未雨绸缪 有备无患

”6.18”大促安全保障的那些事

刘刚 京东安全架构师

330mlcc

https://github.com/330mlcc

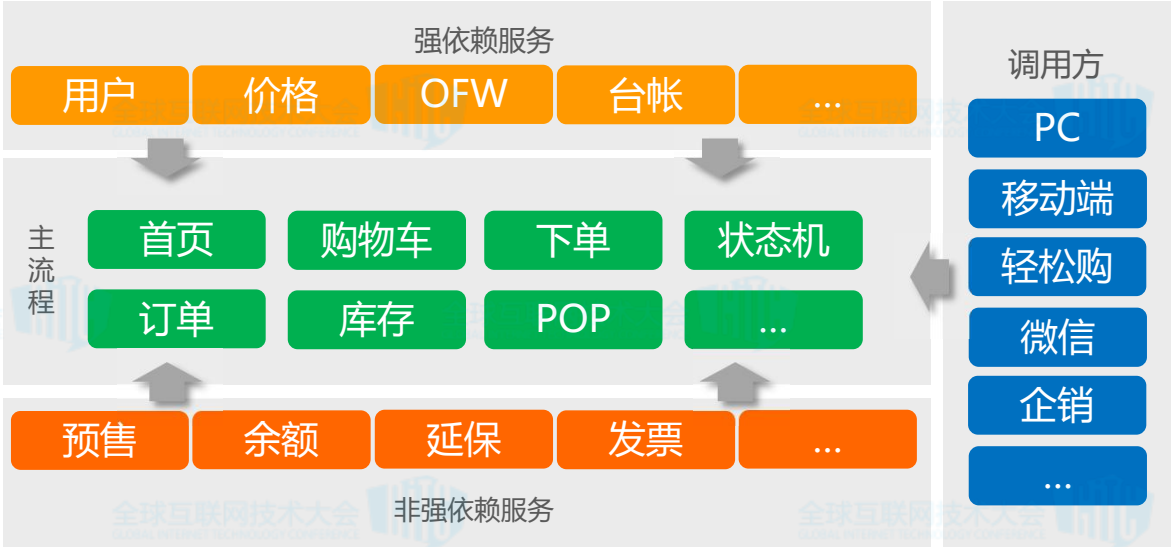
00 提纲

- 大促活动中的难点主要安全风险
- 大促安全保障的管理
- 大促安全保障的组织和动员
- 大促安全保障的技术支撑
- Q&A

01 大促活动中的难点

- 2017年“11.11”大促交易额突破1271亿元人民币
- 京东3C文旅“疯狂两小时”，手机销售额41秒破亿，电脑办公销售额48秒破亿...

- 业务系统重要性高
- 风险影响高
- 系统复杂度高
- 安全防护的头绪多
- 不确定因素多
- 干系人多



02 大促活动中的主要安全风险

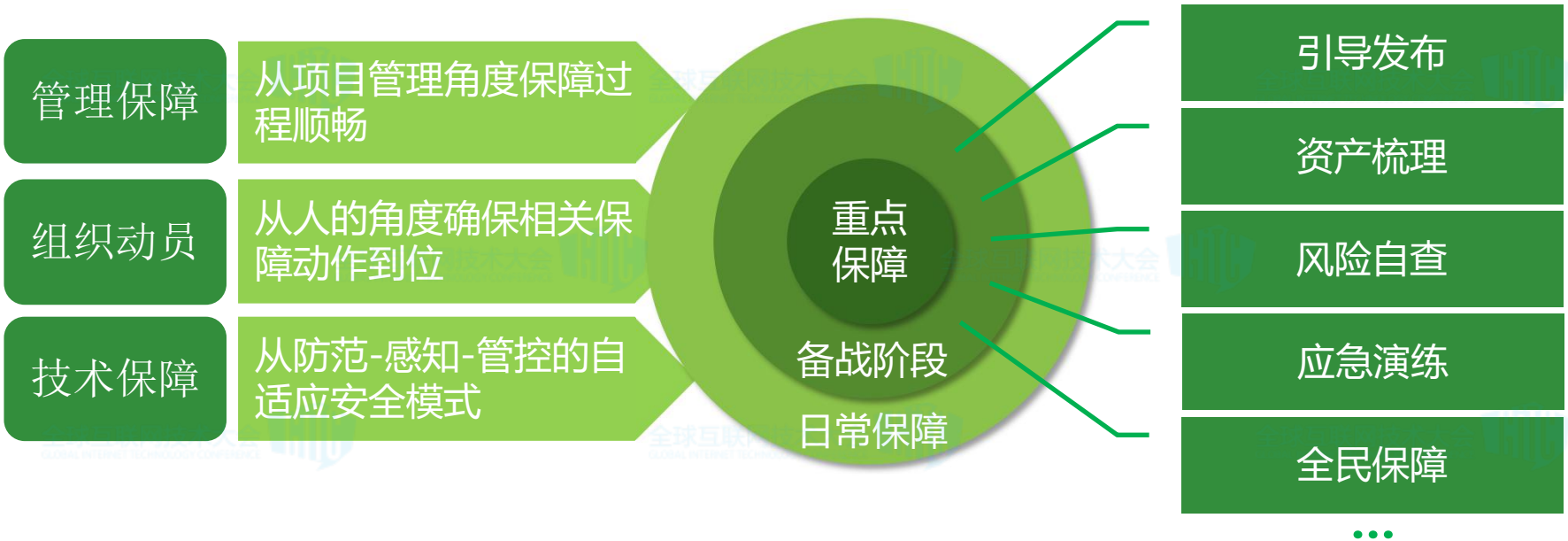
- 京东的业务线安全性已经具备了标准的防御力
- 京东信息安全团队也经历了一个从小到大，由弱到强的过程

- 安全漏洞偶有出现
- 流量劫持取证难
- 钓鱼攻击检测快，但处置难
- 数据流转的链条长，欺诈形式花样翻新…

- 人员安全意识
- 苦练内功，增强安全防护和感知
- 建立SRC品牌，发动内外部力量
- 联合多个企业和行业主管部门

03 大促安全保障的管理

- 分阶段的安全保障
- 精心组织、防护到位、保障有力

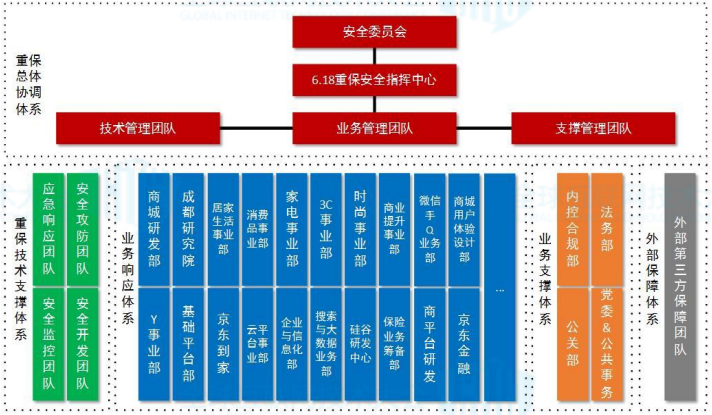


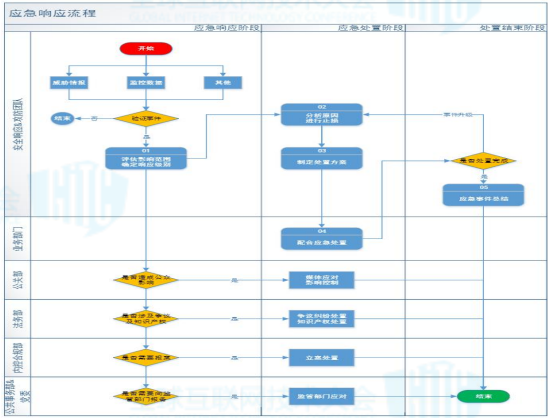
04 大促安全保障的组织和动员

- 覆盖从入职到晋升的各阶段
- 从高管到仓储培训
- 形式多、内容好、重考核

- 横跨各集团和业务体系
- 业务、安全、法务、合规等多个业务部门联动

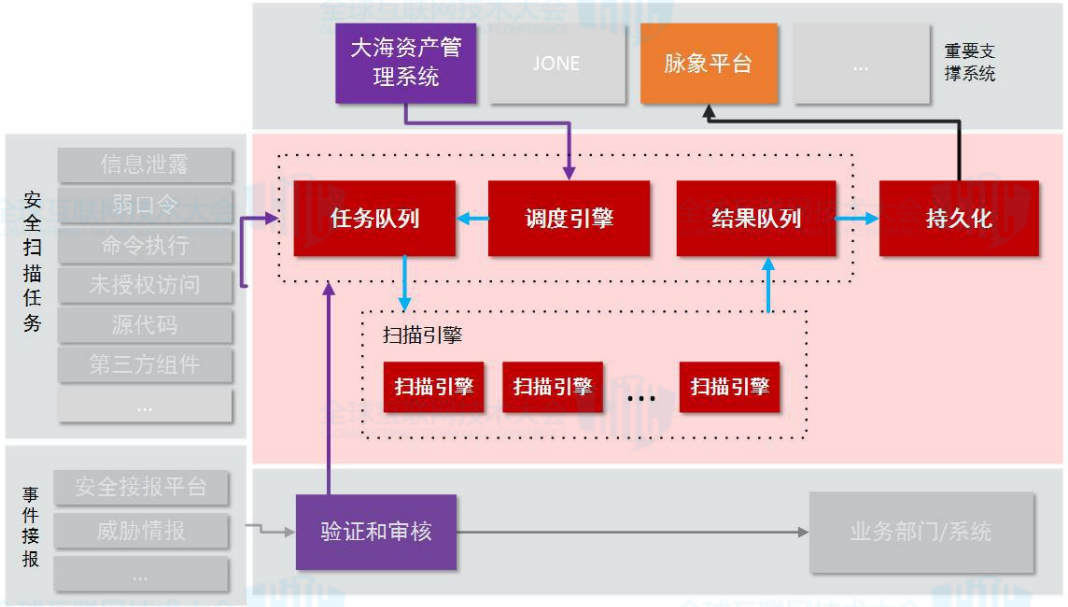
- 应急响应体系环环相扣
- 严格的修复时间要求
- 安全官与业务接口人对接





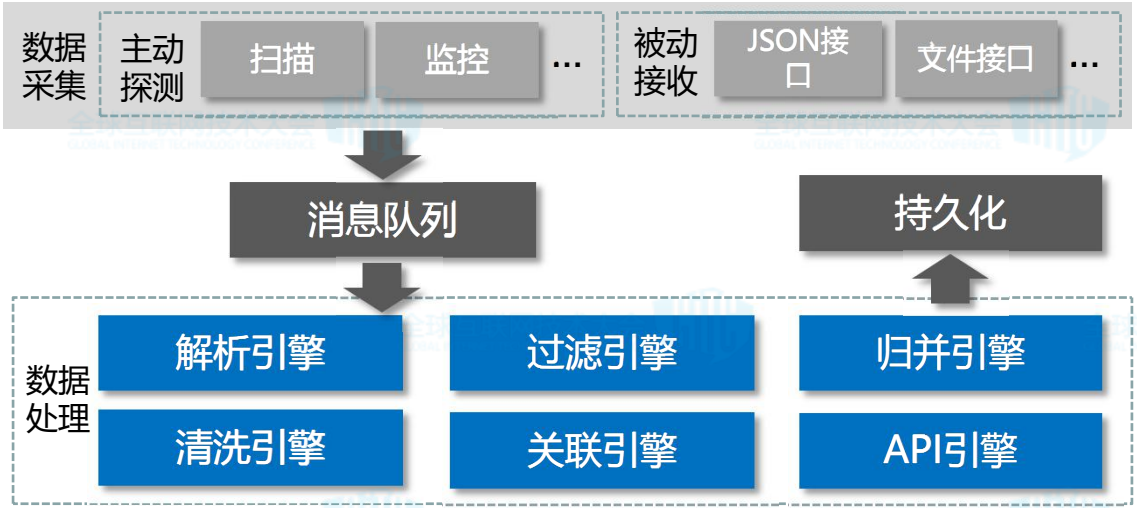
05 技术支撑 - 分布式高并发漏洞扫描

- 支持高并发、多任务的开发语言
- 扫描引擎静态编译，无需任何依赖
- 高性能
  - 单PoC3分钟扫描
  - 全脚本45分钟扫描
- 准确率
  - 高危漏洞100%准确
  - 常见Web漏洞95%准确率



06 技术支撑 – 大海一般多维度的资产汇聚

- 将日常安全保障所需的资产进行集中汇聚
- 数据来源多、数据覆盖面广、信息量全



- 基于机器学习技术的海量URL去重
- 最全资产信息
- 多维度的关联
  - IP/域名与管理者
  - 组件版本与应用系统
  - 数据调用关系...

07 技术支撑 – 脉象全息化平台

全息化展示

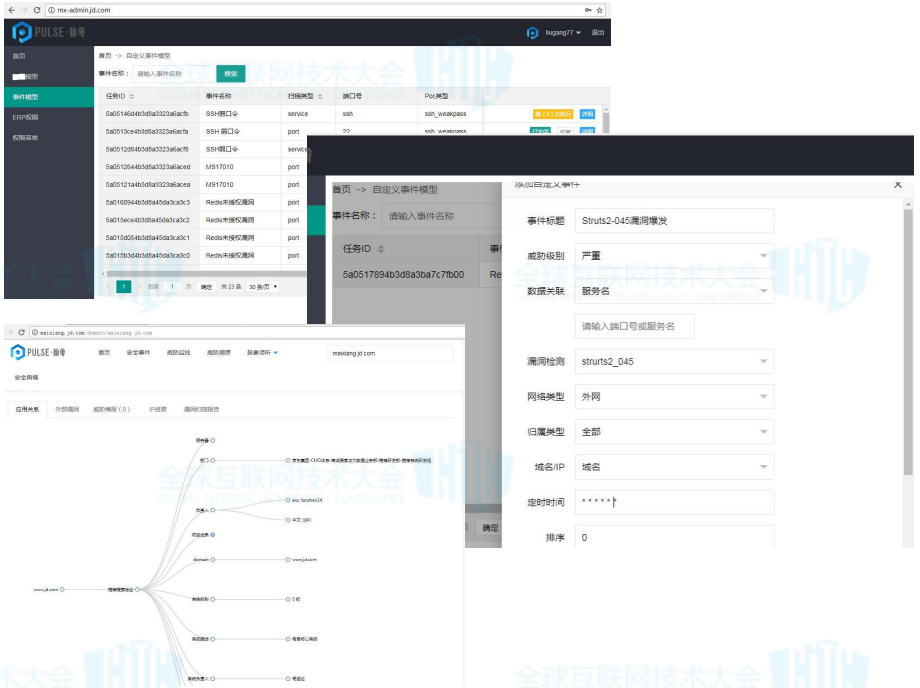
- 基于时间轴的影响范围、处理进度可视
- 基于漏洞、应用指纹和组件的可视
- 基于应用、位置和人的可视

自动化处理

- 多种通知/推送渠道
- 威胁情报与全网快速扫描实时结合

0day监控

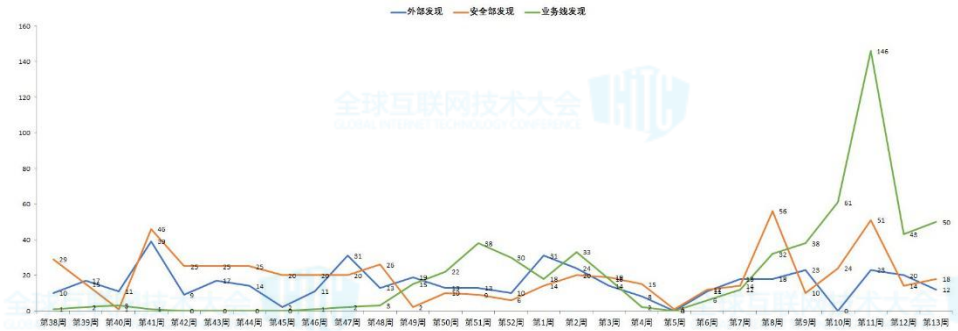
- 50+渠道（漏洞和舆情）实时监控
- 10人的专业分析团队



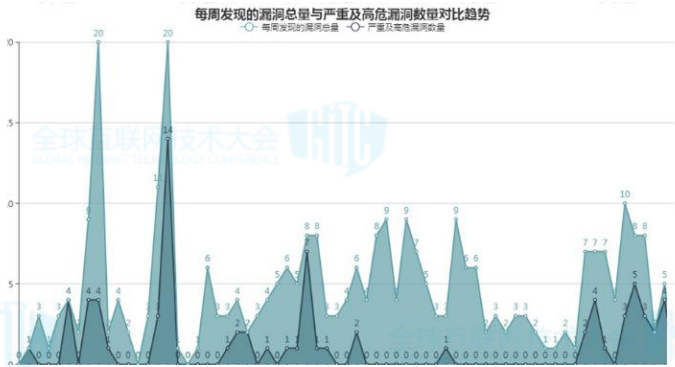
08 技术支撑 - SDL+安全开发控制

管理保障 | 制度保障 | 技术保障 | 保障宣贯

■ 从安全的最初就具备安全的属性，覆盖意识到上线的全过程



业务部门自我漏洞发现能力显著提升



上线前发现的高危严重漏洞

09 技术支撑 – 持续监控和感知

敏感信息泄露	移动应用	联防联控	…
Github SVN泄露 任意文件读取 …	移动发布渠道 应用排名搜索 …	钓鱼 劫持处置 诈骗 …	. . .

自研检测平台

大促数据保障指挥系统

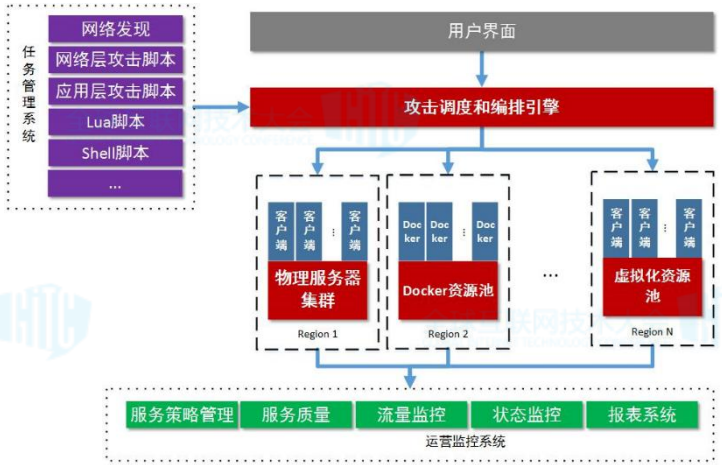
- 对接业界最新威胁情报
- 7*24小时不间断监控
- 覆盖影响最大的信息安全漏洞
- 自研检测平台：业务部门自行操作，傻瓜式一键点击操作操作，快速反馈报告和扫描结果
- 集中指挥：基于京东大促数据墙的保障指挥系统

10 技术支撑 - 全站HTTPS的推广和优化

- 所有流量由JFE统一接入
- 关键节点
  - 预发系统
  - HTTP/HTTPS双支持
  - 硬件加速
- SSL证书改造
- 性能优化

11 技术支撑 - DDoS攻防平台

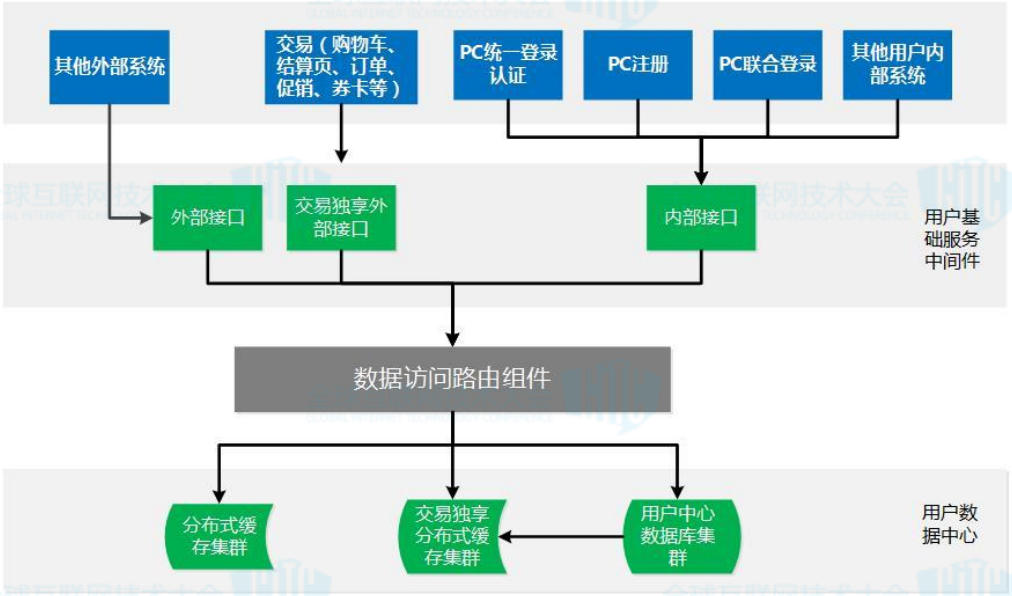
- 覆盖应用层、特殊控制报文和畸形包的攻击平台
- 支持自定义的Lua脚本和shell脚本
- 强大的资源调度和编排能力
- 分级攻击清洗系统
  - JDTP-Detec全流量镜像
  - 基于攻击历史、IP信誉的数据分发、处理
  - 流量规模、成分、行为、攻击指纹的分析
- 攻击流量的集中监控



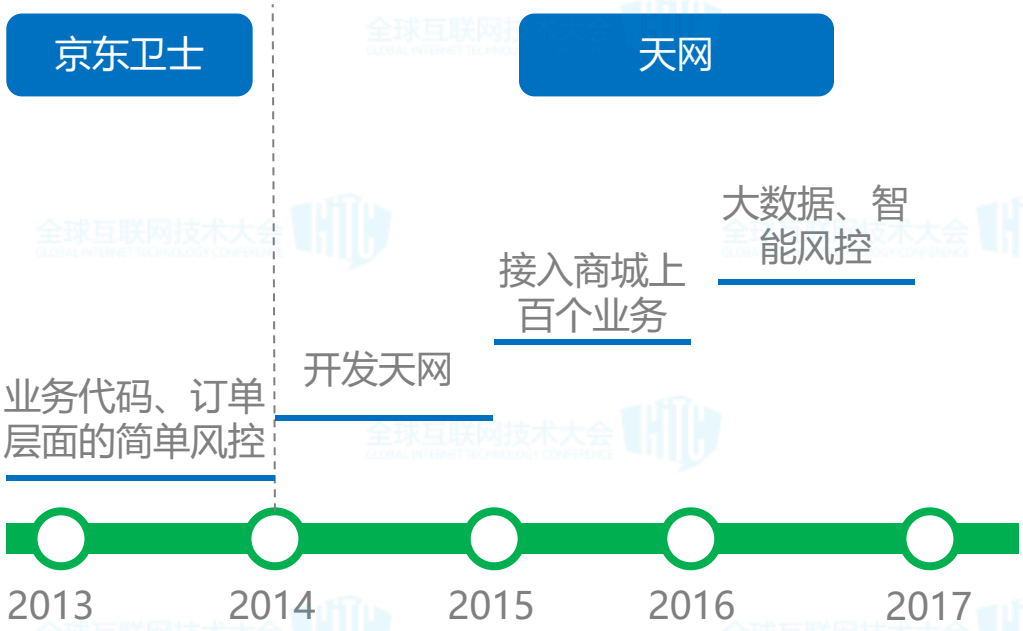
12 技术支撑 – 千万用户的注册和登录

- 用户基础服务中间件是核心，对所有WEB应用提供单一的参数校验和装配

- 根据调用方的业务重要程度、调用量、访问的用户信息字段等进行动态规划
- 根据敏感程度、调用频度、隔离等维度提供服务的精细化和差异化
- 登录、注册建立多层次的安全规则策略
- 多个业务操作的风控模型



13 技术支撑 - 天网恢恢疏而不漏



- 从注册登录、营销到抢购的业务场景
- 风险信用服务（RCS）
- 风控数据支撑系统包括数据层、算法引擎、分析引擎、决策引擎和应用层等
  - 基于用户购买流程的风控指标
  - 基于用户社交网络的风控指标
- 风险监控：应用和服务实时和离线的监控及报表服务

Q&A

谢谢