71SRC
爱奇艺安全应急响应中心

爱奇艺业务安全风控体系的建设实践

爱奇艺 云平台科学家 卢明樊

做一家以科技创新为驱动的伟大的娱乐公司

爱奇艺，中国娱乐行业领导品牌。

2010年4月22日正式上线，秉承“悦享品质”的品牌口号，积极推动产品、技术、内容、营销等全方位创新，为用户提供丰富、高清、流畅的专业视频体验，致力于让人们平等、便捷地获得更多、更好的视频。

目前，爱奇艺已成功构建了包含电商、游戏、移动直播、漫画、阅读、电影票等业务在内、连接人与服务的视频商业生态，引领视频网站商业模式的多元化发展。

爱奇艺会员数在2016年6月起就超过2000万，开启全民VIP时代

做一家以科技创新为驱动的伟大的娱乐公司

爱奇艺，以科技创新为驱动力。

云计算平台、HCDN技术、大数据智能分析平台、视频综合服务平台以及视频搜索引擎技术持续突破

构建了全球规模最大的混合视频网络HCDN,CDN网络节点总数逾500个,总服务带宽30Tbps

技术平台具备了 专业化, 规模化 和标准化的特点

行业数据领跑 位于行业领先地位

2017

爱奇艺APP移动端 综合服务浏览分析

数据来源：艾瑞 MUT，2017年3月

日均独立设备数NO.1

月独立设备数NO.1

月度总有效使用时间NO.1

爱奇艺PC端 综合服务浏览分析

数据来源：艾瑞 IUT，2017年3月

日均覆盖人数NO.1

月度覆盖人数NO.1

月度总有效浏览时间NO.1

2016年热门应用（非游戏类）

全球iOS与Google Play综合收入排名

爱奇艺位列**全球收入排名第七**

国内APP表现最佳

TV端数据

数据来源：爱奇艺龙源数据库，2017年2月

月度TV端UV覆盖超

5,500万+

日均TV端VV超

3.1亿+

普遍业务风险行业的共同的问题

会员

撞库盗号
帐号分享
批量注册

视频

盗播盗看
广告屏蔽
刷量作弊

活动

薅羊毛

直播

挂站人气
恶意图文

电商

恶意下单
订单欺诈

支付

盗号盗卡
洗钱
恶意下单
恶意提现

其他

钓鱼邮件
恶意爆破
短信轰炸

解决方案 安全+风控

2017

元安全
合规 + 制度 +培训 + 手册

安全开发
SDL + 扫描 + 渗透 + 巡检 + 响应

安全运维
VPN + OTP + 堡垒机

流量安全
WAF + 抗D + HTTPS

业务安全
风险评估 + 风险控制

问题多多

01 各自为战

各业务方多以安全事件驱动，多数仅做事前单点防御，**经验数据无法共享**

单点防御容易**被黑产各个击破**，无法做到跨业务跨团队的联防联控

低水平重复建设，平台资源浪费

02 拍脑袋"规则"

大量的风控规则是**专家决策为主**,阈值基本拍脑袋而定;

没有引入数据分析或者机器学习等能力，对事件本质缺乏足够认识及数据支撑，

造成正常用户误杀，损伤用户体验，导致用户流失

03 反应过慢

不能快速识别攻击变化进行调整,无法进行积极对抗

业务代码耦合,依赖业务开发，测试和上线,占用业务排期

某些前置/内置规则容易**成为业务关键路径**，对业务稳定性造成影响

04 手段单一

可用特征维度不多，**严重依赖于IP**，公共出口误杀严重,引发投诉

以限频，限流，黑白名单，图文验证为主，黑白名单难以维护，无生命周期

目标风控系统 用云服务来解决业务的问题

2017

数据驱动，智能对抗

全站全网数据支撑，基于数据进行决策

利用机器学习实现智能异常特征发现

联防联控

各业务联合，在模型,规则,数据等方

面进行共享，联合布控协同防御

策略灵活，有效对抗

独立服务，快速迭代

支持业务的风险多样运营需求

模型,,规则，策略快速实施,，快速反应

延迟可控，低耦合可降级

在实时风控场景下，快速决策，不能明显增加

业务延迟，自身有问题情况下，不能影响业务

维度和拦截手段多样

不依赖单一维度和单一行为

云和端结合，多种拦截手段应对

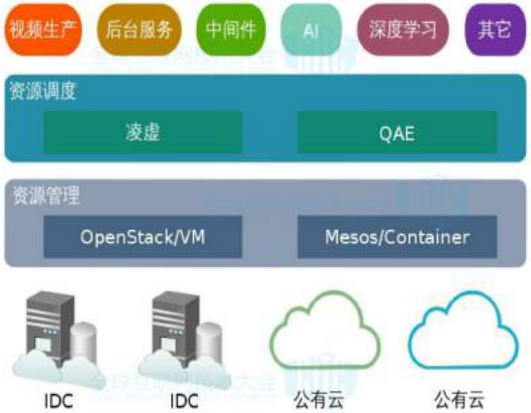
快速实现，高效部署

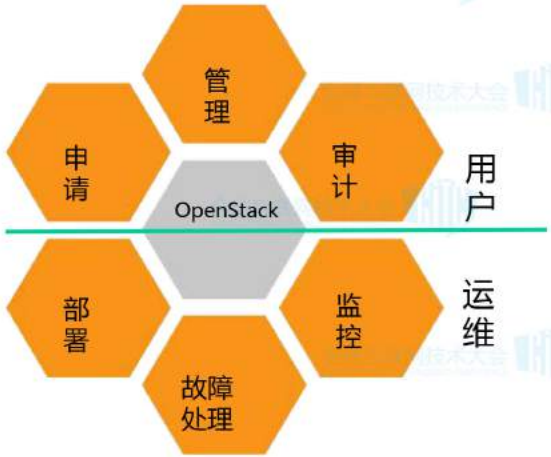
能够快速完成架构. 实现和持续迭代

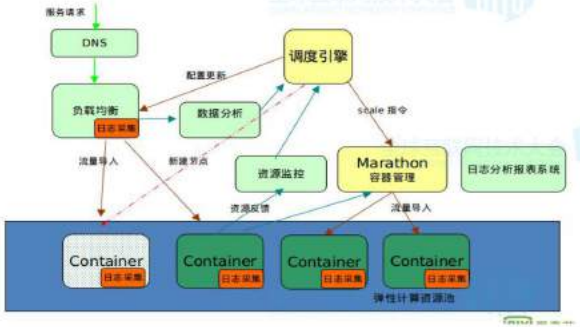
能够面向私有云的复杂拓扑，快速部署

爱奇艺混合云 弹性资源,快速部署

2017

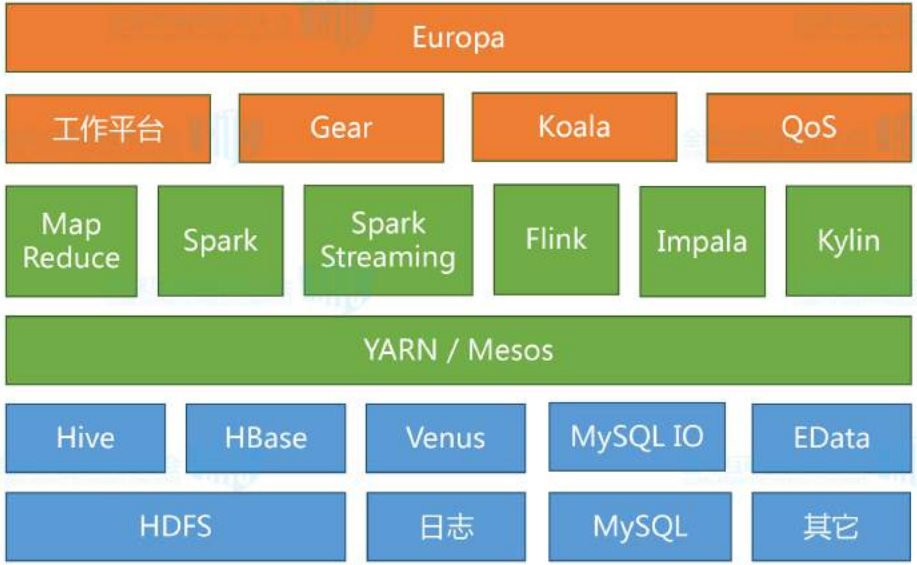






- 支持混合云架构：私有云以及公有云
- 两种计算资源：虚机和容器
- 支撑公司大部分业务
- 虚机云平台(灵虚)
  - 中国开放云联盟（COSCL）成员
  - 基于OpenStack构建高性能云主机
  - 3000+台服务器提供了接近20000+台虚机
- 容器云平台(QAE)
  - 一次部署到处运行
  - 峰值在线容器数约 1.5 万
  - 容器启动数量一周峰值超过 500 万
  - 集群 CPU 利用率月平均值超过 25%
  - 支持 GPU 任务

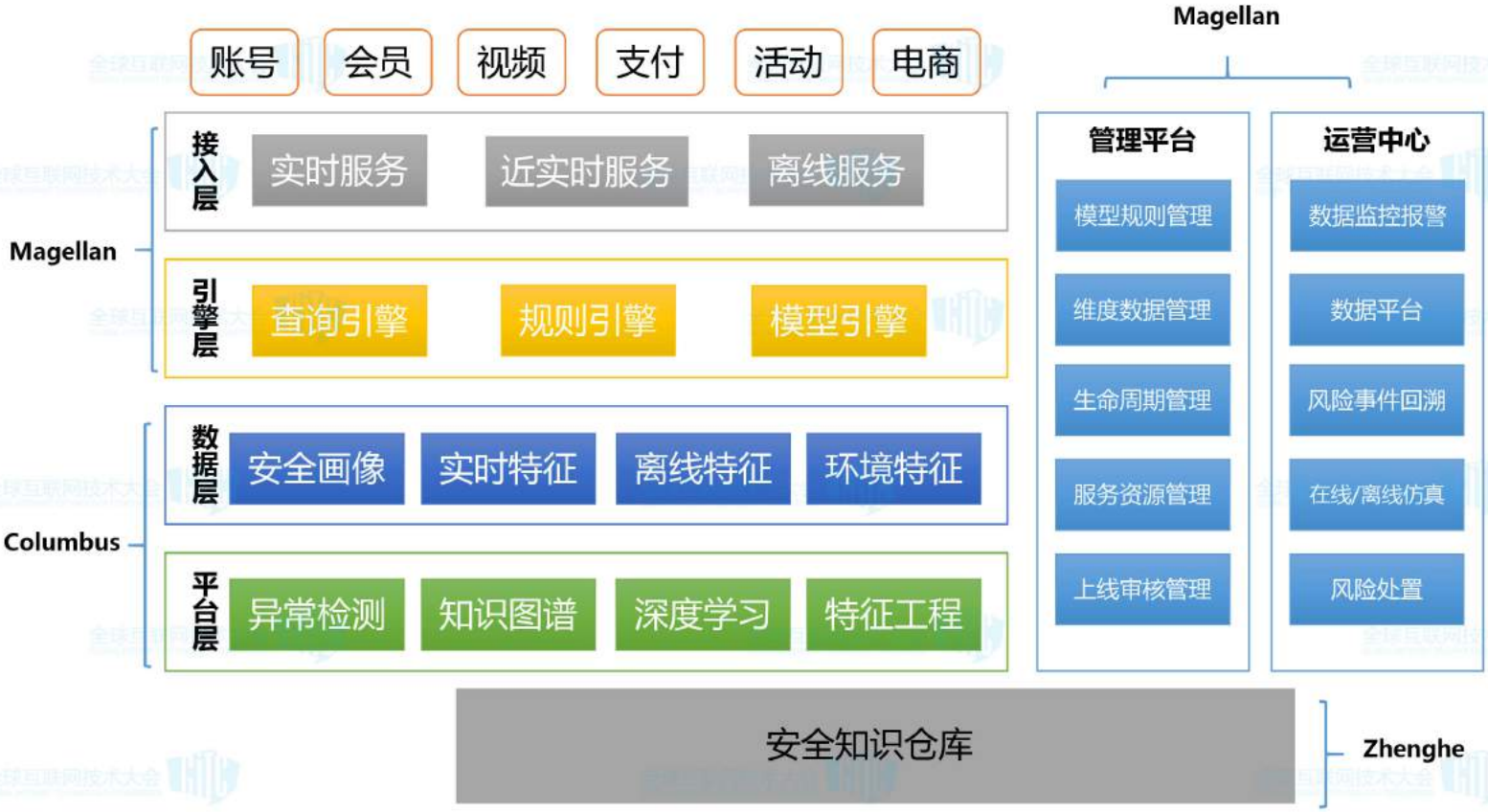
数据驱动



- OLAP查询慢
- 监控报警不够精准
- 运维成本高
- Crontab不易管理
- 日志不易管理、排障难
- 易用性不足、门槛高

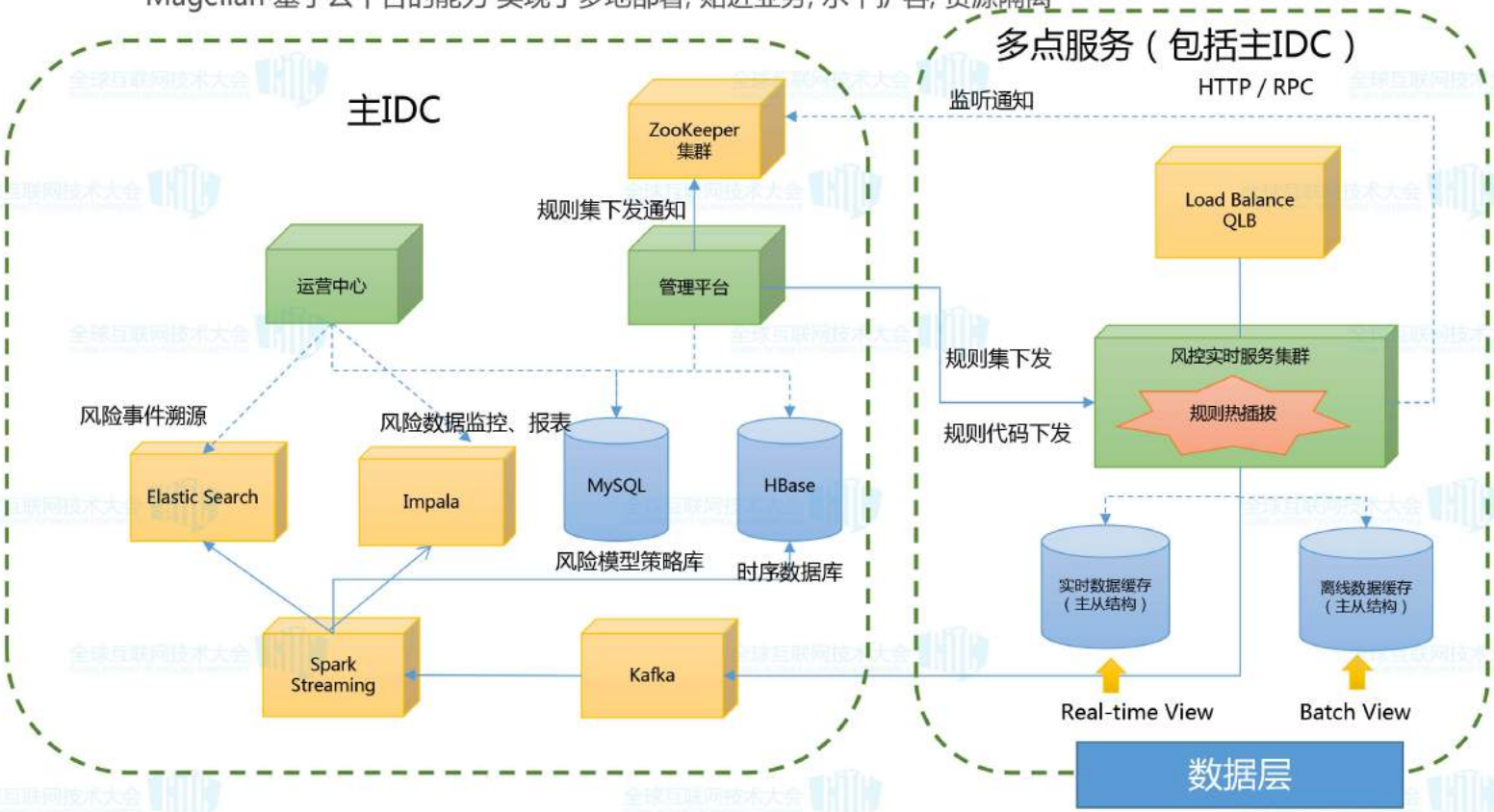
- Impala、Kylin
- Hadoop QoS
- Koala自动化运维系统
- Gear工作流管理系统
- Venus 日志收集计算平台
- Europa 大数据开发平台

风控 - 架构


账号
会员
视频
支付
活动
电商
Magellan
接入层
实时服务
近实时服务
离线服务
引擎层
查询引擎
规则引擎
模型引擎
Magellan
数据层
安全画像
实时特征
离线特征
环境特征
平台层
异常检测
知识图谱
深度学习
特征工程
Columbus
Magellan
管理平台
模型规则管理
维度数据管理
生命周期管理
服务资源管理
上线审核管理
运营中心
数据监控报警
数据平台
风险事件回溯
在线/离线仿真
风险处置
安全知识仓库
Zhenghe

风控 - 部署

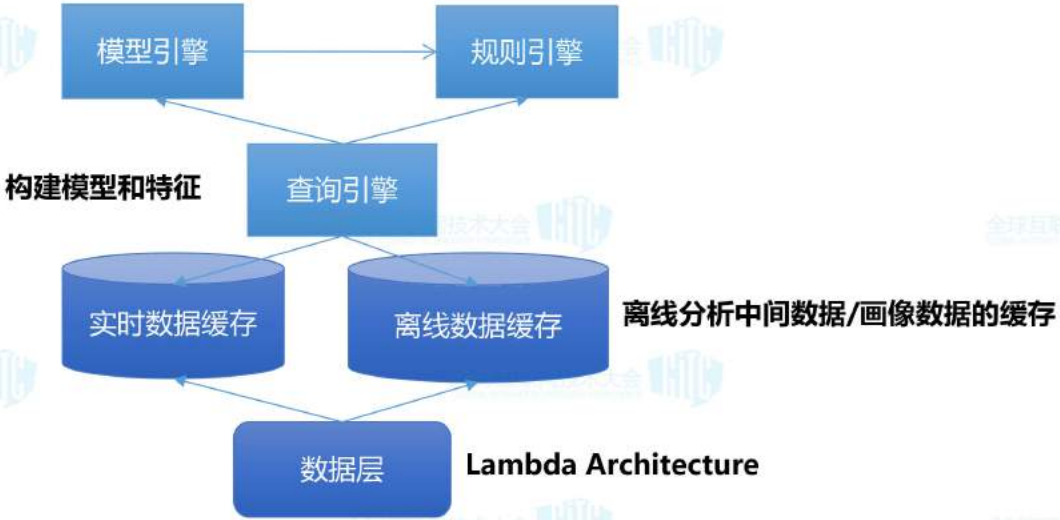
Magellan 基于云平台的能力 实现了多地部署, 贴近业务, 水平扩容, 资源隔离



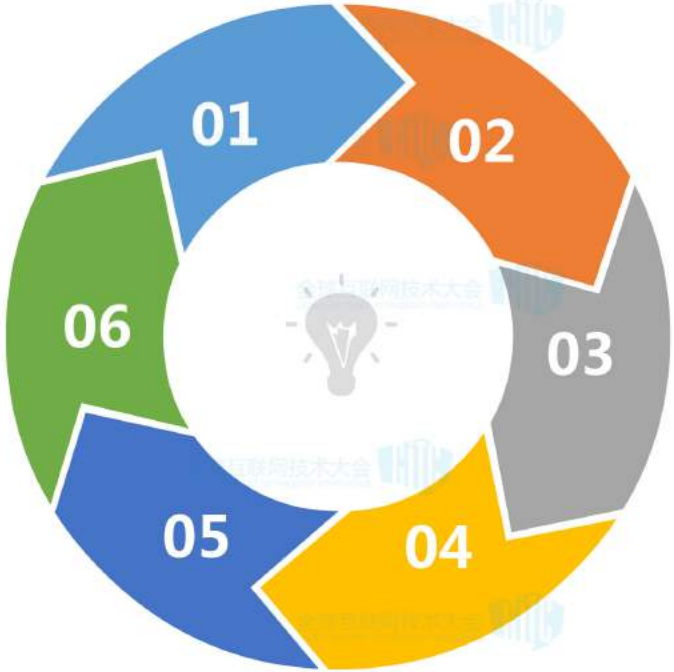
利用云平台能力高效构建和发布：**2.5*4个人月** 从零开始开发构建 上线服务

风控 - 引擎

- 查询引擎:
  - 负责进行实时+离线数据批量查询及聚合
  - 构建为参数/特征组合提供给规则引擎, 模型引擎
- 规则引擎:
  - 负责进行规则匹配
  - 支持自定义执行策略如: 命中退出, 全部执行, 条件退出等
  - 支持多种规则类型, 如:评分卡, 决策树, 决策表, 普通规则等
- 模型引擎: 负责进行特征处理及算法执行



风控 - 运营 满足业务方的运营需求



风控服务

业务风险评估,接入登记,根据场景实施初始规则和模型, 逐步迭代

审批上线

规则模型变更及时通知业务方, 风控运营团队, 相关业务方, 相关负责人确认审批上线

离线/在线仿真

基于案例库中的正/反例, 结合仿真环境进行模型/策略仿真. 利用数据平台进行贡献度, 线上效果比对等分析.

事件查询/处置/回溯

查询被识别为风险案例的上下文, 特征, 模型结果, 数据标注等信息. 供运营进行案例分析及后续仿真

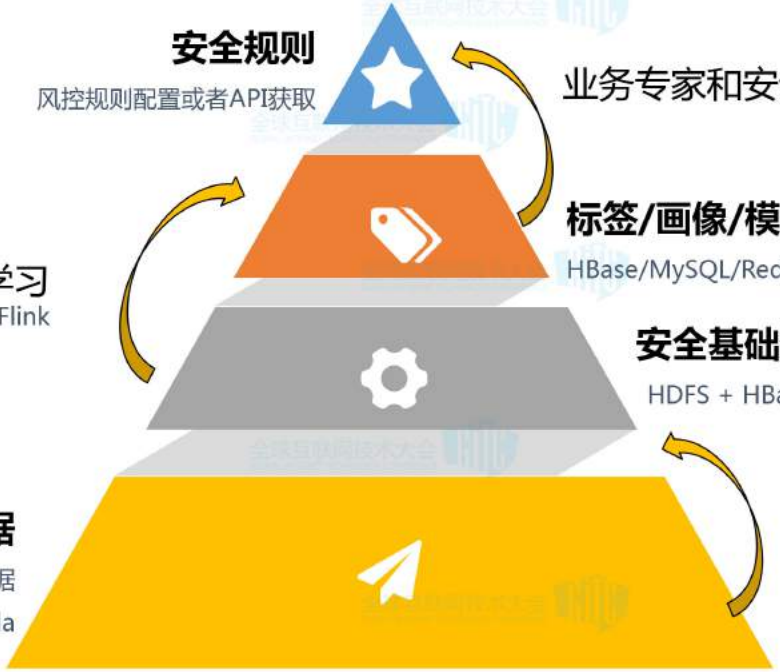
事件监控和报警

业务/风险数据监控看板, 智能报警

adhoc/Daily数据分析

Adhoc/Daily数据报表, 风险数据分析, 模型/规则贡献度分析, 仿真效果分析等

爱奇艺安全数据分析和机器学习引擎 - **Columbus >>>> 让风控更加智能**



安全规则

风控规则配置或者API获取

业务专家和安全专家确认

标签/画像/模型

HBase/MySQL/Redis + CouchBase(缓存)

数据分析和机器学习

Spark SQL/Streaming/Spark Millib/Flink

安全基础数据

HDFS + HBase

业务数据

从业务方获取的海量近实时或者离线数据

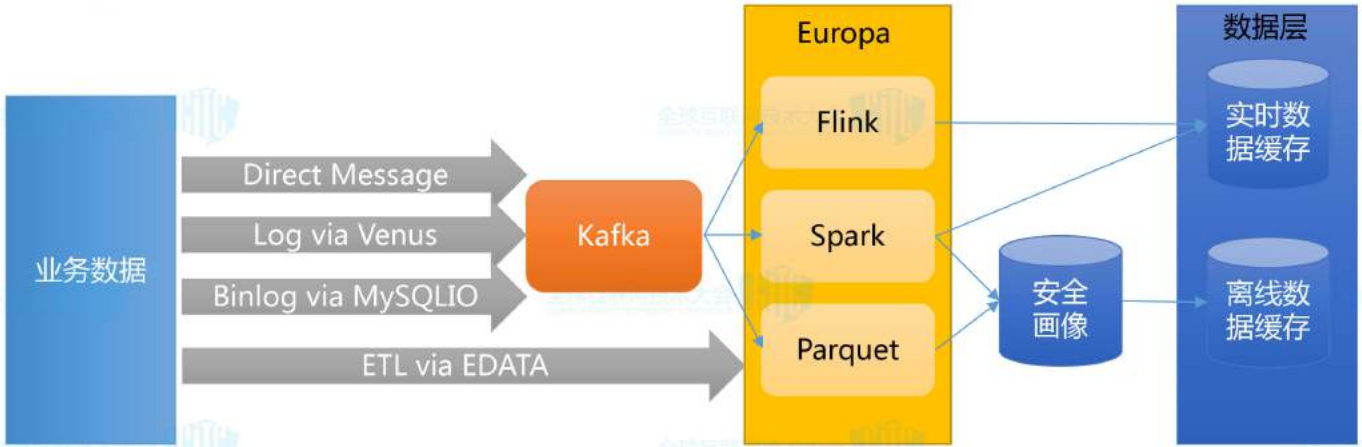
venus+mysqlio+impala

数据清洗和特征工程

Spark SQL/Streaming/Flink/ESQL

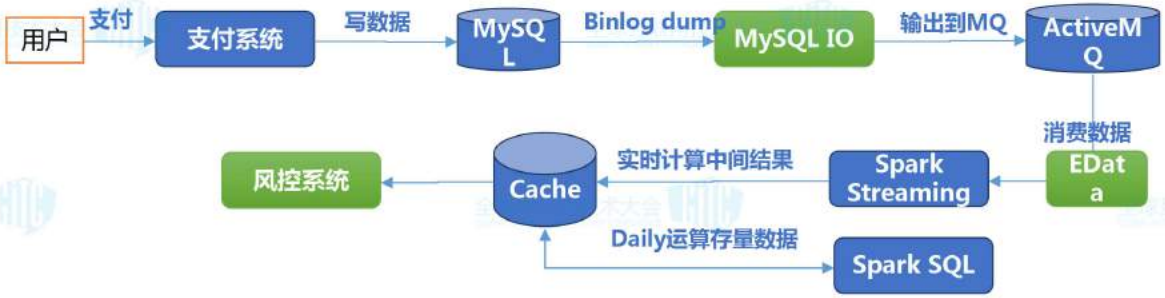
Columbus的多渠道业务数据采集和处理

- 实时数据: 基于Apache Flink构建: 图特征工程, 多维频次特征, 多数据流Complex Event Processing, 毫秒级延时
- 近实时数据: 基于Apache Spark构建: 异常检测, 流式特征工程, 秒级延时
- 离线数据: 基于Apache Spark, Impala/Hive构建: 安全画像, 用户画像, 全业务数据, 小时/天级延时



支付表监听

- 需要实时获取业务方数据变化
- 支付系统存在已久，不便于进行相关数据的实时投递开发
- 结合实时与存量数据，进行事前/中/后风险决策



以支付表监听举例，风控需要实时获取用户的当天支付数据，提现数据等，用于风险决策

安全画像

Columbus的安全画像 - 对全站业务数据分析和提炼以后, 形成海量的多维度标签刻画

>>> 为风控的每一次处理丰富上下文场景和实体特征

维度主题 用户, IP, 手机号, 设备等9大维度主题

标签总数 超过637种

数据总数 19亿以上

服务能力 HBASE+ Couchbase+API

安全知识仓库(zhenghe)

Zhenghe系统是安全云的包括威胁情报在内的基础安全数据集

- 全网安全数据监测和收集，包括 自采，共享和第三方采购
- 对业务安全而言重点关注 - IP信誉分, IP分类识别, 公共出口识别, 代理IP识别, 手机号信誉分, 虚假小号识别等
- 威胁标记类型210个，涵盖13个维度，总共记录数约16亿条

IP信誉分: 融合爱奇艺内部多个系统的数据，参考第三方数据，综合衡量一个IP的长期行为，得到一个-100到100的信誉分

基于行为的对比

安全规则具有保密性，无法详细列举

场景

爬虫　　活动、广告、积分防刷　　人机识别

Now　目前已经有登陆、活动、奇秀等业务使用

风控 - 平台

2017

Columbus的核心是异常检测，主要是通过自研的方式实现各种异常检测的功能。在该核心功能的基础上，构建了整个哥伦布系统的上层架构，实现面向风控Magellan服务的能力

预处理工具

低级特征工程库: 对数特征,归一化特征,主成份特征 ...

高级特征工程库: FPGrowth关联特征,k-means距离特征, 多维自动关联 ...

低级异常检测算法库: 多种分布模型, 单维度异常检测 ...

高级的异常检测算法库: 基于FPGrowth关联的多维异常检测 ...

流式异常检测: 基于FPGrowth关联流式, 基于CEP...

基于时间序列的异常检测: 基于基线曲线预测, 基于深度学习时间序列

自动化数据解析,存储和导入等工具

全端落地

全端覆盖

Android/IOS Phone

Android/IOS TV

PC/MAC/WEB/H5

多维签发

多维设备信息

无单维度决断

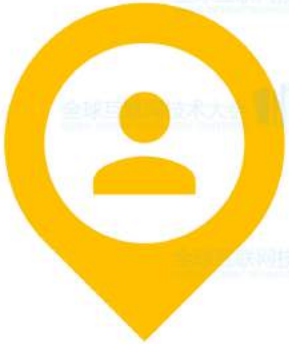
稳定与碰撞平衡

云端分析

海量数据分析

联合安全画像

...



伪造检测

伪造型号

伪造维度

...

验证手段 不只是拒绝

图文验证码

传统的复杂图文验证码

滑动验证码

基于滑动的人机行为识别进行验证

上下行短信验证

发送下行或者上行短信进行验证

基于信任设备的验证

信任设备可以为其他端进行授权和验证

基于安全盾APP的验证

安装爱奇艺安全盾APP可以为其他应用进行 动态口令(OTP), 推送一键确认, 扫码确认

其他: 暂时放行+事后处置, 降级体验或者权益, A业务标识+B业务拦截 ...

风控 - 成果

01	业务覆盖	涵盖帐号, 会员, 活动, 支付, 播放反作弊, 社交, IT, 直播等重要业务
02	服务质量	日均请求量超24亿, 延时5ms以内, 无故障运行
03	柔性风控	平时重监控, 战时重对抗. 注重用户体验
04	核心亮点	事前, 事后纵深防御体系, 结合事中跨业务联防联控及实时流式异常检测,机器撞库接近100%抑制

风控 - 成果

2017

登录

风控量: 55亿

拦截率: 8% ~ 60%

短信爆破

风控量: 12亿

拦截率: 3% ~ 10%

会员鉴权

风控量: 74亿

拦截率: 0.03% ~2%

注册

风控量: 1亿

拦截率: 10% ~ 80%

VV防刷

风控量: 7205亿

拦截率: 6% ~ 10%

会员活动

风控量: 8941W

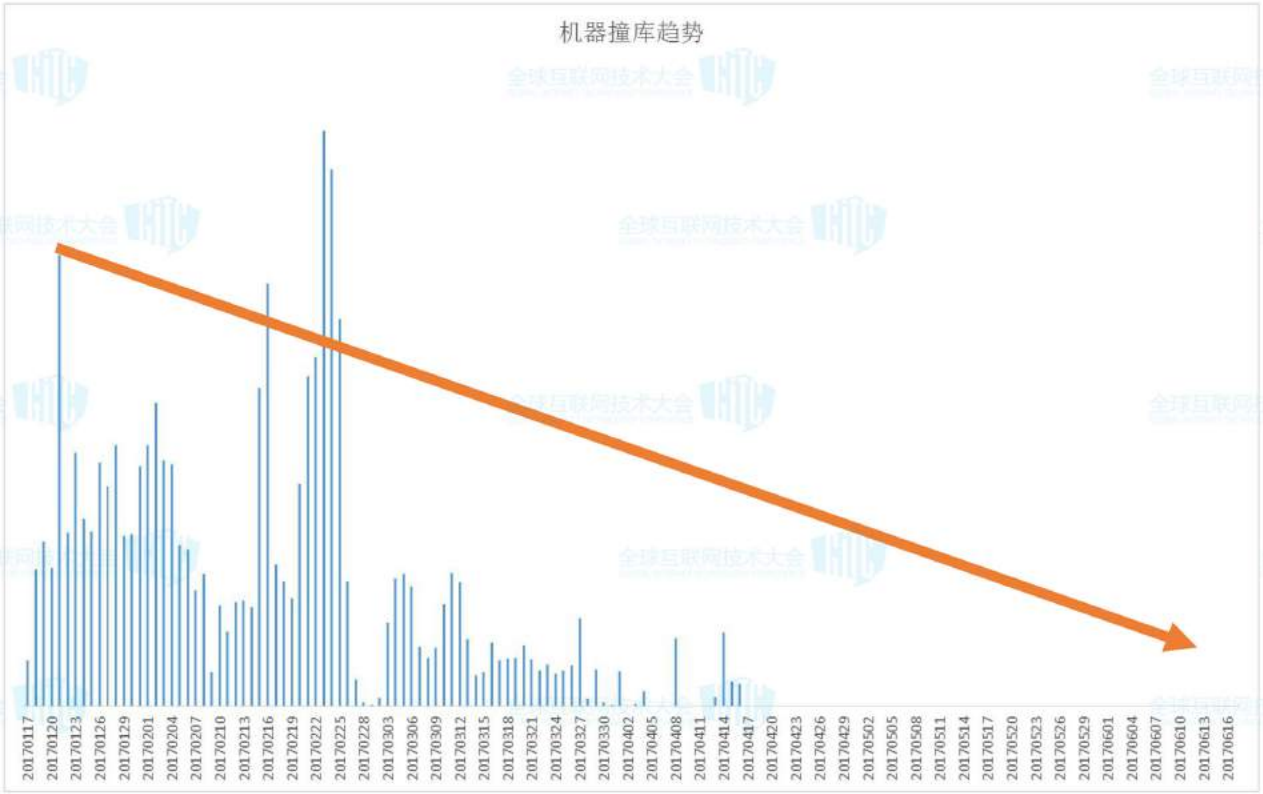
拦截率:5% ~ 10%

风控 - 成果

2017

一个主要撞库黑产公开宣称其今后不对爱奇艺撞库软件进行更新与维护了

该黑产的撞库软件目前对视频行业其他友商的撞库速率仍维持在每小时4-10万的量级



风控 - 心得


立足于云
服务为云
结合与端
安全只有拥抱业务才能体现价值
业务安全需要持续运营
拥抱业务
云端结合
精细运营
数据驱动
二八原则
协同联动
充分挖掘数据价值
优先解决主要风险
多点多层次跨业务防御

欢迎提交各类威胁情报和漏洞，共建安全

71SRC
爱奇艺安全应急响应中心

http://security.iqiyi.com

Q&A

欢迎加入 爱奇艺安全云
联系: lumingfan@qiyi.com