GIAC | 全球互联网架构大会
GLOBAL INTERNET ARCHITECTURE CONFERENCE

金融科技分布式安全架构实践

京东金融 JD Finance

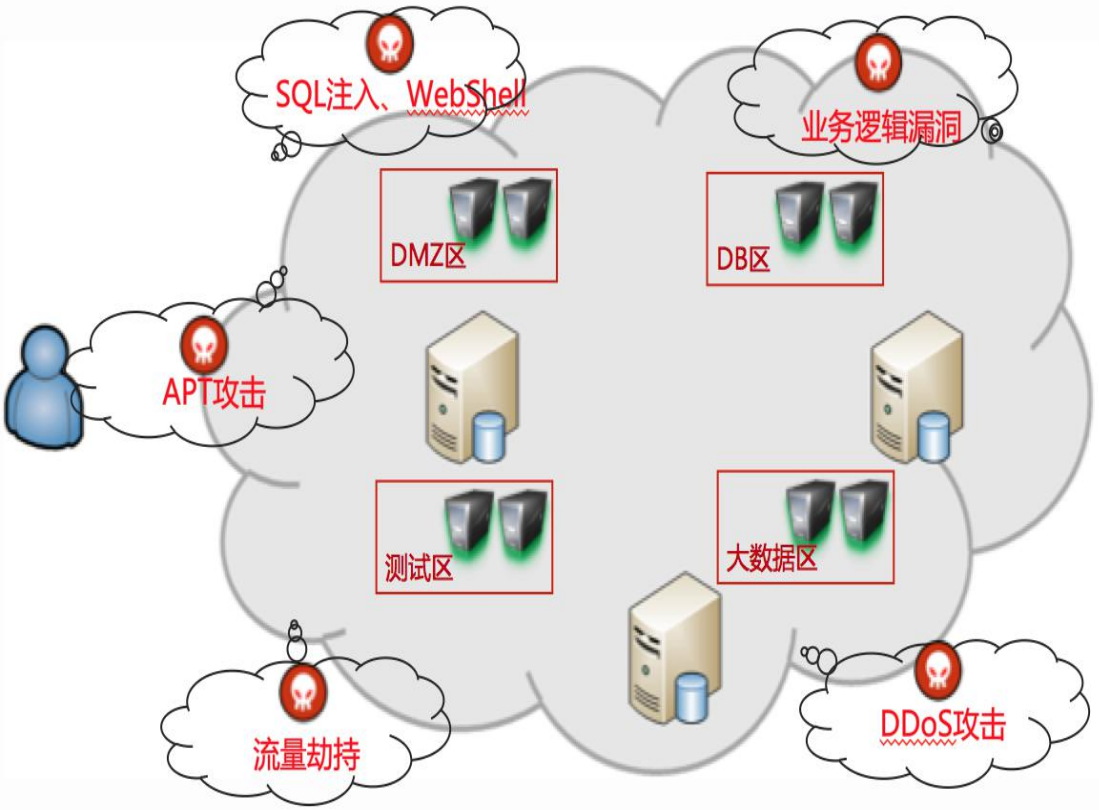
刘明浩
安全管理部负责人

2017.thegiac.com

金融科技分布式安全架构

- 金融科技所面临的安全挑战
- 金融科技分布式安全架构
- 分布式环境下的安全管理
- 威胁情报在京东金融的应用

分布式环境下的安全挑战



分布式环境下的安全风险点

- 外部
  - DDoS攻击、CC攻击
  - Web安全漏洞、远程代码执行漏洞
  - 撞库、盗号、垃圾账号注册
- 内部
  - APT攻击
  - 身份识别与授权访问
  - 移动端产品安全

金融科技分布式安全架构

- 金融科技所面临的安全挑战
- 金融科技分布式安全架构
- 分布式环境下的安全管理
- 威胁情报在京东金融的应用

金融科技分布式安全架构

基于全流量外部威胁防御平台

DDoS防护

- DDoS攻击检测
- DDoS流量清洗

业务安全 数据风控

- 活动防刷
- 登录保护
- 注册保护
- 反欺诈

Web安全 防火墙

- SQL注入
- 命令执行
- 文件上传
- CC攻击

基于资产内部威胁防御平台

SSH安全登录

- 动态口令
- 公私钥免密
- 安全审计

主机入侵 检测

- 资产管理
- 风险分析
- 入侵监控
- 安全基线

移动安全 平台

- APK信息提取
- 代码漏洞扫描
- 敏感API调用
- 动态脱壳

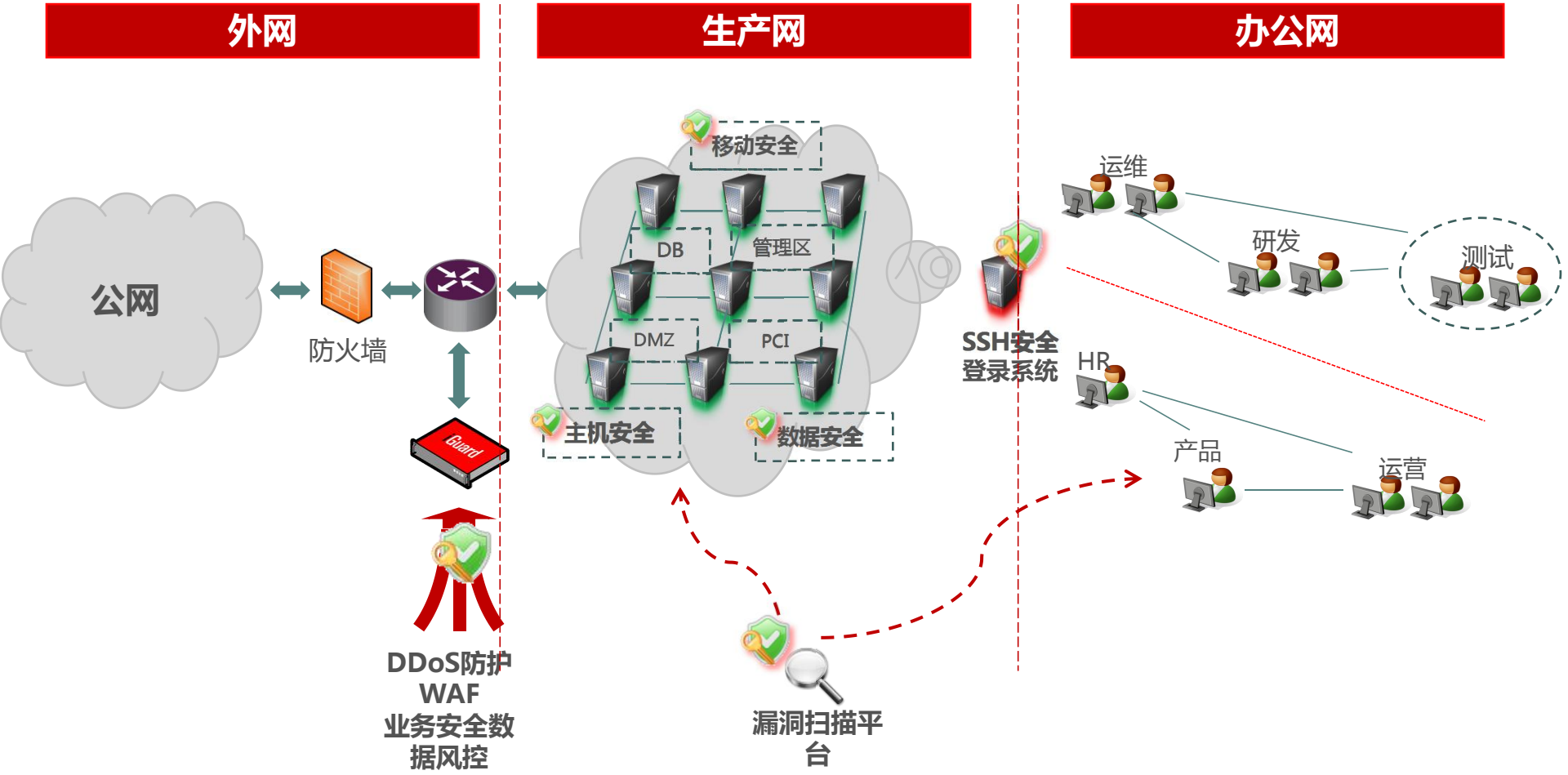
漏洞扫描 平台

- 端口扫描
- 漏洞扫描
- GitHub泄露
- 测试环境流量回放

统一平台 **统一数据** **集中展示**

安全可视化 关联分析 态势感知

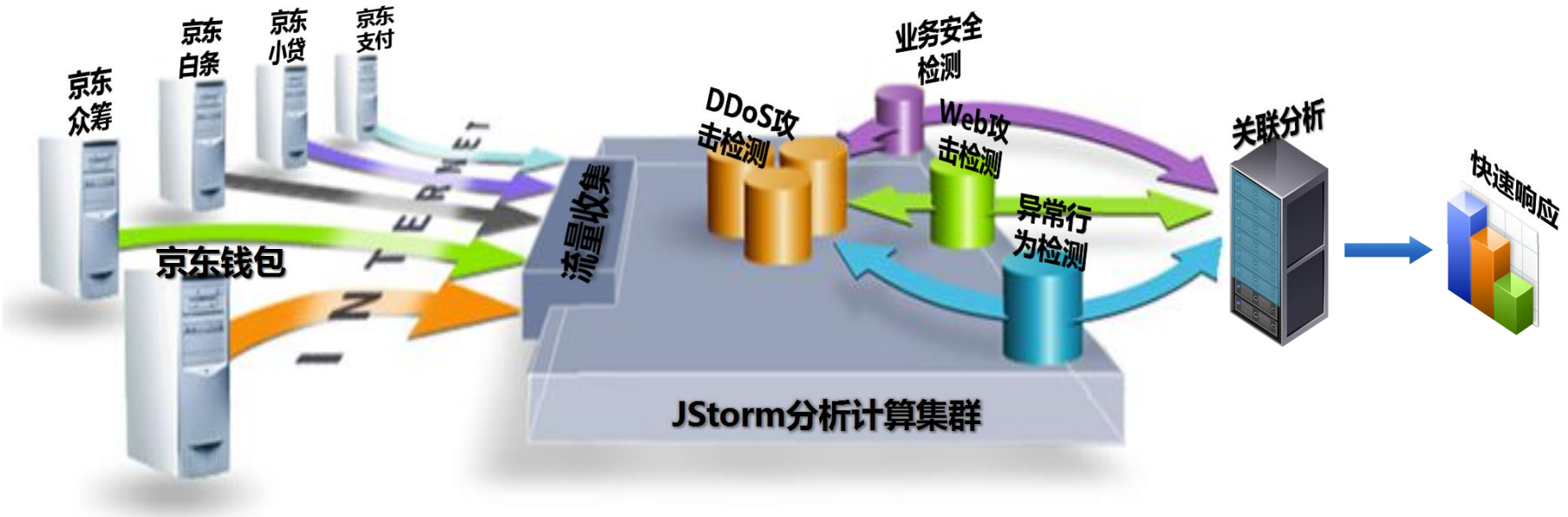
金融科技分布式安全架构



金融科技分布式安全架构

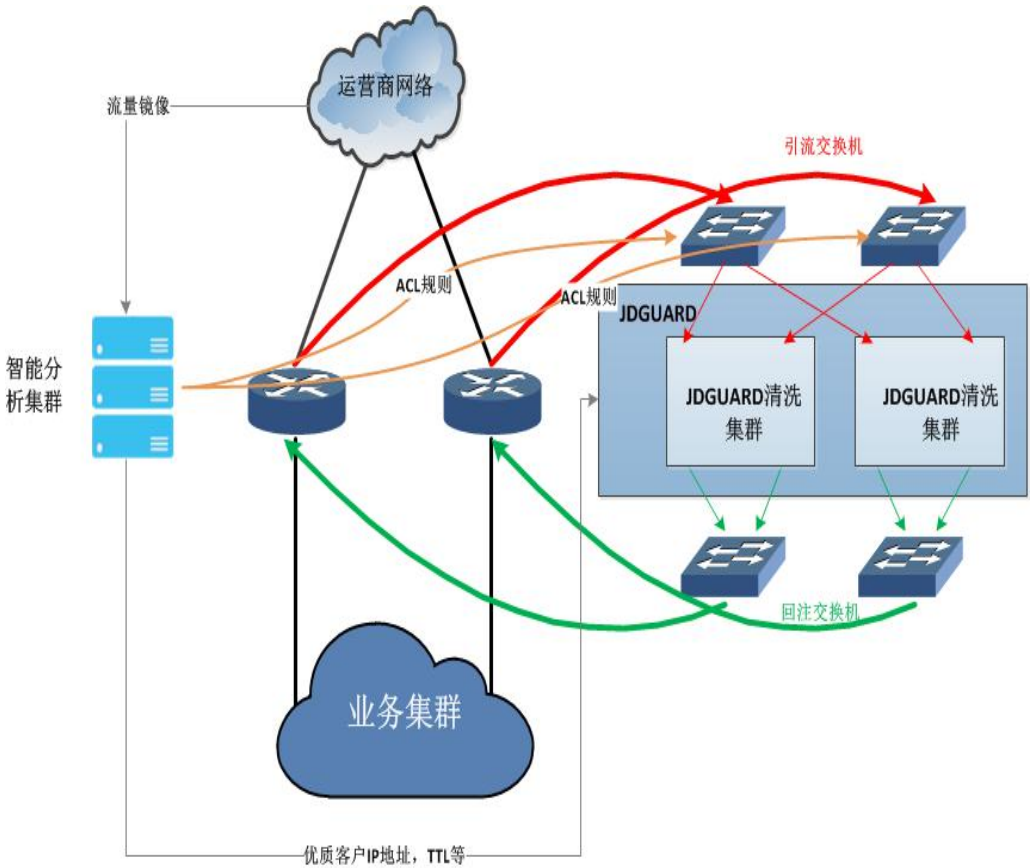
- 金融科技所面临的安全挑战
- 金融科技分布式安全架构
- 分布式环境下的安全管理
- 威胁情报在京东金融的应用

基于全流量的外部威胁检测平台



DDoS攻击防护

DDoS防护通过流量镜像收集运营商网络到IDC机房的所有数据包，对四层网络协议进行安全分析，其中通过解析数据包的内容，提取各项网络特征，统计接收到的数据流量大小、各种协议（包括但不限于ICMP、TCP、UDP、DNS、HTTP/HTTPS）报文数量、网络链接数量，再结合DDoS攻击特征，结合大数据的方法，及时发现DDoS攻击行为并与JDGurad系统联动对攻击流量进行清洗及回注



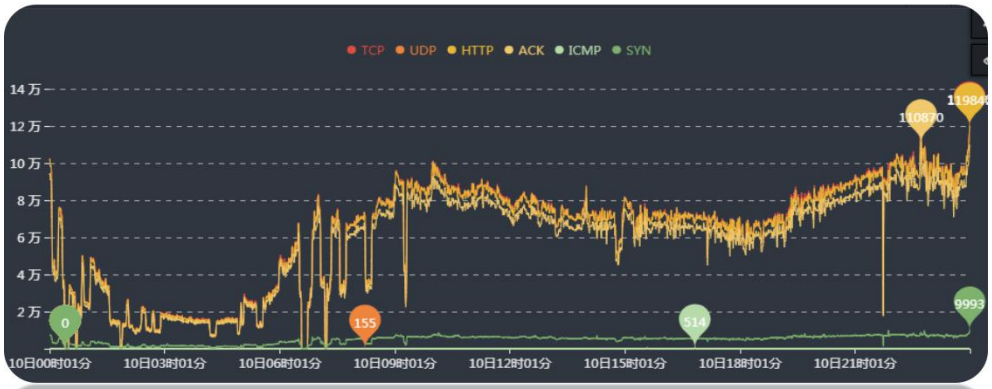
DDoS攻击防护

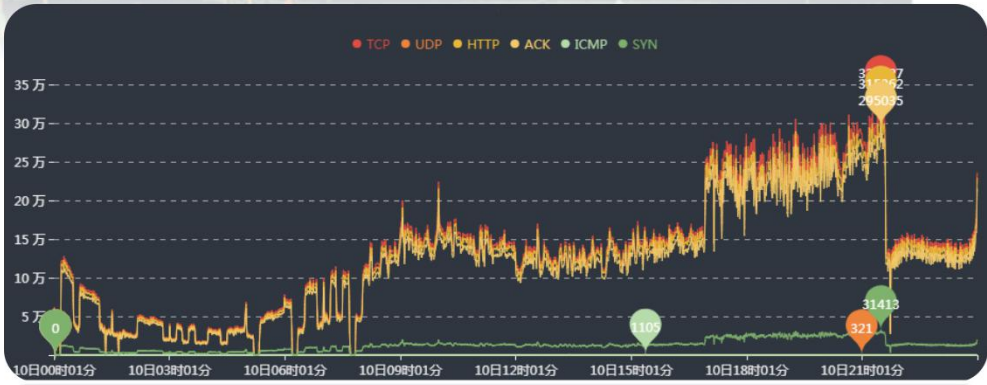
1. 云端清洗集群，单机40G流量清洗能力，可集群扩展

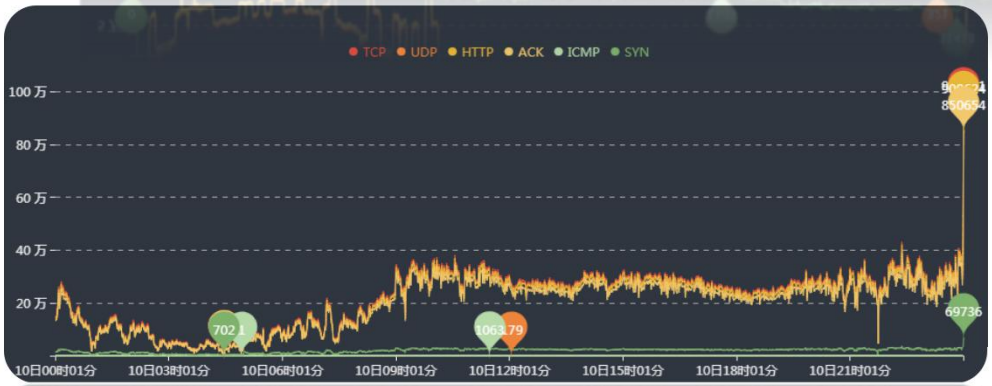
2. 通过与detector联动清洗syn flood， ack flood, udp flood, icmp flood等各类常见DDoS攻击

3. 部署灵活，流量智能牵引，攻击响应精准迅速

4. 支持TCP，UDP，HTTP，HTTPS等各种协议







DDoS攻击防护

畸形报文过滤

对报文的合法性进行检验，对畸形报文进行拦截，防止其穿透到后端系统

自定义黑白名单

可接入安全模块获得黑名单，同时将信任客户，合作伙伴等加入白名单

特征分析判定

对流量进行特征分析，动态维护可信任访问源集合

虚假源认证

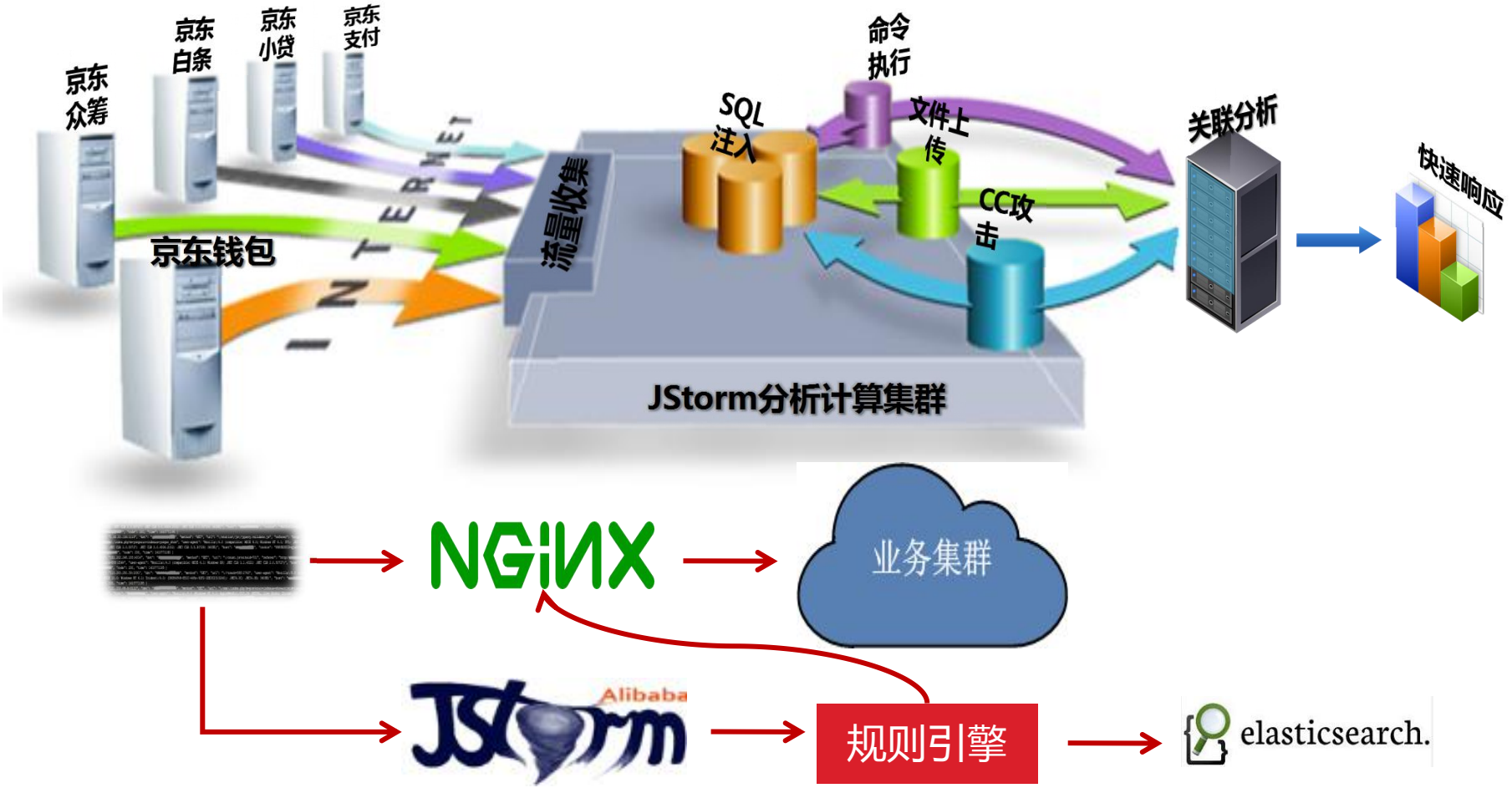
对流量进行源认证，有效过滤sync flood, ack flood, icmp flood等

智能限速

对单个IP进行智能限速，有效防止突发异常流量

Web安全防火墙

基于全流量安全大数据平台进行七层Web攻击行为分析以及Nginx反向代理实现云服务模式Web安全防护，包括海量数据实时及离线分析协同防御，挖掘外网业务攻击行为，精准识别SQL注入、XSS跨站脚本、webshell上传等，避免网站资产数据泄露，保障网站的安全与可用性



业务安全数据风控

基于全流量安全大数据平台及机器学习算法，从最初的有监督机器学习到后期的模型优化智能引擎的无监督机器学习，包括智能评分卡、安全画像、威胁情报等

账号安全

通过分类、回归、聚类的方法从频率、账号属性、行为相似性等角度对撞库、垃圾账号注册进行识别

智能评分卡

将全流量数据与用户的注册数据、登录数据和访问数据关联，对用户账号进行智能评分，并将分级结果作为API对外提供服务

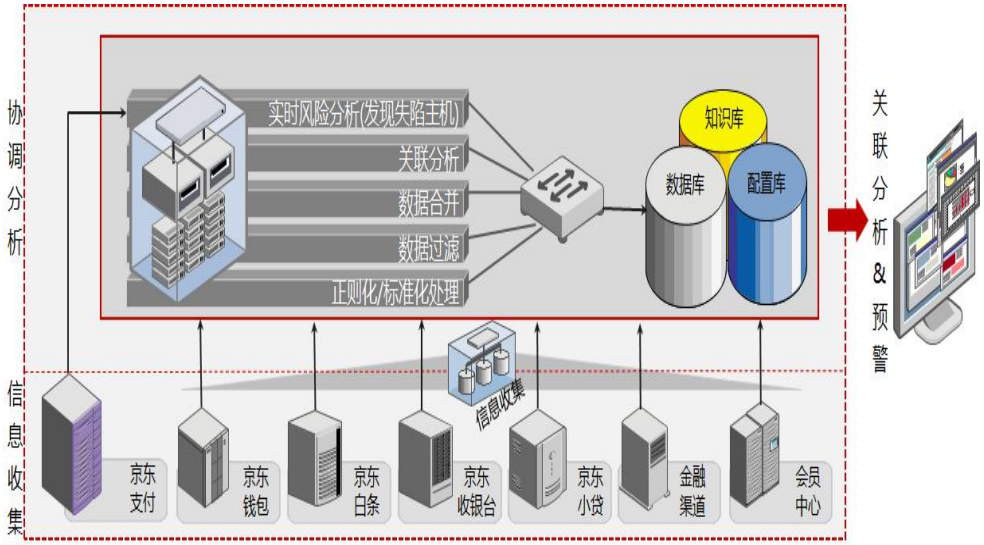
安全画像

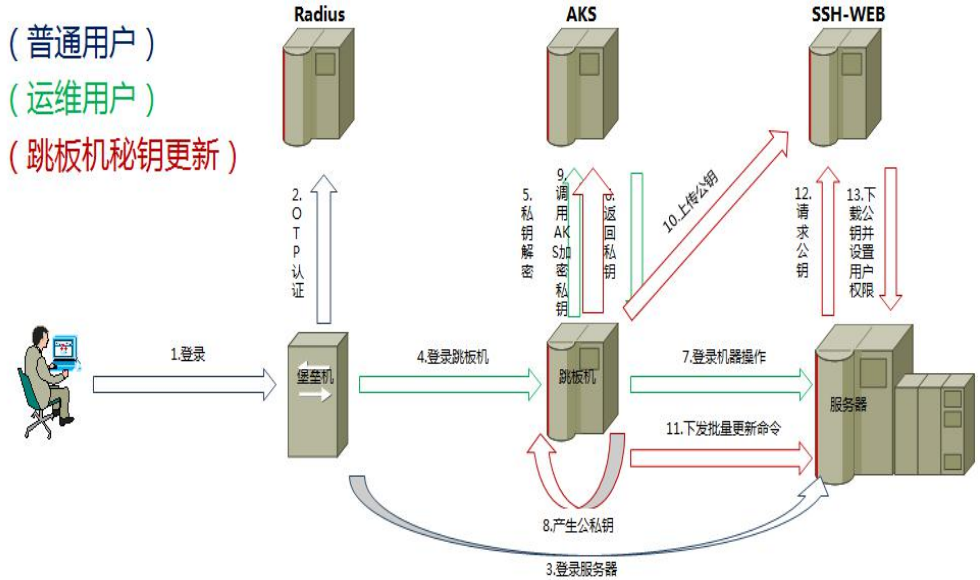
使用基于浏览器指纹和手机设备指纹的方式，还原用户行为轨迹，通过规则引擎及异常行为分析模型，识别出异常访问、刷单、机器人等行为的安全画像

威胁情报

积累IP信誉分,手机号信誉分、公共出口IP、代理IP、虚假小号等威胁情报

基于资产的内部威胁检测平台



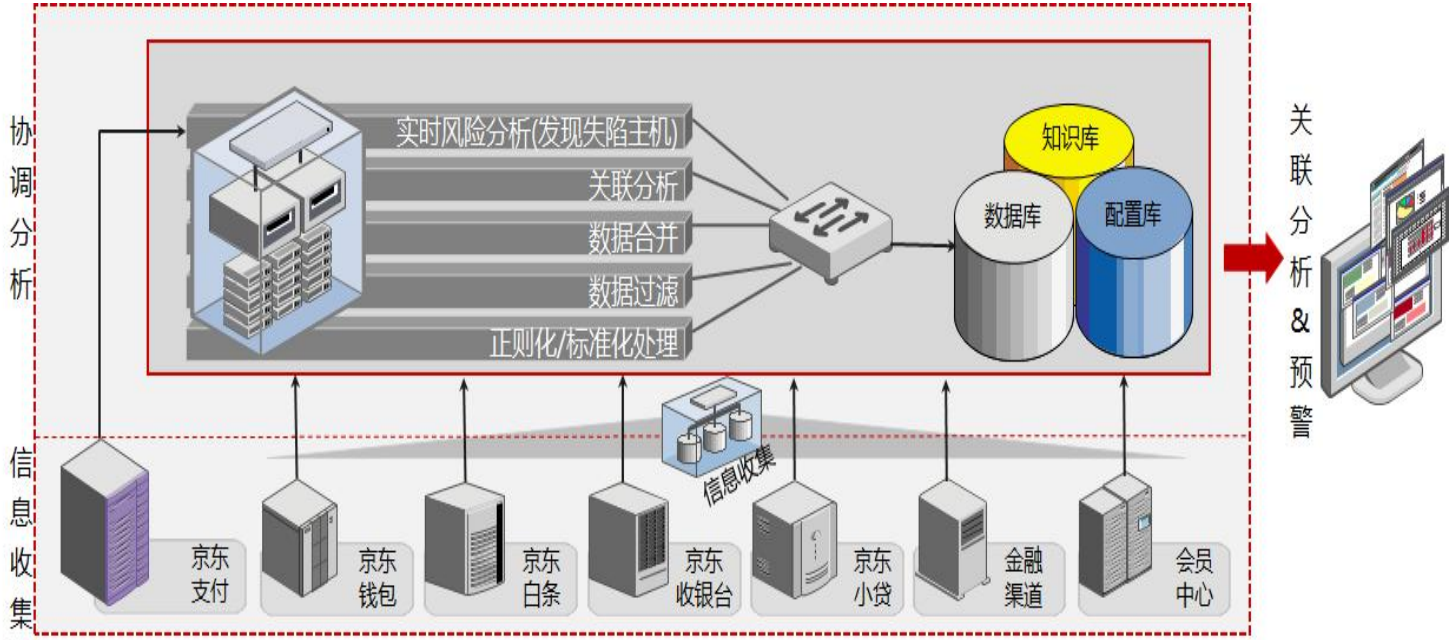


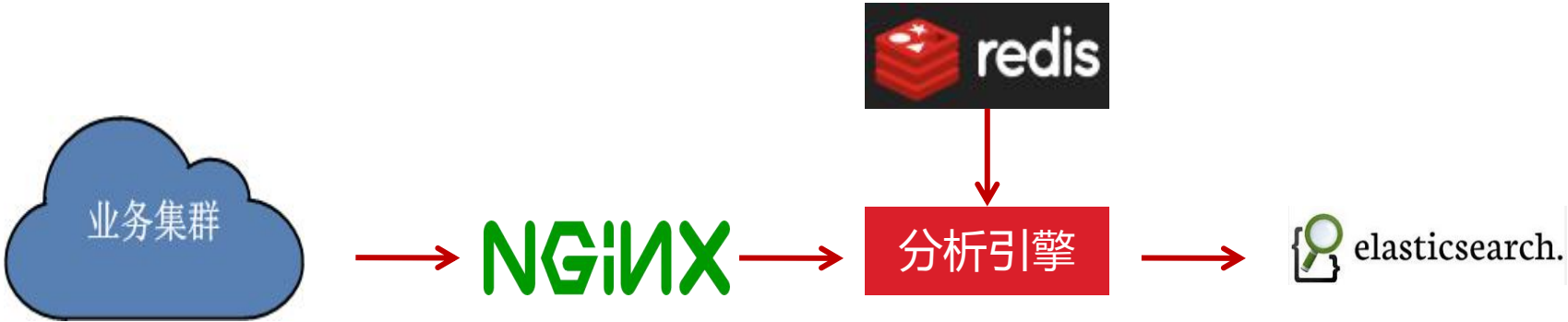
内部威胁安全挑战

- HIDS主机安全
  - 轻量级agent
  - 全方位安全监测
  - 实时大数据分析
- 移动安全平台
- 漏洞扫描平台
- 安全登录系统
  - 堡垒机多因素认证
  - 降低服务器密码泄露
  - 秘钥加解密
  - 集中审计

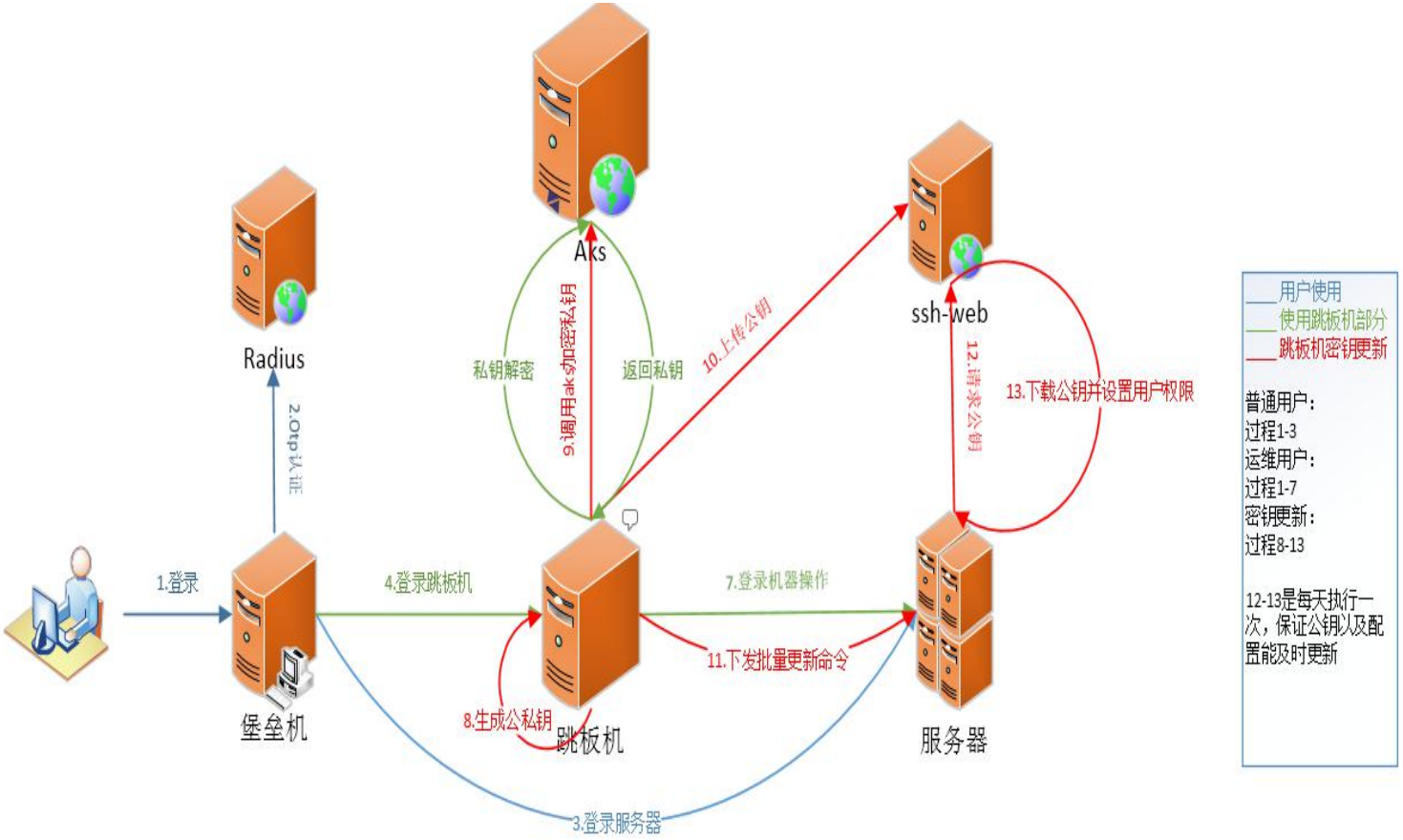
主机入侵检测

主机入侵检测由轻量级Agent和云端组成，集整体安全平台威胁情报于一体，通过Agent和云端大数据的联动，实现对文件完整性监控、内网端口扫描、登录行为监控、webshell创建进程监控、命令执行监控、主机流量监控等功能





SSH安全登录系统



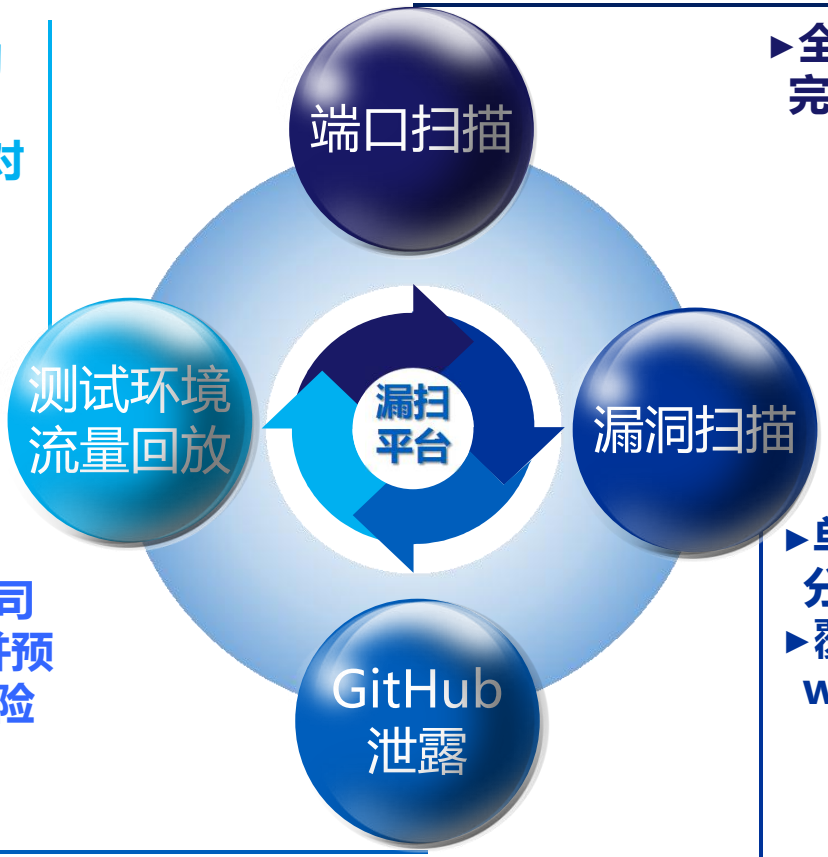
干掉所有密码！

移动安全平台 App Hunter

漏洞扫描平台

►通过流量镜像分析的方式提取出流量中的HTTP请求信息，并对信息中可能存在的安全问题进行检测

►监控github代码库，及时发现员工托管公司代码到Github行为并预警，降低代码泄露风险



►全网全端口24小时内完成

►单PoC全网扫描10分钟

►覆盖系统、应用及web漏洞扫描

金融科技分布式安全架构

- 金融科技所面临的安全挑战
- 金融科技分布式安全架构
- 分布式环境下的安全管理
- 威胁情报在京东金融的应用

威胁情报

通过WAF命令执行成功请求告警

漏洞分析

对告警请求进行分析发现在请求header头中的Content-Type
有注入OGNL执行命令

漏洞复现

通过对抓取到的PoC进行调试命令执行成功

全网扫描

在扫描器中加载PoC进行全网扫描

漏洞修复

编写补丁包，通过过滤Content-Type中的危险语句，指定OGNL表达式的白名单来避免命令执行

持续监控

PoC开始在网上流传，通过WAF监控实时的请求。一是匹配流量中header头中的PoC，二是匹配http请求中的response验证是否执行成功

威胁情报 态势感知
关联分析 深度学习

GIAC | 全球互联网架构大会
GLOBAL INTERNET ARCHITECTURE CONFERENCE

GIAC

全球互联网架构大会

GLOBAL INTERNET ARCHITECTURE CONFERENCE

谢谢！

欢迎交流

2017.thegiac.com