唯品会 | 唯品会安全应急响应中心

因唯安全 所以信赖

2017唯品会第二届电商安全峰会

——深度揭秘唯品会信息安全建设实践

苏州
中国·苏州

安全之弹性管控

无客户端准入系统

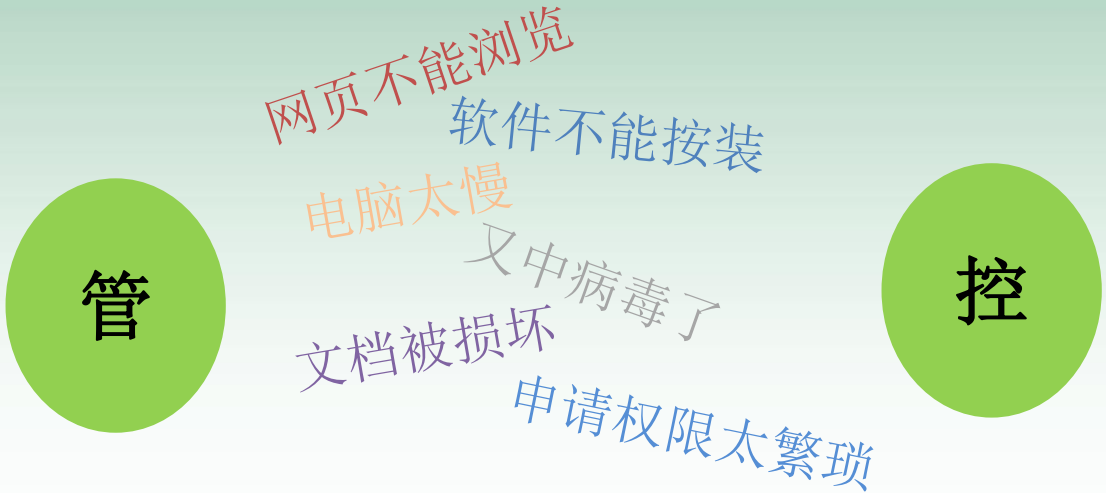
朱应龙

提纲

（一）安全弹性管控

（二）弹性思维实现内网无客户端准入

话说管控



都与安全管控息息相关。。。

思索

管控目的是什么

业务需要什么

为了管控，我们在忙些什么

管控面临问题

策略？　　技术措施？　　真实风险？

新的挑战

管控如何做

端正态度

不为安全而做安全
安全服务业务

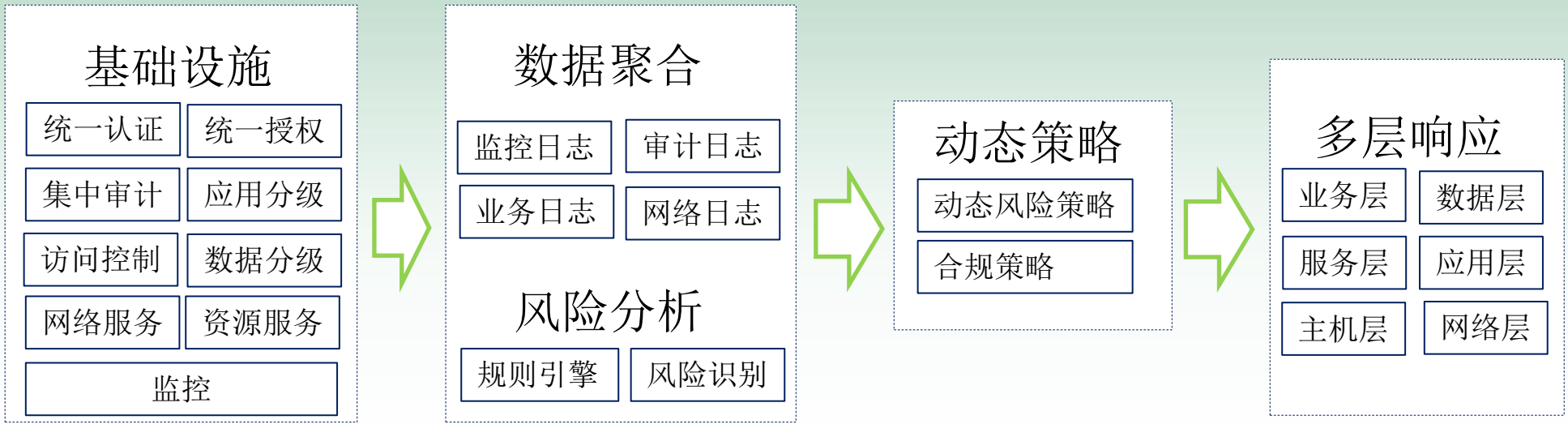
探索出路

适度安全、弹性管控

弹性管控

弹性的核心就是“动”，让规则、策略、响应措施“动”起来，适应动态变化的环境、动态变换的风险，让人、设备更好、更安全地利用资源，让资源得到最大化利用。

弹性管控模型



弹性管控实践

——网络准入系统

概念

网络准入概念说法不一（百度）

功能描述基本一致：

1）用户身份认证

2）终端完整性检查

3）终端安全隔离与修补

4）非法终端网络阻止

5）接入强制技术

主流方案

802.1x	网关	DHCP	ARP
安装客户端 运维工作量大 故障率高	部署专用设备，网络架构调整，控制范围受限	安装客户端 运维工作量大 DHCP服务分散情况下很难实现	子网部署探针， 响应的准确性存在一定的问题

共性问题

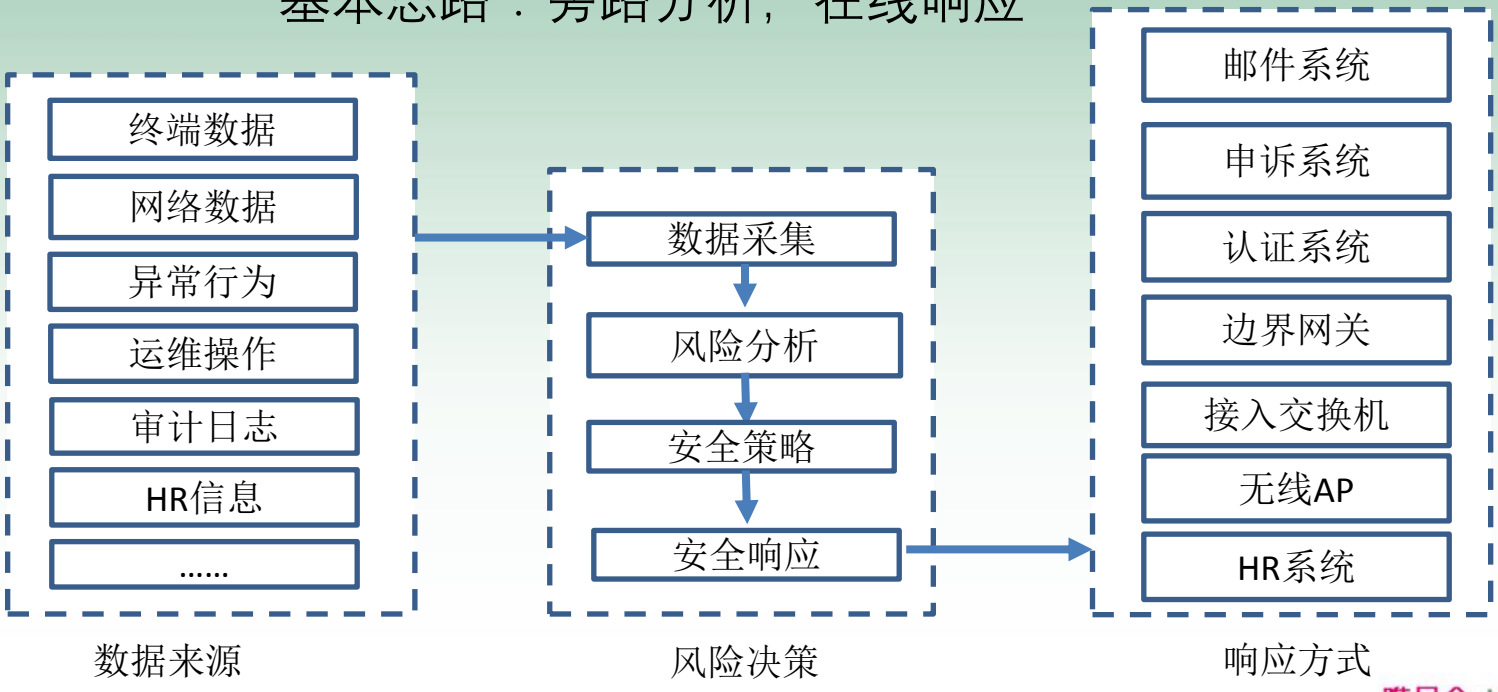
① 需要安装客户端软件
② 基本只关注主机本身合规性
③ 决策链太长，容易出现各种问题，难维护，（客户端-交换机-准入设备-策略服务器）
④ 响应手段单一
⑤ 无法支持全类型客户端（各类型操作系统PC与移动端）

我们需要啥

无客户端	真实风险	动态策略	精准响应
任何人 任何设备 免维护	全方位 真实 因人而异	人 设备 资源	快速定位 快速响应

准入架构图

基本思路：旁路分析，在线响应



数据来源

基础信息

系统	获取信息
接入交换机	MAC、IP、交换机端口
接入认证radius	MAC、IP、用户、上下线时间、AP、交换机、SSID
综合布线系统	面板、AP位置
终端安装软件	计算机基础信息、DLP、病毒
AD域系统	计算机加AD信息
人事系统	组织机构、岗位信息、考勤信息
。。。	

关联：IP-MAC-用户-计算机名-交换机-交换机端口-面板

数据来源

安全日志

系统	获取信息
IDS系统	攻击事件
防病毒系统	病毒感染事件
DLP系统	文档泄露事件
扫描软件	漏洞信息
流量分析	异常流量
。。。	

审计日志

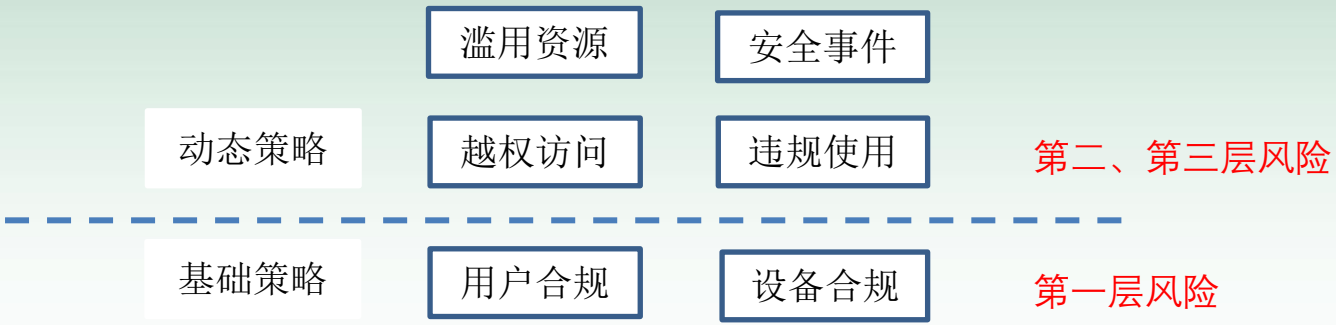
系统	获取信息
认证系统	完整登录信息
关键应用系统	数据导入、导出日志
运维系统	操作日志
。。。	

可采集任何有用信息
适应多种数据采集方式：API、SQL、syslog、snmp、文本、手工录入。。。

风险分析

第三层	隐式安全风险（权限滥用、违规操作等）
第二层	显式安全风险（安全事件触发）
第一层	符合性风险（设备合规、人员合规、权限合规）

动态策略



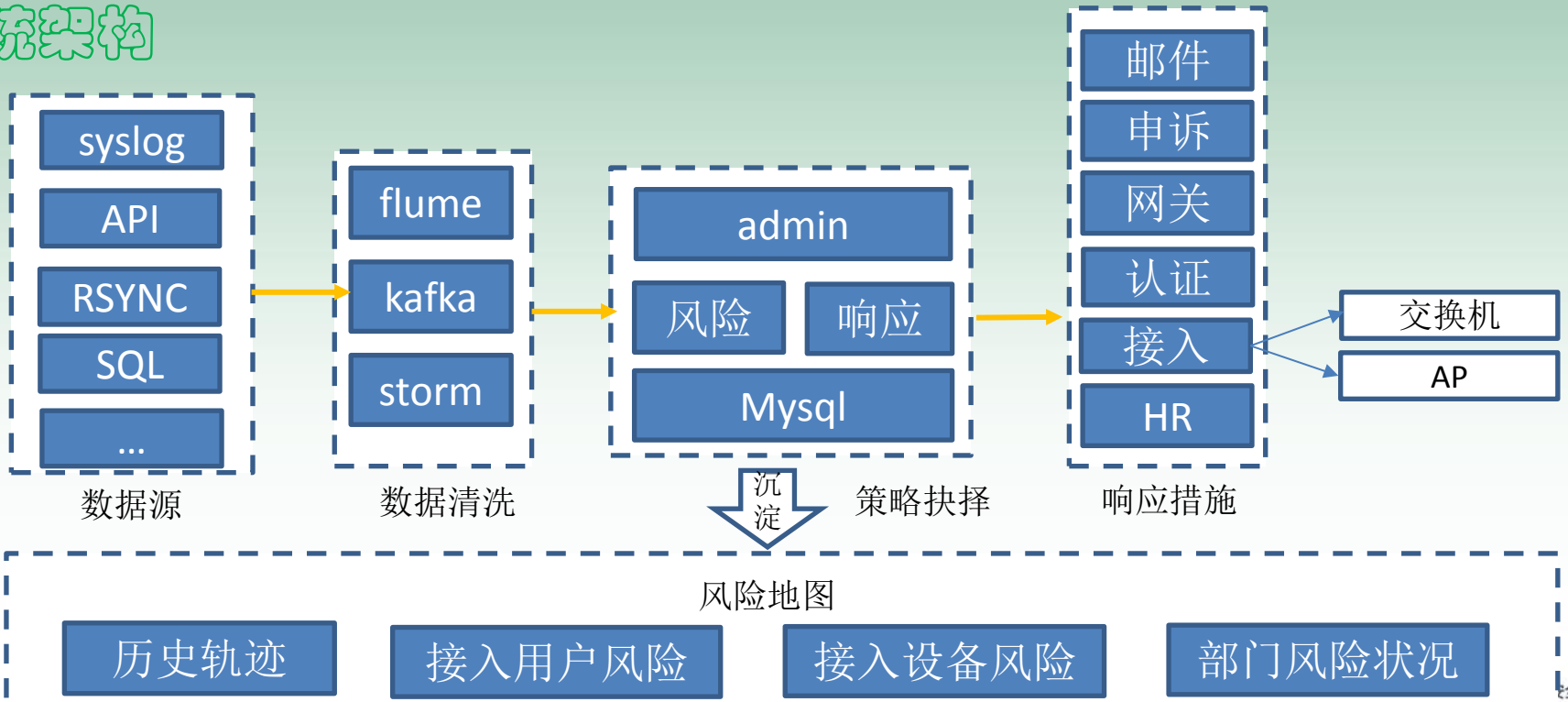
安全响应

高

低

风险	响应级别	响应机制	风险说明
一级响应	禁用账号	HR系统	严重违规、密码泄露
二级响应	禁止接入内网	接入交换机、AP	不满足符合性要求
三级响应	禁止访问应用	统一认证系统	违规操作
四级响应	禁止访问外网	网关设备（代理、FW）	恶意程序、资源滥用
五级响应	告警	邮件告警、申诉页	安全意识、不良使用习惯

系统架构


syslog
API
RSYNC
SQL
...
数据源
flume
kafka
storm
数据清洗
admin
风险
响应
Mysql
沉淀
策略抉择
邮件
申诉
网关
认证
接入
HR
响应措施
交换机
AP
风险地图
历史轨迹
接入用户风险
接入设备风险
部门风险状况

应用场景

1）符合性检查

2）异常行为

3）违规行为

与业界产品对比

对比项	业界产品	咱家
1）支持设备	主流操作系统	支持任何设备
2）检查范围	检查单个主机状态	可以接入的任何有用信息，主机、网络、业务、HR等
3）策略抉择	匹配静态策略，基于文件、进程、注册表、服务等因素	静态策略、动态策略
4）响应手段	响应手段单一	分层次响应：接入交换机、边界网关、认证服务器
5）风险地图	没有数据沉淀，无法展示	通过历史轨迹沉淀可以生成全局风险地图，为安全管控策略抉择提供依据

收益

1. 安全事件精准定位、快速响应
2. 避免管控策略一刀切
3. 安全管控保持足够威慑力
4. 安全意识教育精准匹配
5. 全局安全风险地图

千言万语

① 利旧创新
② 要求第三方系统提供接口（信息采集、响应）
③ 明确弹性的底线：严管核心数据、遵循合规要求

适度弹性

管控因人而异

谢谢您的倾听！

唯品会 | 唯品会安全应急响应中心

VIP Security Response Center

唯品会安全应急响应中心

专业

我们致力于保护用户信息安全

我们积极营造更加安全的

线上电商购物平台

微信号：VIP_SRC

官方网站：http://sec.vip.com

微信公众号：唯品会安全应急响应中心

漏洞接收邮箱：sec@vipshop.com