

ArchSummit 2014

"敢付敢赔"背后的互联网实时风控技术

——支付宝风控实践

李俊奎@支付宝
2014-07

目录

1. 从“敢付敢赔”说起

2. 支付宝如何做到“敢付敢赔”？

3. 风控技术的挑战与实践

目录

1. 从“敢付敢赔”说起

2. 支付宝如何做到“敢付敢赔”？

3. 风控技术的挑战与实践

“敢付敢赔” 一路走来

2013年

2011年—2012年

2005年

再发展

发展

初期

- 推出**在线购物**"你敢付，我敢赔"支付联盟计划(2005)

- 推出**快捷支付**被盗72小时全额赔付(2011)

- 升级会员保障，提出**支付宝账户余额**被盗72小时全额赔付(2012)

- 推出**余额宝资金**被盗全额赔付(2013)

- 推出**手机支付资金**被盗全额赔付(2013)

- 增加1个工作日内的**"极速补偿"**(2013)

- ? 传说中的**秒级即赔，来电即赔**

支付宝会员保障：<https://my.alipay.com/portal/account/safeguard.htm>

“敢付敢赔” 背后

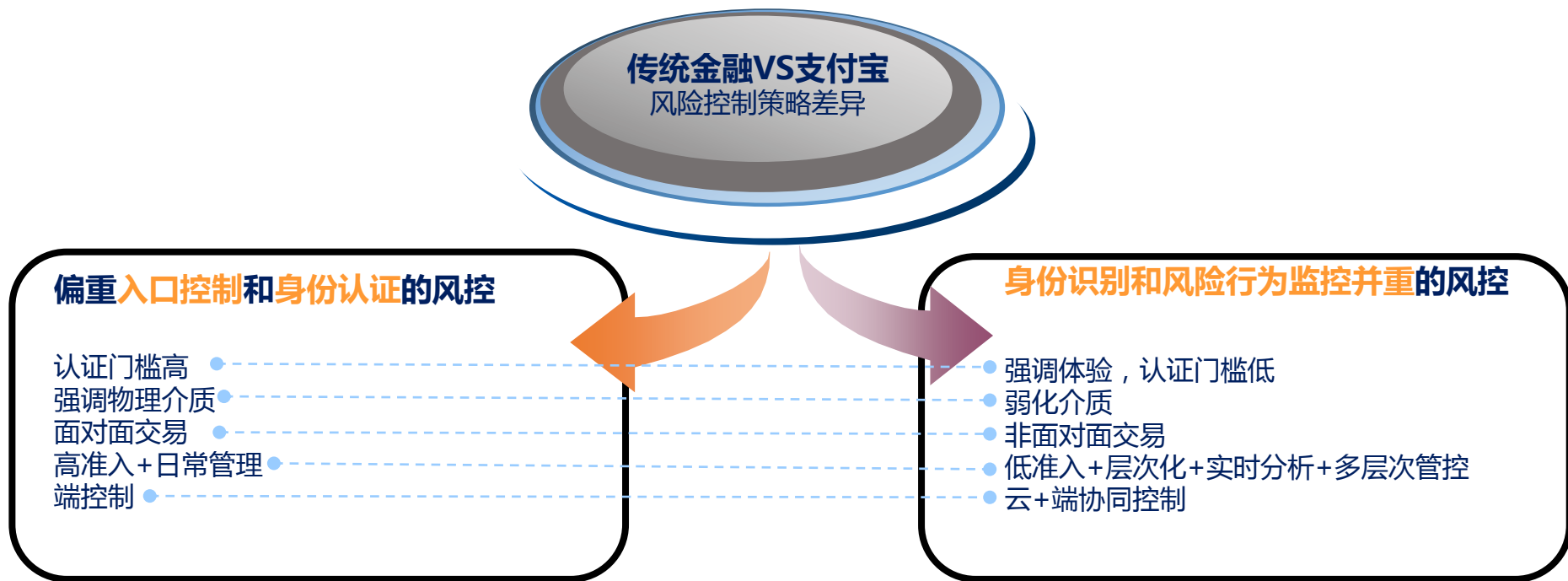
“敢付敢赔”

✓考验的是：
风险控制的能力
(风控能力是金融企业的核心能力)

✓体现的是：
金融企业的担当和责任

✓带来的是：
用户的信任和顾虑打消

不同于传统金融的风险控制策略



目录

1. 从“敢付敢赔”说起

2. 支付宝如何做到“敢付敢赔”？

3. 风控技术的挑战与实践

李嘉诚豪宅的安保



2. 特许进入通道、独立天台

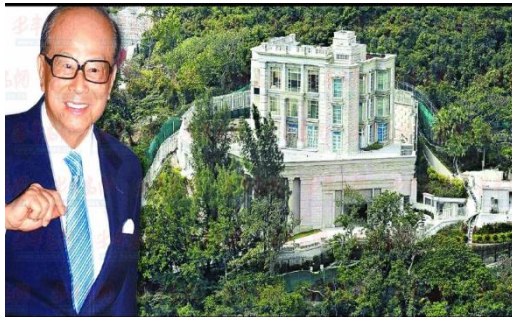


1. 电网围栏、遍布隐秘式监视器、半山隐蔽、3米围墙、顶级防弹玻璃建筑

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



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

安全的综合述求

- 有感知的、能确信的安全
- 有控制的安全

用户安全感诉求

提升防御能力
与减少风险短板

- 安保人员培训
- 保镖团队
- 不间断的监控
- ...

提升攻击成本
降低攻击损失

- 密布监视器
- 防弹玻璃
- 独立通道
- ...

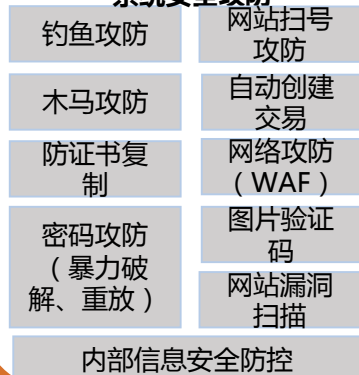
快速响应与
灵活管控

- 与警方联动
- 定期分析评估
- ...

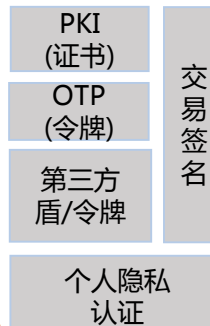
从端到云——多层次风险控制技术体系

安全防护技术体系

(第一层) 系统安全攻防



(第二层) 身份认证



(第三层) 风险评估



(第四层) 风险管控决策



风险
核查

案件分析

赔付

深度分析

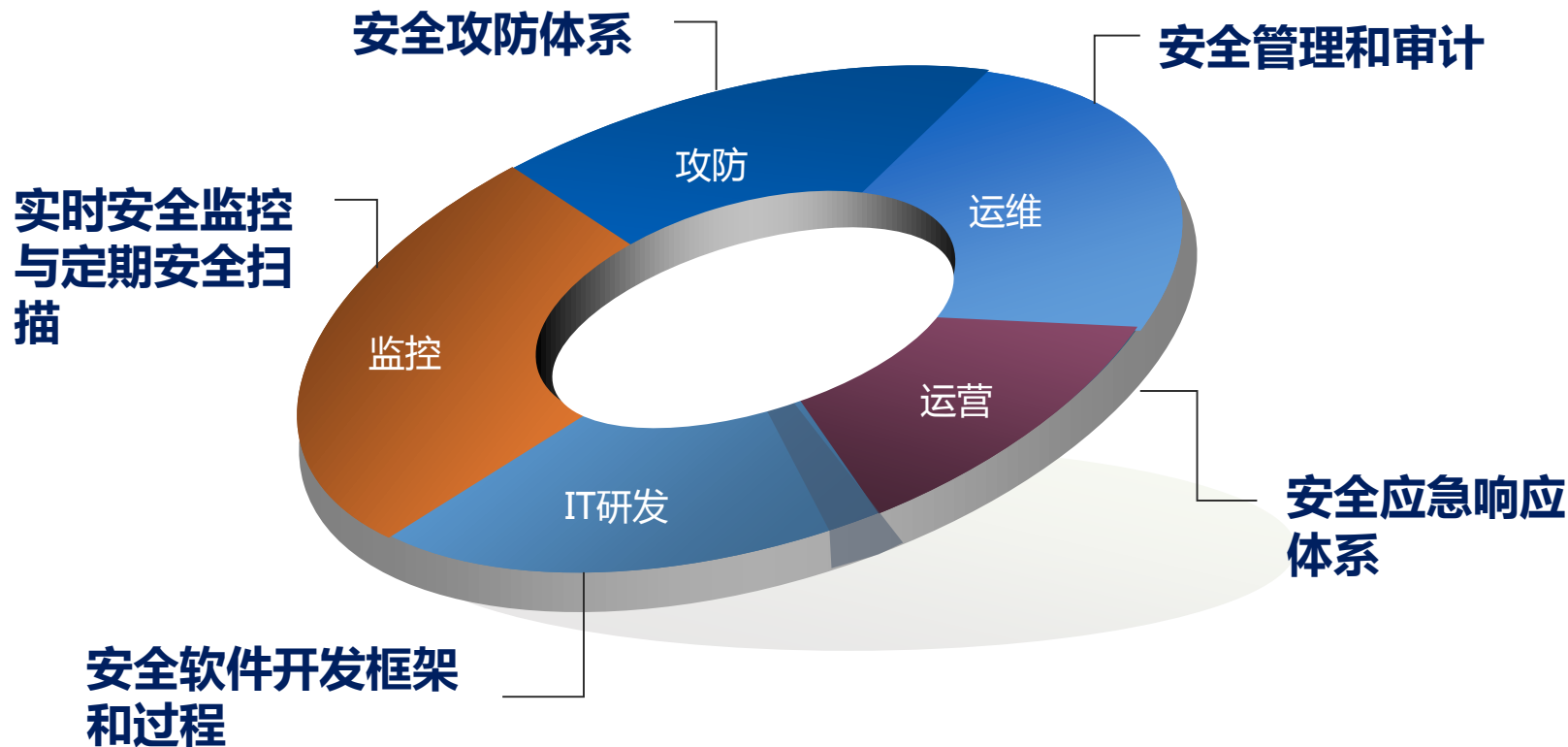
风险

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
----------	--------	------------------	------------------	------------	------------------	-------------	------------------	------------------	------------------	----------------------------	----------------------------	-------------	------------------	------------------	------------------

风险控制体系实现全流程



目录

1. 从“敢付敢赔”说起

2. 支付宝如何做到“敢付敢赔”？

3. 风控技术的挑战与实践

一页数据管窥支付宝风险控制技术现状

容量指标现状

- 3W+/秒、10亿+/天的交易风险识别与管控容量
- 2W+条规则部署容量
- 平均100ms风险处理响应能力
- 20+亿/天的事件写入与计算容量
- 单次2000+衍生变量累积计算能力

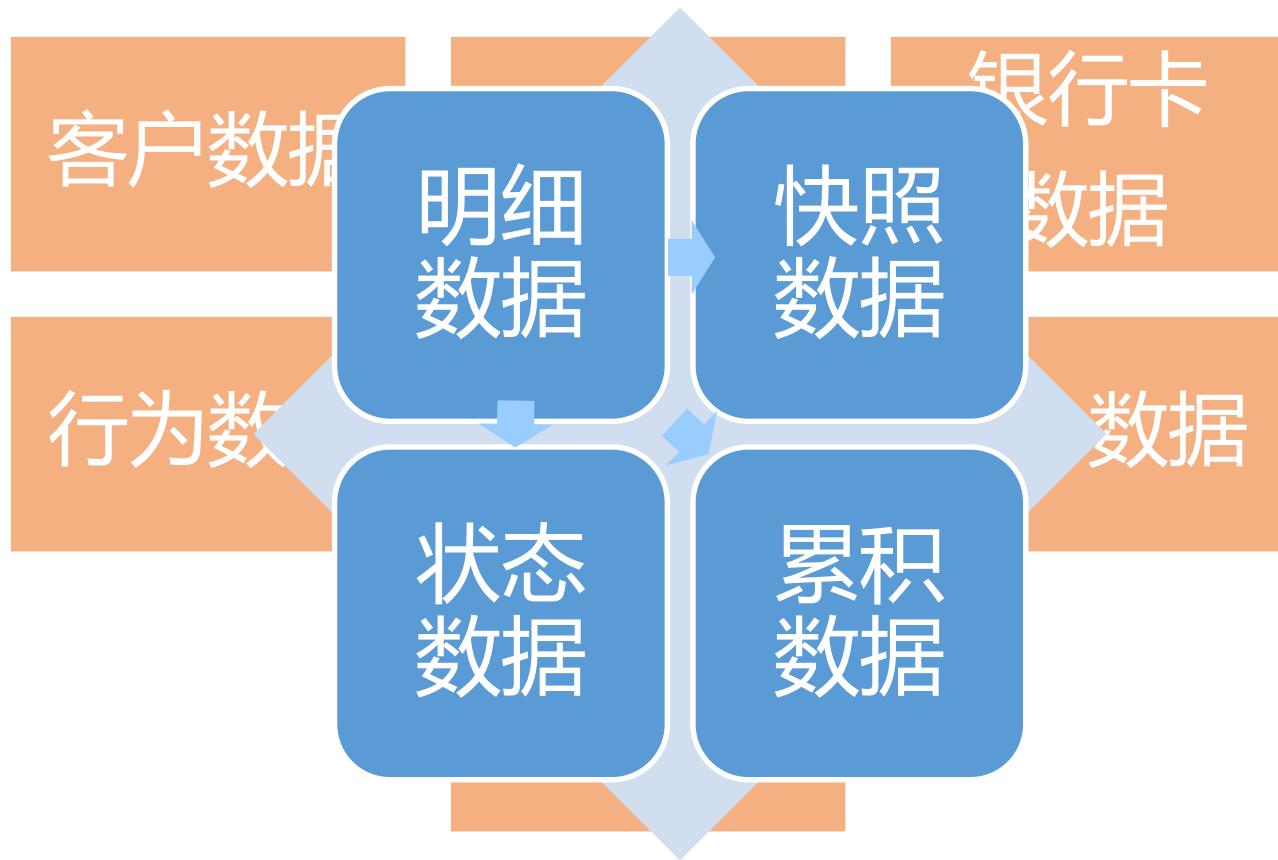
处理峰值 (20131111)

- 当天风险分析超过两亿次
- 事件写入和处理总量10+亿次，超过3T
- 同步峰值风险分析量超过130W次/分钟
- 平均响应时间<100ms

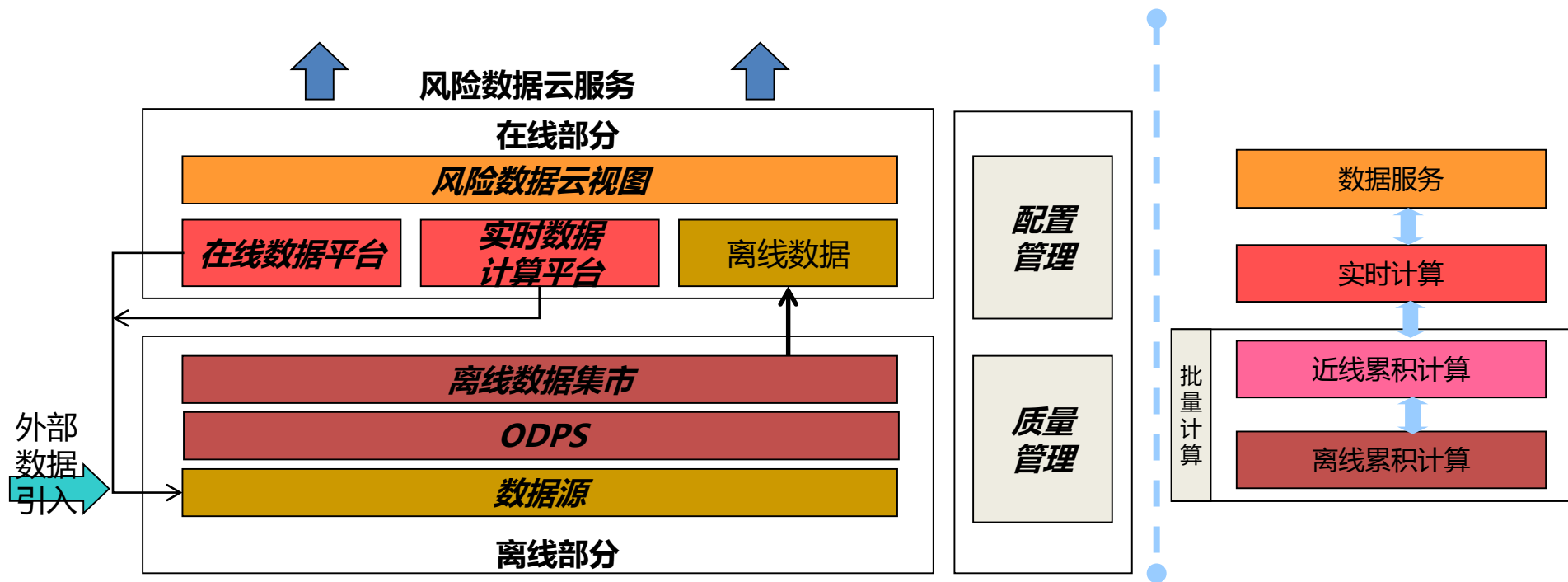
挑战



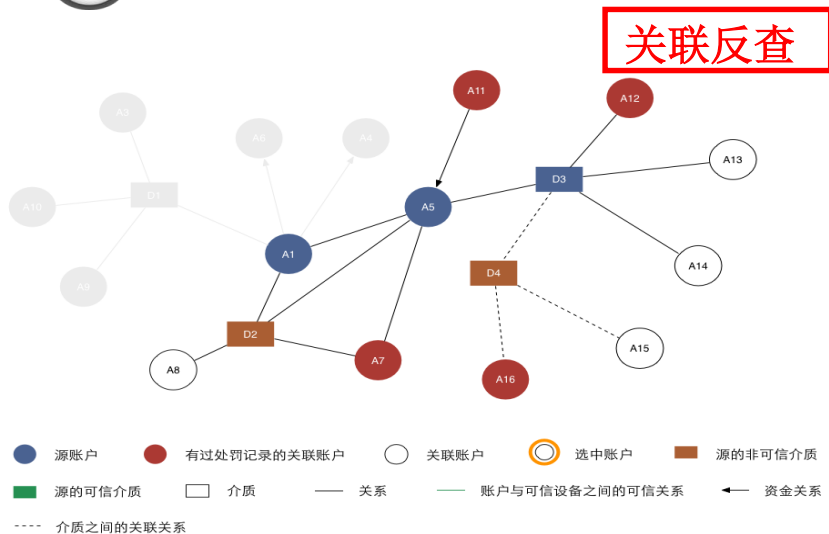
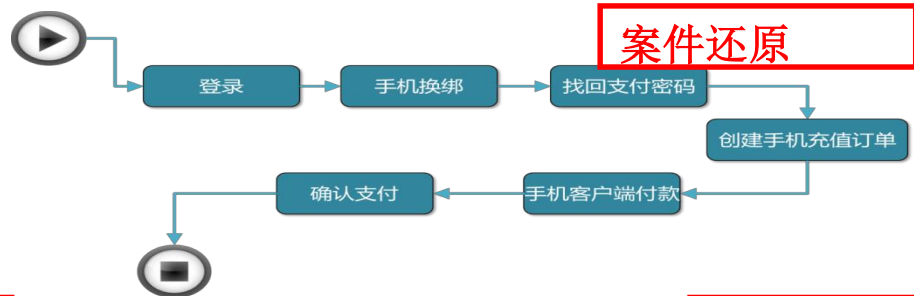
容量性能关键点——数据分类(从明细数据出发)



容量性能关键点——数据计算(风险数据云：分层计算)



快速发现关键点——全方位实时监控及风险分析

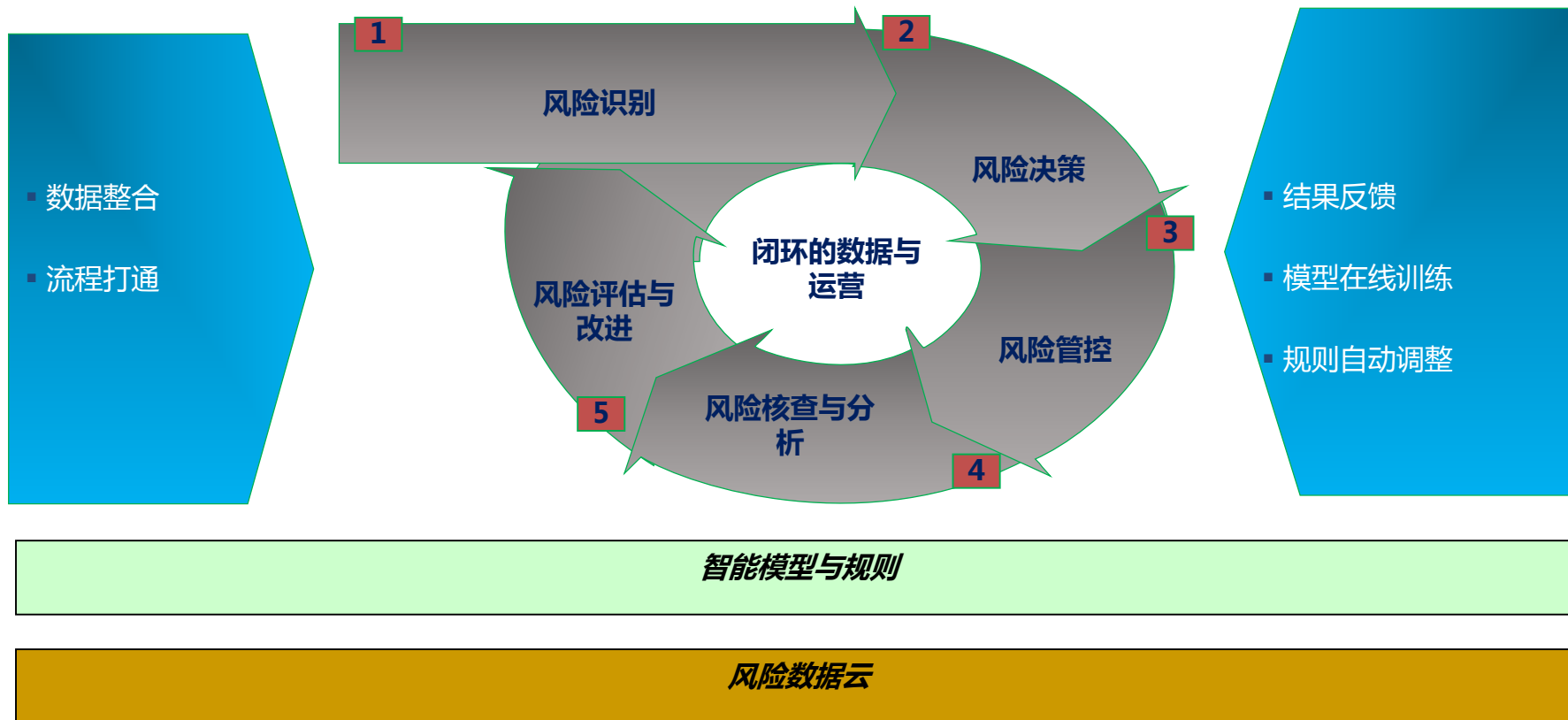


modelcenter模型平均输出分值(11:38)

模型	调用来源	模型平均分
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

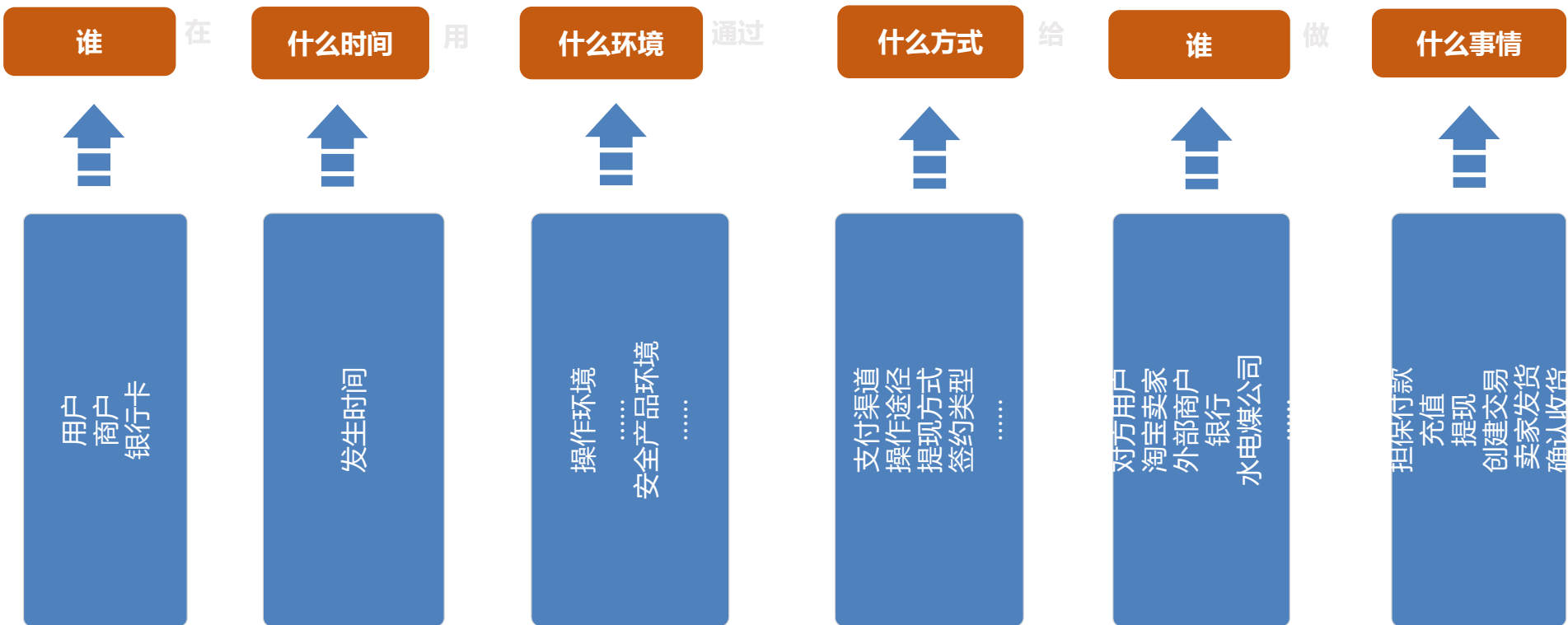
灵活调整关键点——模型和规则的自适应



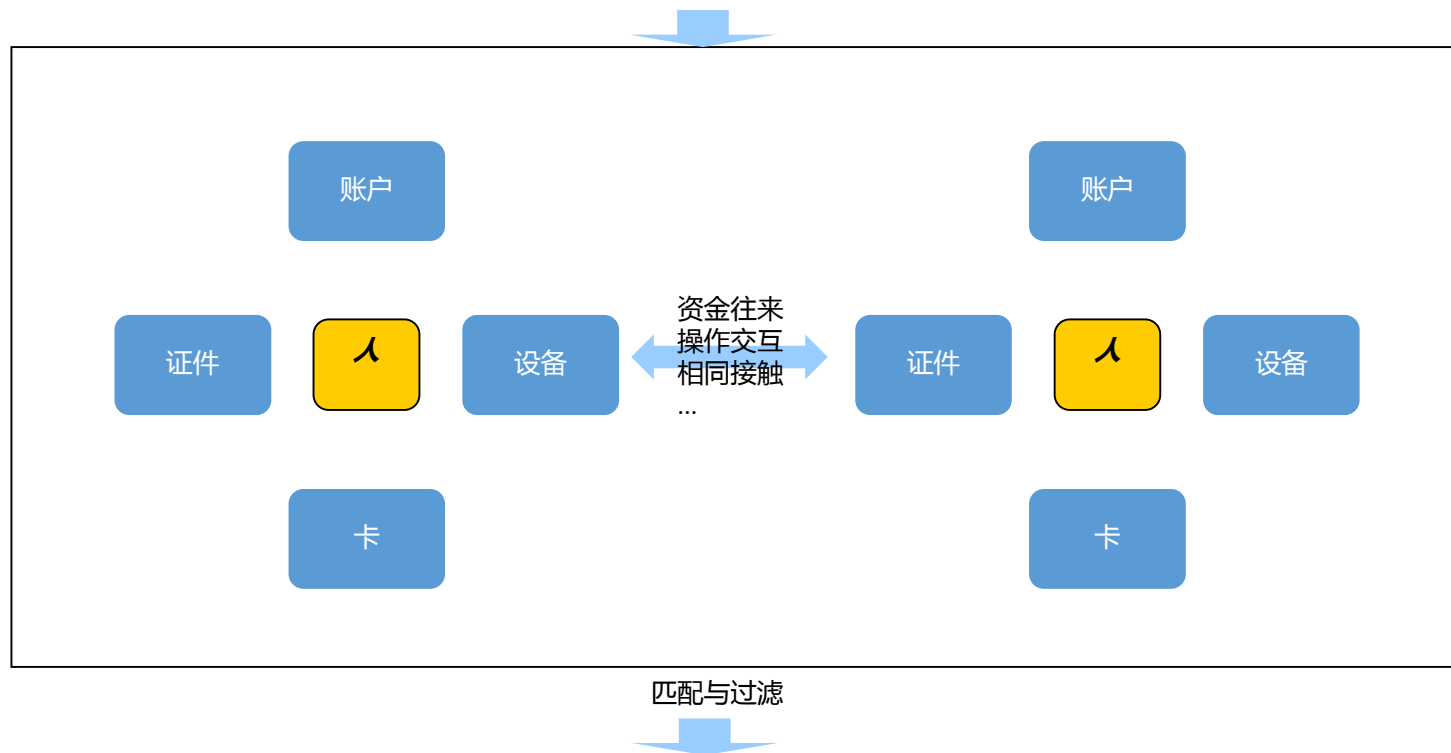
灵活部署关键点——决策的灵活部署(决策手段多样化)



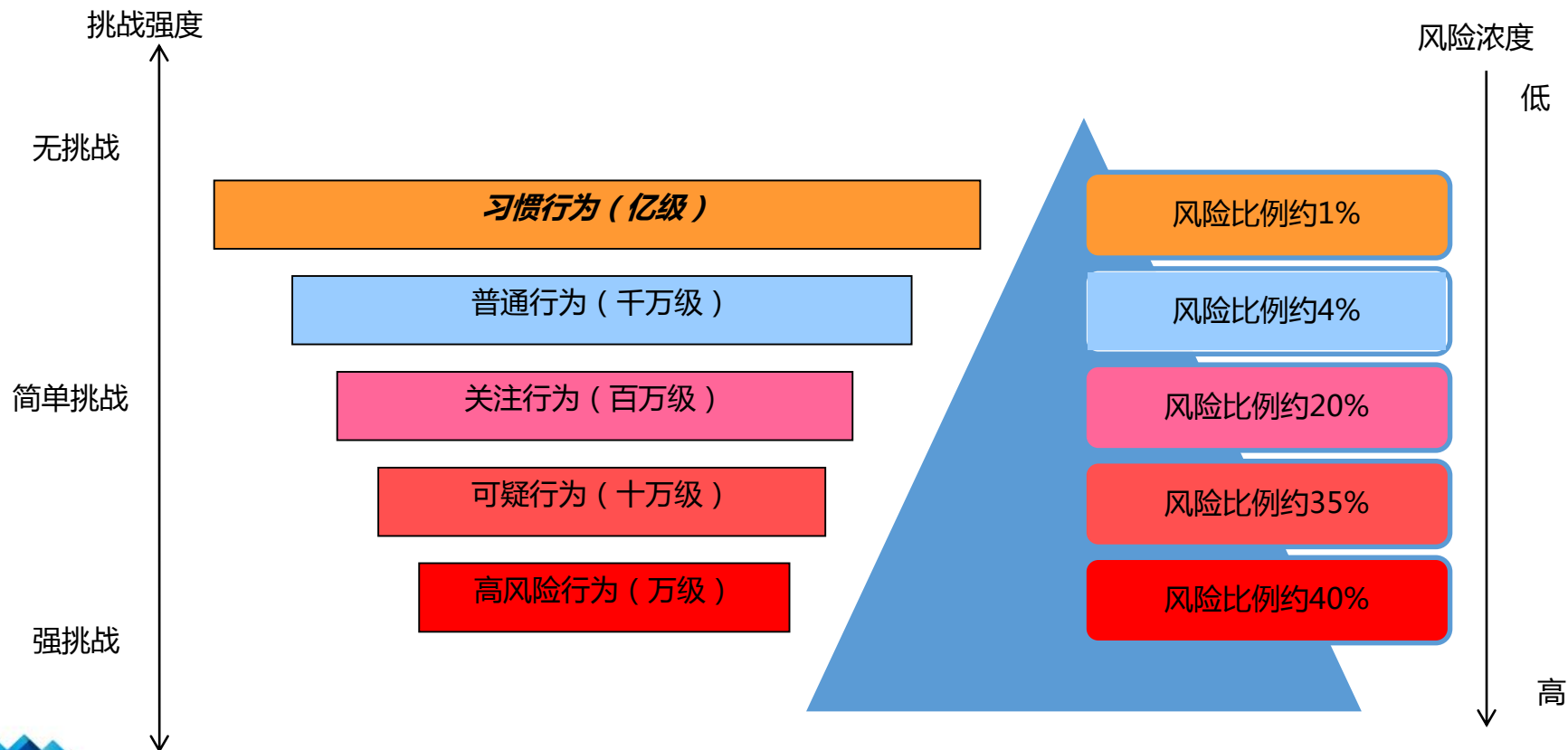
立体布控关键点——事件触发的多维风险监控



立体布控关键点——多主体复杂关系的识别与应用（识别背后自然人）



智能分析决策关键点——多层行为风险漏斗模型



小结



Thanks!

李俊奎@支付宝
kui.ljk@alipay.com

