消金风控联盟

反欺诈实践与应用

刘鹏程 资深互联网风控专家

2021/7/7

课程主旨

- 少一些大道理与名词，多一些案例与实操
- 通过对实际工作应用的整理与汇总，形成专业的反欺诈策略体系，为职业赋能

反欺诈常见内容与手段

痛点分析

互联网黑产已经在全球范围内，形成了规范化、产业化、链条化的行业“生态”,行业上下游形成有序分工、规模合作。据经济观察网《618背后的黑产大战：你在通宵抢优惠券，阻止“羊毛党”的人同样彻夜不眠》报道：2019年黑灰产从业人员超过150万人，黑灰产规模高达1000亿元。黑产利用打码平台、黑产软件等工具，套取平台补贴，影响营销活动效果，给平台带来严重的金钱和名誉损失。如何规避黑产带来的损失，保障业务良性发展，成为各公司关注焦点

黑产产业链

黑产套利技术、手段和危害

羊毛党/黑产 套利技术举例

- 机器注册获取批量账号
- 手机猫池
- 利用黑产软件刷发券接口
- 利用打码平台破解验证码

羊毛党/黑产 套利手段举例

- 恶意高频退换货
- 恶意拒收
- 售后套赠/套运费险
- 闪电退坏账
- 商家恶意套券平台优惠券

羊毛党/黑产的危害

- 影响商品毛利、物流成本、库存周转、商品销售，给平台/商家带来**金钱**、**名誉损失**
- 影响**营销活动效果**和用户体验
- 影响系统，导致系统性能问题
- 犯罪（洗钱、敲诈、勒索），影响社会稳定

在线反欺诈现状

黑产群体

1 组织化

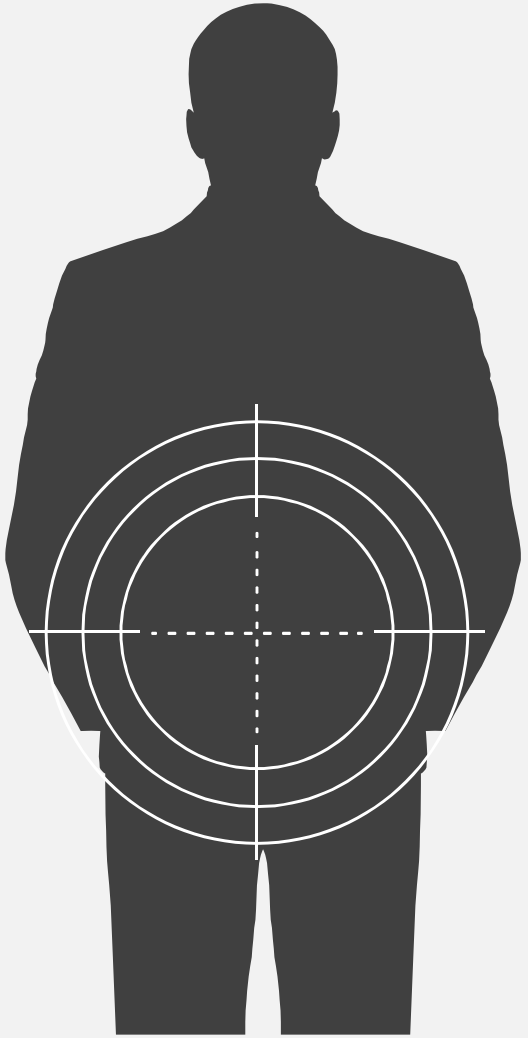
企业数字化转型导致大量个体黑灰产从业者慢慢聚集形成了黑产组织

2 平台化

部分黑产组织基于自己的专业优势，慢慢孵化出了大量的黑产平台 & 开发框架

3 生态化

最终的结果是，黑产从业者不再是栉风沐雨的扒手，通过上下游拆分协同，降低了犯罪的各环节成本&门槛，提升了犯罪的隐蔽性，同时衍生出了大量的灰产，已形成了成规模的黑灰产生态



攻击形式

1 常态化

移动5G网络的普及，O2O服务、手机购物和移动支付等业务的快速发展导致攻击频率越来越高，与黑灰产的实时对抗形成了常态

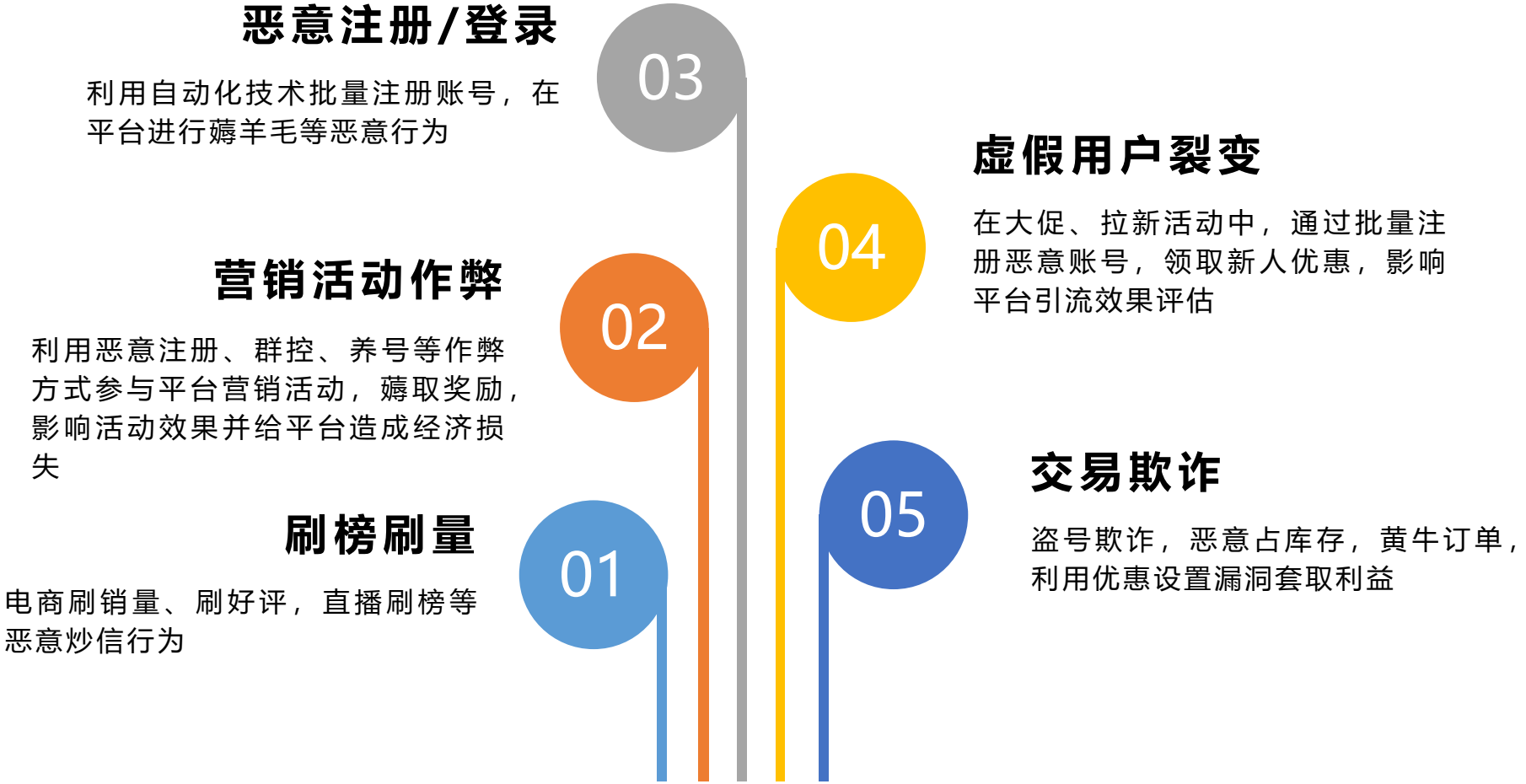
2 多样化

黑灰产的攻击方式已由传统的线下渠道的单点突破转变成线上渠道的多点爆发；黑灰产欺诈种类多，在互联网服务领域，欺诈可谓无处不在；

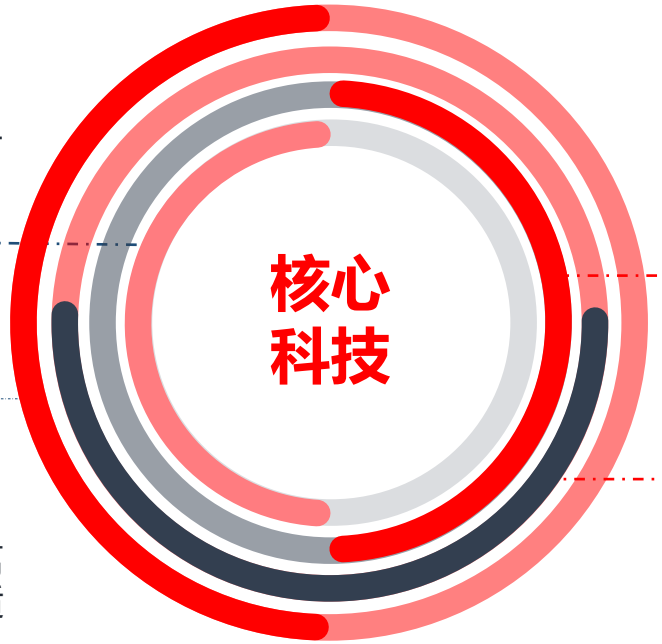
3 智能化

国内黑产团伙的技术升级迭代很快，已处于全球领先水平，例如，利用AI深度学习破解网络登录验证码的技术

欺诈行为介绍


03
恶意注册/登录
利用自动化技术批量注册账号，在平台进行薅羊毛等恶意行为
04
虚假用户裂变
在大促、拉新活动中，通过批量注册恶意账号，领取新人优惠，影响平台引流效果评估
02
营销活动作弊
利用恶意注册、群控、养号等作弊方式参与平台营销活动，薅取奖励，影响活动效果并给平台造成经济损失
05
交易欺诈
盗号欺诈，恶意占库存，黄牛订单，利用优惠设置漏洞套取利益
01
刷榜刷量
电商刷销量、刷好评，直播刷榜等恶意炒信行为

构建反欺诈决策平台的几个能力



决策引擎 高效

毫秒级决策服务，支持分钟百万级并发，支持动态扩缩容

规则+模型 准确

支持与模型、数据对接，通过离线分析实现自我演进，更好的适应业务风险的变化速度，

自身风控能力 融合

融合“在线欺诈检测”产品接口，规则配置中直接引用，即可将风控大数据集成到自建策略体系中

专家策略：针对不同风险场景提供的策略和特征模板，实现策略一键部署

策略实验室 易用

支持使用本地数据和线上数据对策略进行在线验证和对比分析，提升策略开发、调优工作的人效，降低错误率

反欺诈架构示意图

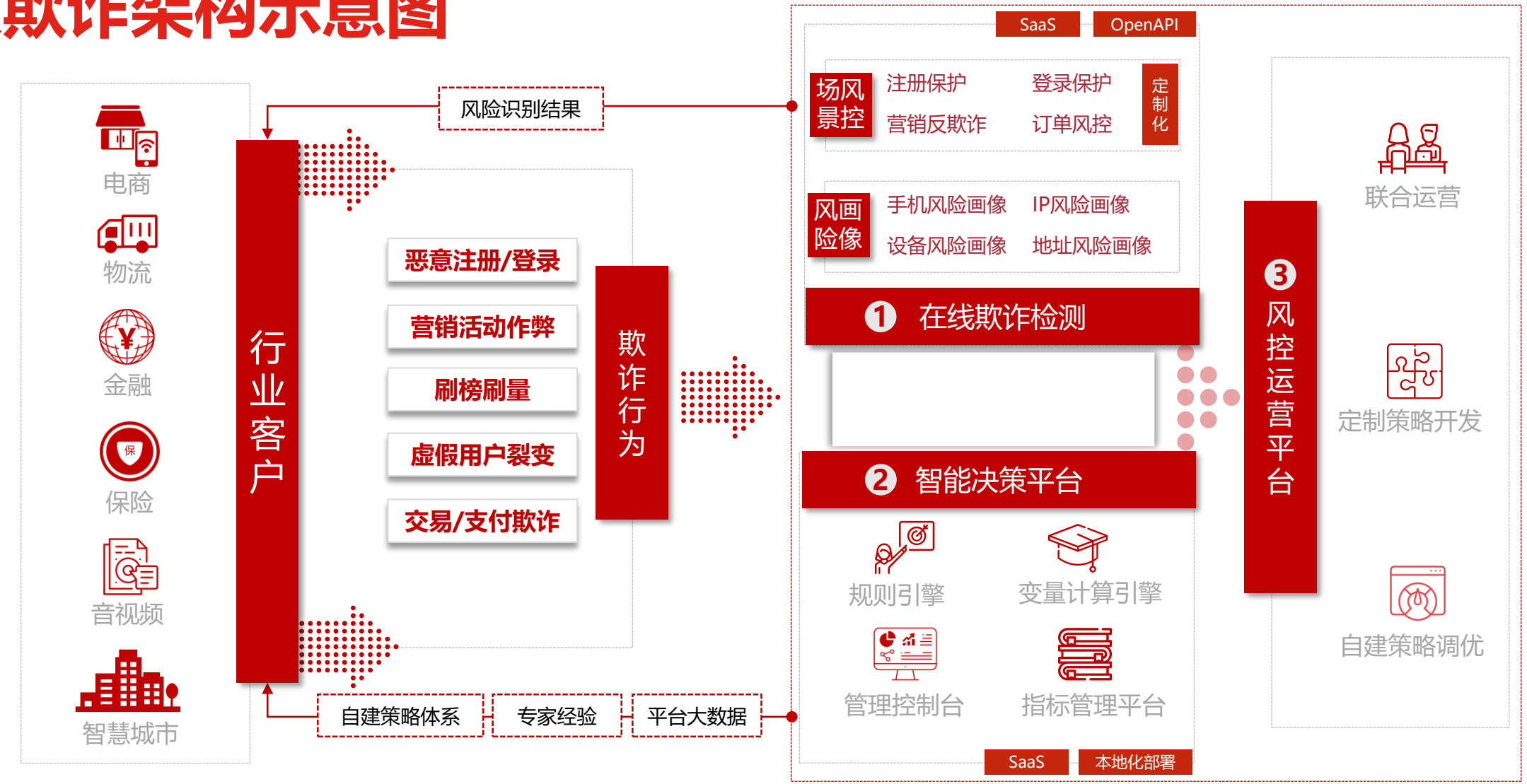
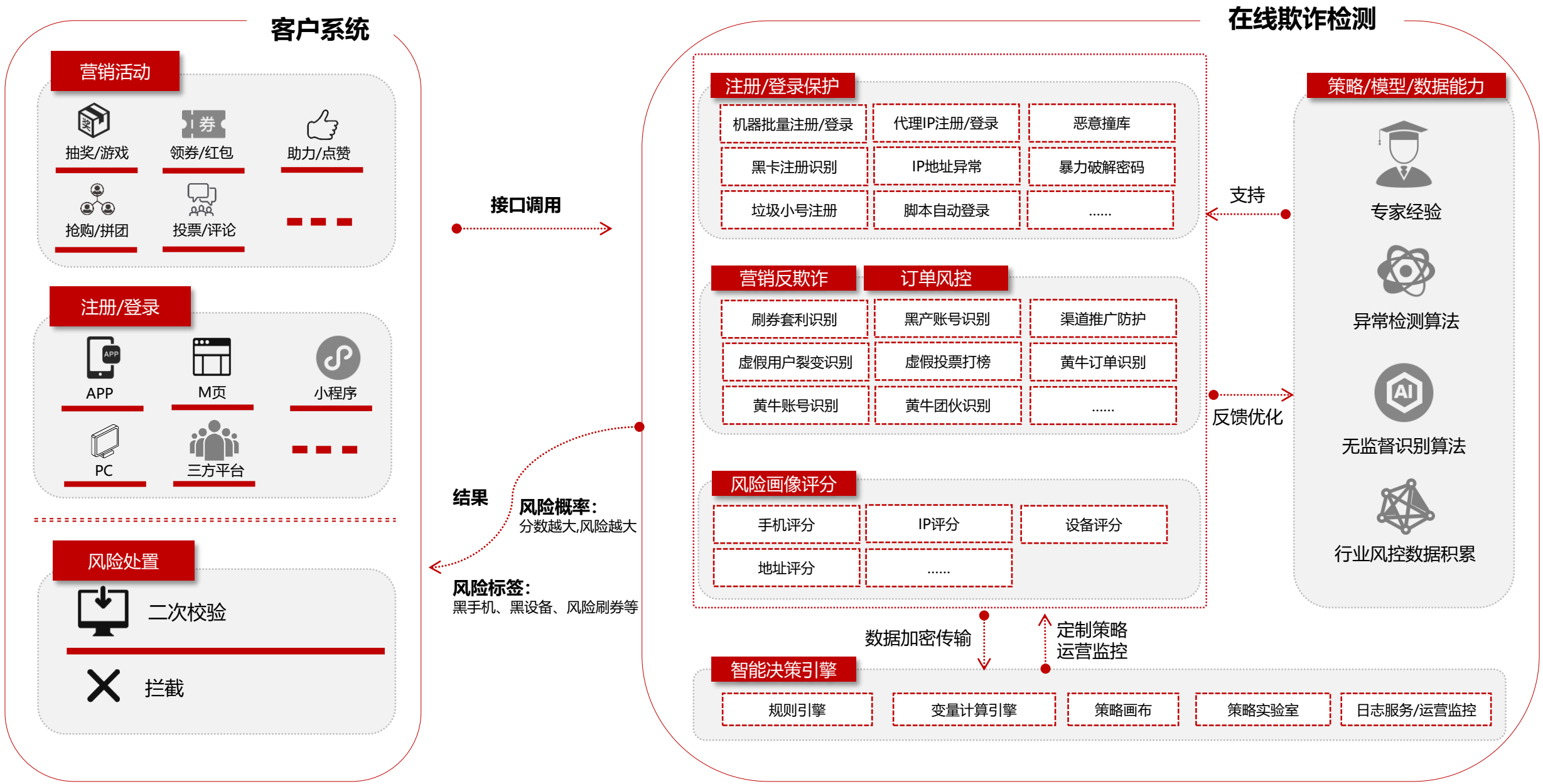

SaaS
OpenAPI
场风景控
注册保护
登录保护
营销反欺诈
订单风控
定制化
风画险像
手机风险画像
IP风险画像
设备风险画像
地址风险画像
1 在线欺诈检测
2 智能决策平台
规则引擎
变量计算引擎
管理控制台
指标管理平台
SaaS
本地化部署
3 风控运营平台
联合运营
定制策略开发
自建策略调优
风险识别结果
行业客户
电商
物流
金融
保险
音视频
智慧城市
欺诈行为
恶意注册/登录
营销活动作弊
刷榜刷量
虚假用户裂变
交易/支付欺诈
自建策略体系
专家经验
平台大数据

示意图-构建反欺诈应用


客户系统
营销活动
抽奖/游戏
领券/红包
助力/点赞
抢购/拼团
投票/评论
注册/登录
APP
M页
小程序
PC
三方平台
风险处置
二次校验
拦截
接口调用
结果
风险概率：
分数越大,风险越大
风险标签：
黑手机、黑设备、风险刷券等
在线欺诈检测
注册/登录保护
机器批量注册/登录
代理IP注册/登录
恶意撞库
黑卡注册识别
IP地址异常
暴力破解密码
垃圾小号注册
脚本自动登录
.....
营销反欺诈
订单风控
刷券套利识别
黑产账号识别
渠道推广防护
虚假用户裂变识别
虚假投票打榜
黄牛订单识别
黄牛账号识别
黄牛团伙识别
.....
风险画像评分
手机评分
IP评分
设备评分
地址评分
.....
支持
反馈优化
策略/模型/数据能力
专家经验
异常检测算法
无监督识别算法
行业风控数据积累
数据加密传输
定制策略
运营监控
智能决策引擎
规则引擎
变量计算引擎
策略画布
策略实验室
日志服务/运营监控

- 注册风险识别

  - 注册风险识别主要针对企业在拉新、营销等活动中出现的大量虚假用户风险，云风险识别通过行为异常、风险网络、地理位置等手段结合安全对垃圾账号多年的特征积累，快速判断当前注册用户风险程度并反馈给企业，企业可根据风险程度作出处理。从而有效打击虚假注册风险，提升客户平台账户质量，减少因垃圾账户引发的平台资损及声誉品牌影响。

- 登录风险识别

  - 登录风险识别主要针对具有高价值资产（例如：余额、银行卡、积分、信用额度等）的账户，防止被黑产通过恶意手段产生盗号资损甚至引发账户用户安全感问题的风险；云风险识别拥有多年对于十几亿用户的账号安全攻防经验，针对钓鱼木马，撞库扫号等引起的被盗问题，搭建基于地理位置、风险网络、设备环境、行为异常等多维识别策略与模型，可以快速精准识别账户被盗行为风险，提升平台账号安全强度，有助于建立平台的用户安全感与品牌信任。

- 营销风险识别

  - 营销风险识别主要针对企业在采用补贴、优惠等方式获取用户时产生的“薅羊毛”风险，云风险识别通过大数据、人工智能结合淘宝、支付宝等多年的活动作弊防控经验，有效、快速、准确的识别活动作弊风险行为和用户；有效保护企业资金安全，提升营销资源精准投放能力，取得良好的活动效果。

- 设备风险识别

  - 设备风险识别主要针对企业在移动APP业务场景中遇到的恶意用户使用模拟器、多开软件等攫取收益产生的风险。云风险识别拥有精准硬件检测技术、海量真机样本库和亿级风险样本，能精准、全面覆盖各类模拟器和恶意软件，有效协助企业甄别恶意设备，提前发现恶意设备，避免资产损失。

- 业务风险情报

  - 业务风险情报主要针对互联网、金融等企业的平台遭遇黑灰产使用虚假信息进行恶意欺诈、作弊、虚假交易等问题。风险识别基于云端大数据以及长期以来与黑灰产攻防对抗的特征策略算法经验，有效帮助企业降低因恶意欺诈导致的运营成本，提升欺诈团伙作案成本。

- 邮箱画像

  - 邮箱画像主要针对企业在面对黑灰产大量使用低成本批量生成的邮箱产生的批量注册、刷票、薅羊毛等风险，云风险识别通过亿级风险样本学习、机器学习算法、情报分析等手段高精度、快速识别问题邮箱；有效帮助企业预防大规模风险的发生，减少资损，提升黑灰产在平台的作案门槛和成本。

- 地址评分

  - 地址评分主要针对电商、物流、银行等企业在面对恶意用户大量使用无效地址而造成的公司人力资源浪费和资金损失风险；云风险识别通过人工智能算法与自然语言处理技术等手段快速识别虚假地址；有效帮助企业减少因为虚假地址而造成的人力和资源浪费，提升平台运营效率。

• 应用场景

登录风险识别产品适用于帮助用户发现账户被盗行为，可以运用到网站的登录、下单、付款、提现等业务流程中，通过传入识别所需信息，系统自动返回账户登录风险情况。用户可以根据返回风险信息执行后续操作（如短信二次验证、身份证验证、人脸验证、锁定账户等）。

营销风险识别产品适用于帮助用户发现在营销活动中出现的作弊、薅羊毛、套利等风险，可以运用到限时抽奖、免费拉新、优惠折扣、推广返利等类型活动中，通过传入识别所需信息，系统自动返回营销风险情况，用户可以将风险返回结果应用到营销资源差异化投放中（如账号打标、阻断行为、调整中奖/券概率等）。

注册风险识别产品适用于帮助用户发现业务中的批量注册行为，可以运用到用户的注册、登录、下单、付款等流程中，通过传入识别所需信息，系统自动返回账户注册风险情况。用户可以根据返回风险信息执行后续操作（如账号打标、阻断任务、风险传递等）。

设备风险识别产品适用于对移动APP上的恶意设备行为进行识别，可以应用到注册、登录、下单、领券等场景，通过传入设备信息，系统进行模拟器检测、恶意工具检测，返回设备风险信息。用户可以根据返回信息甄别模拟器、批量、多开等风险行为。

- 应用场景

业务风险情报

- 业务风险情报产品适用于对企业平台的账户或用户进行风险检测，可以应用到存量已登记的账户信息以及新增账户信息的风险检测，通过传入账户信息，系统会自动返回虚假、无效、低质量、高危风险等特征与量化评分的结果。

邮箱画像

- 邮箱画像产品适用于帮助用户发现邮箱风险，可以运用到用户的注册、登录、修改信息等业务流程中，通过传入邮箱信息，系统自动返回邮箱风险情况。用户可以根据返回的风险标签个性化处理账户及账户行为（如账号打标、二次核验、高危行为阻断等）

地址评分

- 地址评分产品适用于帮助用户发现无效地址，可以运用到用户的注册、下单、修改信息等业务流程中，通过传入地址信息，系统自动返回地址风险情况。用户可以根据返回信息执行后续操作（如进一步核实信息，降低处理优先级等）。

17大类反欺诈策略详解

反欺诈核心策略


★17类反欺诈策略集详解
疑似团伙申请策略
多头应用统计
历史申请多头
历史复杂关系网络策略
通讯录风险比对
舆论风险策略
百度
微信&QQ
微博
GPS区域检测策略
风险
地址风险
流量控制策略
营销
注册
申请
订单&交易
异常贷款策略
失信风险策略
恶意贷款策略
联系人风险名单比对策略
联系人多头名单比对策略
信息检验策略
复杂关系网络策略
多头风险策略
手机号身份证关联设备风险识别

17类策略集详解

XXXX多条策略


提
问
答
疑

T 谢谢观看

HANK YOU!