网络安全创新大会
Cyber Security Innovation Summit

面向实战的云安全体系构建与实践

张斌　云溪智联（北京）科技有限公司创始人

目录

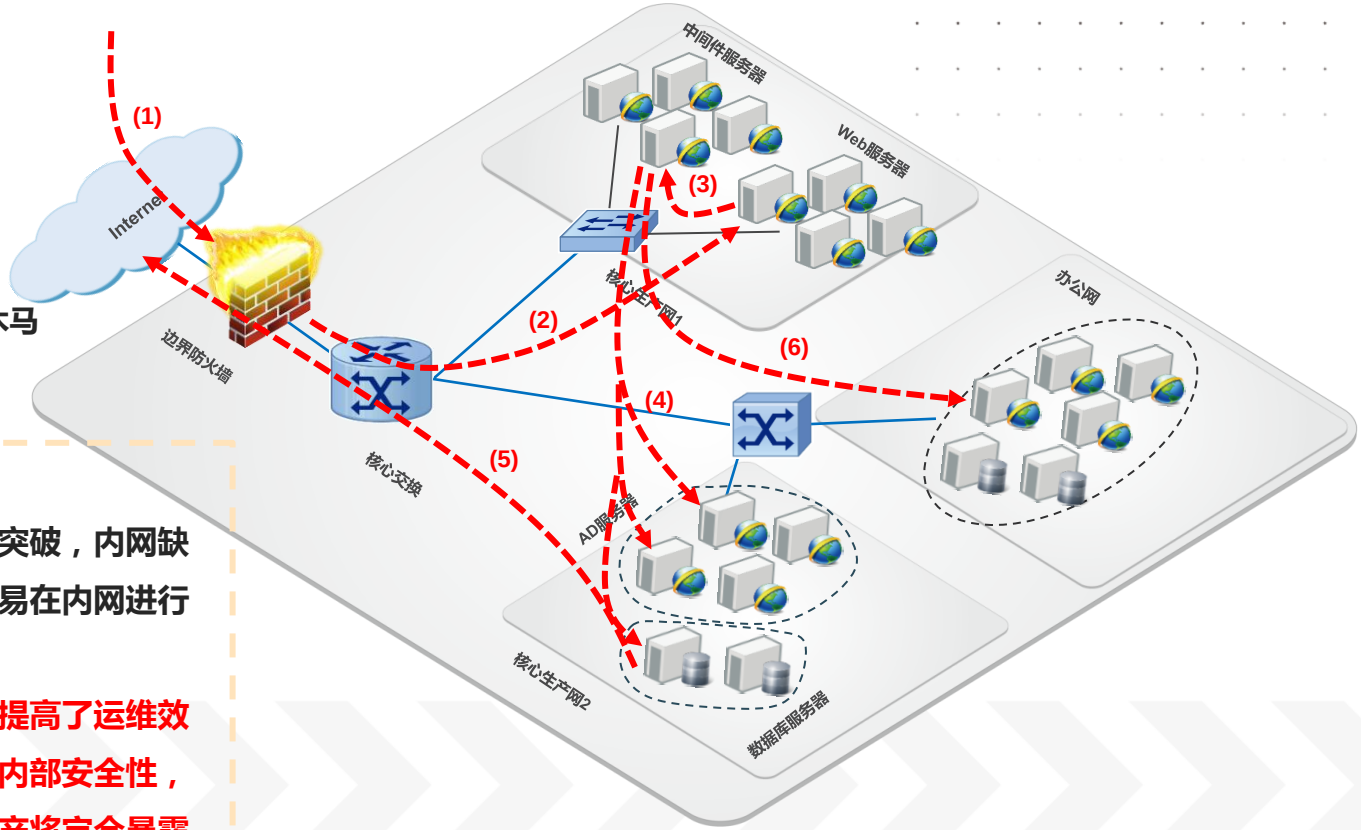
CONTENTS

HW带来的思考

某知名酒店数据泄露事件

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：

当传统的边界安全防护设施被突破，内网缺少纵深防御能力，攻击者很容易在内网进行东西向横向渗透。

云环境简化了内部网络拓扑，提高了运维效率和灵活性；副作用是牺牲了内部安全性，外部边界一旦被突破，内部资产将完全暴露。

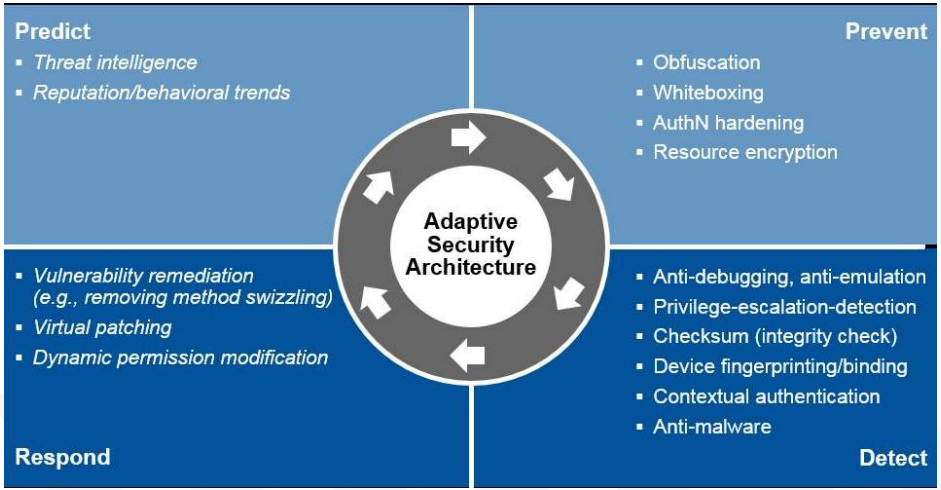
HW蓝军流程剖析

PHASE1：备战阶段（兵马未动、粮草先行）

- 技术准备：安全设备策略加固、系统升级、终端加固、网络加固
- 人员准备：上百人驻场支持，团队培训、融合，提供7x24小时服务

PHASE2：实战阶段（大规模多兵种协同作战阶段）

- “检测”集团军群：IDS、WAF、探针、EDR
- “监控”集团军群：资产探查、应用监控、态势感知、威胁情报、安全通告
- “分析研判”集团军群：总部分析研判、分支分析研判、溯源取证
- “响应处置”集团军群：攻击处置、策略调整、业务恢复



问题总结

备战阶段

- 资产探查不彻底，存在死角，进而形成攻击暴露面
- 人员培训缺少横向的交流——不知己

实战阶段

- 团队多、协调不善
- 响应速度慢、处置方式简单粗暴不治本
- 非核心业务系统关闭下线
- 缺乏自动化、人困马乏

结论：惨胜，不是真正面向实战的，难以复制

改进思路

总体思路：人与武器充分结合，构建以资产为核心的大纵深防御体系

战法改进：

- 资产为核心
- 纵深防御
- 协防协控
- 重日常运维

武器改进：

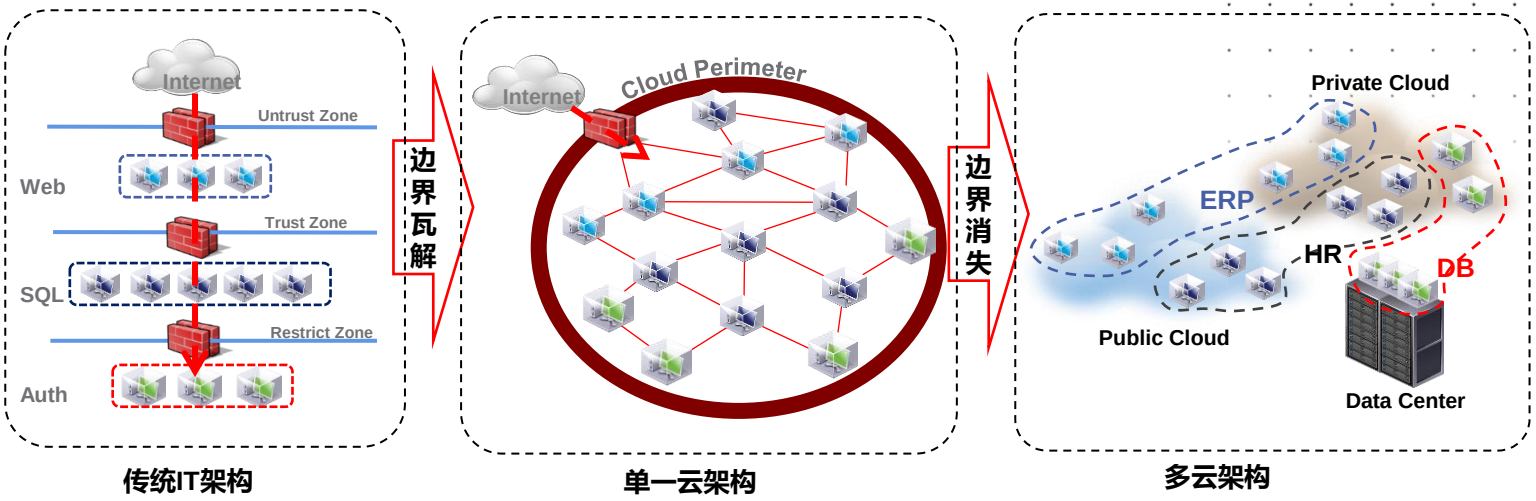
- 零信任体系
- 自动化、智能化

人的改进：

- 人的智能+机器的智能
- 运维流程与安全工具的结合
- 人和武器能力边界的打通

云安全难在哪里？

云时代 IT运维新挑战



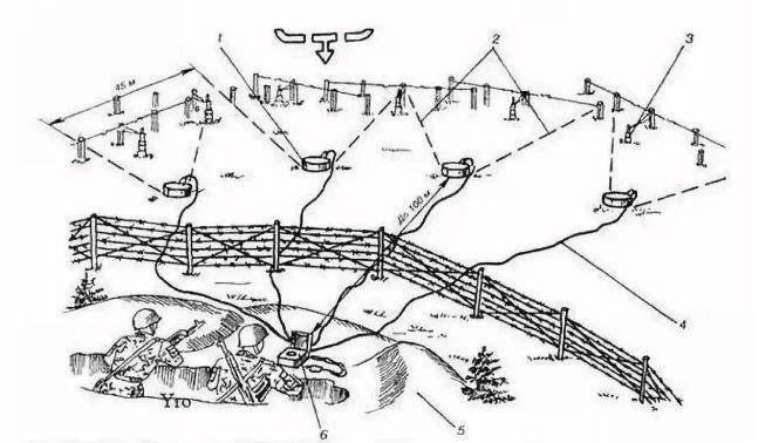
1. 结构复杂
- 公有云、私有云、物理机、容器混杂部署
- 安全管理与网络管理进一步分离
- 安全管理变得碎片化

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

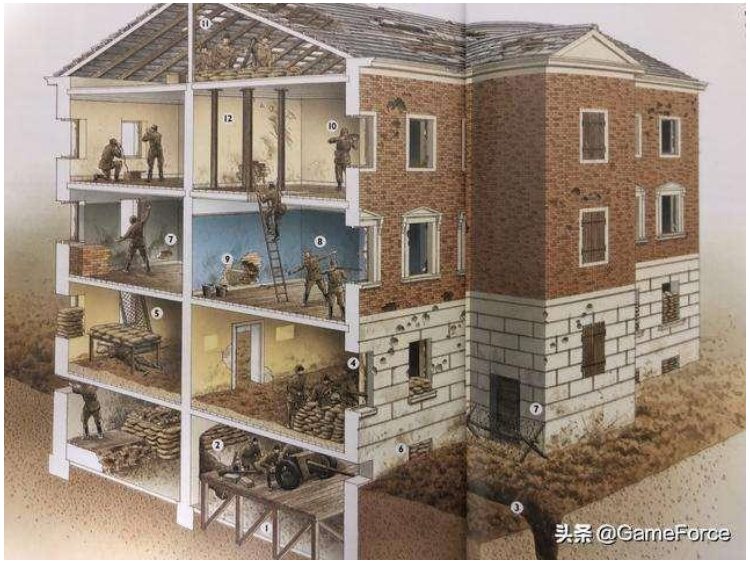
3. 变化快
- 业务交付和业务变更加速，由传统的以月计算，加速为以天计算，甚至一天几变
- 虚拟机、容器频繁进行规模伸缩和位置迁移

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

想象与现实



想象



现实

云安全为何难做？

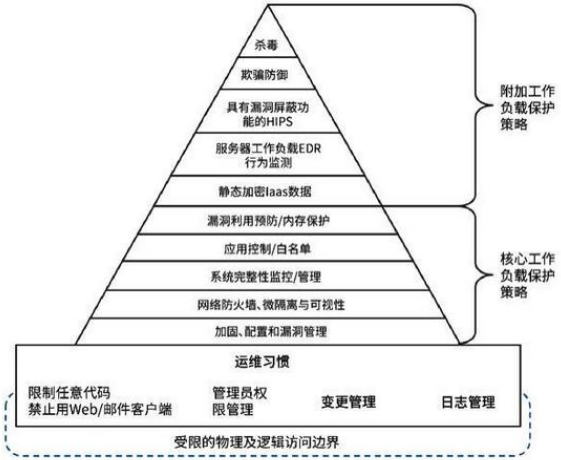
- 云内流量不可见，无法解决威胁、攻击问题。
- 虚机数量众多、分散。
- 策略影响未知，操作提心吊胆。

- 多云，混合云等异构环境，无法适应部署。
- 环境中可能即有物理服务器，虚拟机，也有容器。

- 云内虚机数量动辄千计，东西向策略数量数量庞大。
- 业务变化或扩展、 虚机迁移、业务迁移时运维难以进行。

面向实战的云安全体系构建

技术方向



CWPP：纵深防御体系

零信任：灵魂思想

DevSecOps：人与武器的结合

产品安全理念

可见 可管 可控

安全起始于“**所知**”，止于“**管控**”。

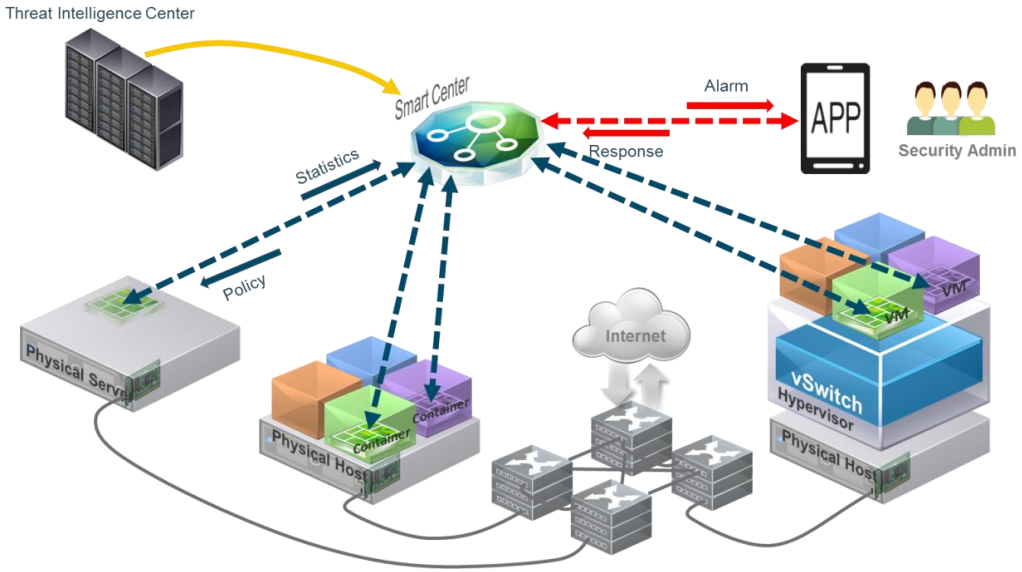
“**知**”：知识可以是通过人的经验总结、规章制度形成的经验知识。

“**见**”：知识获取后，我们将它们分为“who”、“what”、“how”、“where”四个大的维度，再进一步分别划分为“进程”、“漏洞”、“地域”、“用户”、“行为”等几十个细分维度，同时将它们进行可视化呈现。

“**感**”：**安全是动态变化的，**当人的知识无法做到预判的时候，就通过可视化，智能化帮助用户发现风险和威胁，**通过持续运营的方式，用户又可以基于所知，所见，对所有维度进行细粒度管控，持续缩小攻击面，使安全闭环。**

云溪科技解决方案

自适应云安全管控系统



云溪自适应云安全管控系统：能够在混合云体系下，对云内东西向流量做全面精细的可视化分析，并进行统一的细粒度安全策略管理。通过革命性的自适应微隔离技术，可减少策略总数90%，大幅提升运维效率，大幅缩短业务交付时间，让安全能够跟随用户业务实时适配。

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

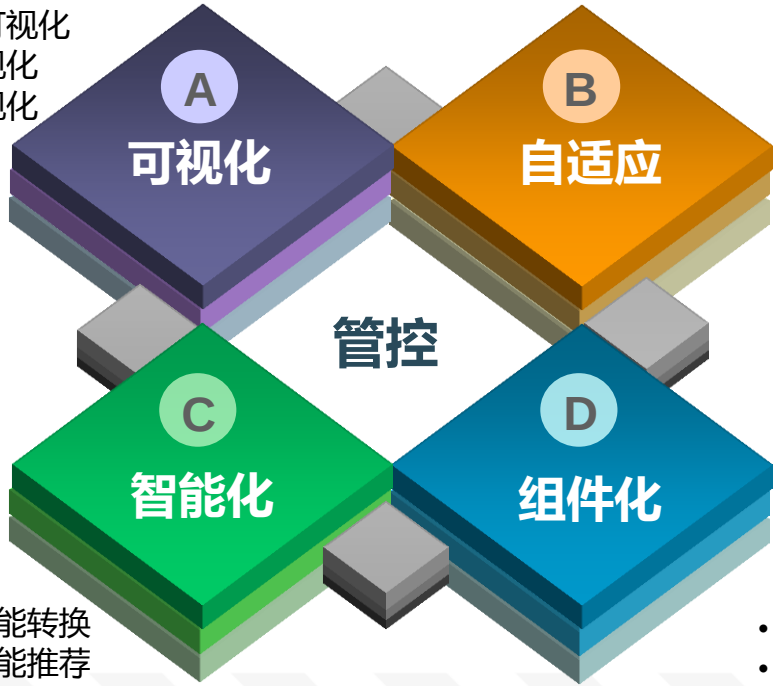
管控中心发现安全威胁，可以在本地管理界面告警，也可以通过手机管控应用实时告警。管理员可以通过手机应用查看告警并做出响应。

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。

核心技术能力

- 东西向流量可视化
- 安全策略可视化
- 攻击威胁可视化
- 资产可视化
- 风险可视化



- 实时感知工作负载状态变化：创建、销毁、迁移、配置等变化
- 管控策略跟随业务系统变化自动适应
- 角色、环境、位置、应用等标签维度在异构混合环境中自适应

- 标签策略智能转换
- 安全策略智能推荐
- 安全态势智能感知

- 产品每个组件都具备API化能力
- DevSecOps自动化支持

核心价值总结

保障合规	按照等保2.0体系要求设计，助力云上合规要求。
摸清家底	资产可视，业务系统、操作系统、中间件等核心资产。
看清风险	资产风险可视，业务系统等脆弱性漏洞情况清晰可见。
揪出失陷	大数据行为分析、情报碰撞等核心技术发现失陷主机。
管控威胁	精细化的微隔离管控，缩小攻击面，关闭暴露面。

网络安全创新大会
Cyber Security Innovation Summit

THANKS