

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**

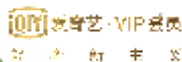


品牌升级日

- 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
量级



爱奇艺VIP会员
抢先看

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

追剧不等待
海量随心看
视听更震撼

2016年4月15日
《太阳的后裔》独家上线爱奇艺
VIP会员畅享零时差观剧体验

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

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

薅羊毛

恶意注册

撞库

会员分享

视频

刷播次

盗链

广告屏蔽

社交

黄色图文

恶意广告

诈骗

直播

刷人气

恶意广告
图文

人身攻击

电商

薅羊毛

恶意下单

订单欺诈

支付

盗号盗卡

洗钱

恶意提现

其他

短信轰炸

钓鱼邮件

内部帐号
爆破

- 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

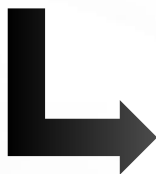
低技术门槛
低法律风险
高黑色收益



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

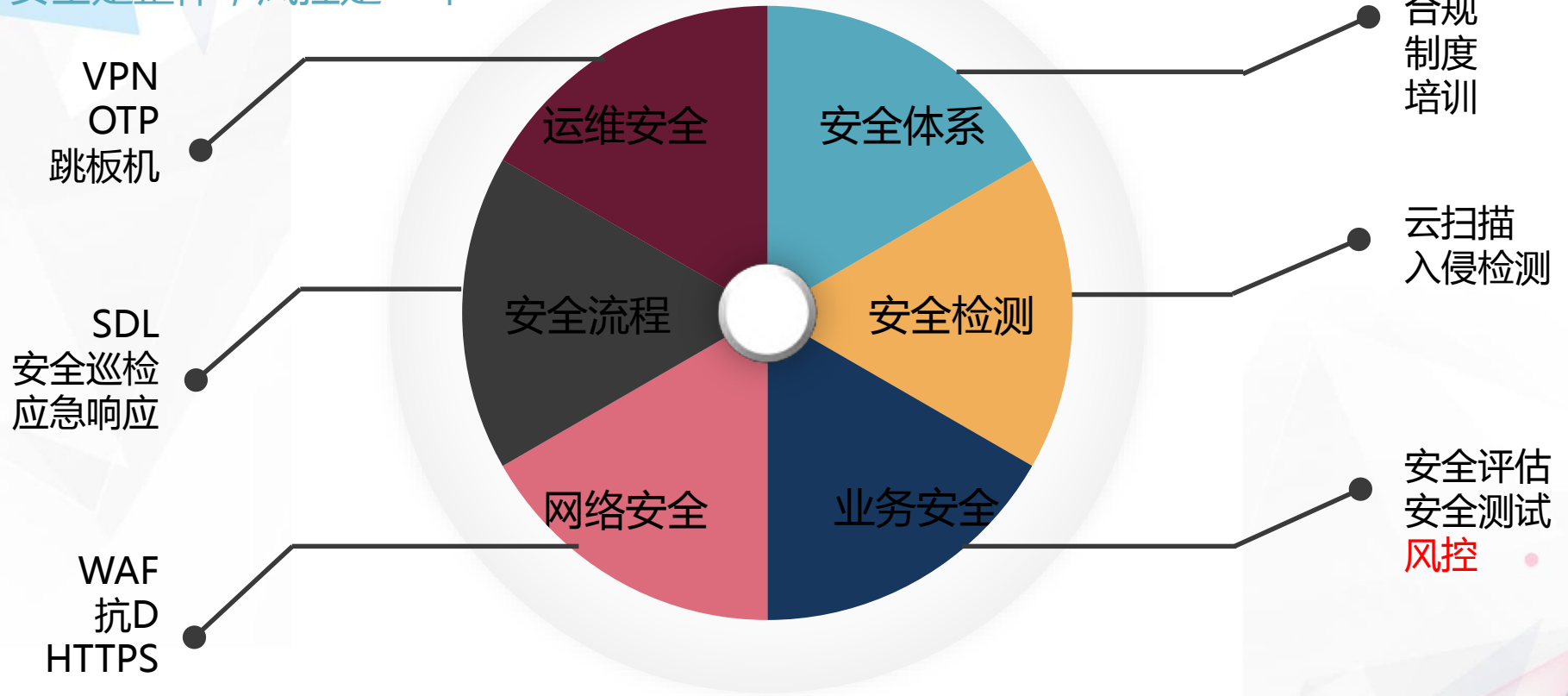


极端情况下妨碍业务

- 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

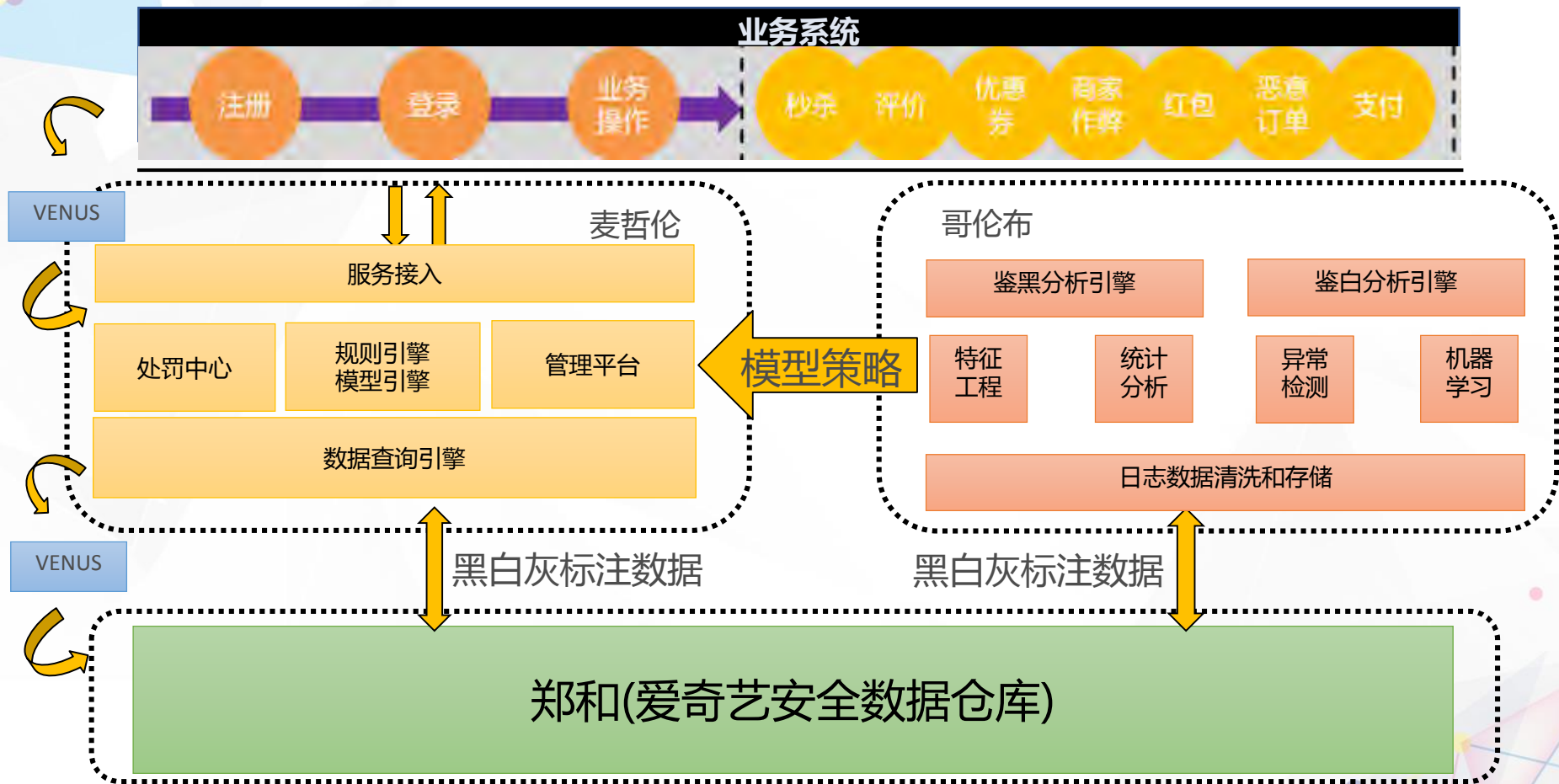
延迟可控

数据驱动

前后端结合

服务质量保证

爱奇艺风控系统



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

219,241,281

当前安全威胁数据总量

651,397,035

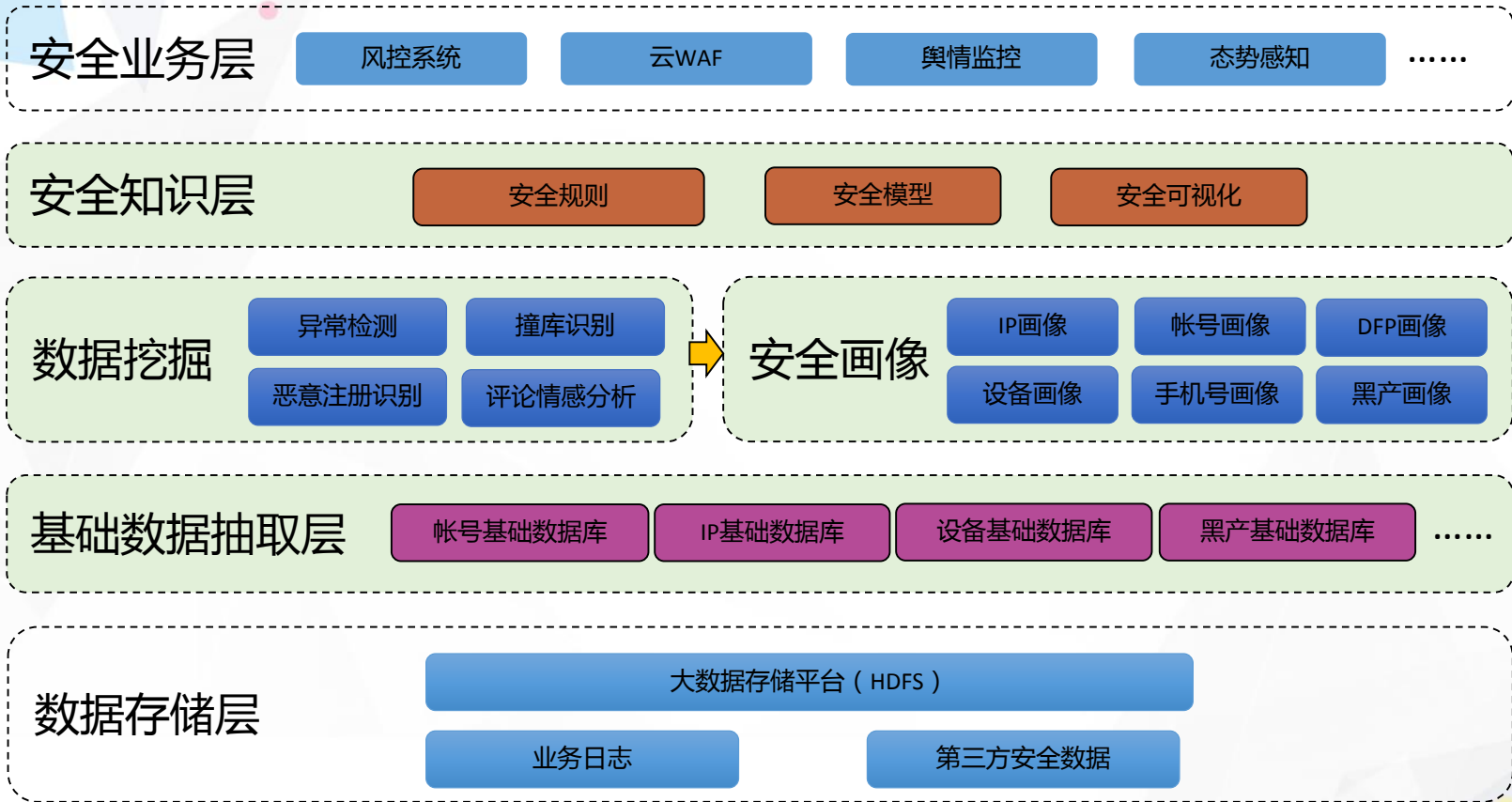
当前社工库数据总量

1,397,035

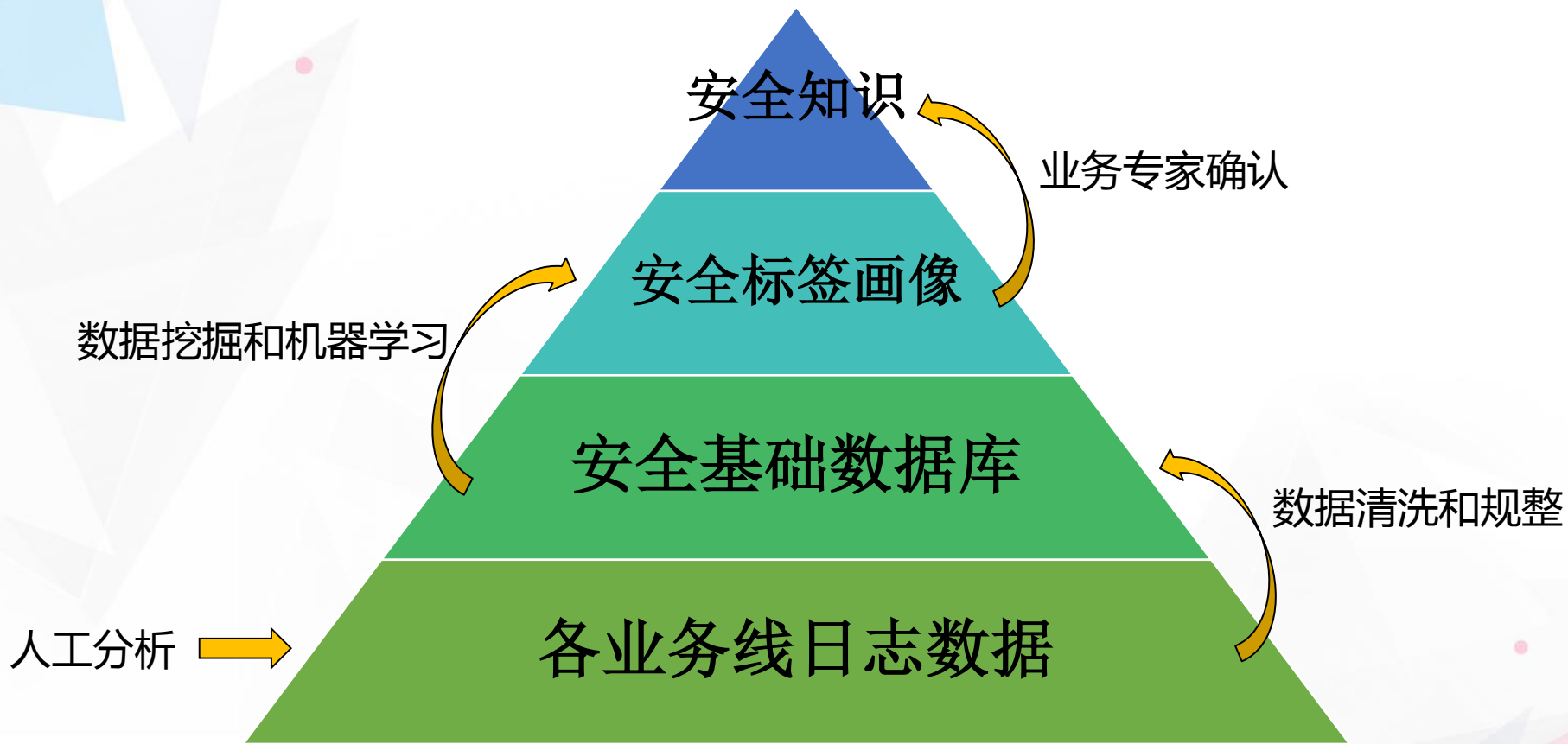
本周数据更新总量

持续增加...

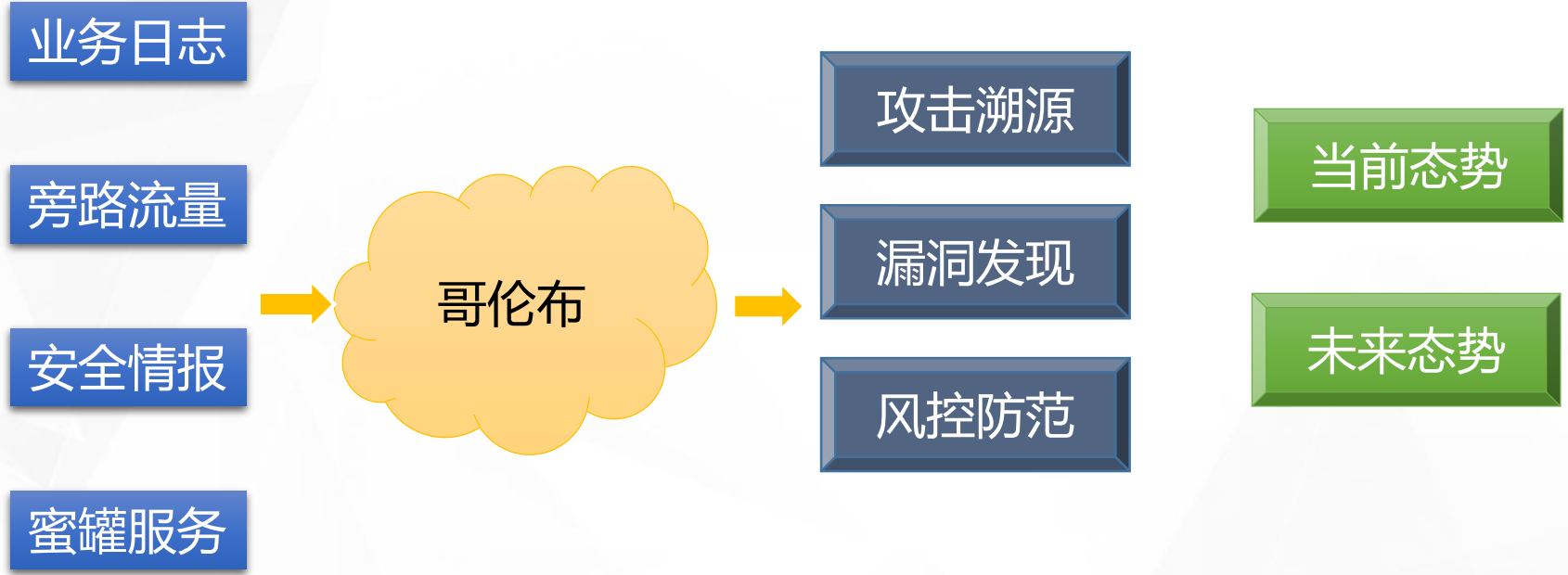
哥伦布 - 大数据层



哥伦布 - 数据提炼过程



哥伦布-态势感知

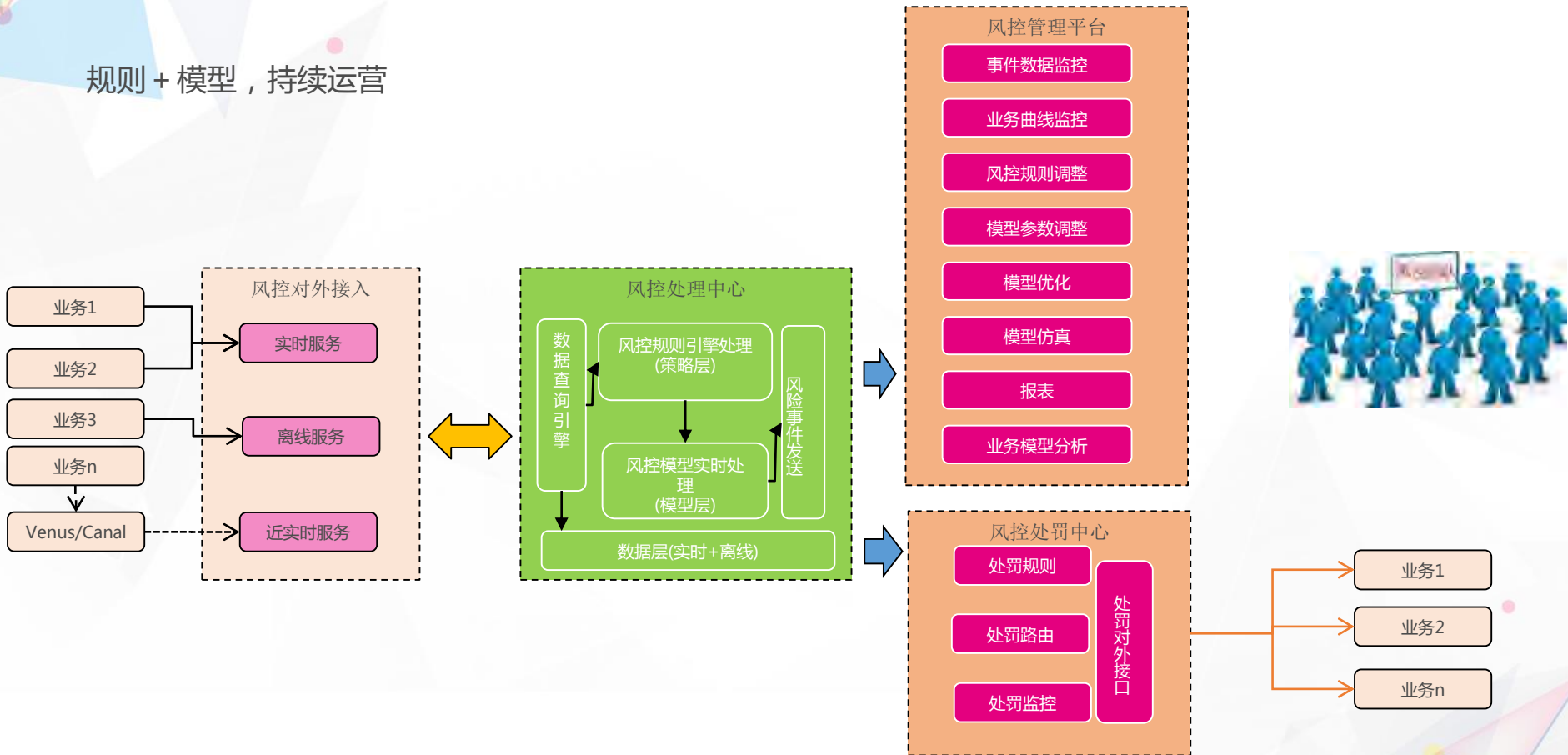


哥伦布 - 风控精度

- **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



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

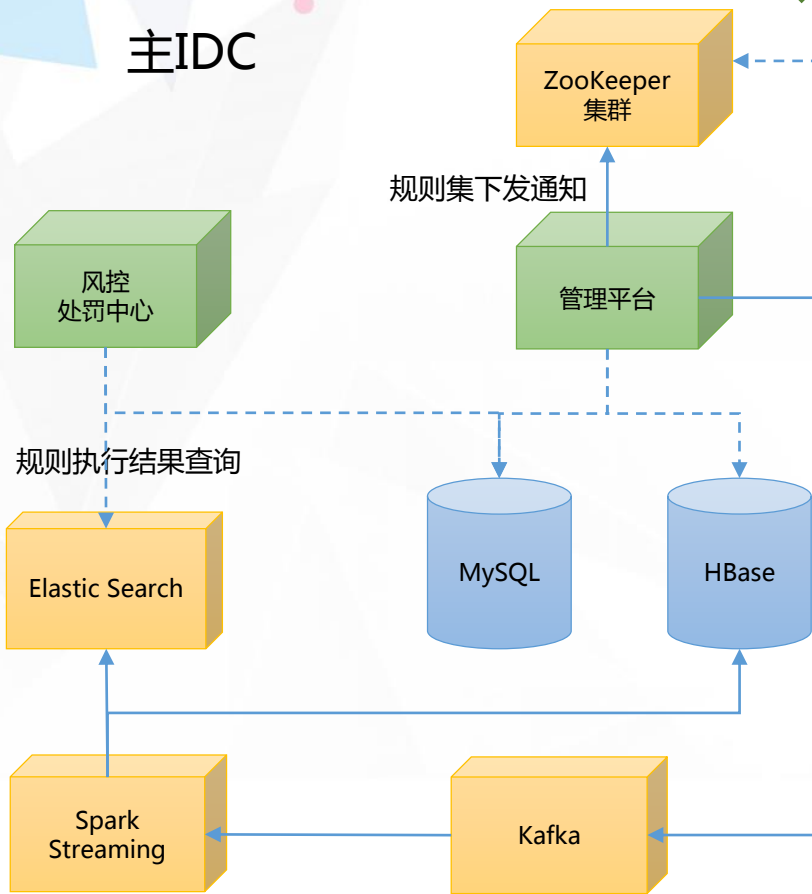


安全阈值

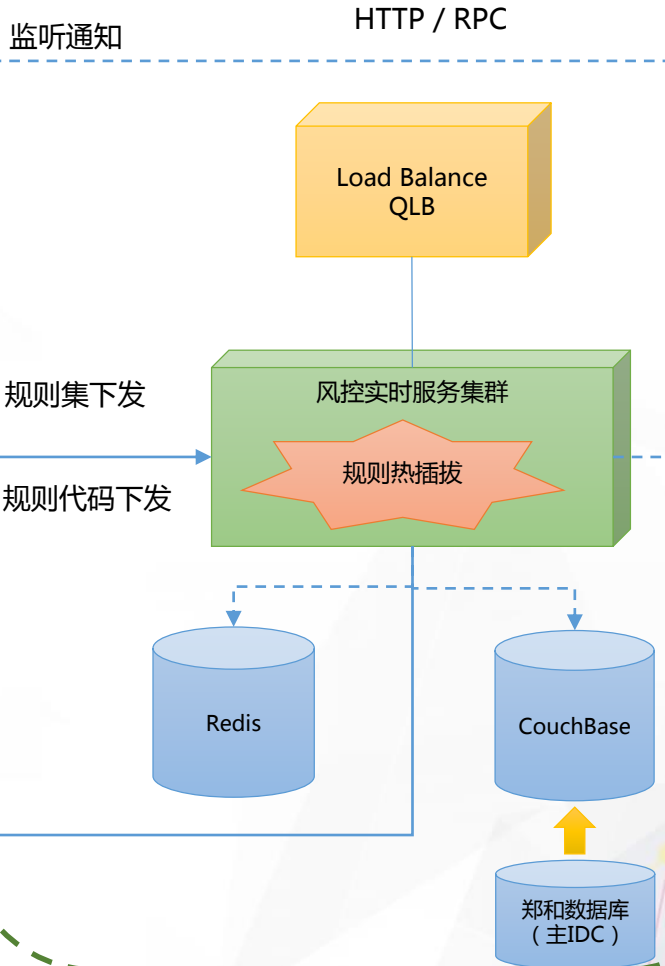
部署方案

多地部署, 贴近业务, 水平扩容, 资源隔离

主IDC



多点服务 (包括主IDC)



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

短期规划

- 完善安全画像
- 提升模型的精确度和召回率
- 提升跨业务的保护能力

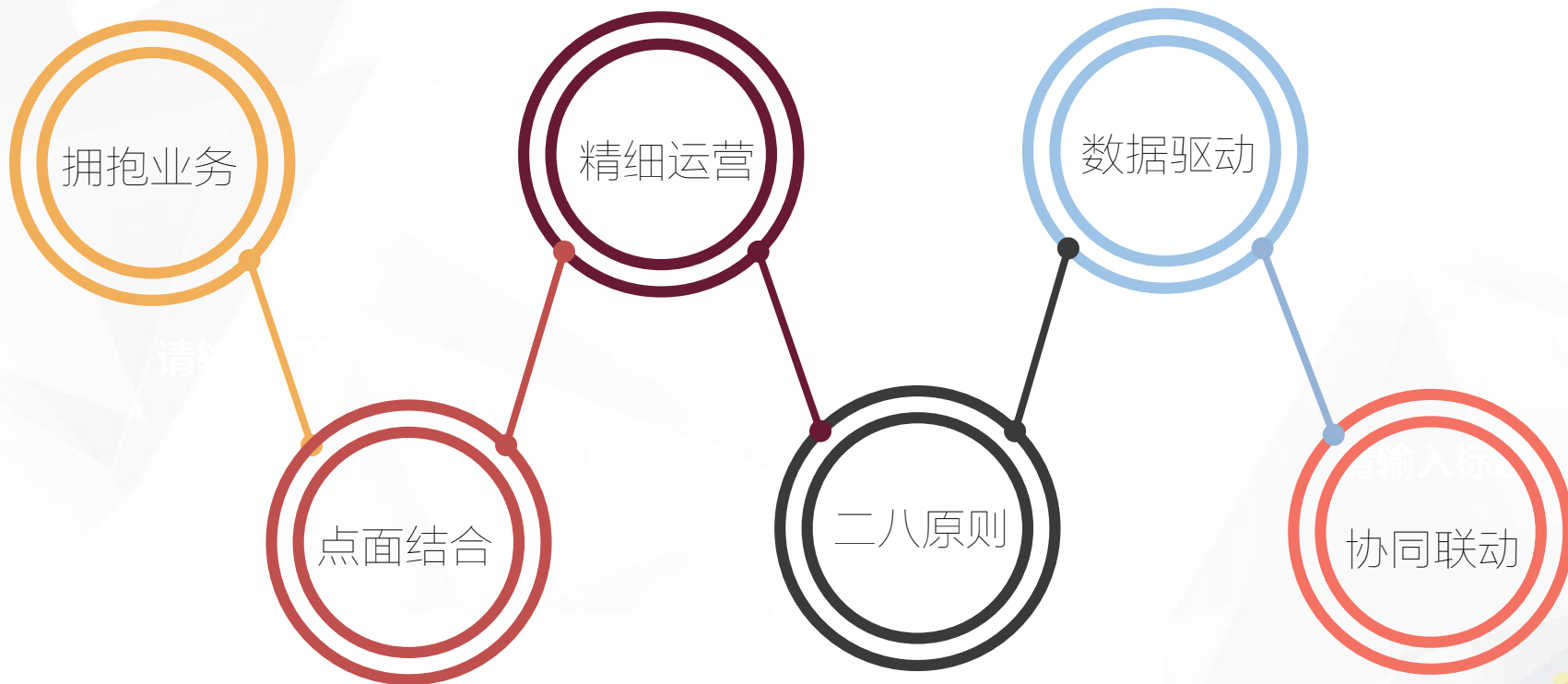
中期规划

- 建立安全数据流转机制
- 模型在线训练及反馈, 精细运营
- 打造深度学习框架, 神经网络模型

长远期望

- 构建全站安全大脑
- 打造纵深安全防护体系

总结



71SRC - 爱奇艺安全应急响应中心

<https://security.iqiyi.com>



THANKS

SequeMedia
盛拓传媒

IT168.com
1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025

ChinaUnix

ITPUB
www.itpub.net