SACC 2016 第八届中国系统架构师大会
SYSTEM ARCHITECT CONFERENCE CHINA 2016
架构创新之路

专业化的风控服务平台的技术架构和实践

深圳瑞赛网络科技　张 平

2016.10.28

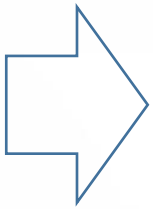
- 专业化风控服务平台的兴起和发展
- 专业化风控平台面对的需求和挑战
- 专业化风控平台的技术架构上的选择
- 客户选择专业化风控服务平台的注意事项

专业化风控服务平台的现状

以支付为始发的互联网金融服务的蓬勃发展：

- 电商，支付，
- P2P，小贷，
- 理财，基金，
- 消费金融，

互联网全面渗透到流通和消费的各个领域，对风险管理产生强烈的需求



传统互联网企业的专业化风控服务

代表： 蚂蚁金服，360安全，百度，阿里聚安全，腾讯安全

优点：信息和技术上的积累
弱点：业务重合，缺乏专注

创始企业的专业化风控服务

代表： 邦盛，通付盾，同盾，百融，深圳瑞赛网络

优点：灵活，专注
弱点：信息和技术积累不足

美国到2004年才兴起专业化的第三方反欺诈风控服务

兴起和发展的原由

宏观因素：

中国经济发展到一个阶段的产物：

经济发展的减缓，不断上涨的人供和租金迫使企业比以往任何时候都注重效率和成本，迫使企业将一部分专业 岗位的服务外包到专业的第三方服务商；反欺诈风险管理领域也不例外

行业因素：

有一定的行业准入门槛，从而避免初创企业的蜂拥而至

行业诉求：

✓ 共享反欺诈信息的需求：

专业化的第三方服务平台有能力收集，整理和共享跨单个企业的欺诈信息，提升整个社会反欺诈的效率

✓ 共享反欺诈策略和方式的需求

骗子的团伙性蜕变要求在应对上不同企业间必须协同才能收到良好的效果

专业化风控平台面对的需求：与内部平台的对比

企业内部风控服务

- ✓ 服务对象单一，一个或企业内多个服务对象
- ✓ 一套系统
- ✓ 数据收集，传输，整理，存储和使用上的限制少
- ✓ 对业务了解深入，可搭建针对性强的模型和规则

专业平台服务

- ✓ N多个服务对象
- ✓ 数据的多样化和必要的规范
- ✓ 模型和规则的多样和分层
- ✓ 商户技术水平参差不齐：系统建设技术能力 + 分析能力
- ✓ 敏感信息的保护和信息共享：各企业的诉求不同
- ✓ 数据保护和分隔

专业平台在技术上的挑战

- 数据收集的标准化：
  客户的系统千差万别，但允许过多的灵活变动，在数据存储和使用上会出现凌乱

- 变量的标准化：
  规则和模型要求变量遵守严格的规范，但不同企业，尤其是不同行业的企业，适用的变量很不同

- 规则库：
  适合N多家客户使用的规则库的搭建和管理

- 后台见面：
  适合N多家客户使用的案件处理后台见面和流程的搭建和管理

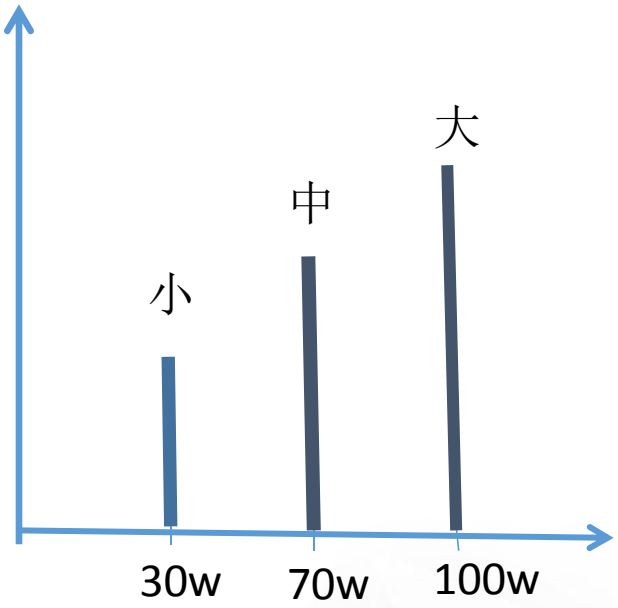
- 对分析师要求：
  分析师对不同行业的了解和理解，训练出切合实际的，行之有效的模型和规则

企业建立反欺诈团队的成本分析

- 人工成本（保守估计）：
  - 最小配置： 1个开发 + 1个分析师
  - 中团队配置： 2个开发 + 2个分析师 + 1个运维
  - 大团队配置： 4个开发 + 4个分析师 + 1个运维
- 系统

  一年5- 20万
- 租金

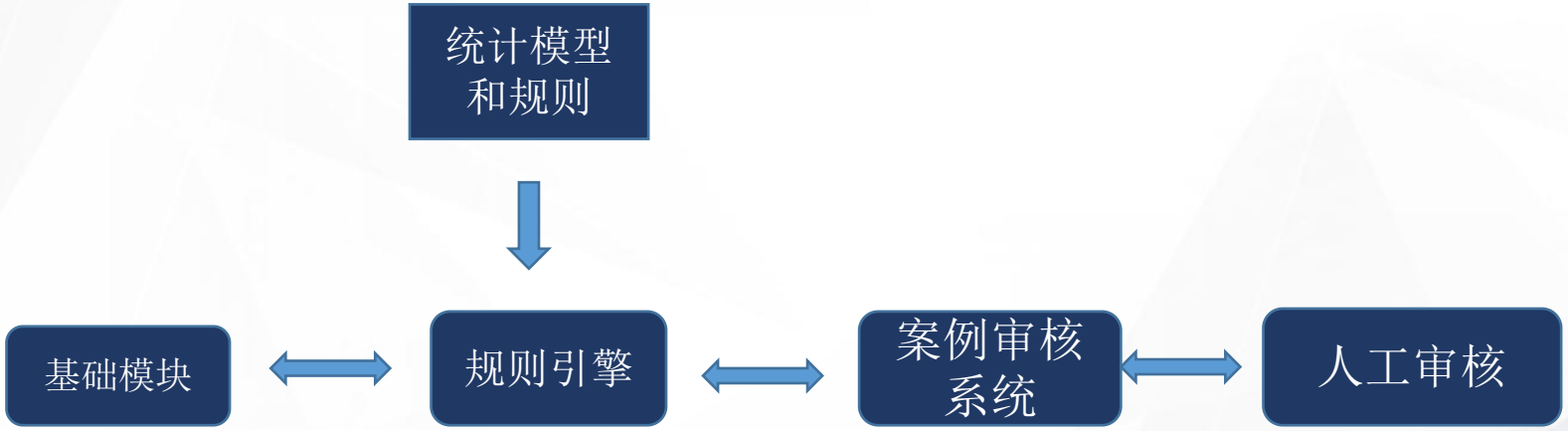
  一年5- 20万



- ✓ 成本：建立一个反欺诈小团队：年成本至少在30万以上；不到10个人的团队，一年的费用会超过100万
- ✓ 困难：不一定能找到合适的人才，来提供一流的反欺诈服务
- ✓ 耗时：搭建团队，系统到能提供满意的服务一般需要耗时至少半年
- ✓ 能力：即使建立起一个反欺诈的小团队，但能力上未必能达到公司发展所要求的水准，而欺诈分子往往首先攻击全产业链上的薄弱环节，从而成为首当其冲的受害者

反欺诈风险管理平台的设计理念和关键模块

- ✓ 系统基础功能齐全稳定，请求处理能力强大
- ✓ 规则引擎为核心，将规则引擎与规则分离，以及时建立和测试规则，对面临的风险迅速作出有效反应
- ✓ 建立顺畅的，资料齐全的，使用方便的调查见面，易学易用，以提高人工审核效率
- ✓ 培养训练有素的人工队伍



主要模块的内容和性能要求

基础模块

- 分布式架构
- 平移扩展
- 起始qps >5000
- 平均耗时100ms
- 最大不超200ms
- 连续性：99.99%
- 无单点
- 容灾：同城两机房，过渡到两地三中心
- 实时数据采集和处理

规则引擎

- 灵活配置规则
- 短时间内配置并
- 上线规则（分钟级）
- 规则测试和有效性观察和检测环境
- 规则管理系统
- 原始变量定义和规范
- 衍生变量定义和规范
- 规则和模型效果追踪

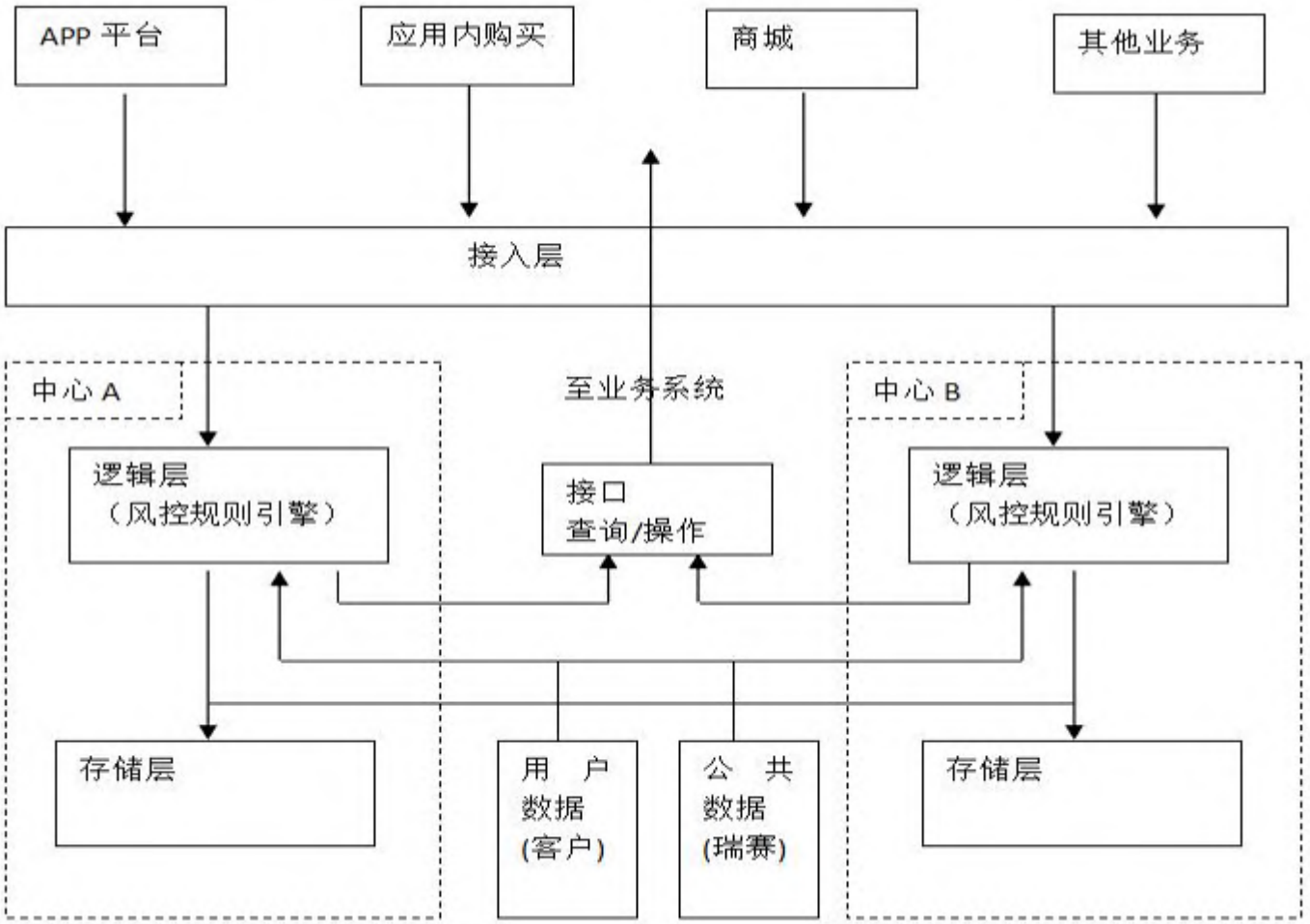
统计模型和规则

- 实时模型和规则
- 离线模型和规则
- 业务流程分析
- 数据分析
- 分析师培训和分析
- 团队搭建

人工审核

- 后台人工处理系统
- 人工处理标准和流程
- 人员培训

专业化风控平台的技术架构：双中心系统架构



风控的分场景策略：瑞赛网络科技

- 帐号和支付欺诈：
  - 帐号安全（与帐号威胁一同应对，从注册，登录和使用各环节把控，引入身份验证工具和通过行为分析）
  - 支付安全 （大数据实时和离线分析，制定模型，规则和策略）

- 黄牛：黄牛身份识别和营销规则优化

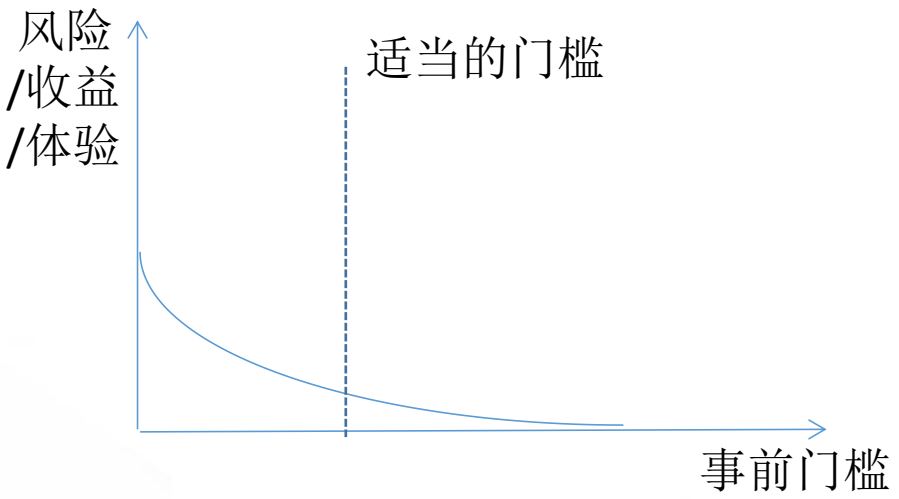
- 帐号威胁：
  - 帐号安全（帐号注册和登录监控和流程建设）
  - 安全情报（部分由瑞赛网络提供, 部分与合作伙伴合作）
  - 身份验证工具（人脸识别，指纹识别，声纹识别技术。。。，与合作伙伴合作）
  - 手机身份验证（与合作伙伴合作）
  - 银行卡验证（与合作伙伴合作）

- 应用刷榜： 用户身份识别/用户设备识别和规则优化

- 刷奖/刷会员/积分：用户身份识别/用户设备识别，奖品/会员/积分规则优化

客户选择专业化风控服务平台的注意事项

- 事前控制门槛设置的高度
  - 事前门槛高能有效降低欺诈损失
  - 但也会导致新用户难以吸引和老用户流失
  - 还会导致运营成本上涨
  - 不当用户体验： 过多短信验证，难以识别验证码验证，复杂的注册流程和身份验证流程
  - 从公司整体利益调节风险和体验的动态平衡，既要有效控制风险，又要兼顾用户体验



- 正确理解平台模型和规则的准确度
  - 对交易或帐号的拦截有两中错误：该拦没有拦，不该拦被拦；
  - 要看对的比例
  - 该拦的没有拦与不该拦而被拦的比例
  - 简单利用黑名单机制，会导致对用户体验的误伤，从而导致用户流失，还导致企业整体收益的减少

		实际拦截结果	
		Y	N
预测拦截	Y	对	错
	N	错	对

客户选择专业化风控服务平台的注意事项

- 关注资金损失率：
  因欺诈导致的损失/交易流水总额

- 选择专业平台风控服务时，要评估需要服务的范围：
  - 外包某项功能：如黑信息分享
  - 混合型：介于外包某项功能或全外包
  - 后台处理：如风控案件的审核处理全部任务
  - 全包

- 风险管理服务平台的类型选择
  - 身份验证服务商：提供身份验证服务
  - 反欺诈统计评分服务商：提供基于统计模型的评分（scoring）服务
  - 数据分享服务商：提供交易数据，设备或黑名单数据
  - 技术服务商：搭建系统
  - 分析业务服务商：提供分析服务
  - 数据清洗、整理和规范服务商
  - 运营服务商

  选择能弥补企业风险管理短板的服务商

深圳瑞赛网络科技有限公司

www.reedsec.com