SACC 2014中国系统架构师大会
SYSTEM ARCHITECT CONFERENCE CHINA 2014

发现架构之美

多层风控技术体系及挑战

——支付宝风控实践

李俊奎@支付宝

2014.09

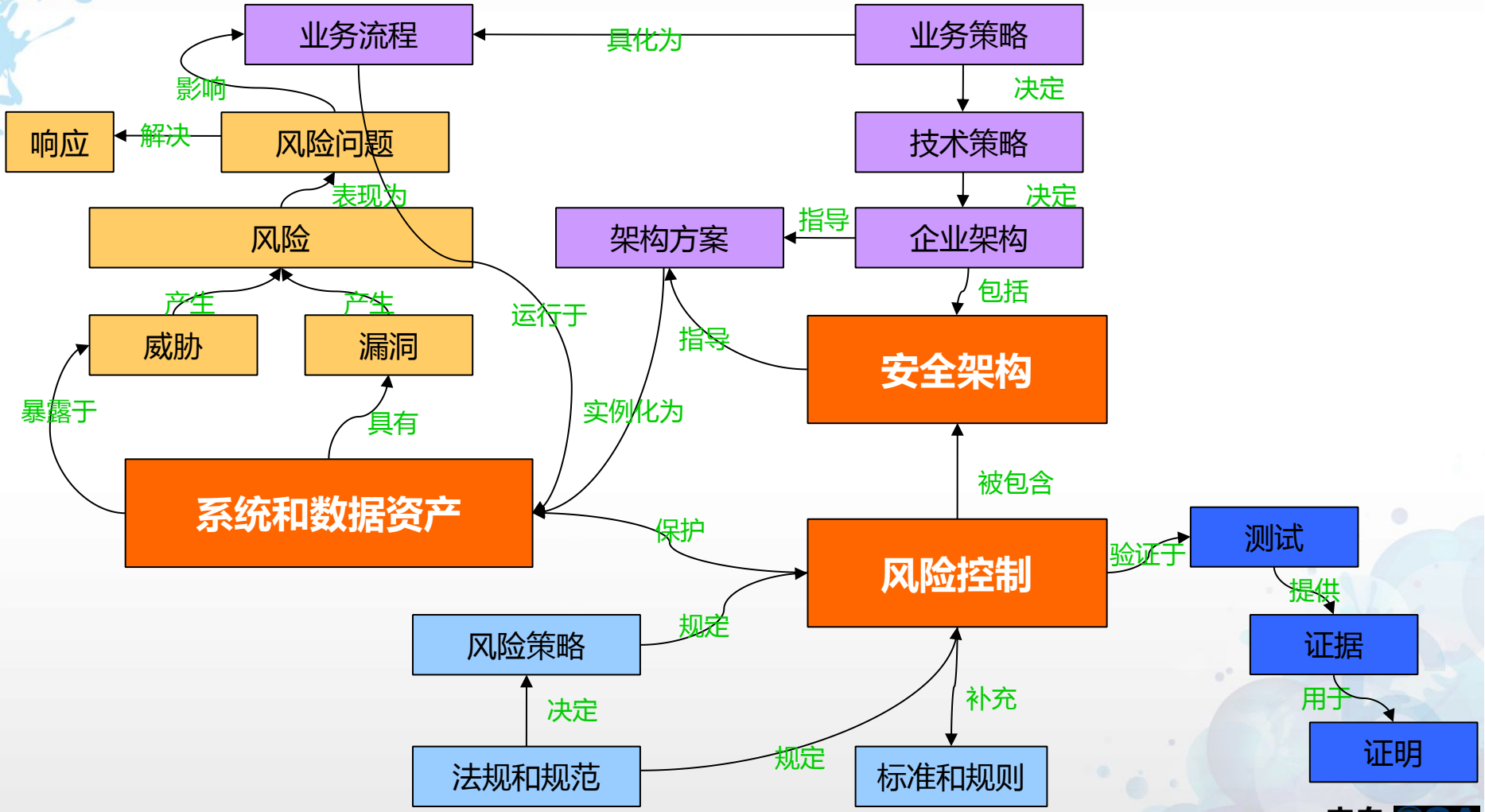
目录

- 支付宝多层风控技术体系
- 支付宝风控技术的挑战与实践

目录

- 支付宝多层风控技术体系
- 支付宝风控技术的挑战与实践

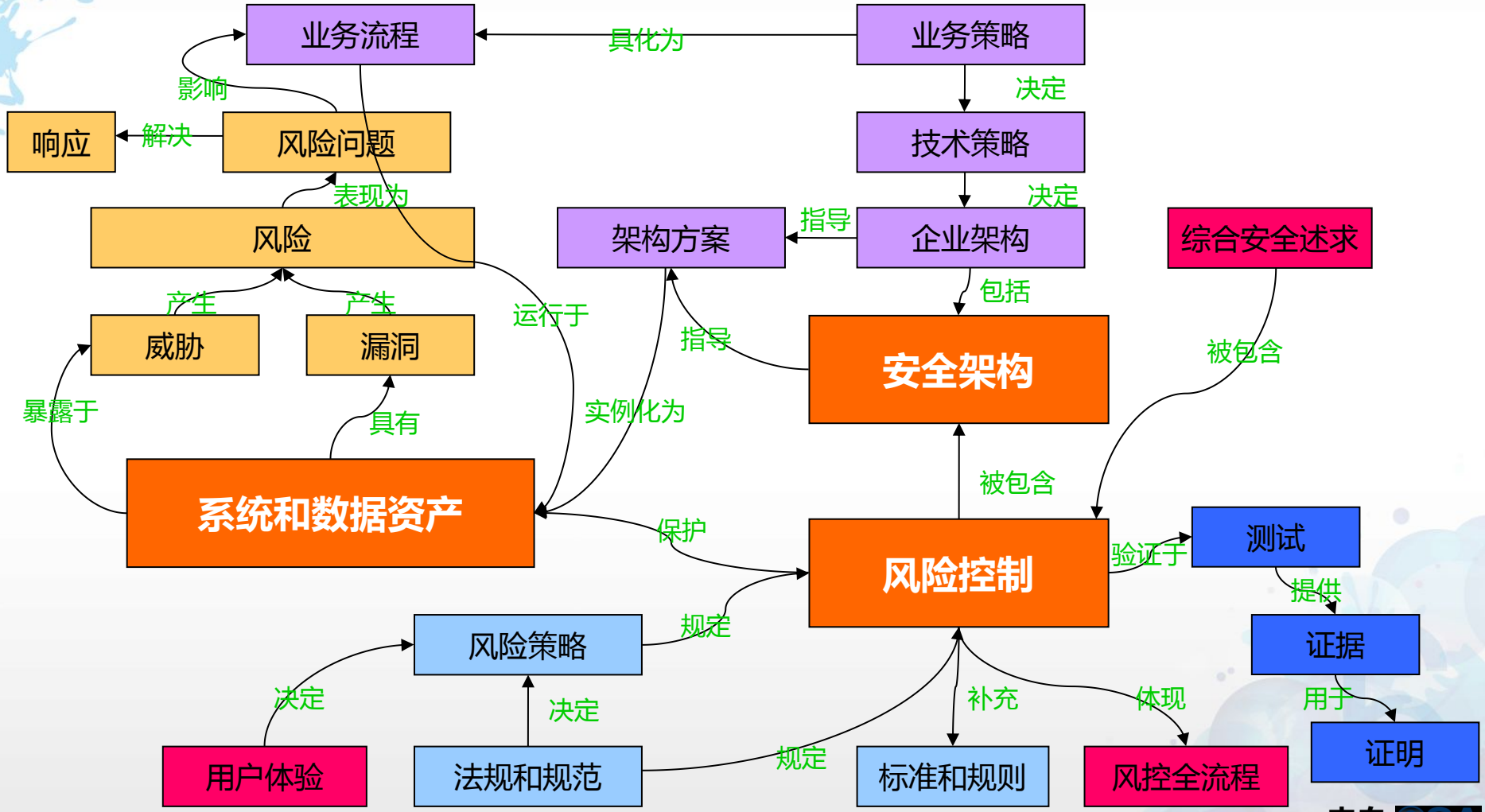
全局图



http://www.opensecurityarchitecture.org/cms/foundations/osa-taxonomy

来自 OSA

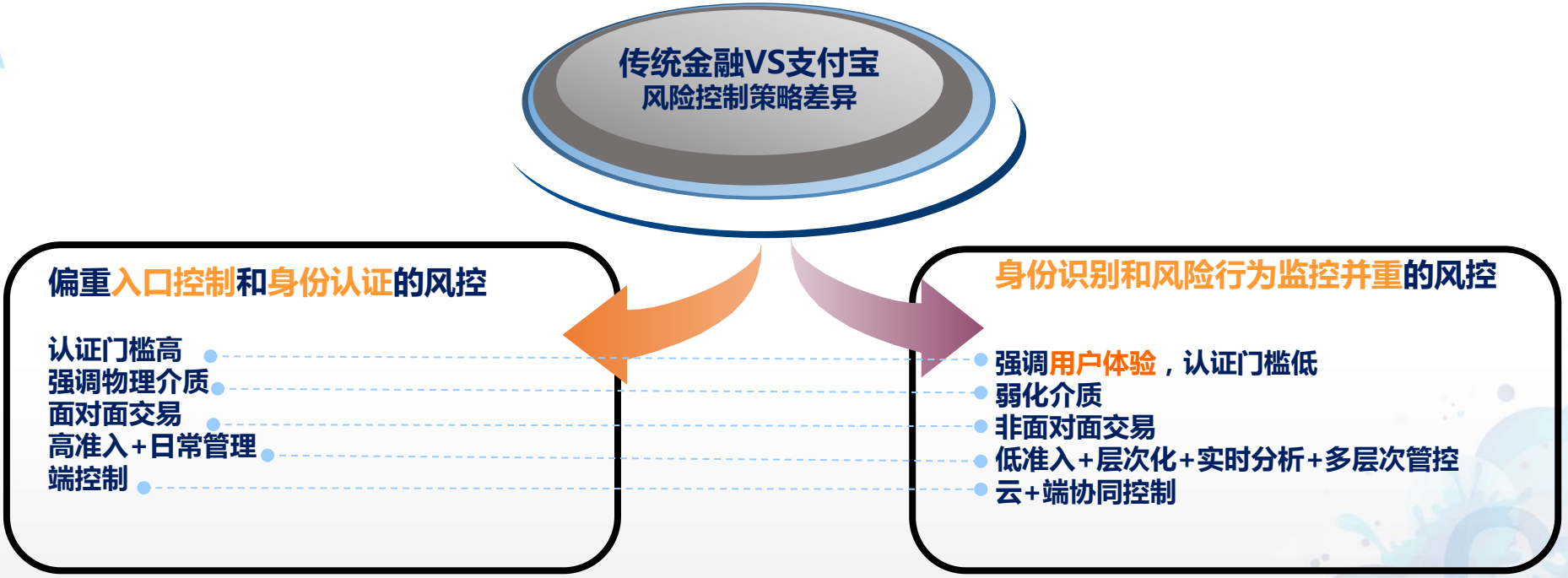
全局图



http://www.opensecurityarchitecture.org/cms/foundations/osa-taxonomy

来自 OSA

互联网时代：不同于传统金融的风险策略



安全述求：李嘉诚豪宅的安保

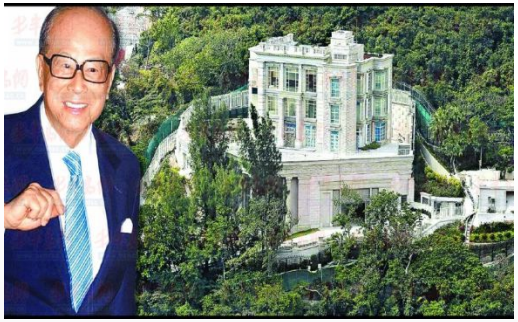
2. 特许进入通道、独立天台

3. 英国军情五处培训安保、廓尔喀雇佣兵保镖，香港007

4. 全天候无死角监控告警、异常闯入处理

5. 与香港警方、安保公司等武装力量迅速联动

6. 定期专业情报分析、综合风险形势评估、隐患预警排除

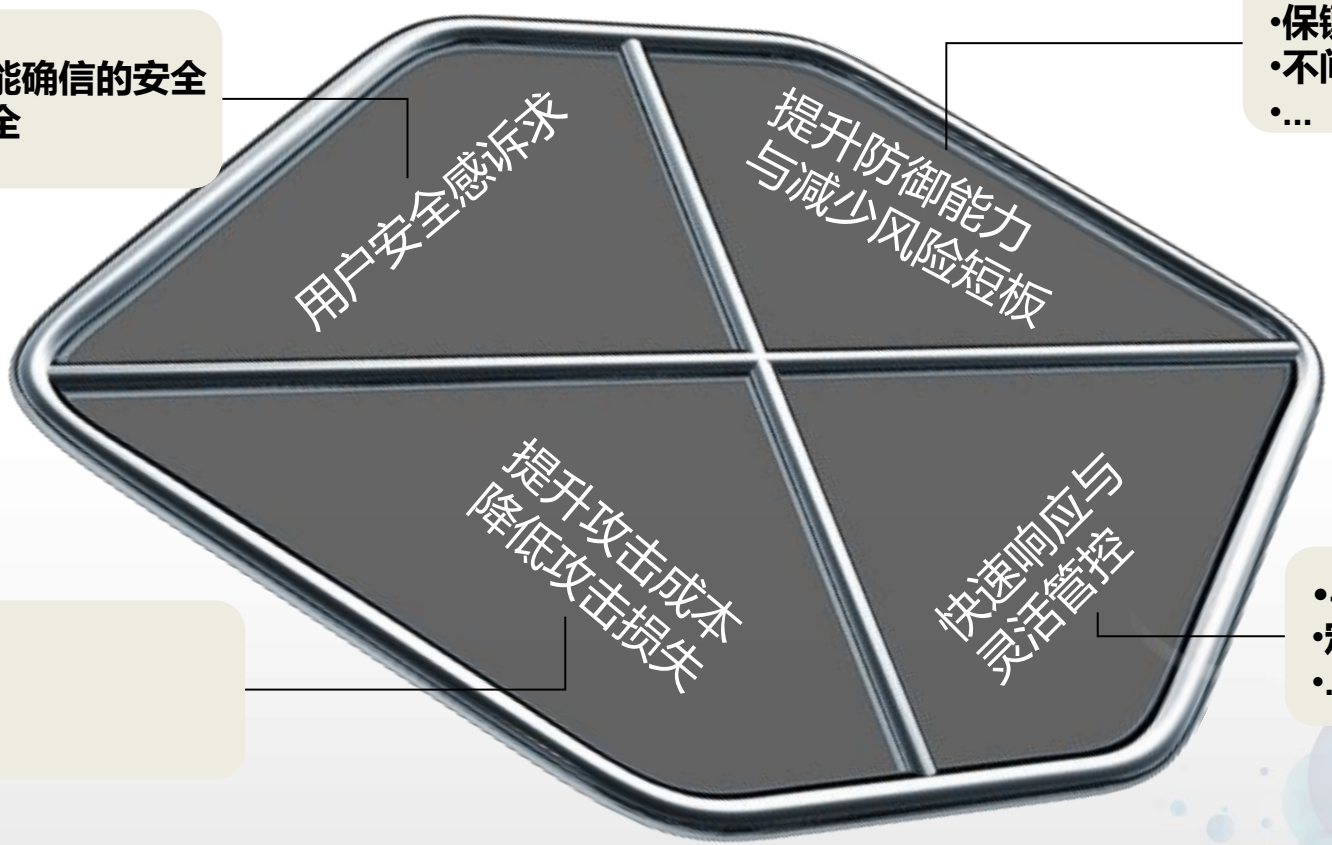


1. 电网围栏、遍布隐秘式监视器、半山隐蔽、3米围墙、顶级防弹玻璃建筑

李嘉诚豪宅挖地道都进不去：http://news.163.com/13/1120/12/9E4I8VMG00014Q4P.html

安全的综合述求

- 有感知的、能确信的安全
- 有控制的安全

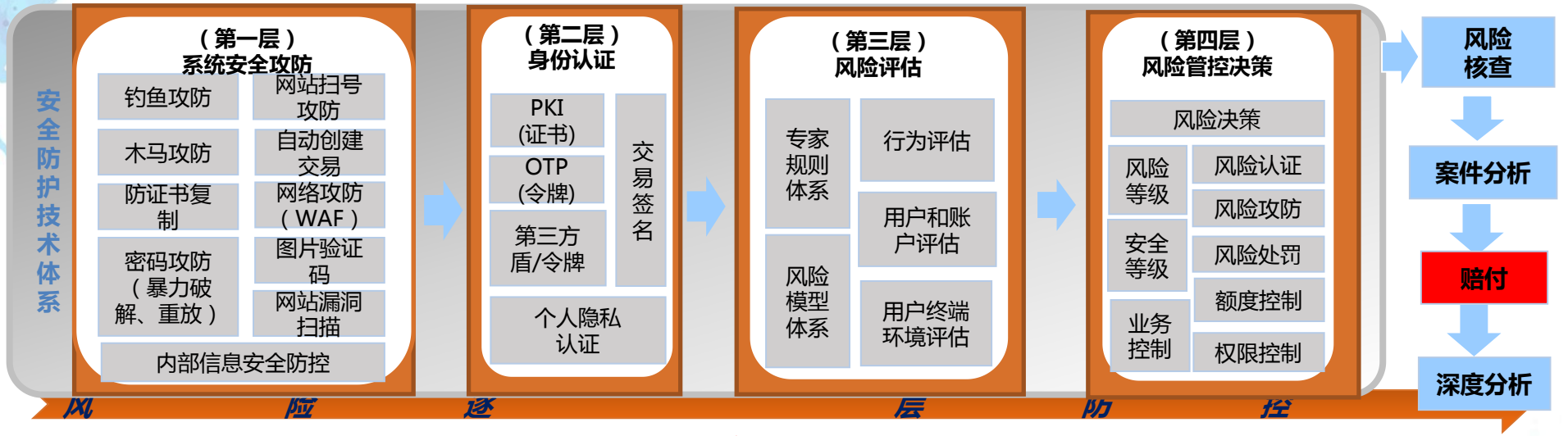


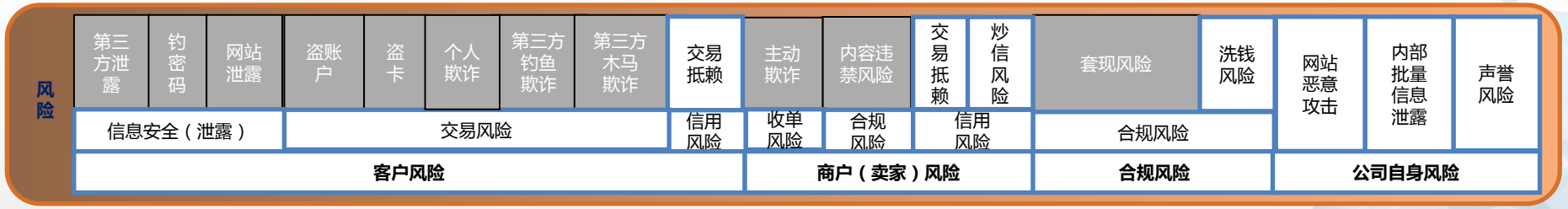
- 安保人员培训
- 保镖团队
- 不间断的监控
- …

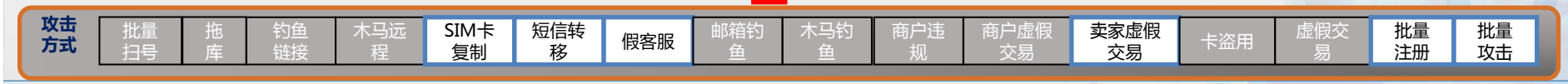
- 密布监视器
- 防弹玻璃
- 独立通道
- …

- 与警方联动
- 定期分析评估
- …

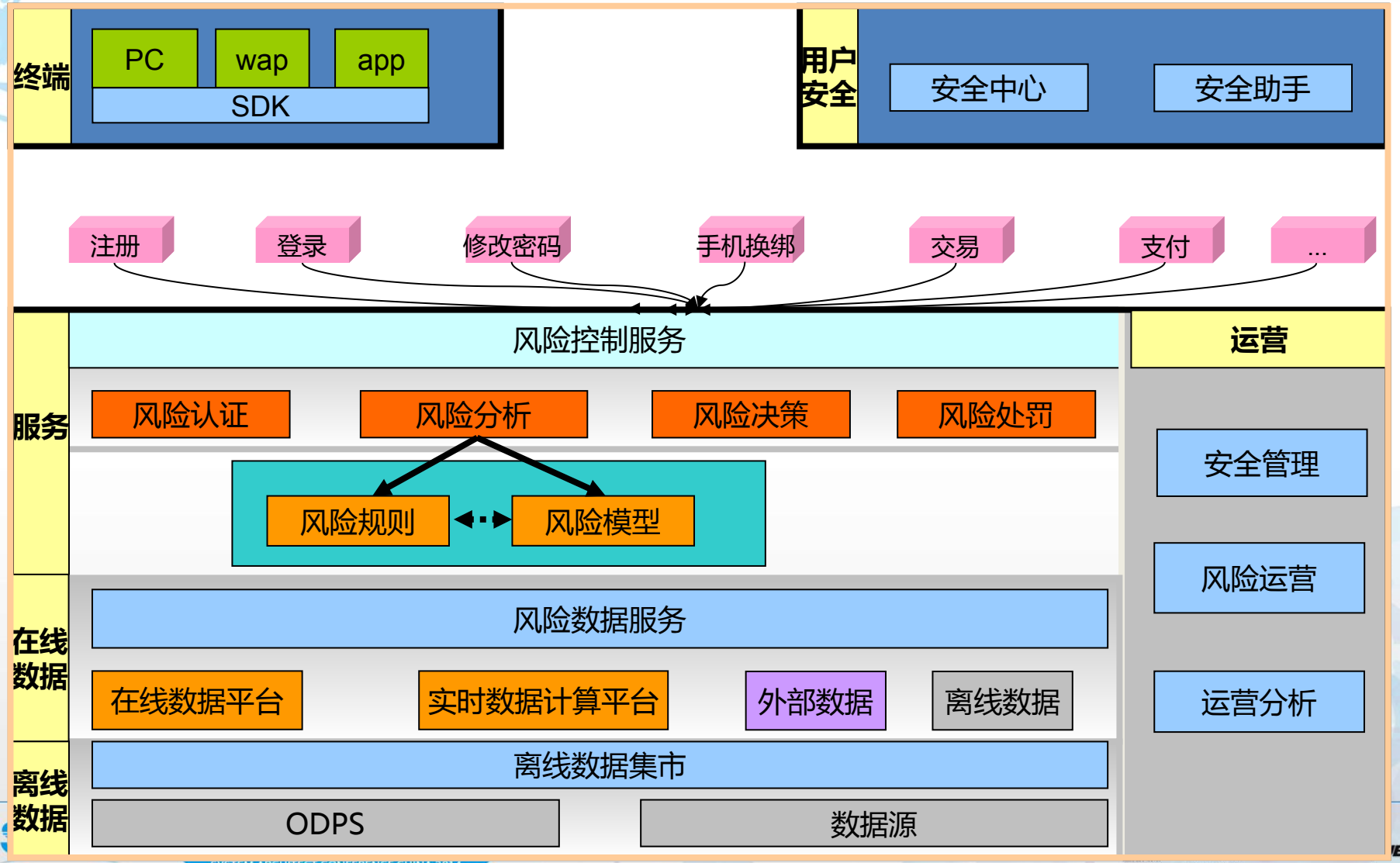
风险控制


安全防护技术体系
（第一层）
系统安全攻防
钓鱼攻防
网站扫号攻防
木马攻防
自动创建交易
防证书复制
网络攻防（WAF）
密码攻防（暴力破解、重放）
图片验证码
网站漏洞扫描
内部信息安全防控
（第二层）
身份认证
PKI（证书）
OTP（令牌）
第三方盾/令牌
交易签名
个人隐私认证
（第三层）
风险评估
专家规则体系
行为评估
用户和账户评估
风险模型体系
用户终端环境评估
（第四层）
风险管控决策
风险决策
风险等级
风险认证
风险攻防
安全等级
风险处罚
额度控制
业务控制
权限控制
风险核查
案件分析
赔付
深度分析
风险逐层防控

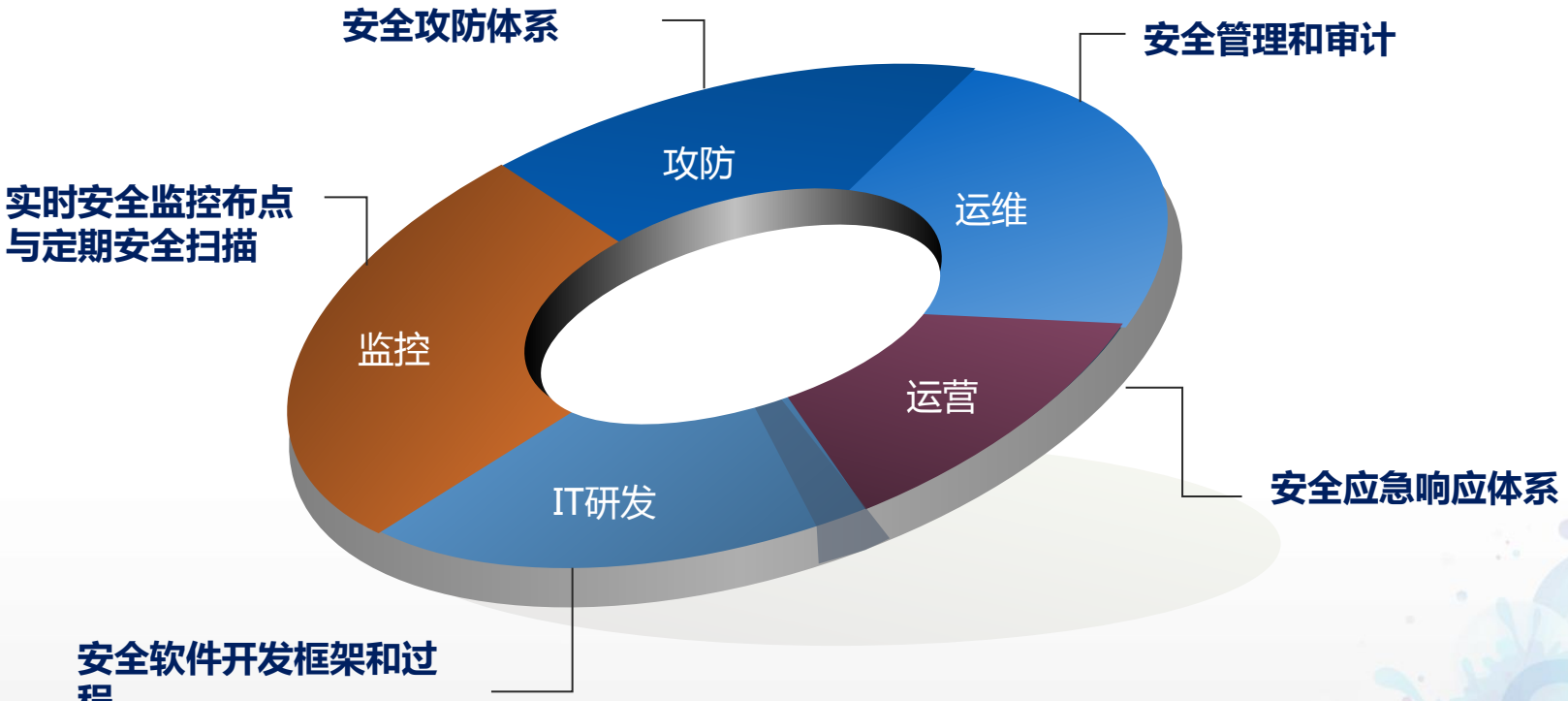

风险
第三方泄露
钓密码
网站泄露
盗账户
盗卡
个人欺诈
第三方钓鱼欺诈
第三方木马欺诈
交易抵赖
主动欺诈
内容违禁风险
交易抵赖
炒信风险
套现风险
洗钱风险
网站恶意攻击
内部批量信息泄露
声誉风险
信息安全（泄露）
交易风险
信用风险
收单风险
合规风险
信用风险
合规风险
客户风险
商户（卖家）风险
合规风险
公司自身风险


攻击方式
批量扫号
拖库
钓鱼链接
木马远程
SIM卡复制
短信转移
假客服
邮箱钓鱼
木马钓鱼
商户违规
商户虚假交易
卖家虚假交易
卡盗用
虚假交易
批量注册
批量攻击

安全架构


终端
PC
wap
app
SDK
用户安全
安全中心
安全助手
注册
登录
修改密码
手机换绑
交易
支付
...
服务
风险控制服务
风险认证
风险分析
风险决策
风险处罚
风险规则
风险模型
在线数据
风险数据服务
在线数据平台
实时数据计算平台
外部数据
离线数据
离线数据
离线数据集市
ODPS
数据源
运营
安全管理
风险运营
运营分析

风险控制体系实现全流程

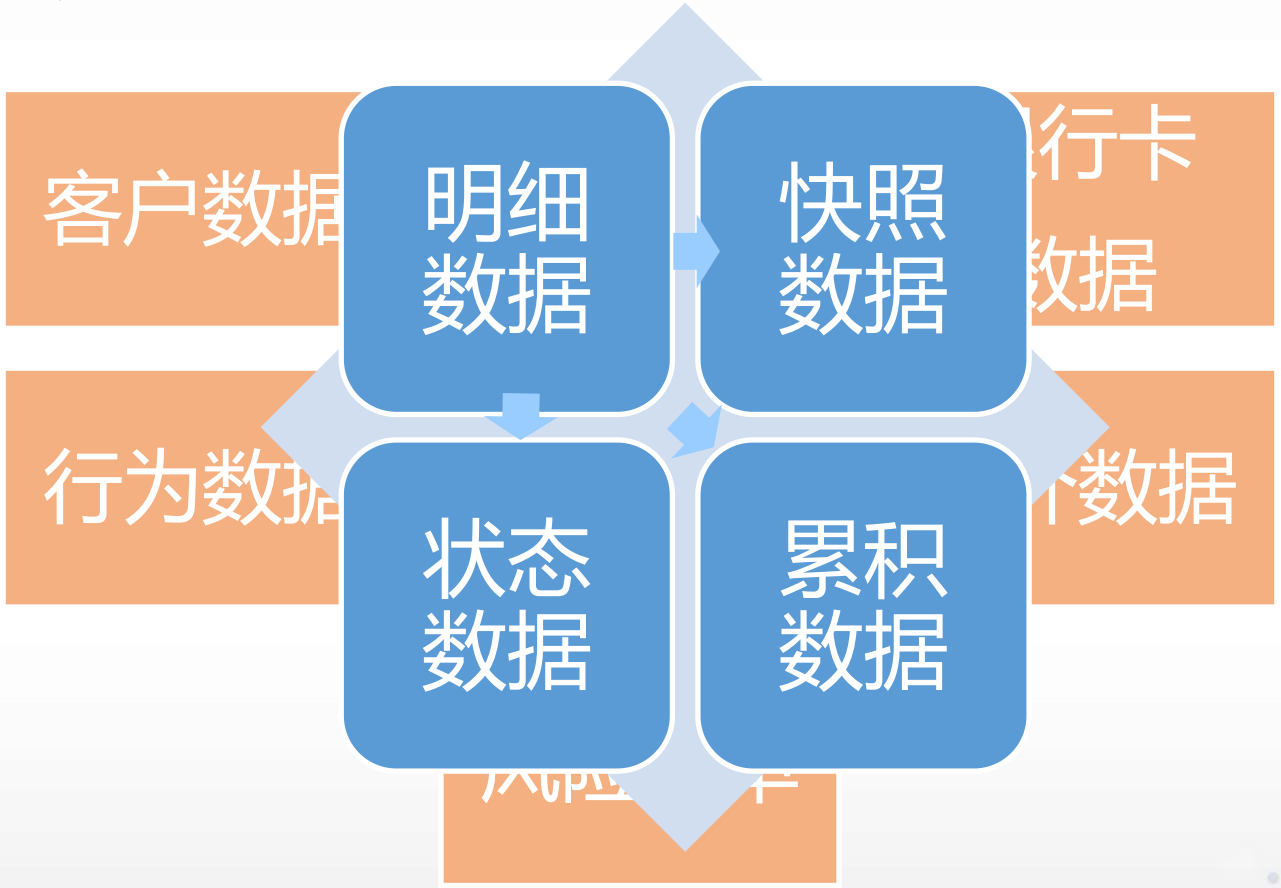


目录

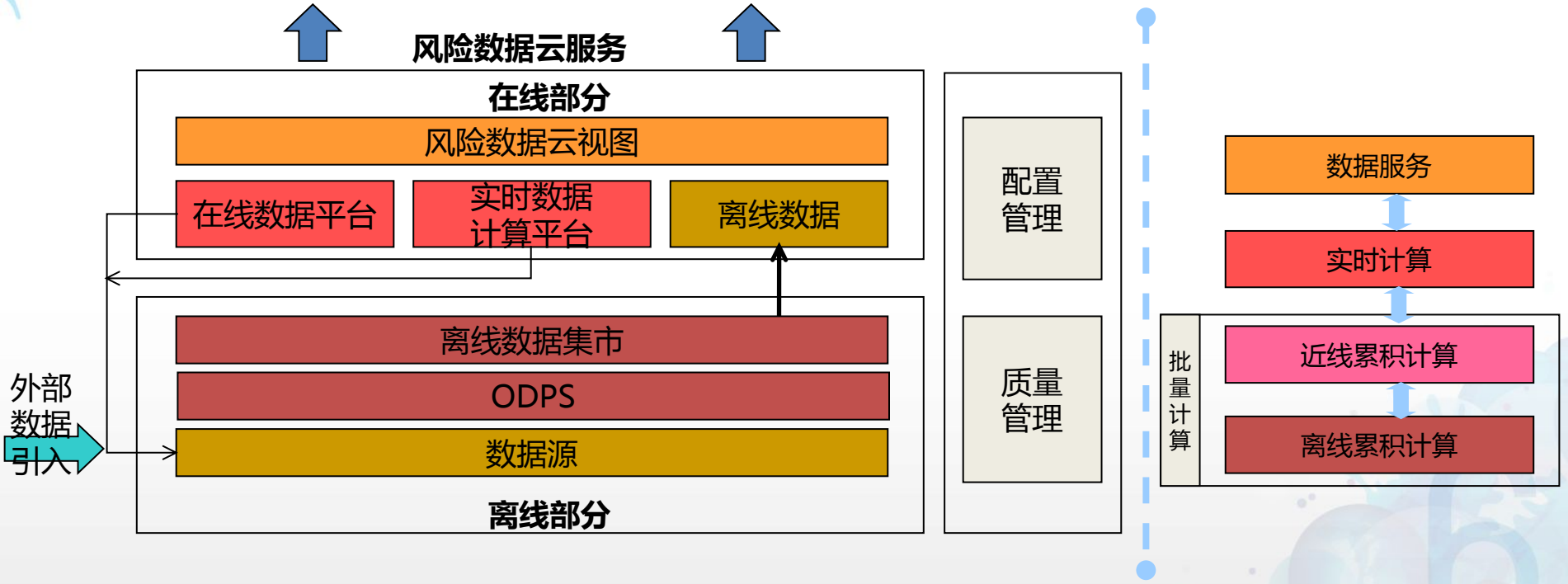
- 支付宝多层风控技术体系
- 支付宝风控技术的挑战与实践

业务发展对风控带来的挑战

数据是风控的基础

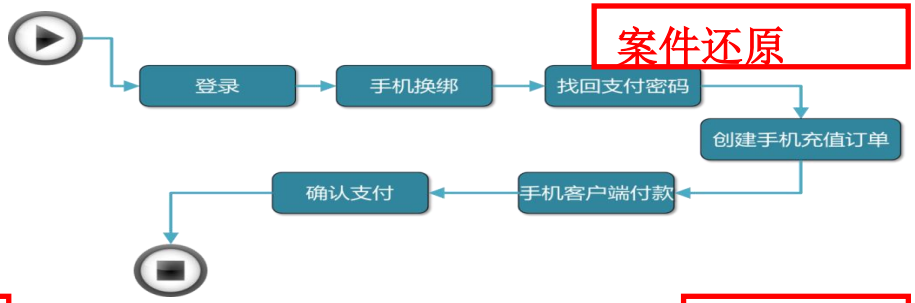


容量性能关键点—数据计算



快速发现关键点—实时监控及风险分析

实时业务大屏

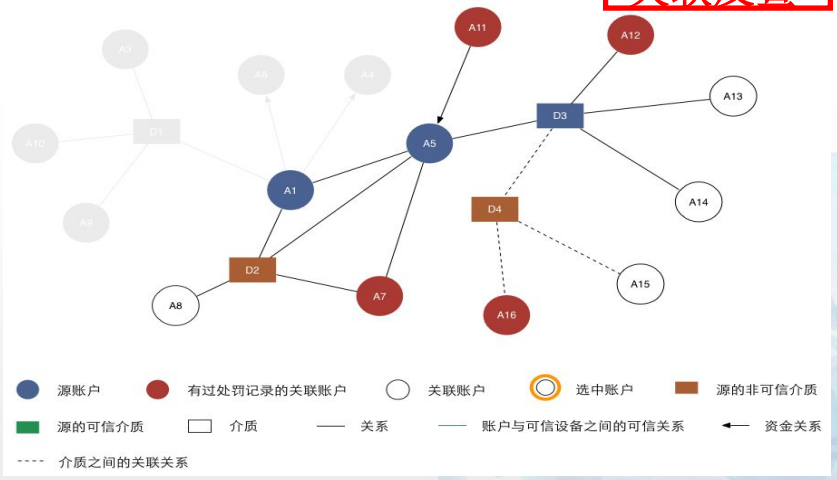


案件还原

modelcenter模型平均输出分值(11:38)

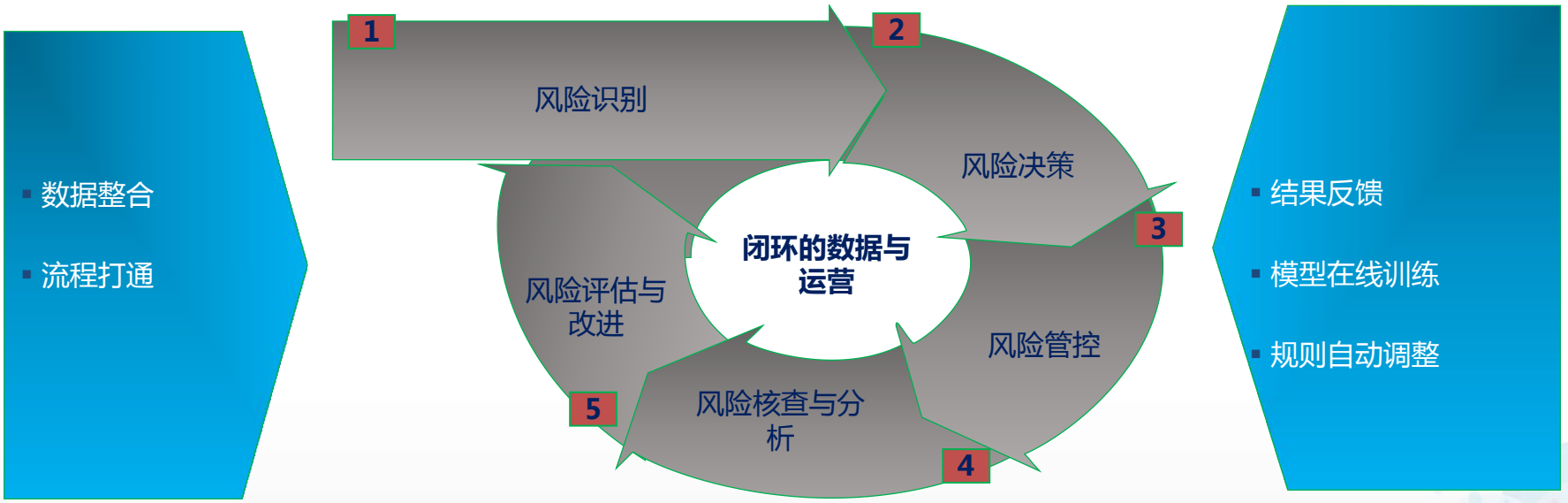
模型	调用来源	模型平均分值
M_Rsk_Txn_Una...	cnctu	0.45
M_Rsk_Txn_Una...	cnctu	0.32
M_Rsk_Txn_Una...	ctu	0.18
M_Rsk_Txn_Una...	cnctu	0.18
M_Rsk_Txn_Una...	cnctu	0.18
M_Rsk_Txn_Una...	cnctu	0.17
M_Rsk_Txn_Una...	ctu	0.17
M_Rsk_Txn_FpB...	cnctu	0.16
M_Rsk_Txn_Una...	cnctu	0.15
M_Rsk_Txn_Una...	ctu	0.14
M_Rsk_Txn_Una...	cnctu	0.14
M_Rsk_Txn_Una...	cnctu	0.11

风险模型监控



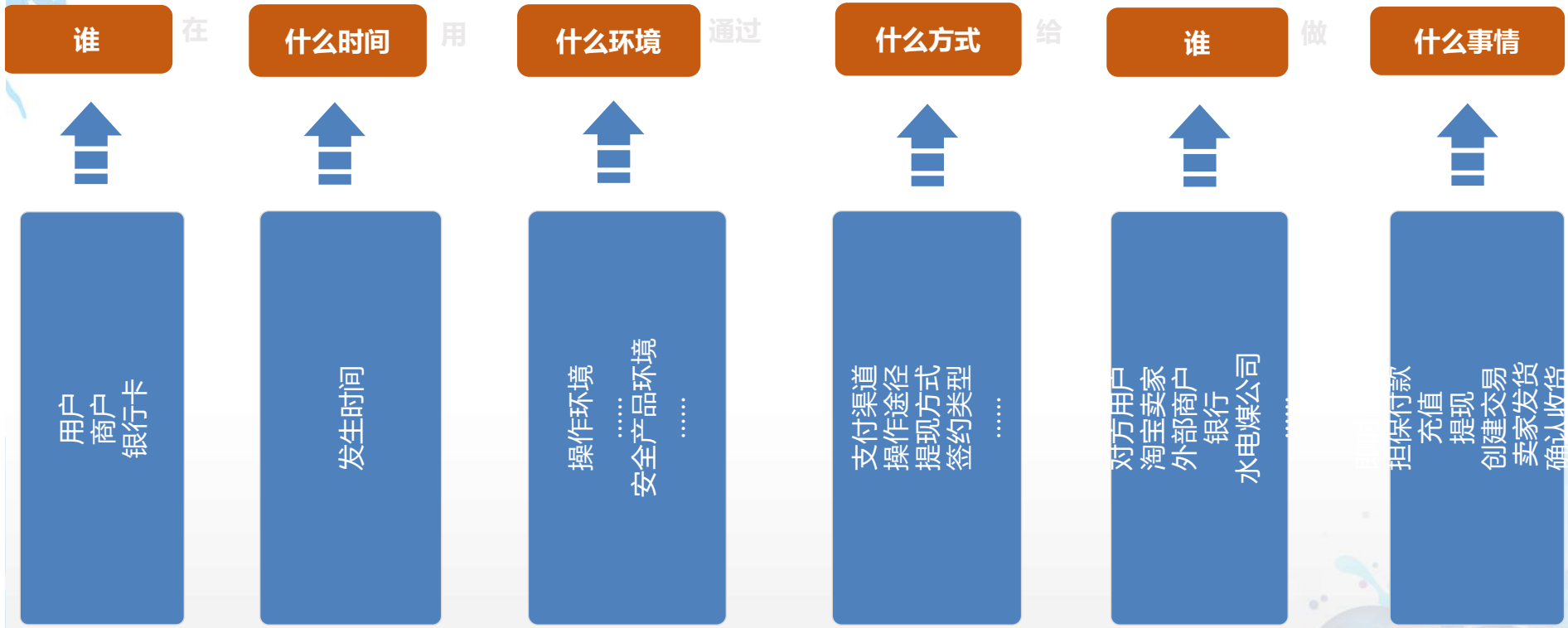
关联反查

灵活调整关键点—模型和规则的自适应

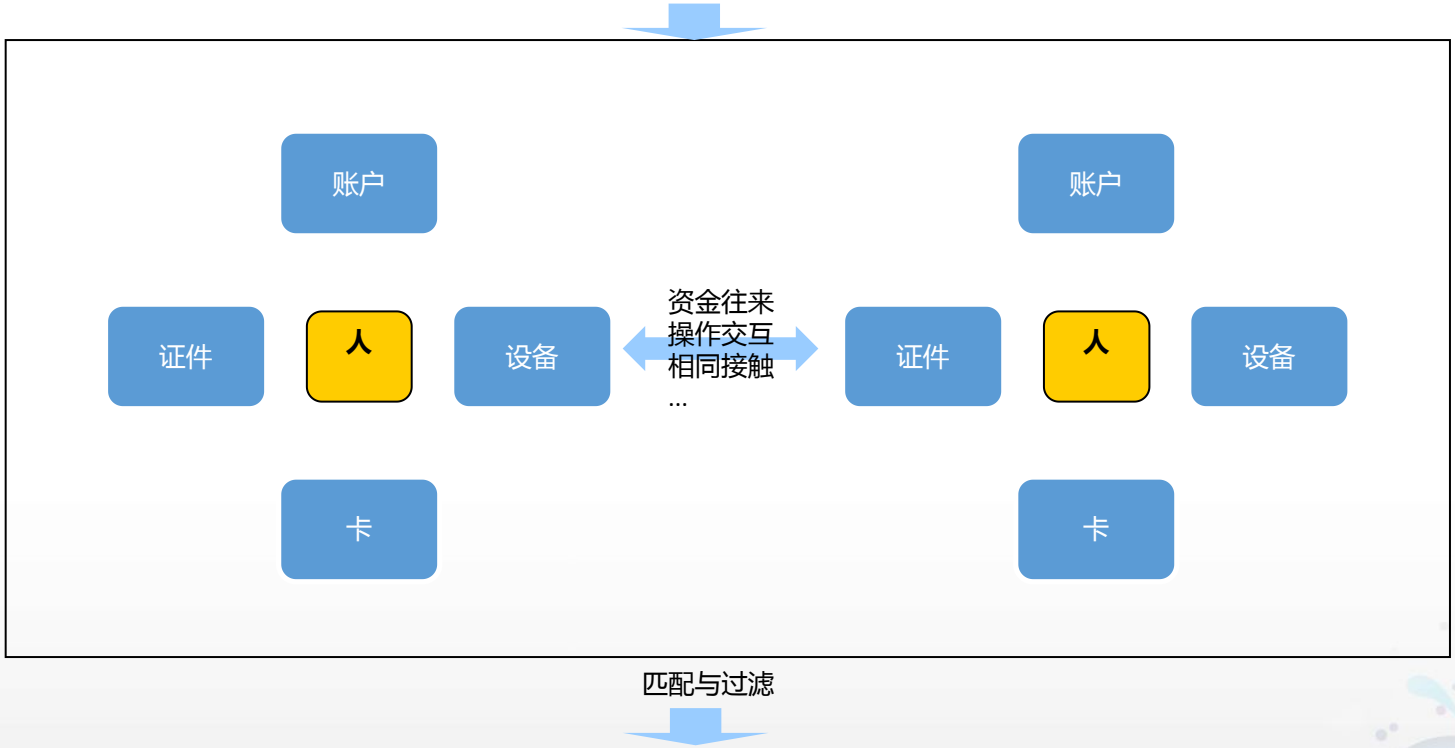


灵活部署关键点—决策手段多样化

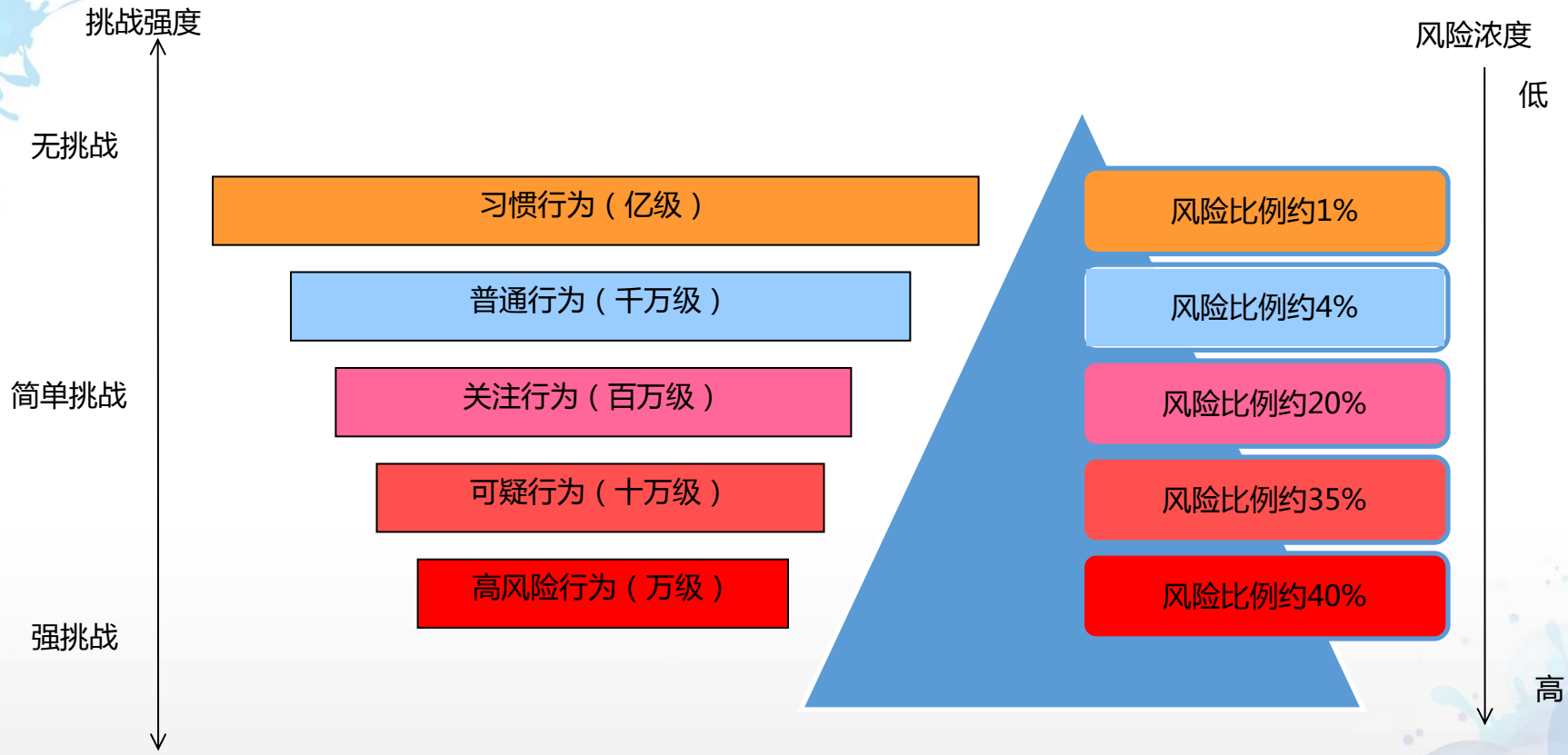
立体布控关键点—事件的多维风险监控



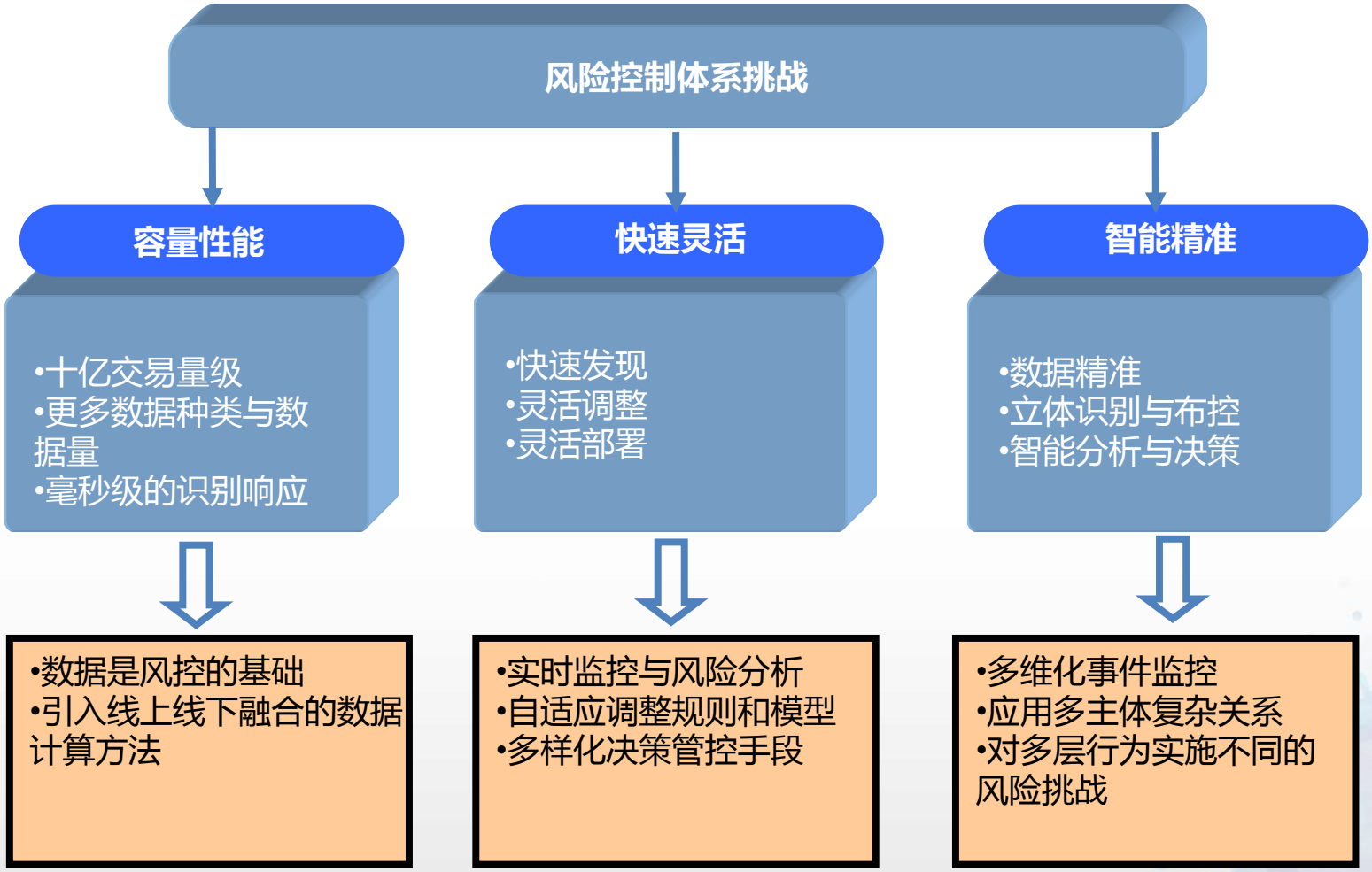
立体布控关键点—多主体复杂关系的应用



智能分析决策关键点—多层行为风险挑战



小结


风险控制体系挑战
容量性能
•十亿交易量级
•更多数据种类与数据量
•毫秒级的识别响应
快速灵活
•快速发现
•灵活调整
•灵活部署
智能精准
•数据精准
•立体识别与布控
•智能分析与决策
•数据是风控的基础
•引入线上线下融合的数据计算方法
•实时监控与风险分析
•自适应调整规则和模型
•多样化决策管控手段
•多维化事件监控
•应用多主体复杂关系
•对多层行为实施不同的风险挑战

Q&A

THANKS

SequeMedia 盛拓传媒 | IT168 www.it168.com | ChinaUnix | ITPUB