



新型微隔离技术在云内横向攻击 防护中的应用

云溪科技创始人 & 首席执行官

张斌

电话/微信: 13439623544

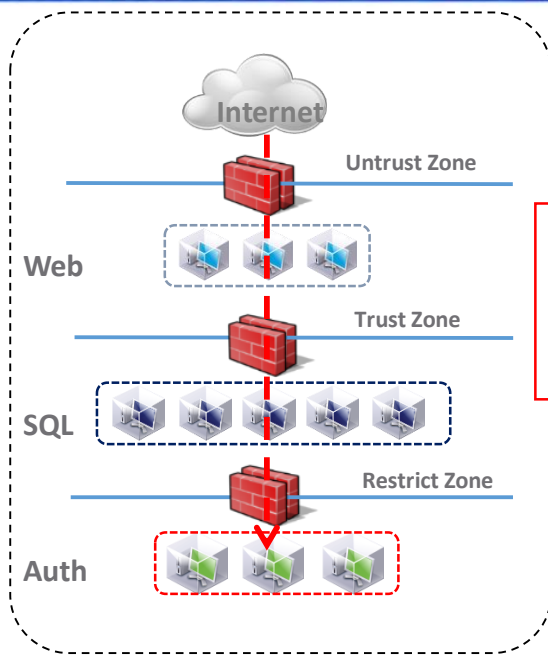
目录

云时代的新挑战

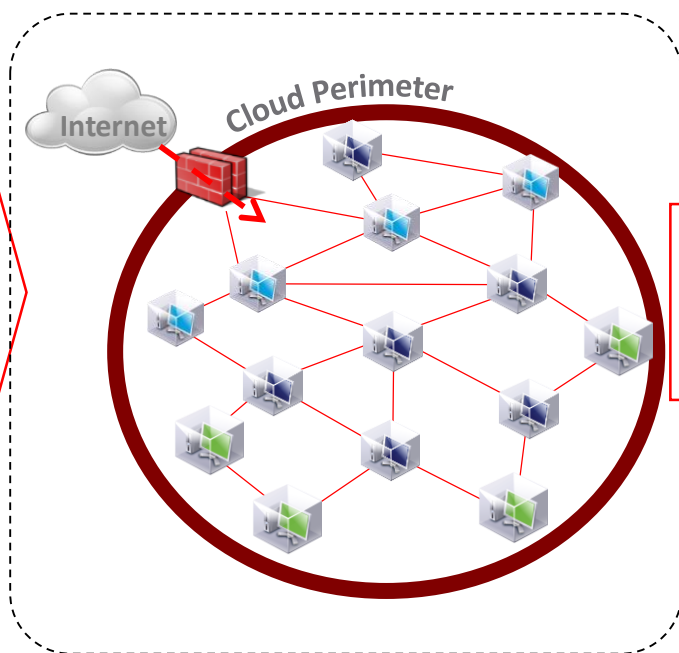
解决东西向安全的关键要素

什么是进程级微隔离技术

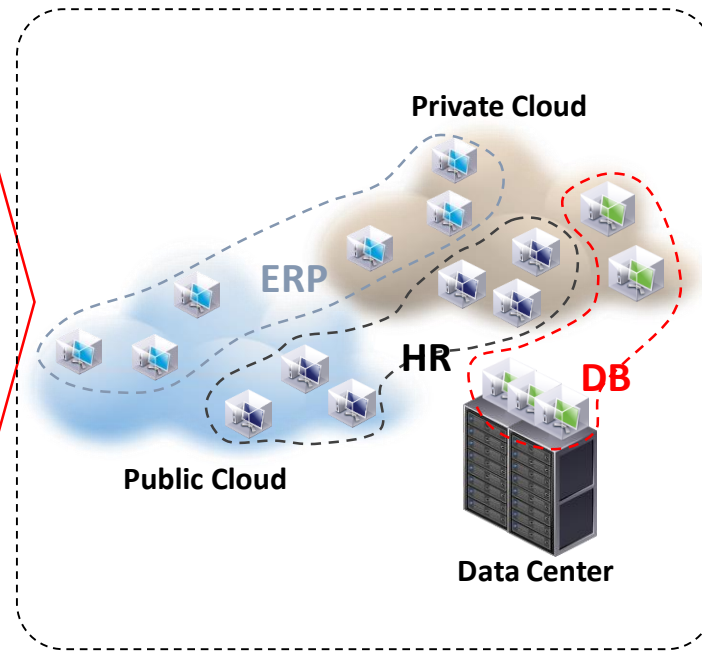
进程级微隔离技术的应用



传统IT架构



单一云架构



多云架构

1. 结构复杂

- 公有云、私有云、物理机、容器混杂部署
- 安全管理与网络管理进一步分离
- 安全管理变得碎片化

2. 流量模型改变

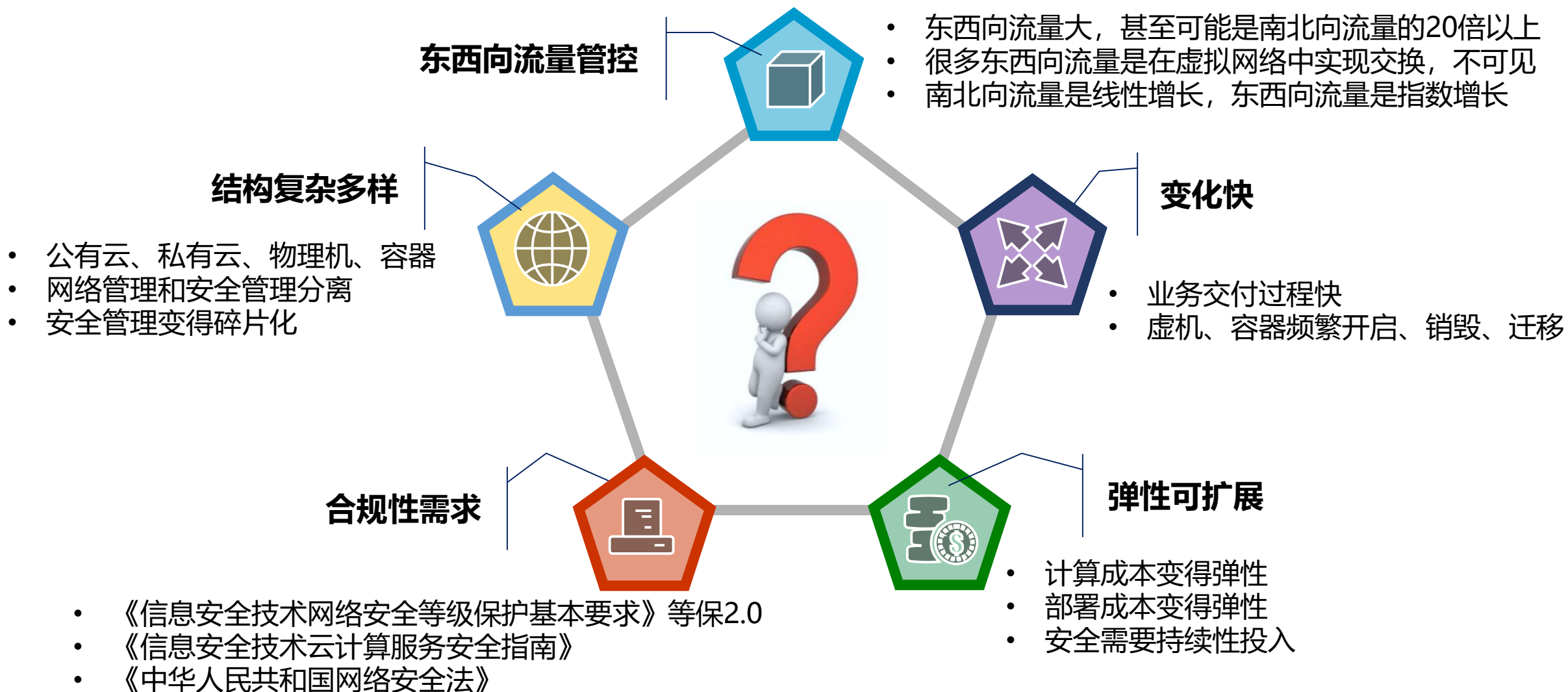
- 东西向流量大，甚至可能是南北向流量的20倍以上
- 很多东西向流量是在虚拟网络中实现交换，不可见
- 南北向流量是线性增长，东西向流量是指数增长

3. 变化快

- 业务交付和业务变更加速，由传统的以月计算，加速为以天计算，甚至一天几变
- 虚拟机、容器频繁进行规模伸缩和位置迁移

4. 成本更敏感

- 计算成本、部署成本、运维成本均变得更有弹性
- 安全需要持续性投入和运维



目录

云时代的新挑战

解决东西向安全的关键要素

什么是进程级微隔离技术

进程级微隔离技术的应用

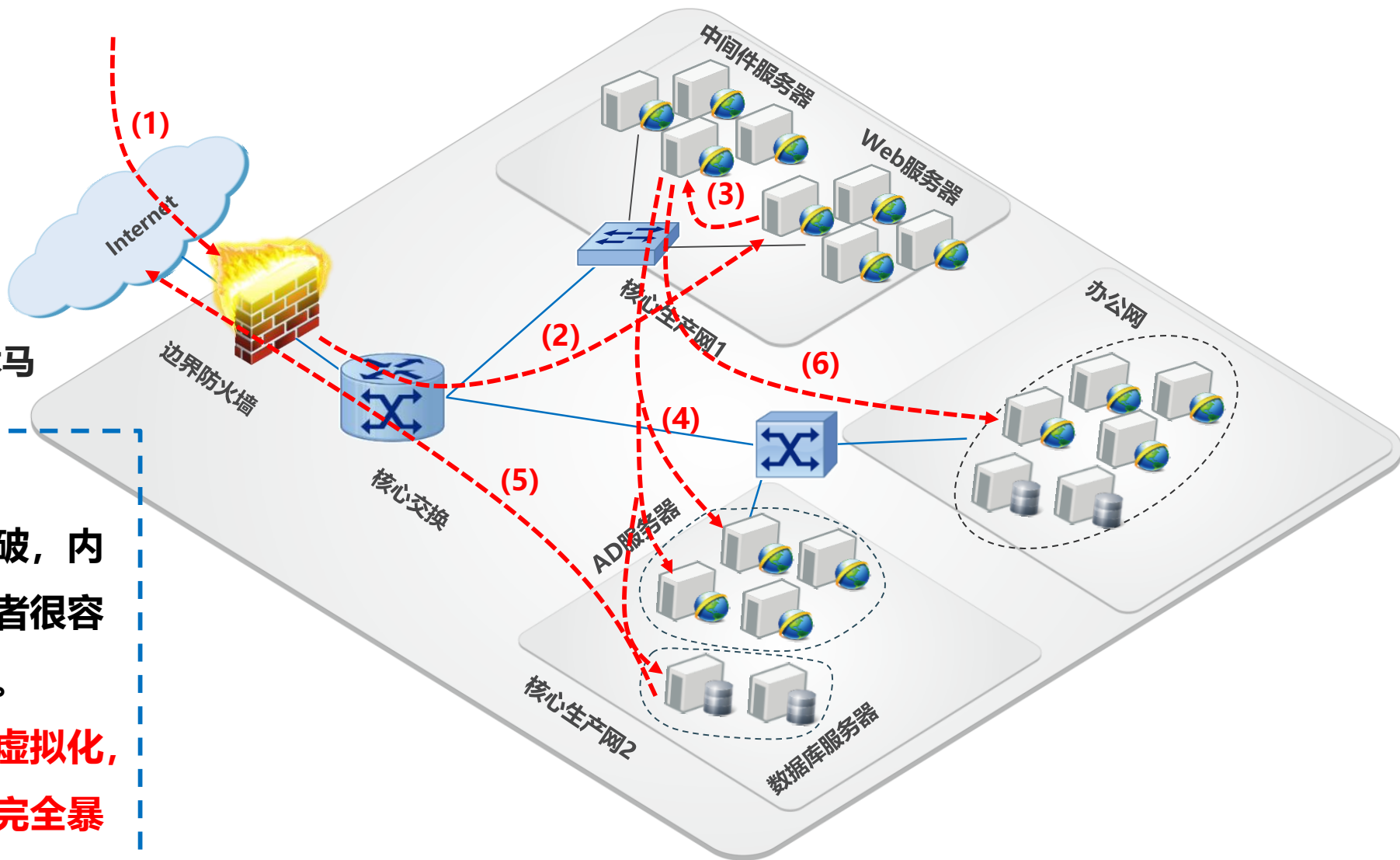
攻击过程还原：

- 1, 利用弱口令, VPN连入内网
- 2, 渗透Web服务器, 上传木马
- 3, 横向渗透, 攻克中转服务器
- 4, 横向渗透, 攻克DB服务器
- 5, 打包数据库文件, 拖库
- 6, 进一步攻陷办公电脑, 上传木马

案例启示：

当传统的边界的安全防护被突破, 内网将缺少纵深防御能力, 攻击者很容易在内网进行东西向横向渗透。

云环境下, 资源更是高度集中虚拟化, 一旦穿透进去, 东西向资产将完全暴露。





- ◆ 工作负载漂移是常态
- ◆ 业务迁移，弹性扩容总在路上
- ◆ “看不见”东西向流量

- ◆ 因为摸不到流量，所以无力检测
- ◆ 业务系统关联复杂，始终动态变化
- ◆ 传统网络检测需要引流，加剧流量复杂，覆盖不全，实可操作性差

- ◆ 边界防火墙鞭长莫及
- ◆ 虚拟机或容器间流量无法管控
- ◆ 工作负载数量庞大，五元组策略无法运维
- ◆ 无法实现快速响应

支撑关键要素的核心技术



可视化技术

资产可视化，动态标签化
流量可视化，进程可视化
威胁可视化



基于行为模型、流量模型的检测技术

业务关系建模
正常行为模型，流量模型自学习
异常网络行为识别



进程级微隔离技术

基于进程级的微隔离闭环，将攻击面缩到最小
策略计算引擎，自动生成微隔离策略
感知策略对业务影响



目录

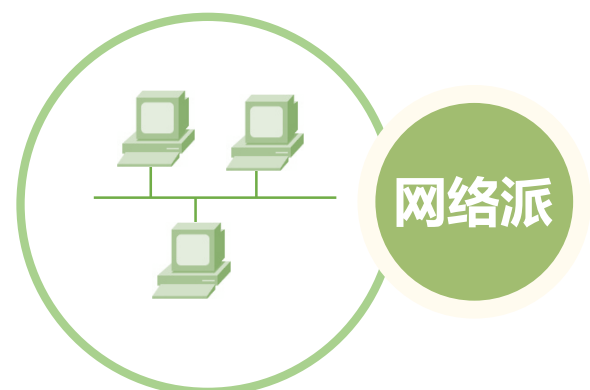
云时代的新挑战

解决东西向安全的关键要素

什么是进程级微隔离技术

进程级微隔离技术的应用

网络检测 VS. 主机检测



VS



典型产品	NGFW/NIPS	Sandbox/Honeypot
技术特征	<ul style="list-style-type: none">网络代理模式网络流量行为分析	<ul style="list-style-type: none">主机代理模式文件静态分析进程运行时行为分析
优势	<ul style="list-style-type: none">分析速度快对主机系统无影响	<ul style="list-style-type: none">信息更完整、精确度高主机管控能力强
劣势	<ul style="list-style-type: none">精确度差易误报对加密流量难以处理	<ul style="list-style-type: none">消耗资源高终端适配难

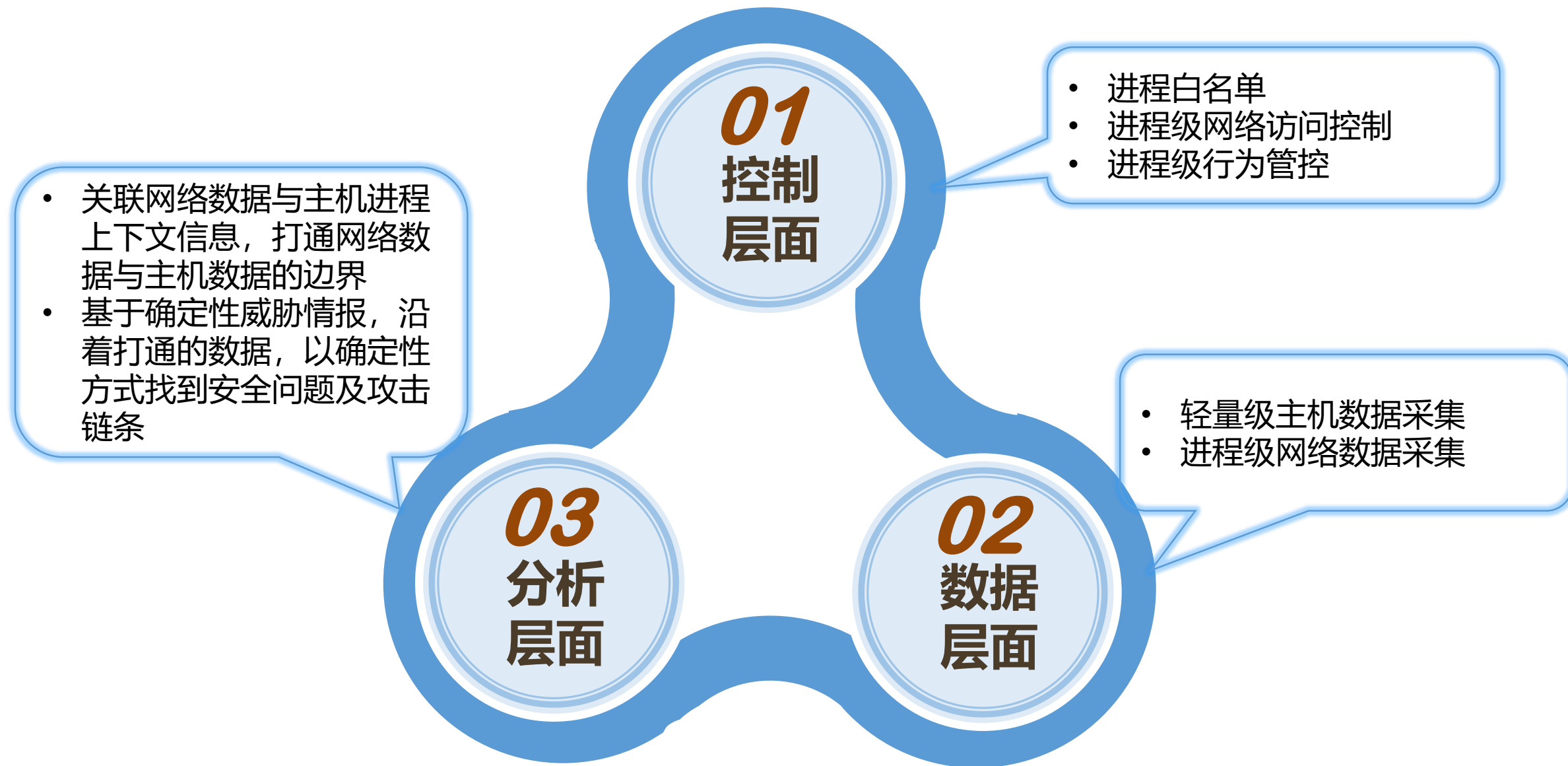
DL/AI来救场？

关联关系 VS. 因果关系

- 机器学习得到的结果更多地是一种“关联关系”
- 攻击判定所需要的是“因果关系”
- 问题：**关联关系可以替代因果关系吗？** 再多可能性的堆叠一定能推导出必然性？



进程级微隔离技术



传统管控方式

- ◆ 基于IP分组/网络分段管理，维护成千上万的地址簿
- ◆ 基于静态端口的控制，服务端口发生变化策略即告失效
- ◆ 基于静态策略，调整困难
- ◆ 基于IP白名单可信的前提，白名单若被攻陷，整体失控
- ◆ 基于暴力封堵，杀敌一千，自损八百

(只有开放式手术能力)

检测分析是过程
管控是最终目的



进程微隔离管控技术

- ◆ 基于标签化管理，维护若干标签
- ◆ 基于业务进程的精准控制
- ◆ 基于适应策略动态调整场景
- ◆ 基于白名单也不可信的前提，白名单基础上查行为
- ◆ 结合进程上下文的网络行为分析，让检测过程更精确且高效
- ◆ 基于进程隔离有效管控，兼顾安全与业务

(兼具微创与开放式手术能力)

目录

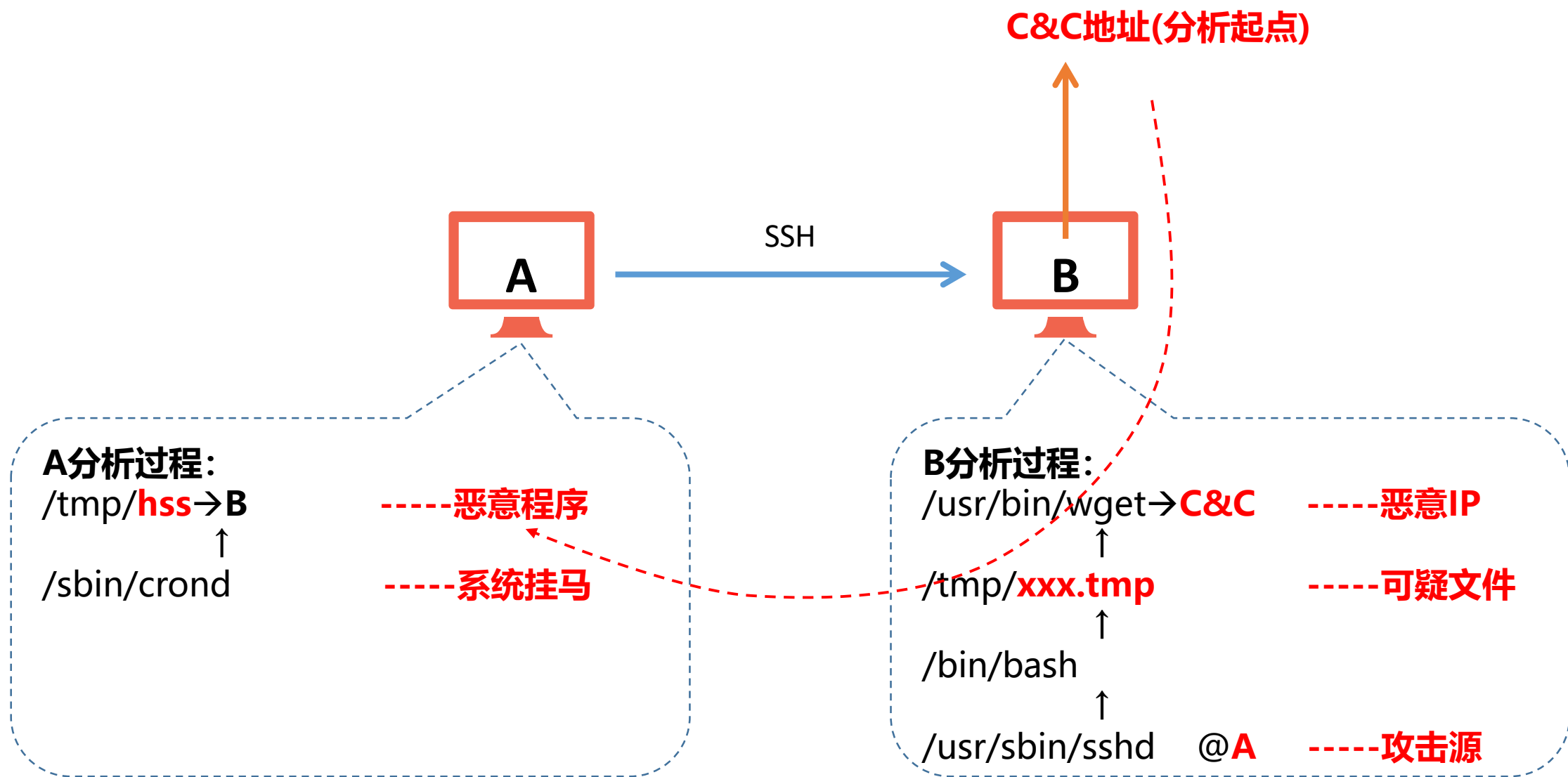
云时代的新挑战

解决东西向安全的关键要素

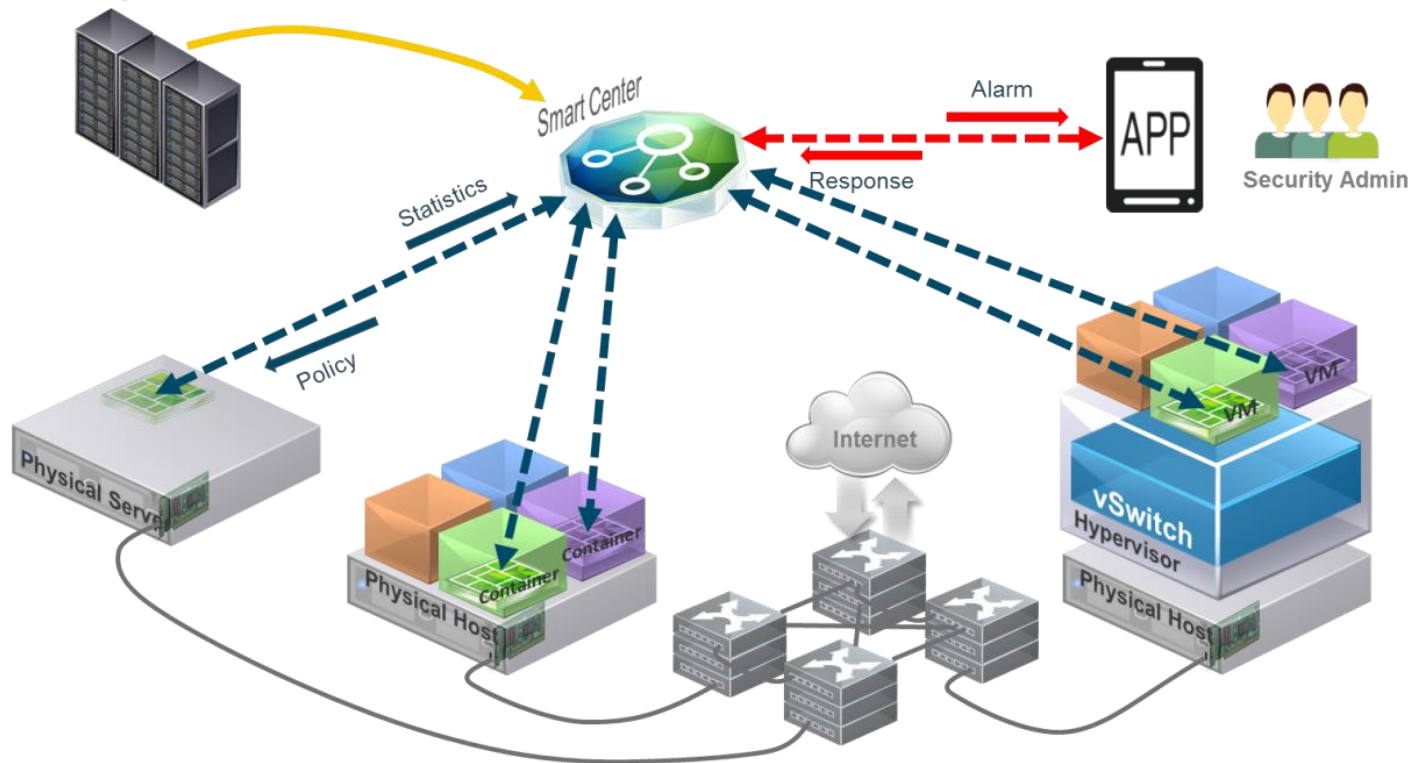
什么是进程级微隔离技术

进程级微隔离技术的应用

举例



Threat Intelligence Center



工作负载端探针



收集服务器网络连接信息，上报管控中心，并接受管控中心计算得到的本地防火墙策略并下发本地操作系统。

管控中心 (Smart Center)



负责接收工作负载探针上报的网络信息并根据管理员配置的策略实时计算并下发每一台被管理的工作负载上的本地策略。管控中心可以是服务器，也可以是一个SaaS服务。

手机管控应用

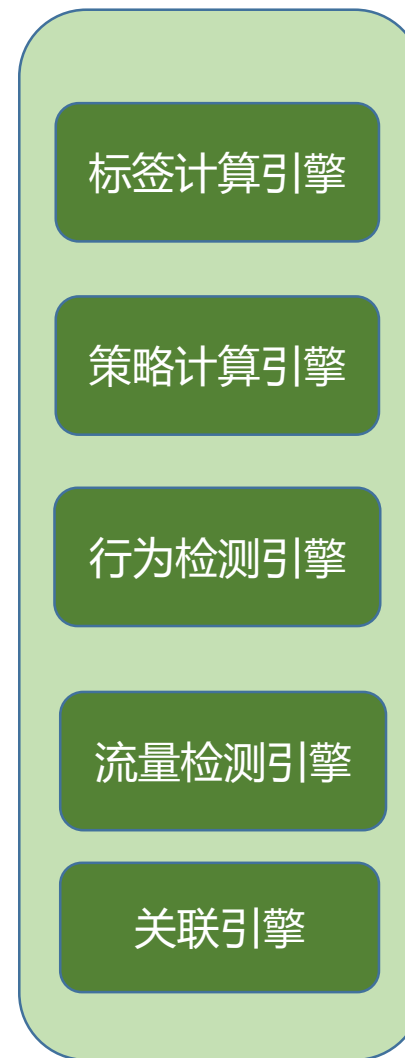
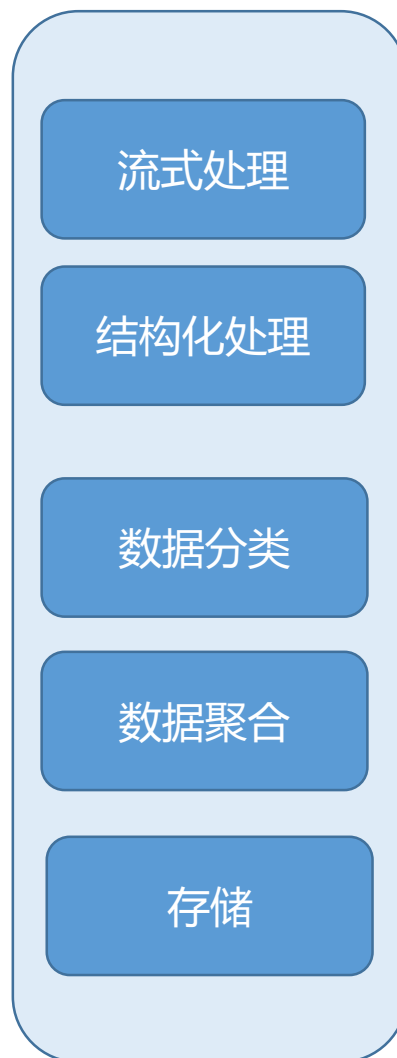
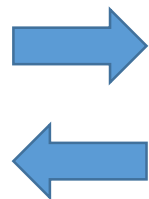



管控中心发现安全威胁，可以在本地管理界面告警，也可以通过手机管控应用实时告警。管理员可以通过手机应用查看告警并做出响应。

智能情报中心



依托安全专家，使用大数据及人工智能技术，将安全威胁情报、网络安全态势、网络流量模型推送到管控中心，使得管控中心可以根据安全情报进行流量智能分析和策略智能下发。





THANKS

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE