业务安全风险控制实践

李 斌

议题引入

业务开展营销活动过程中，本意通过优惠或让利，吸引用户参与。

很容易被黑产盯上：

- 优惠券瞬间被刷光
- 积分被恶意获取
- 游戏奖品被恶意领券
- 更有甚者，账号被盗

黑产异常灵敏，获利空间巨大！

目录

- 业务安全风险简介
- 安全风控系统
- 产品安全风险控制实践

业务安全风险介绍

注册登录

- 恶意注册
- 撞库攻击
- 暴力破解

营销活动

- 恶意领券
- 抢红包
- 游戏作弊
- 批量签到
- 垃圾广告

交易支付

- 恶意下单
- 虚假交易
- 盗卡盗刷

黑产作案手法分析

资源准备

- 手机号/微信号
- 短信代收
- 打码平台
- 群控平台

破解逆向

- APP破解
- H5破解
- 设备指纹破解

批量操作

- 批量注册
- 批量登录
- 养号（定期活跃）
- 批量刷单/领券等

快速变现

- 抵用消费
- 低价售卖
- 兑换话费/Q币
- 购买E卡/会员券

如何防范业务安全威胁？

1、单个业务行为都是正常的（漏洞除外）

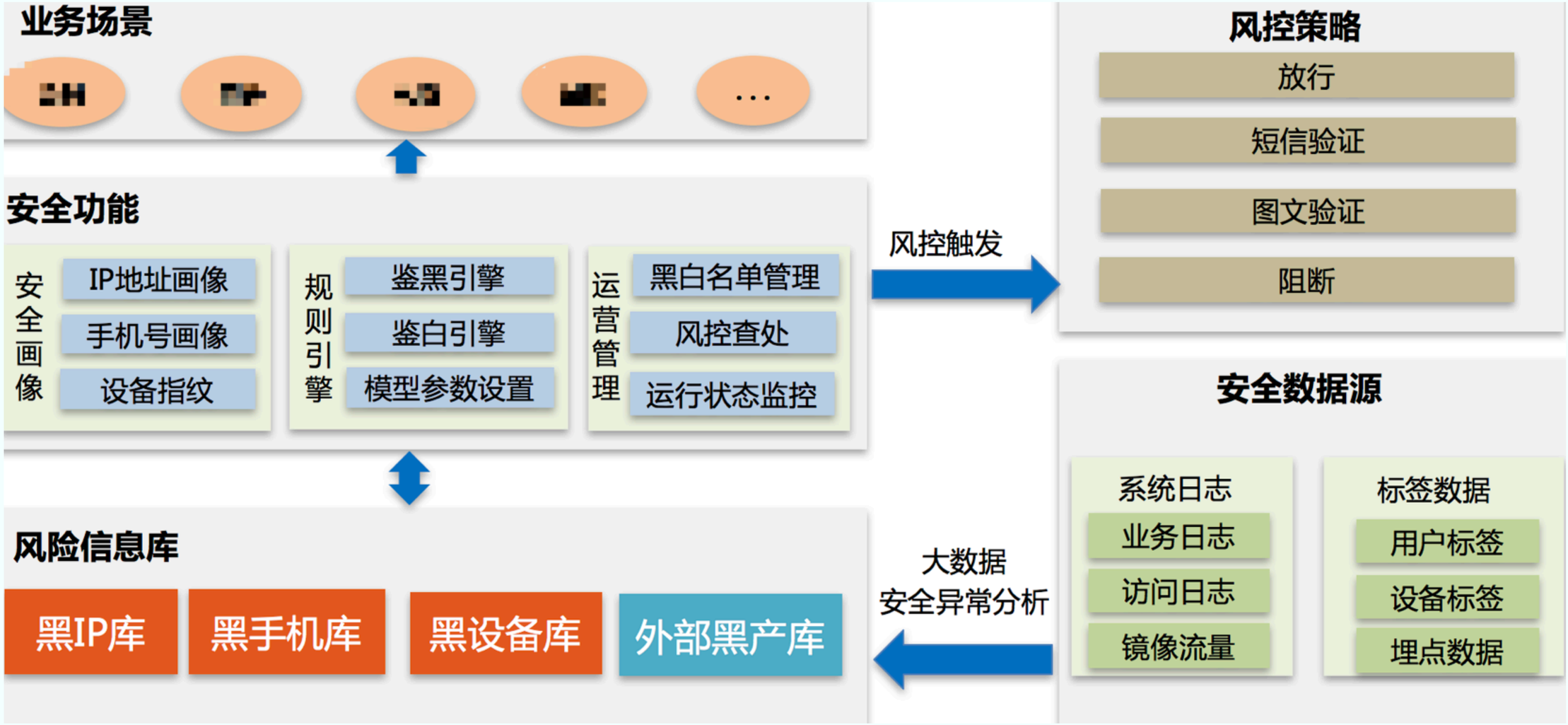
2、需要解析业务行为，关联分析，判断是否异常

3、防火墙、IPS、WAF等系统很难防护

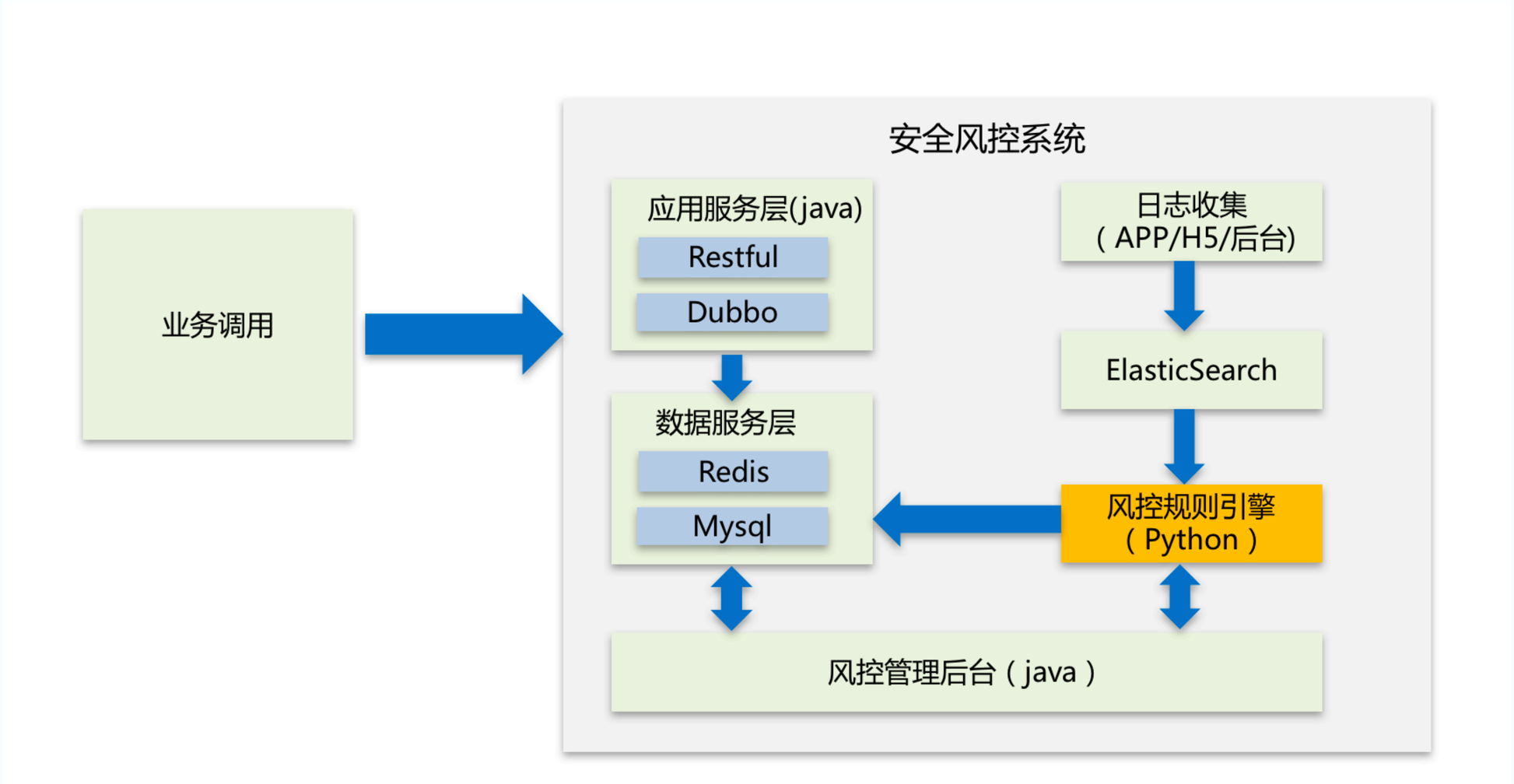
4、需要从业务层加以防范

安全风控系统

安全风控系统-功能架构


业务场景
[redacted]
...
安全功能
安全画像
IP地址画像
手机号画像
设备指纹
规则引擎
鉴黑引擎
鉴白引擎
模型参数设置
运营管理
黑白名单管理
风控查处
运行状态监控
风险信息库
黑IP库
黑手机库
黑设备库
外部黑产库
风控触发
大数据
安全异常分析
风控策略
放行
短信验证
图文验证
阻断
安全数据源
系统日志
业务日志
访问日志
镜像流量
标签数据
用户标签
设备标签
埋点数据

安全风控系统-技术架构


安全风控系统
业务调用
应用服务层(java)
Restful
Dubbo
数据服务层
Redis
Mysql
日志收集
（APP/H5/后台）
ElasticSearch
风控规则引擎
（Python）
风控管理后台（java）

安全风控系统-设备指纹

采集设备信息，为每个设备产生唯一ID，称为设备指纹

mobile	client_id
135[redacted]	3ce[redacted]80ce64551

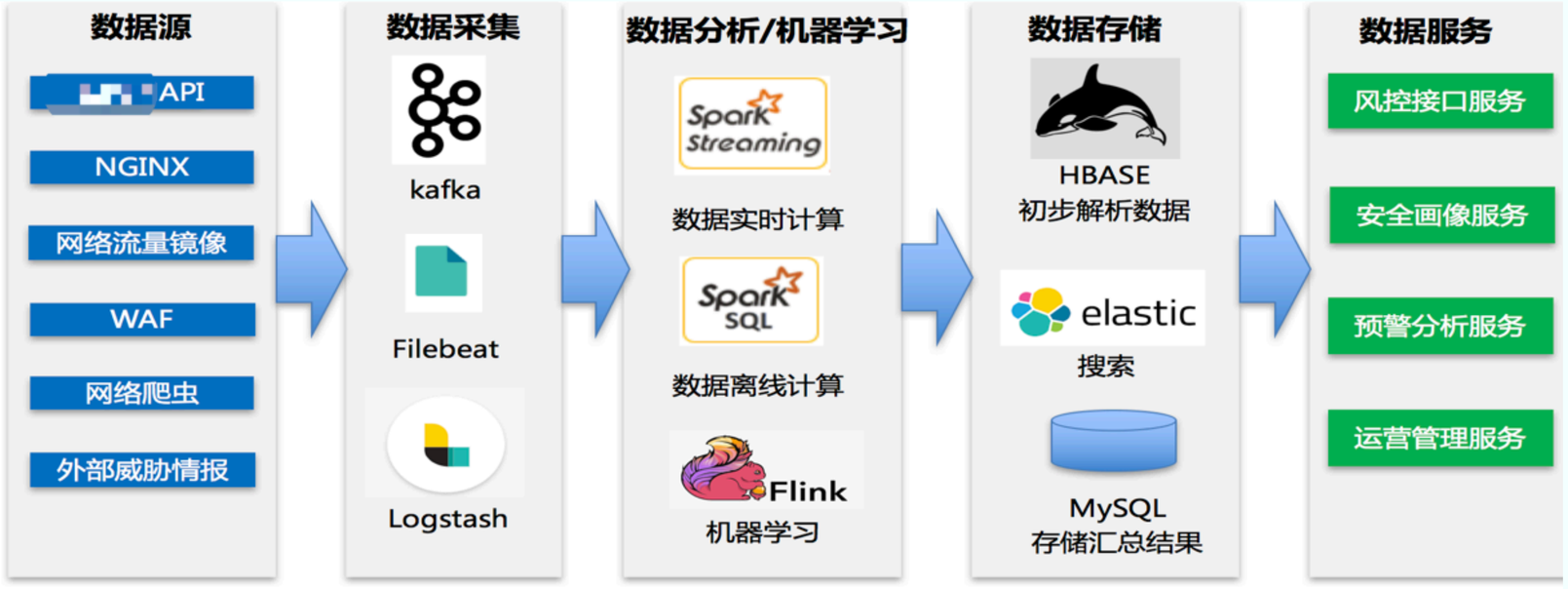
用户验证后，将设备指纹和手机号关联，存储入库

假设账号被盗，由于盗用者设备指纹和合法用户指纹不一致，无法通过认证

解决**撞库盗号**问题！

目前设备指纹主要覆盖Android和iOS

安全风控系统-大数据异常分析



已累计数十条规则：

- ✓ 同IP访问异常行为
- ✓ 同设备指纹异常行为
- ✓ 行为路径异常（如登录后只访问某接口、行为路径区分与正常用户）
- ✓ 养号行为（异常时段集中登录）
- ✓ 登录失败率过高

用于恶意用户识别，产出黑IP、黑手机号、黑指纹！

业务风险控制实践-安全设计评审

1、业务安全评审

深入参与业务安全评审，在设计阶段控制产品安全风险，形成非常良好的机制

产品、业务、开发的安全意识非常高

2、容易出问题的地方

- 账号要一对一绑定（如微信账号和会员账号绑定）
- 营销券发放（注意门槛限制、数量限制）
- 注册登录接口要收紧和统一，决不允许新开口子
- 高并发导致超限问题（突破限制领券、兑换等）
- 一定要有风险控制预案（熔断、作废、冻结）
- 业务规则非常重要，做得好，能大大降低安全事件发生概率

业务风险控制案例-注册登录

注册、登录的重要性再多强调都不为过！

1、注册

- 使用外部API做事前风险决策

2、登录

- 根据风险级别采用不通策略（通过、图文验证、阻断）

3、共性问题

- 统一注册和登录入口（APP、H5），下线旧接口，接入风控（花了1年时间统一）
- APP的破解只是时间问题，但是还是要做APP加固（提高门槛）
- 所有策略的变更，前端改了后端也要改
- 注意旧版本问题，必要时强制更新

业务风险控制案例-业务实践案例

1、恶意签到

- 某日，发现有团伙拿多个账号在签到，马上洗入黑名单
- 黑名单用户签到无法获取积分
- 第二天就无法签到了，黑产放弃

2、积分抽奖游戏活动

- 发现有恶意用户在用机器批量玩游戏
- 限制中奖率，无法中大奖
- 保持活跃度，控制恶意用户

3、优惠券活动

- 发放高性价比优惠券，吸引用户使用
- 限制恶意程度为一定级别以上的用户领取
- 提高活动营销效果

只要有获利空间，对抗不会停止！

业务安全风控实践小结

终端	注册	登录	业务
APP加固	人机交互	人机交互	安全评审
H5混淆加密	黑产库API	盗号保护	业务规则限制
设备指纹采集		风控接入	安全漏洞评估
			风控接入
			应急方案

Q&A