爱奇艺业务风控系统

爱奇艺云平台高级技术总监
谢丹铭

爱奇艺视频业务

- 爱奇艺移动端以**2.99亿**人的月度覆盖位列行业第一，总体占比高达**58%**，行业领先优势持续加大
- 爱奇艺移动端凭借人均单日使用次数**5.01次**，成为视频用户首选

(数据来源：艾瑞MUT，2016年5月)

日均覆盖人数 NO.1

月度覆盖人数 NO.1

月度浏览时间 NO.1

爱奇艺会员业务

品牌升级日

- 2015年10月14日
  爱奇艺VIP会员品牌全面升级
  杨洋、Angelababy、黄渤
  成为爱奇艺VIP会员品牌代言人
  诠释爱奇艺VIP会员核心理念

爱奇艺·VIP会员
轻 奢 新 主 义

爱奇艺VIP会员 量级

- 2016年06月：爱奇艺VIP会员数量超过2000万
- 2015年12月：爱奇艺VIP会员数量超过1000万
- 2015年6月：爱奇艺VIP会员数量超过500万

爱奇艺VIP会员 抢先看

《太阳的后裔》独家上线爱奇艺
VIP会员畅享零时差观剧体验

至2016年4月15日

《太阳的后裔》总播放量高达**26.85亿**
刷新《来自星星的你》首轮13亿的韩剧网播记录

追剧不等待
海量随心看
视听更震撼

爱奇艺泛娱乐平台

- 集 **视频、社交、阅读、商城、购票、游戏** 多种生活服务于一体
- 为用户打造一个更贴近生活、全方位的移动平台

业务风险

会员	视频	社交	直播	电商	支付	其他
薅羊毛	刷播次	黄色图文	刷人气	薅羊毛	盗号盗卡	短信轰炸
恶意注册	盗链	恶意广告	恶意广告图文	恶意下单	洗钱	钓鱼邮件
撞库	广告屏蔽	诈骗	人身攻击	订单欺诈	恶意提现	内部帐号爆破
会员分享						

- 用户层面:
  - 权益受损
  - 体验变差
  - 忠诚度变差
  - 受到骚扰
- 公司层面:
  - 财务损失
  - 业务故障
  - 名誉破坏
  - 机密泄露
  - 法律风险

黑色产业链

病毒木马
漏洞利用
数据窃取(内部,外部)
流量劫持
社会工程学

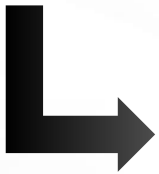
团伙1：产出疑似帐号密码数据

低技术门槛
低法律风险
高黑色收益

入侵/钓鱼
爆破/撞库
自动化工具，OCR识别
代理服务，虚拟设备

团伙2:确信帐号密码数据, 洗号

用户在各个网站之间共用帐号密码；
多家重要网站帐号安全不重视，密码明文存储或者MD5不加盐存储；
几十亿用户数据已在暗网存在多年



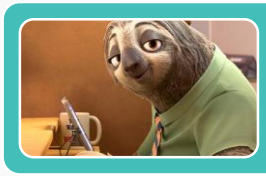
网络贩卖销赃
电话诈骗
盗取虚拟资产
转账套现

团伙3:帐号变现

传统防范的问题

手段单一

- 前置防刷
- 频次，黑白名单



策略不够灵活

- 与业务代码耦合
- 严重依赖业务开发测试和上线流程，占用业务排期，难以快速响应

缺乏数据支撑

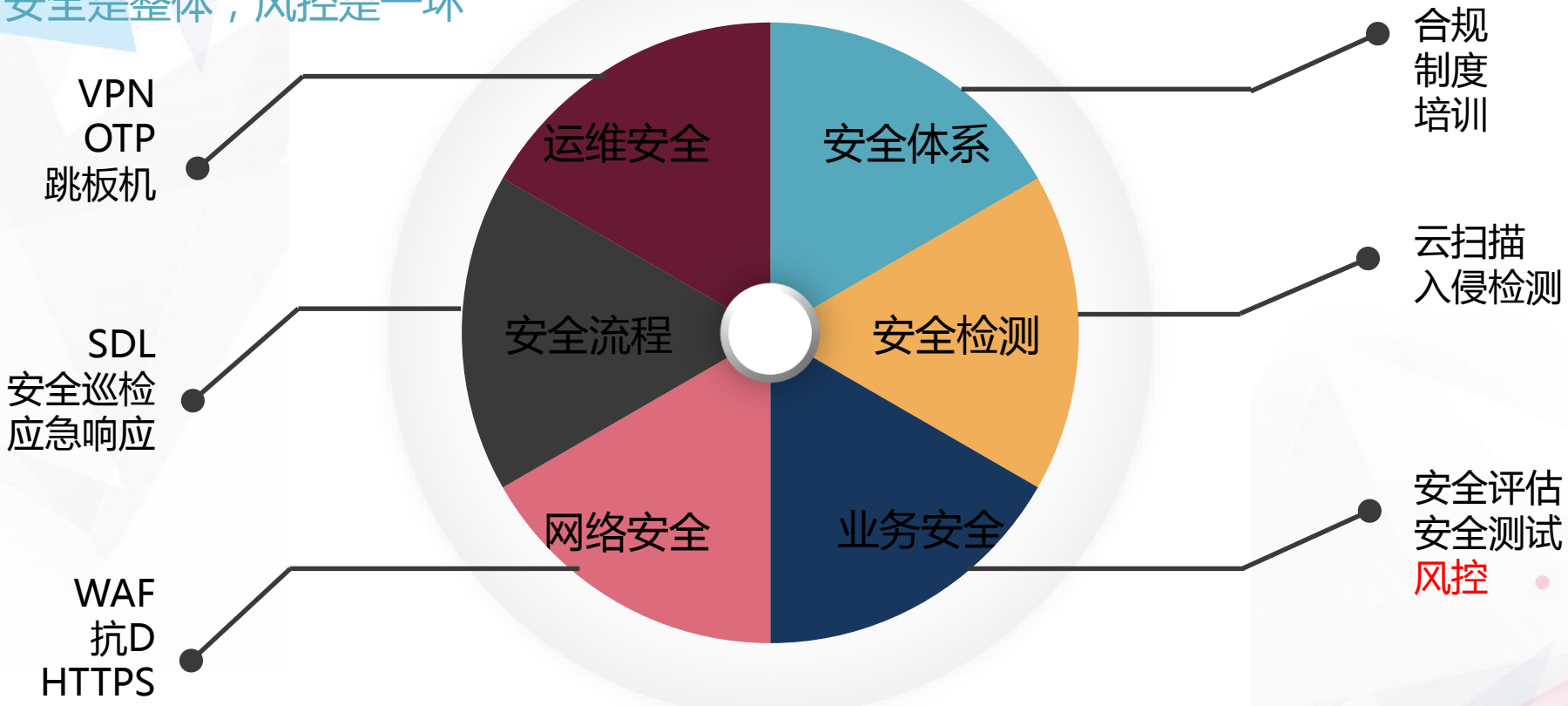
- 没有全站，全网历史数据支撑
- 各个业务方各自为战，经验以及数据不能分享

极端情况下妨碍业务

- 安全服务成为业务关键路径，服务挂，业务挂

解决方案-安全+风控

安全是整体，风控是一环



如何做一个好的风控系统

低耦合

可降级

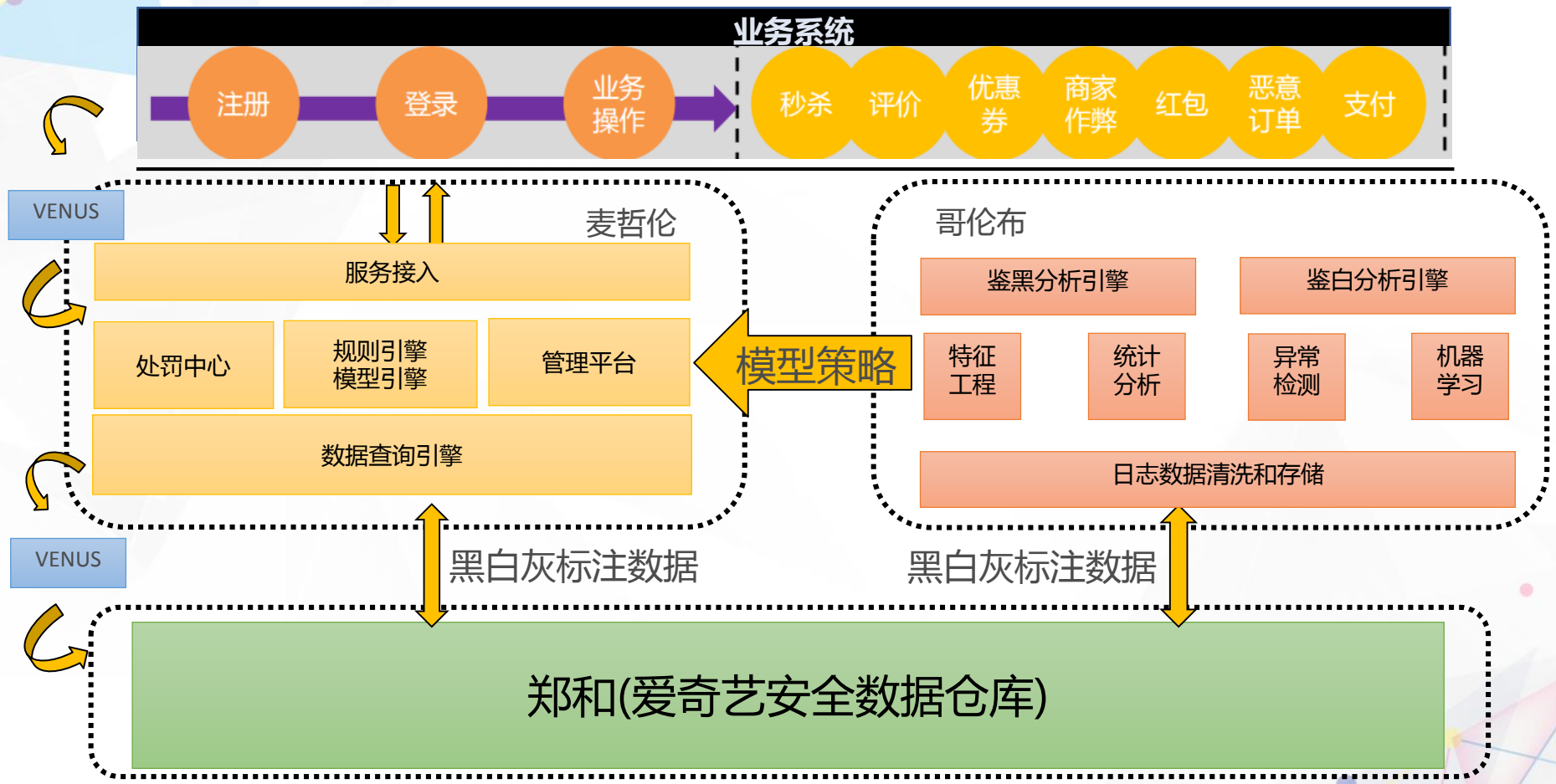
延迟可控

数据驱动

前后端结合

服务质量保证

爱奇艺风控系统

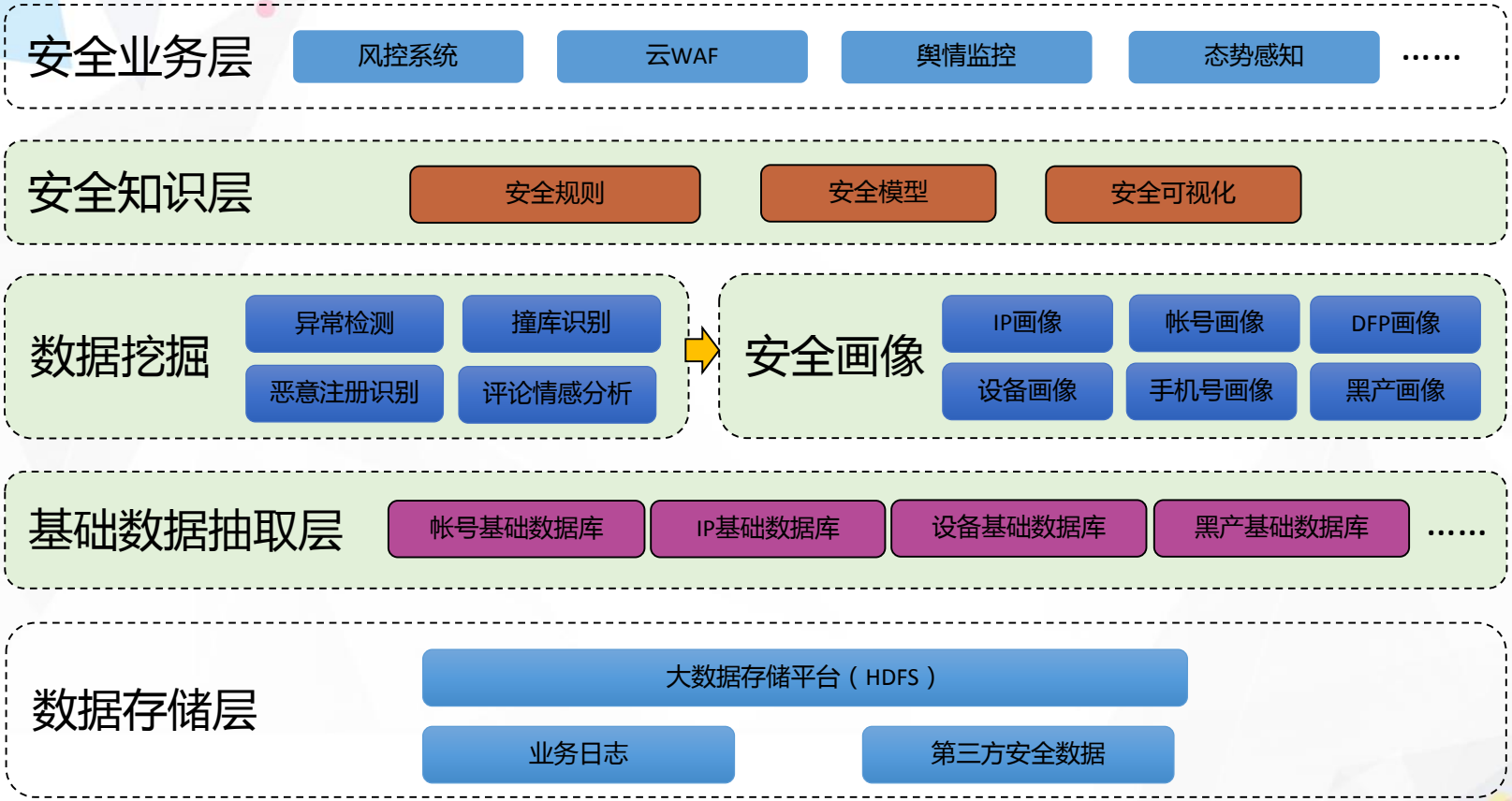

业务系统
注册
登录
业务操作
秒杀
评价
优惠券
商家作弊
红包
恶意订单
支付
VENUS
麦哲伦
服务接入
处罚中心
规则引擎
模型引擎
管理平台
数据查询引擎
模型策略
哥伦布
鉴黑分析引擎
鉴白分析引擎
特征工程
统计分析
异常检测
机器学习
日志数据清洗和存储
VENUS
黑白灰标注数据
黑白灰标注数据
郑和(爱奇艺安全数据仓库)

数据驱动安全

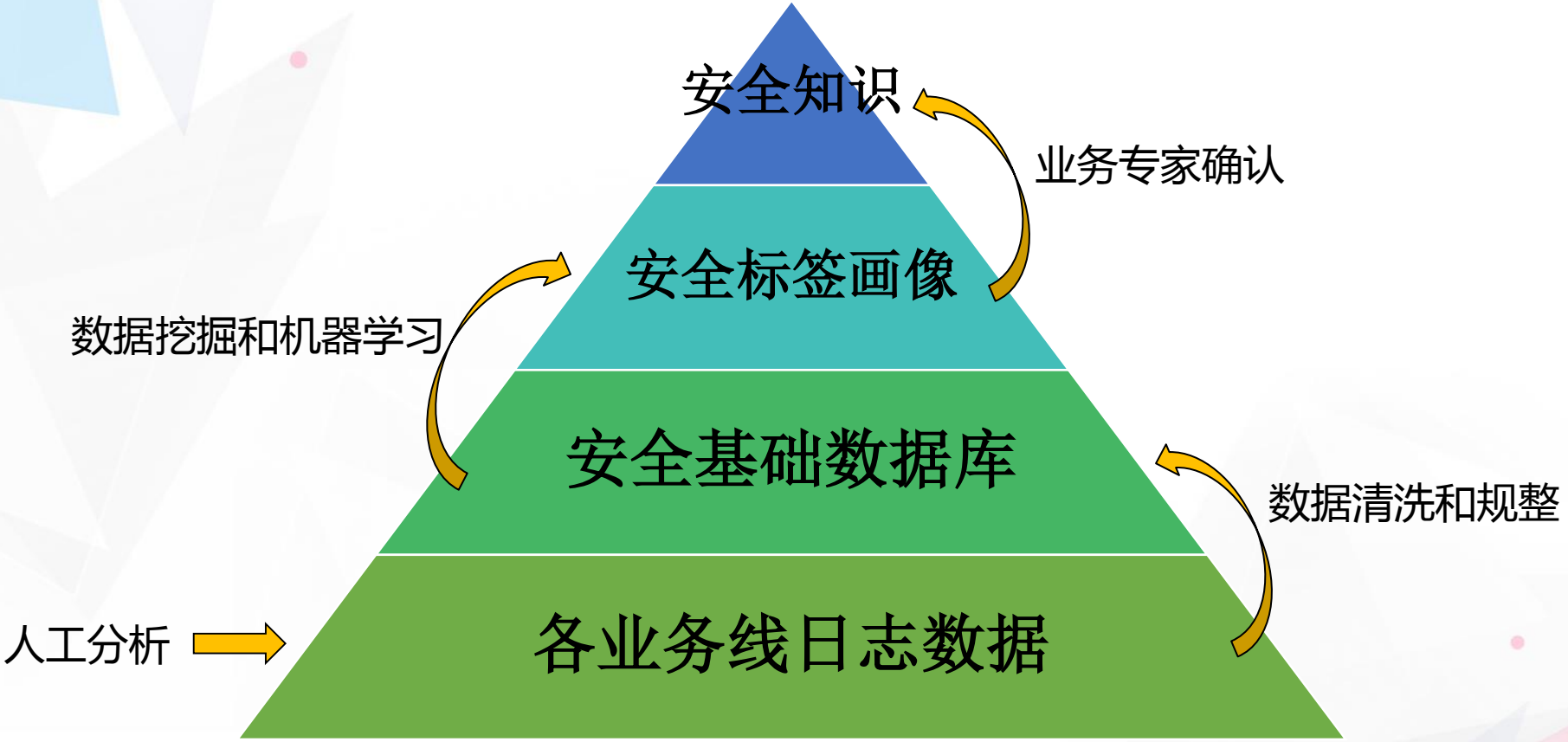
- 14种数据来源
- 147个数据集合
- 47类业务标签
- 11种数据维度
- 49种威胁指标

持续增加...

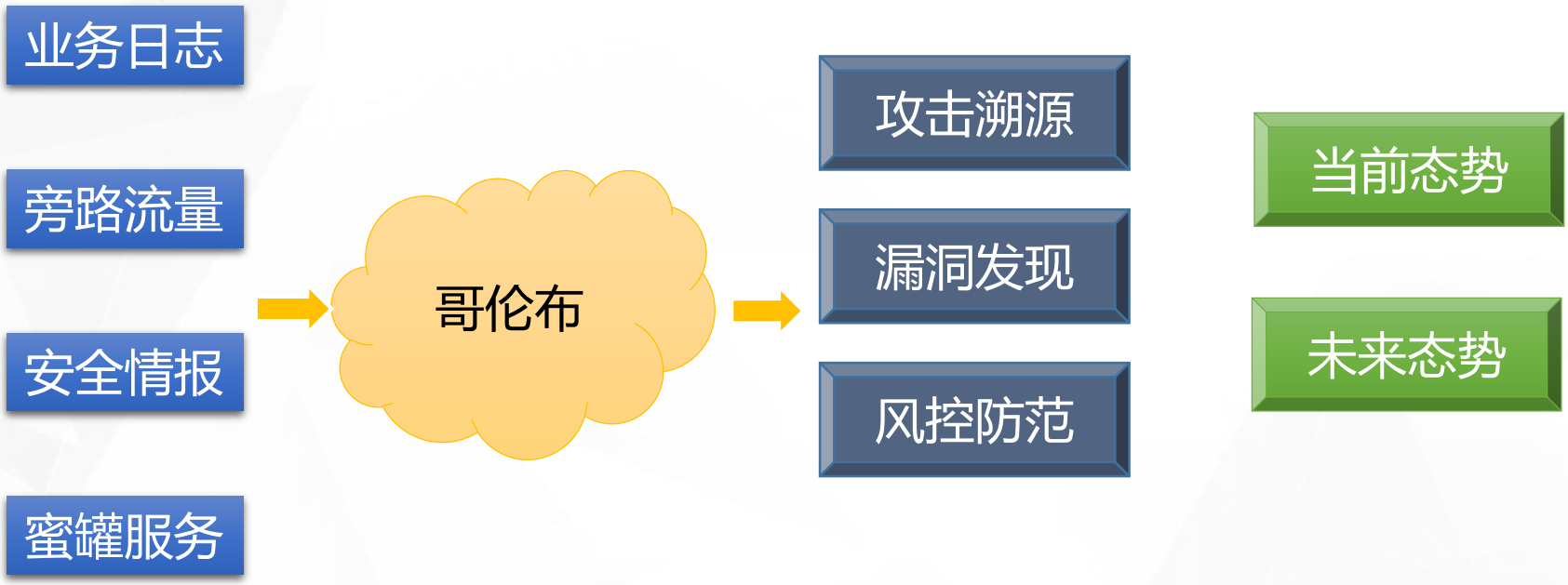
哥伦布 – 大数据层


安全业务层
风控系统
云WAF
舆情监控
态势感知
……
安全知识层
安全规则
安全模型
安全可视化
数据挖掘
异常检测
撞库识别
恶意注册识别
评论情感分析
安全画像
IP画像
帐号画像
DFP画像
设备画像
手机号画像
黑产画像
基础数据抽取层
帐号基础数据库
IP基础数据库
设备基础数据库
黑产基础数据库
……
数据存储层
大数据存储平台（HDFS）
业务日志
第三方安全数据

哥伦布 – 数据提炼过程


安全知识
安全标签画像
安全基础数据库
各业务线日志数据
业务专家确认
数据挖掘和机器学习
数据清洗和规整
人工分析

哥伦布-态势感知

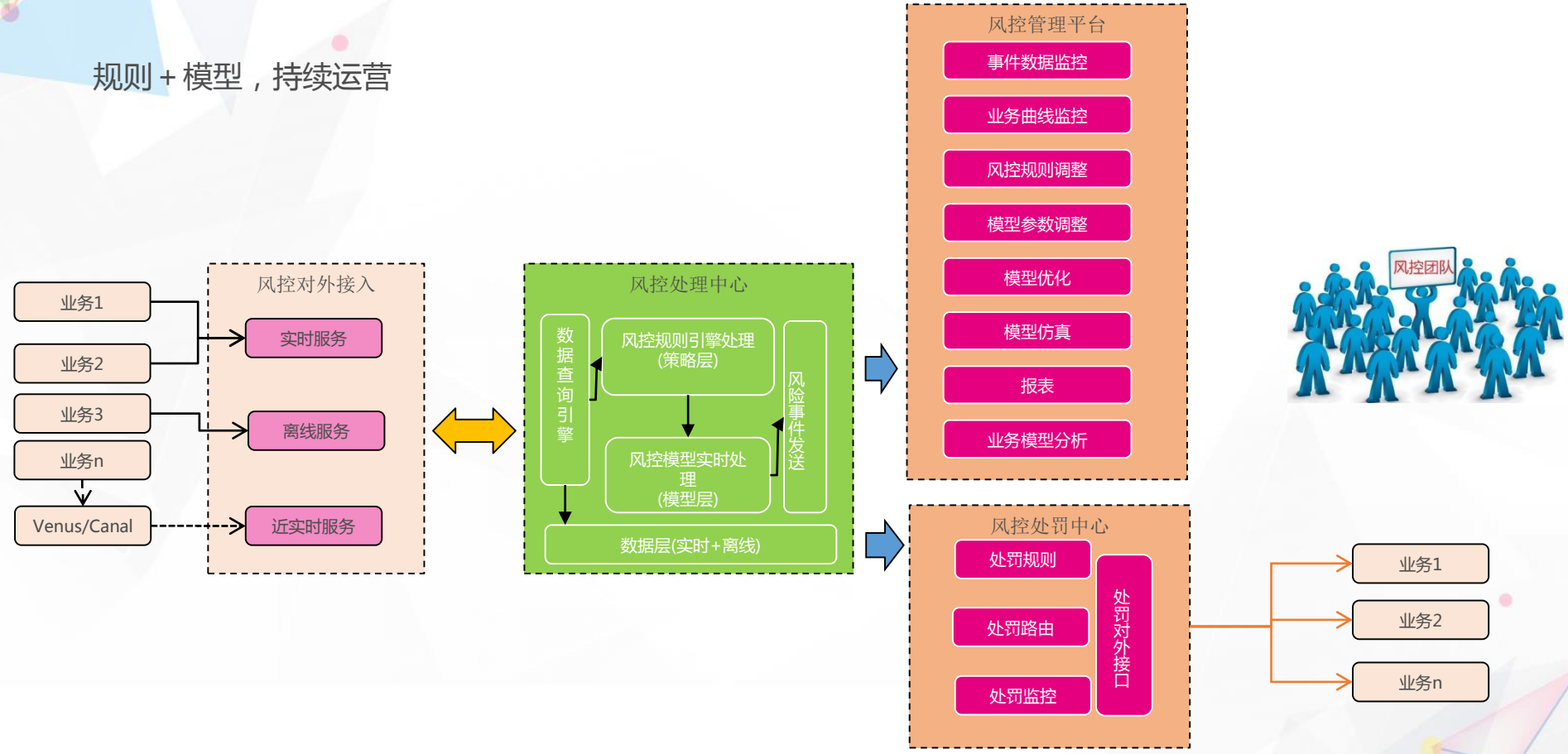


哥伦布 – 风控精度

- **评分卡，决策表**
  - 单维度，易误伤
  - 多维度，分权重评分
- **安全鉴白**
  - 从已经被黑产攻击的请求中找出正常用户的请求
- **数据更新**
  - 及时更新安全数据库
- **惩罚降级**
  - 用二次确认代替拒绝策略
- **Dry Run**
  - 利用历史数据Dry Run
  - 利用线上数据，不处罚Dry Run

麦哲伦 – 业务承接

规则 + 模型，持续运营



麦哲伦 – 实时风控与业务联动

适合不可逆的一些操作，比如注册，登录，短信发送，支付

业务联动，二次验证手段：

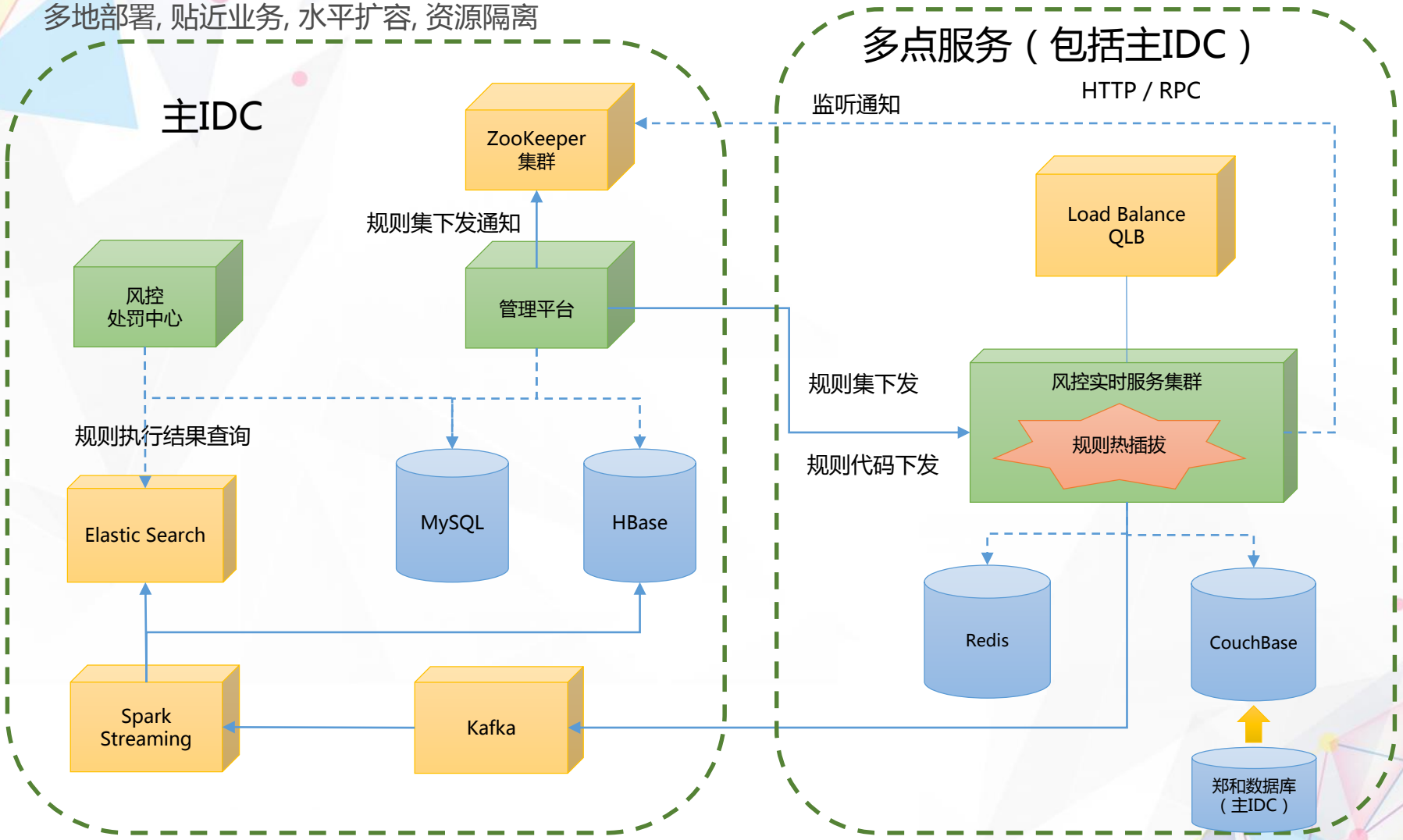
- 图文验证码
- 滑动验证码
- 短信验证码
- OTP
- 推送确认
- 信任设备确认
- 安全中心应用确认

用户体验

安全阈值

部署方案

多地部署, 贴近业务, 水平扩容, 资源隔离



风控依赖 - 设备指纹

如何证明你是你？

- 身份证
- DNA
- 血型
- 指纹
- 脸　　（整容）
- 身高　（长高）
- 知识　（进步）
- …

如何证明此设备是已认知的设备

- 设备ID
- IMEI号/ IDFA　（可能取不到）
- Android ID
- 机型
- 硬件信息
- SIM卡　　（换卡）
- 计算能力
- 软件信息　（安装卸载）
- …

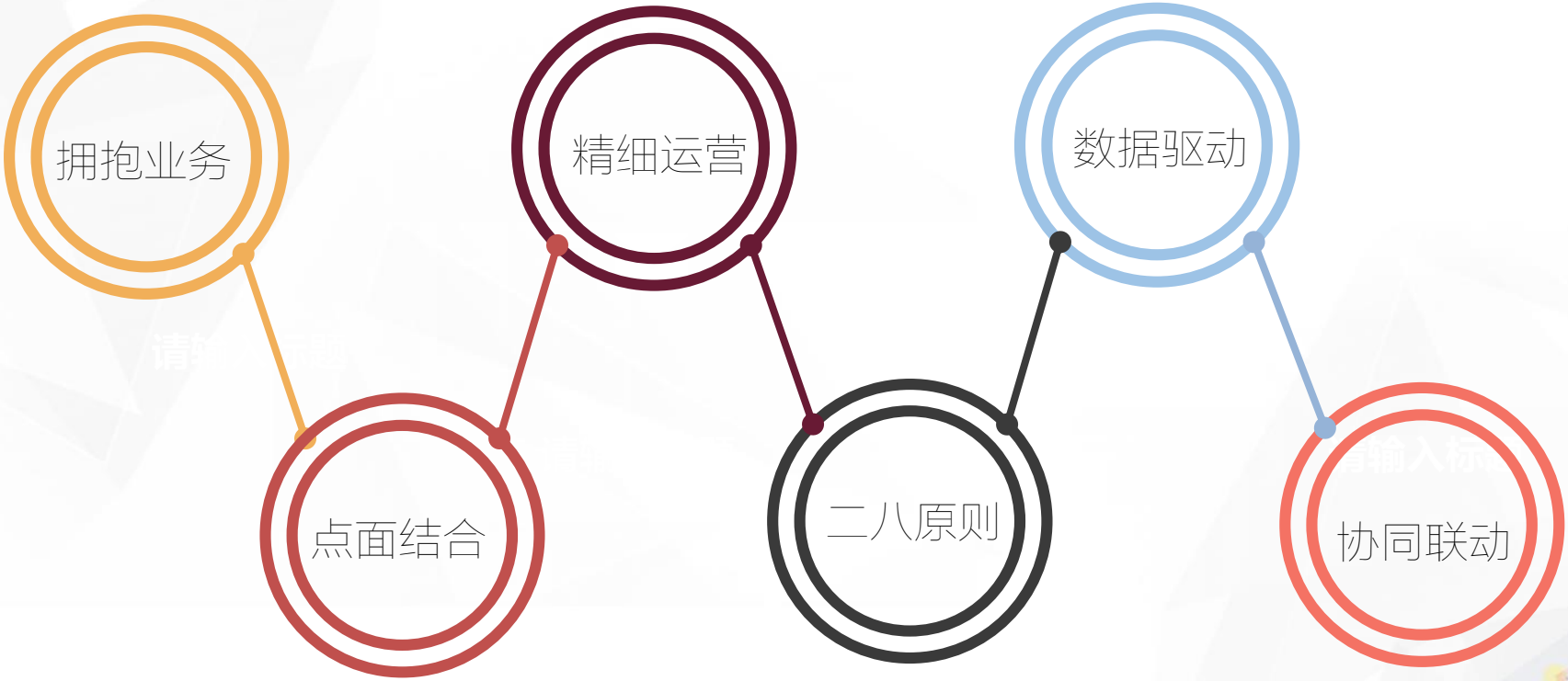
- 多维度建模识别，保证次要维度变更时的一致性
- 露出的指纹ID可变，后台唯一标识，提高复制门槛
- 请求带指纹ID和环境参数，做校验
- 识别非法请求，冒名请求

风控成果

帐号安全	虚假人气	社区	观影数据作弊	短信	办公安全
登录 80% 帐号检查 20%	长连接 挂站 8-55%	Feed 防广告 5%	VV统计 风云榜 5%	防刷 防骚扰 30%	弱密码 社工密码 校验 改密码 校验

智能安全防护体系: 不只是风险控制

总结



71SRC - 爱奇艺安全应急响应中心

https://security.iqiyi.com

THANKS

SequeMedia 盛拓传媒 | ITT168.com 专注导购16年 | ChinaUnix.net | ITPUB www.itpub.net