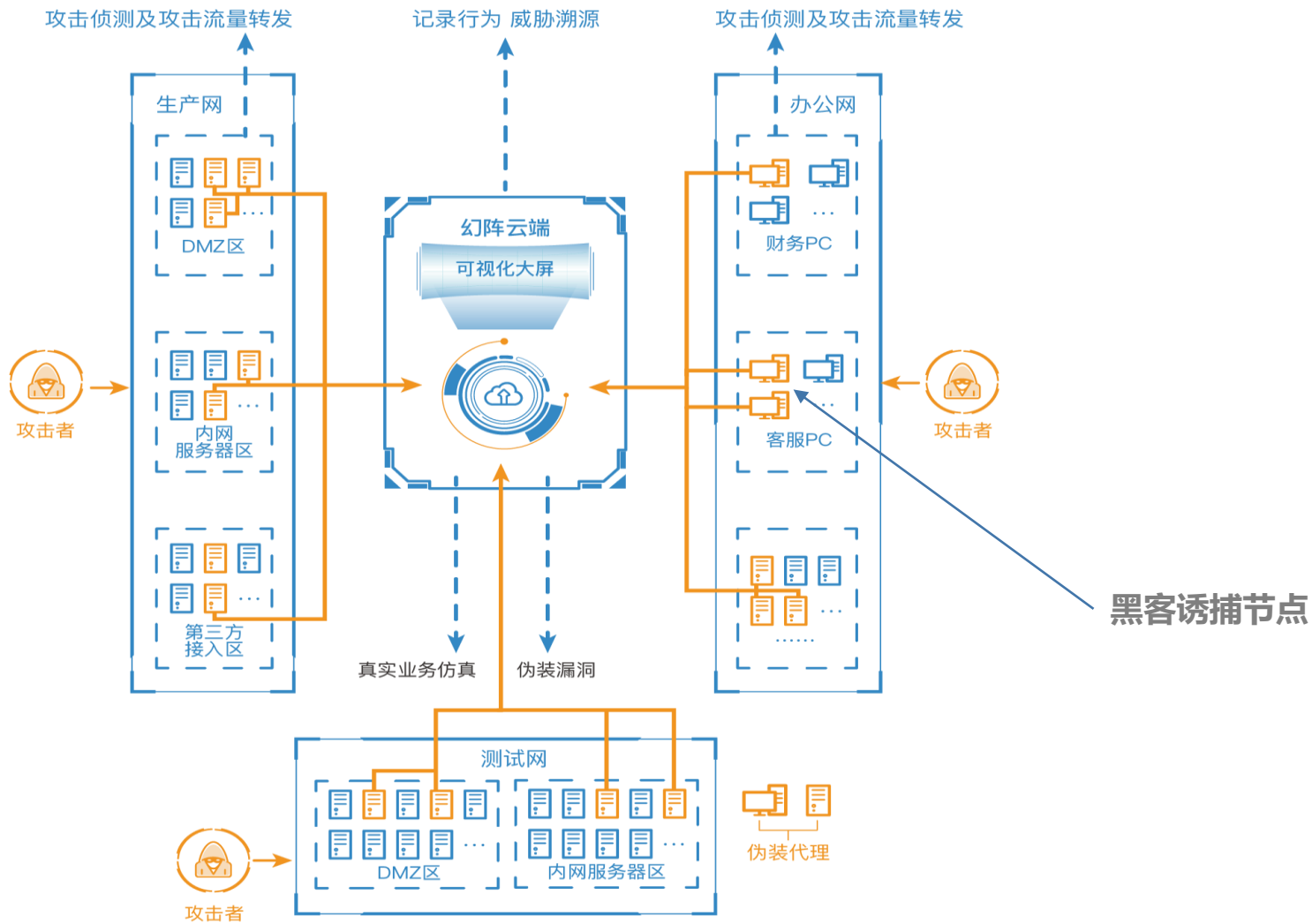
突破边界防御的高级持续性威胁，我们如何发现?

传统防护产品的局限



- 基于签名，需要升级
- 单点部署，局部风险检测
- 通常误报率较高
- 串联，故障风险高
- 无攻击溯源

旁路部署，分布式部署的安全产品



谢谢！