从甲方到乙方

云安全实践之路

腾讯

刘宁

Geekbang.
极客邦科技

整合全球最优质学习资源，帮助技术人和企业成长

Growing Technicians, Growing Companies

InfoQ queue

专注中高端技术人员的
技术媒体

EGO EXTRA GEEKS' ORGANIZATION NETWORKS

高端技术人员
学习型社交网络

StuQ queue

实践驱动的
IT职业学习和服务平台

GiT GEEKBANG INTERNATIONAL TRAINING 极客邦培训

一线专家驱动的
企业培训服务

地址：北京市朝阳区洛娃大厦C座6层1607室　　网址：www.geekbang.org

自我介绍

刘宁：07年进入腾讯，安全平台部

- 09年：IDS（宙斯盾）
- 10年：挂马检测
- 11年：SOC
- 13年：入侵对抗（洋葱）
- 15年：云安全（天御、大禹）

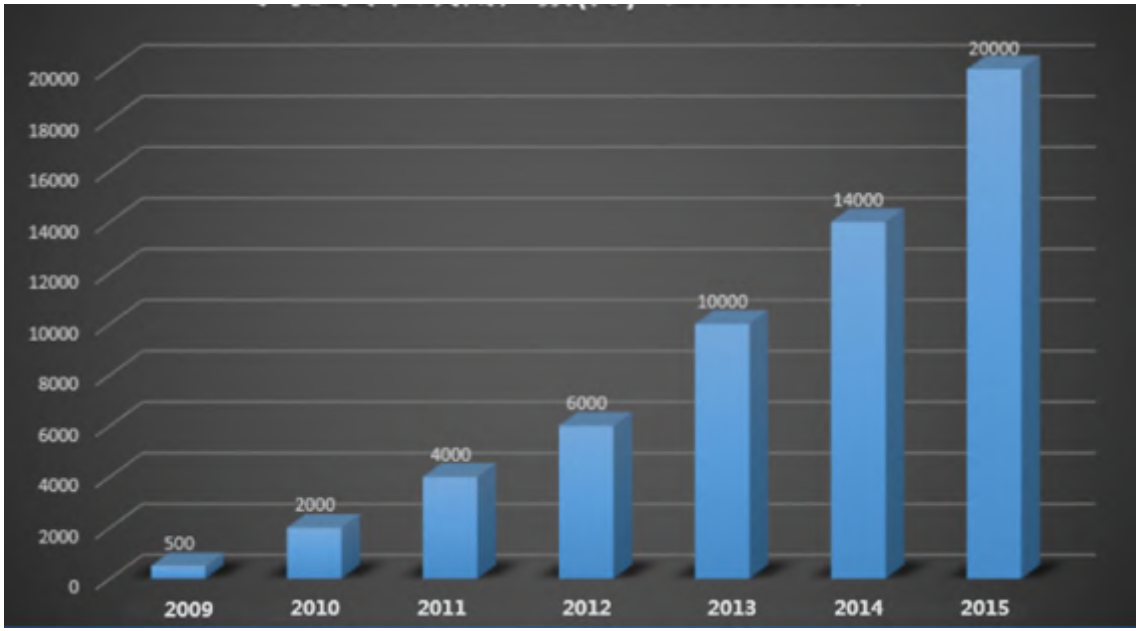
大纲

- 面临的挑战
- 云上的安全风险
- DDoS对抗
- 业务安全对抗
- 总结

面临的挑战

业务持续增长，机遇＋挑战

600w CGI



30亿登录

4.6Tps流量

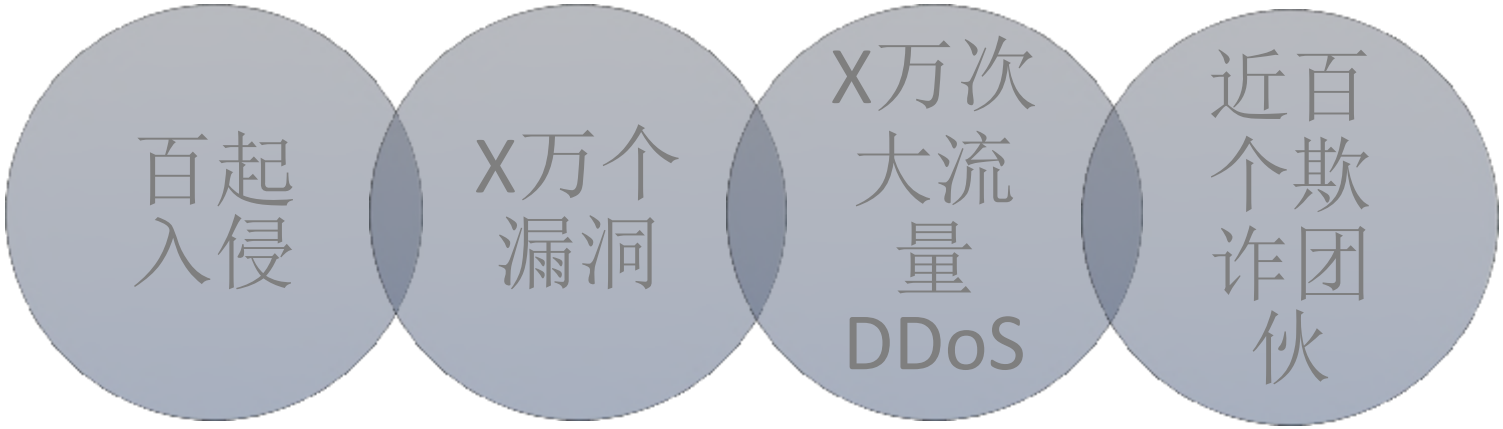
2亿＋用户

面临的挑战

可以说，再怎么“安全”的公司和产品，只要出WEB服务，都是渣，不管你是FireEYE，还是Palo Alto Networks，或是Telegram。 网页链接

面临的挑战

- 05年“朽木”事件
- 10年“游戏DDoS对抗”
- 11年 “广西欺诈团伙”
- 14年“openssl / shell shock漏洞”



面临的挑战

安全平台部

业务的核心竞争力

全面保障业务发展

应急响应

面临的挑战

业务安全

- 反盗号——QQ安全中心
- 反欺诈——安全大数据

应用运维安全

- 网络保障——宙斯盾
- 漏洞发现——扫描器 / 金刚
- 入侵对抗——洋葱

云上的风险

云上的安全风险

老办法，保姆式服务，行么？

云上的安全风险

不行！

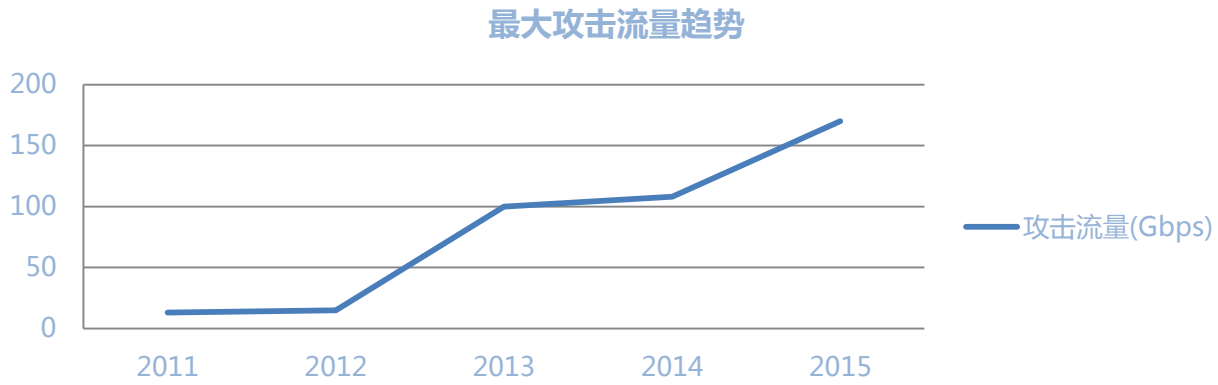
- 有价值
- 找长处

云上的风险——DDoS对抗

DDoS对抗

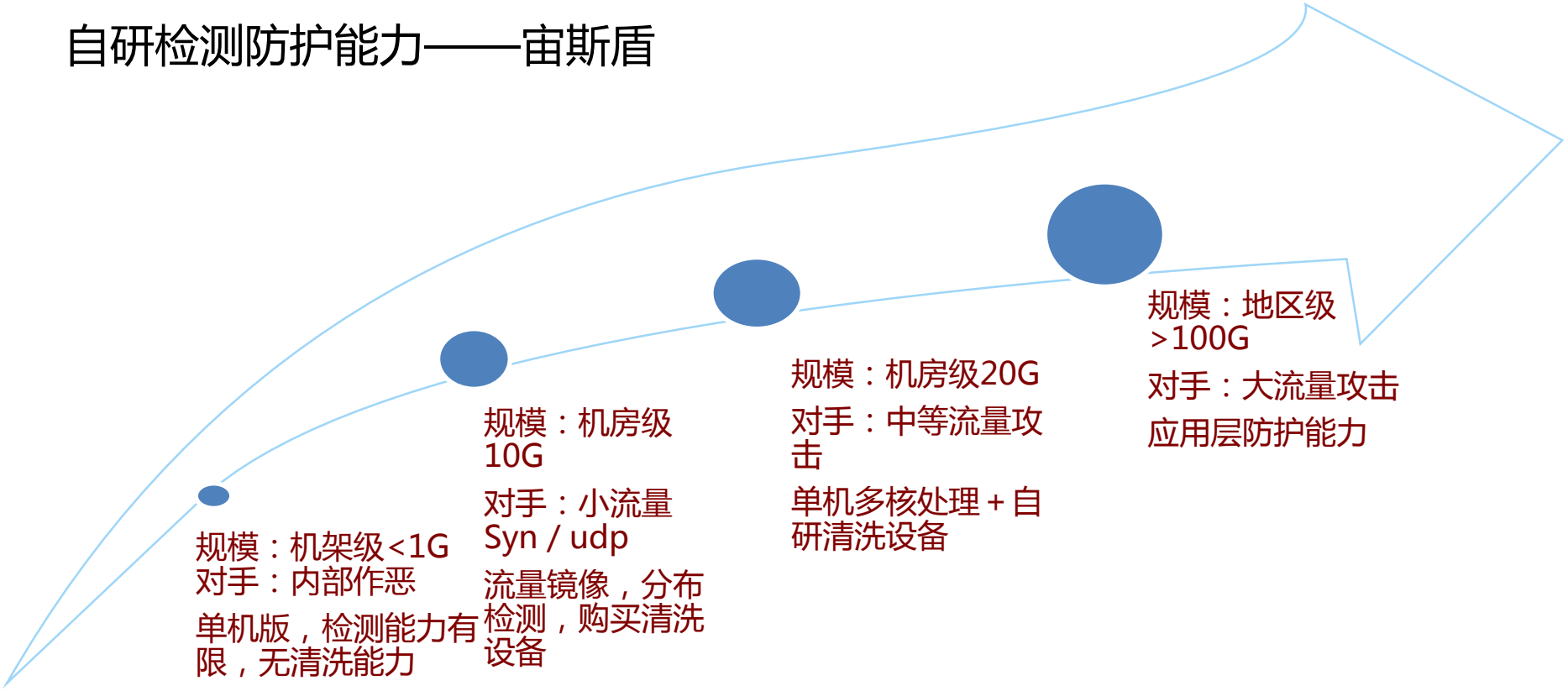
DDoS愈来愈频繁

- 低成本
- 高收益



DDoS对抗

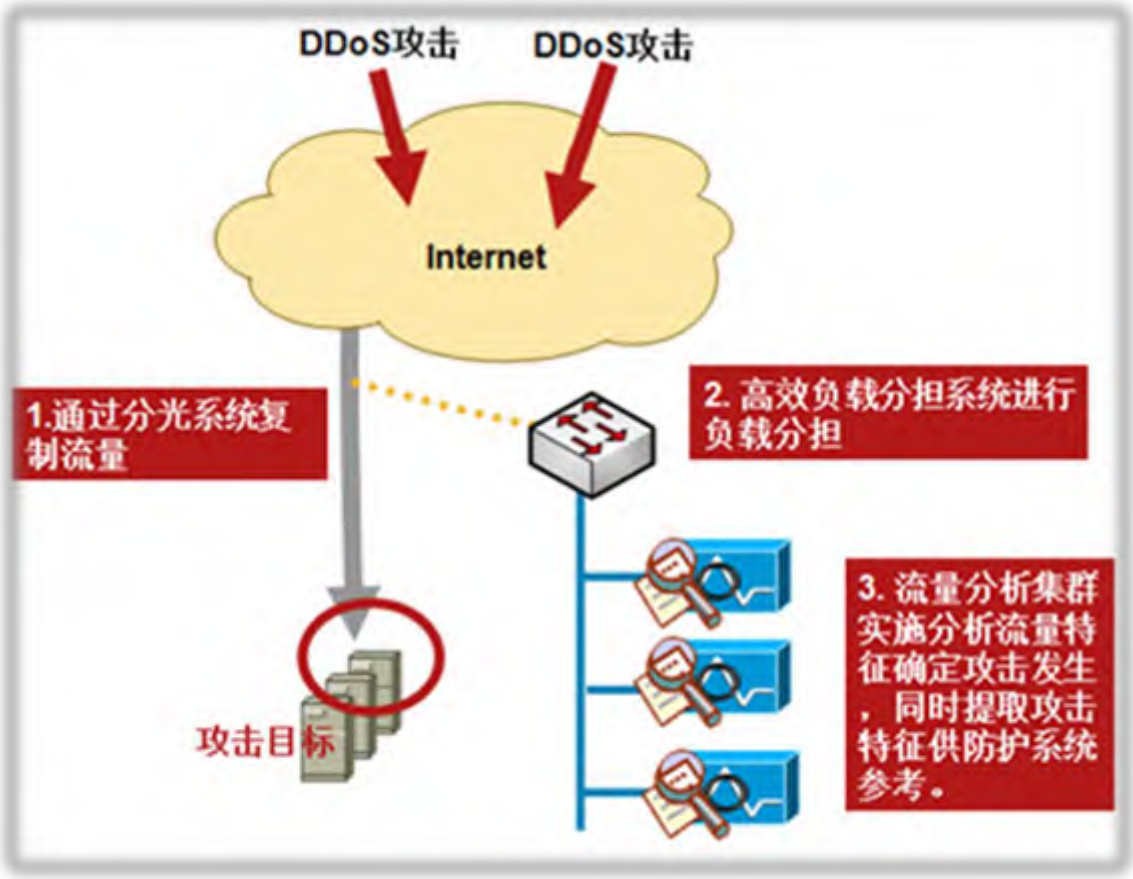
自研检测防护能力——宙斯盾



DDoS对抗

1.0版本——基于机房的对抗

- 带宽瓶颈
- 防护短板

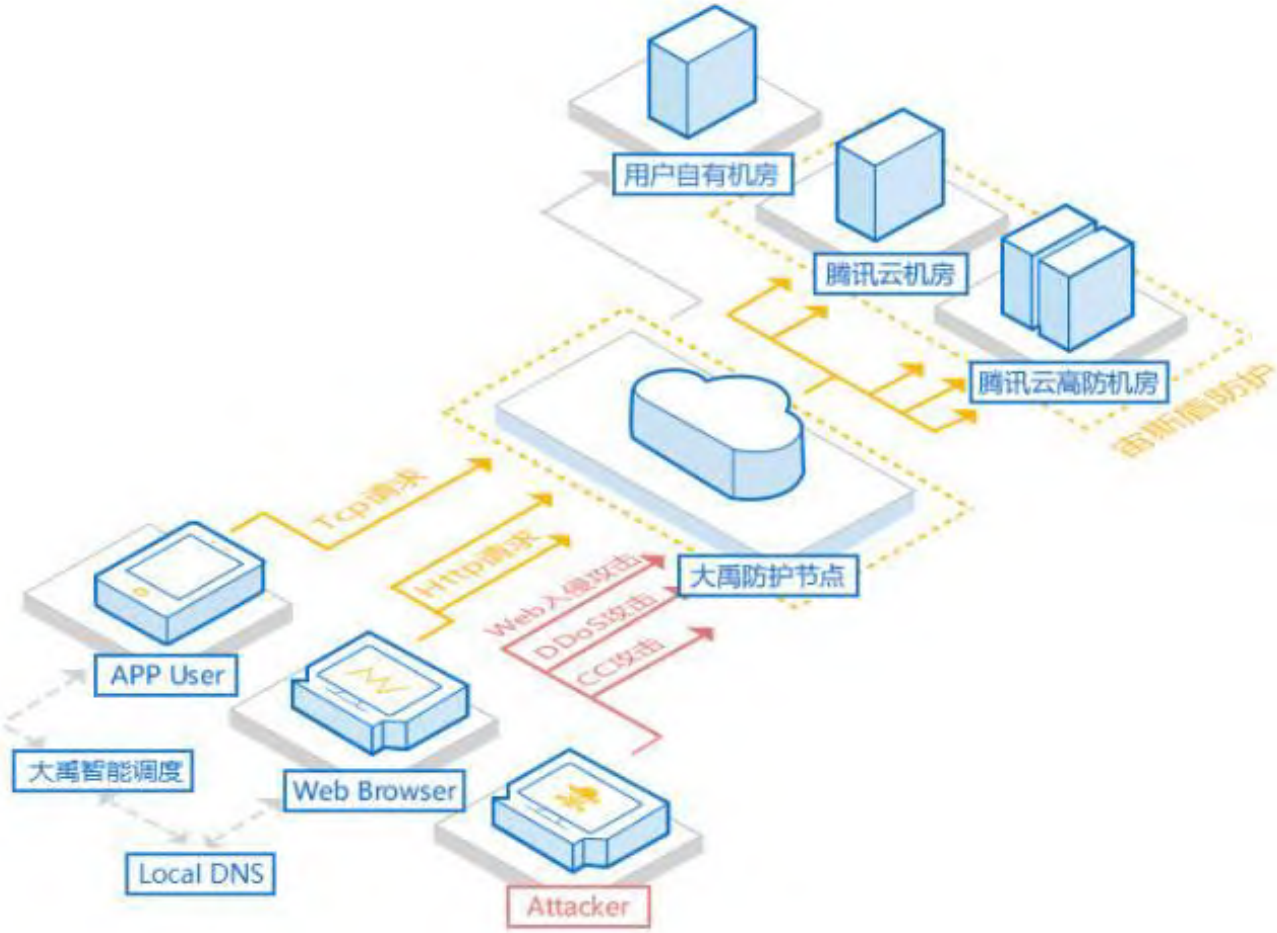


不能满足需求！

DDoS对抗

2.0版本——分布式防御

- DNS调度
- CDN抗流量攻击



DDoS对抗

防护总带宽xT

全国部署节点100+

通过全网调度对抗攻击流量

云上的风险——业务安全对抗

业务安全对抗

1 帐号与虚拟财产

帐号
Q币
装备

2 关系链

欺诈
画皮

3 金钱

支付
金融

业务安全对抗

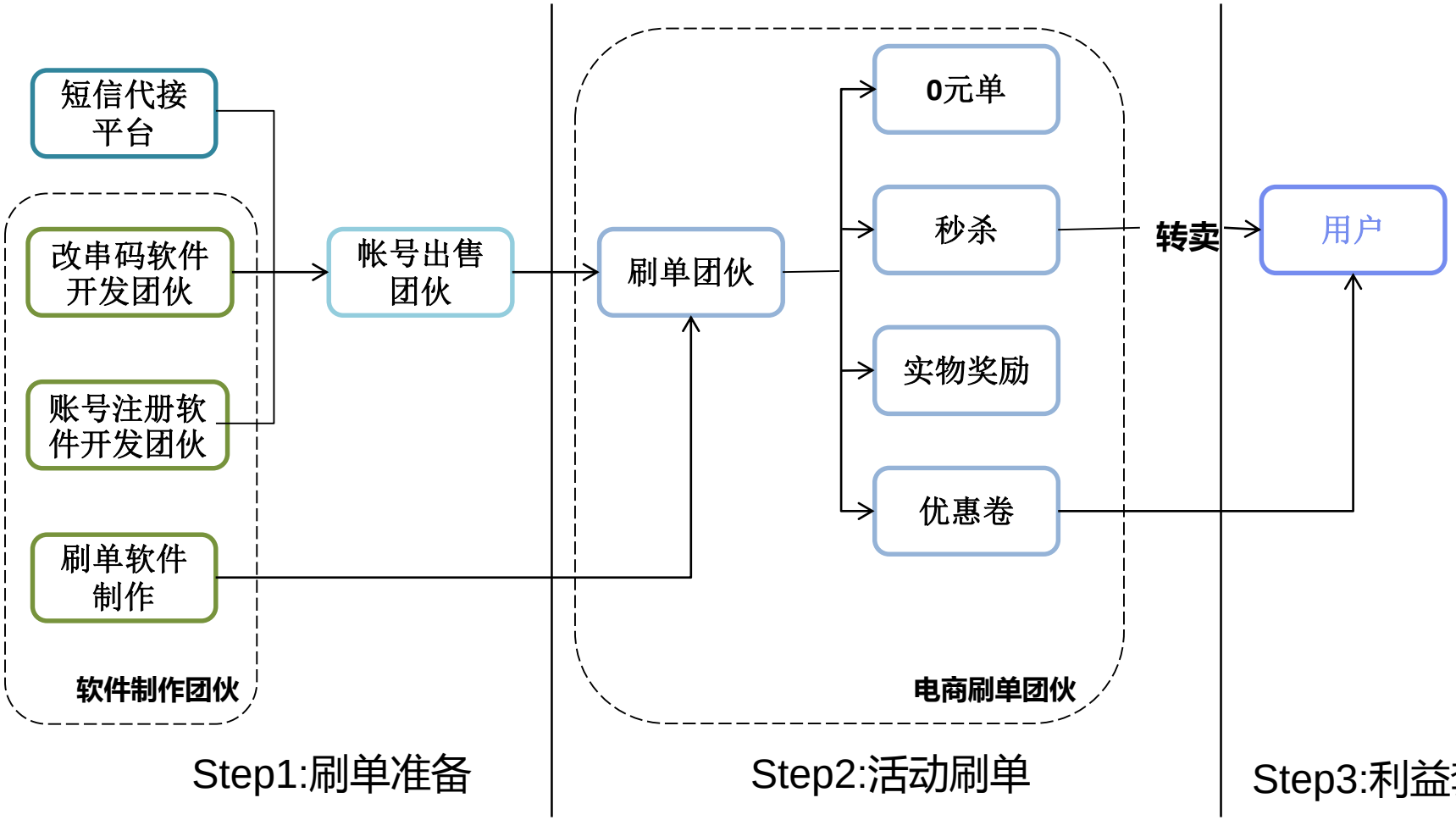
一个案例

某电商平台为提升品牌口碑，斥巨资筹办一次0元抢购活动。就在活动刚开始时，大批羊毛党利用自动化软件开始批量刷取活动资源，导致正常用户无法打开网页，持续30分钟以上。待用户可以正常访问网页时，发现优惠商品已被羊毛党抢购一空。一时间论坛、微博吐槽声一片。

业务安全对抗

电商行业放血式补贴催生大量羊毛党：20W！

业务安全对抗

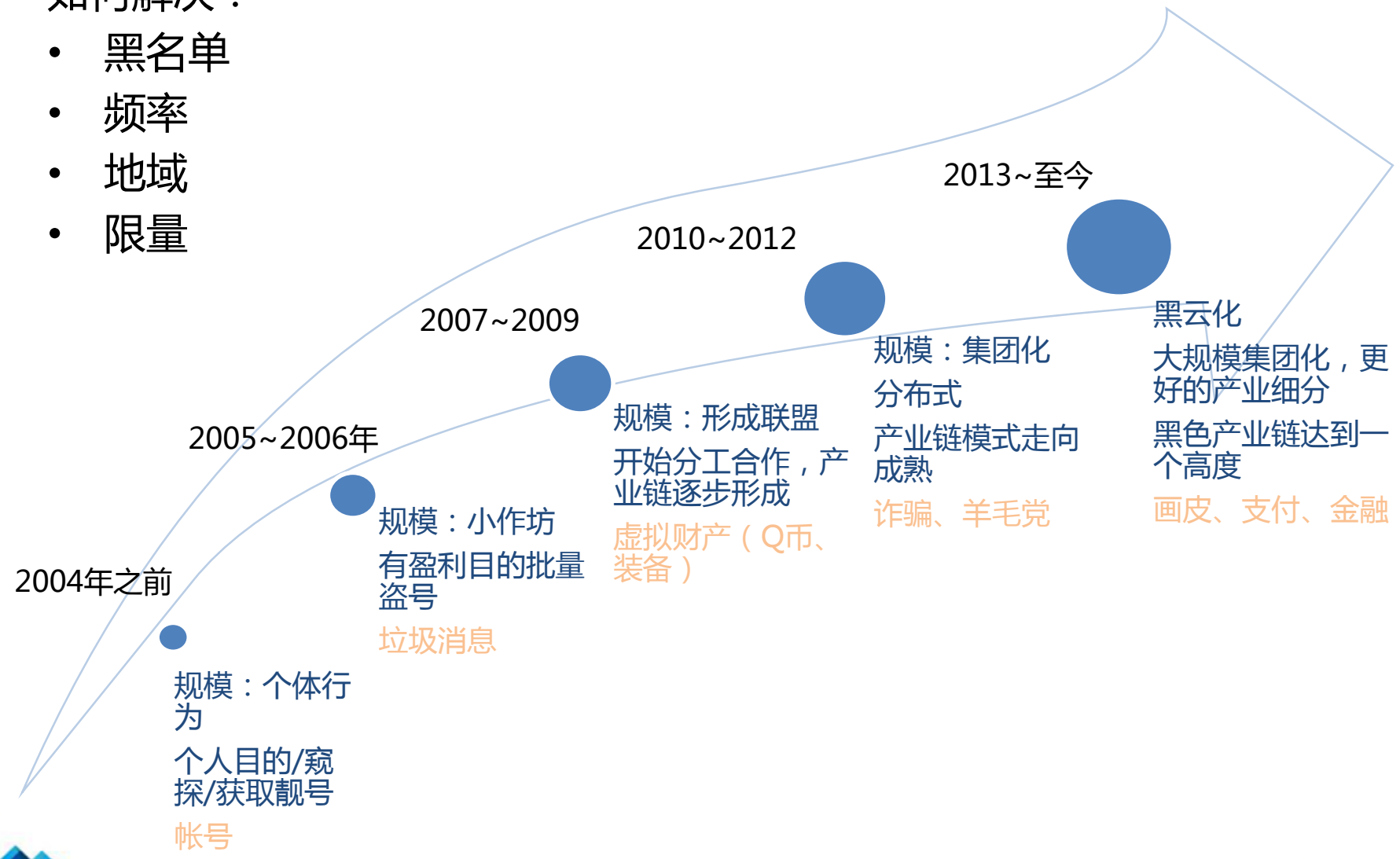


细化的产业分工，让刷单门槛低、专业化

业务安全对抗

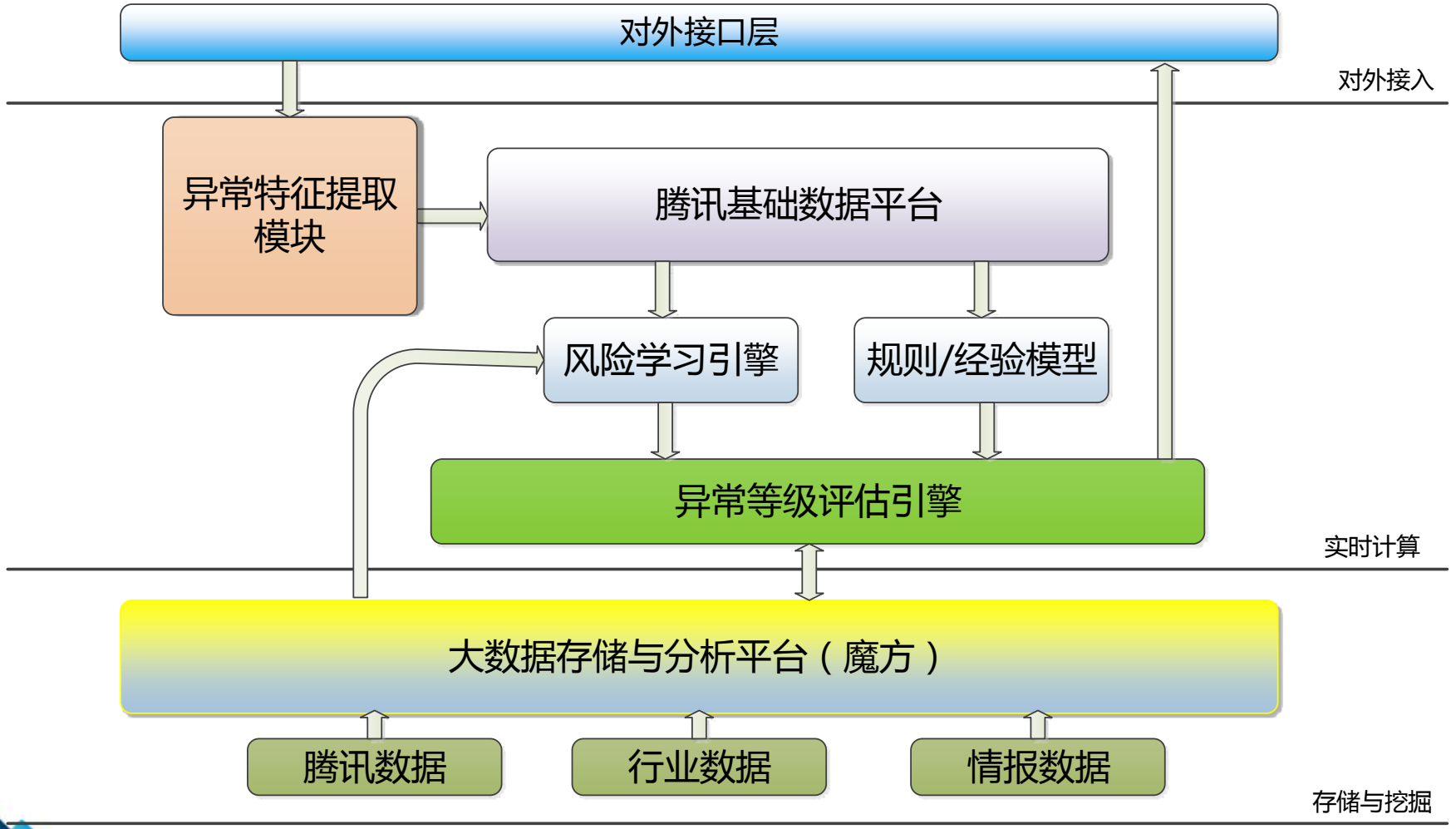
如何解决？

- 黑名单
- 频率
- 地域
- 限量

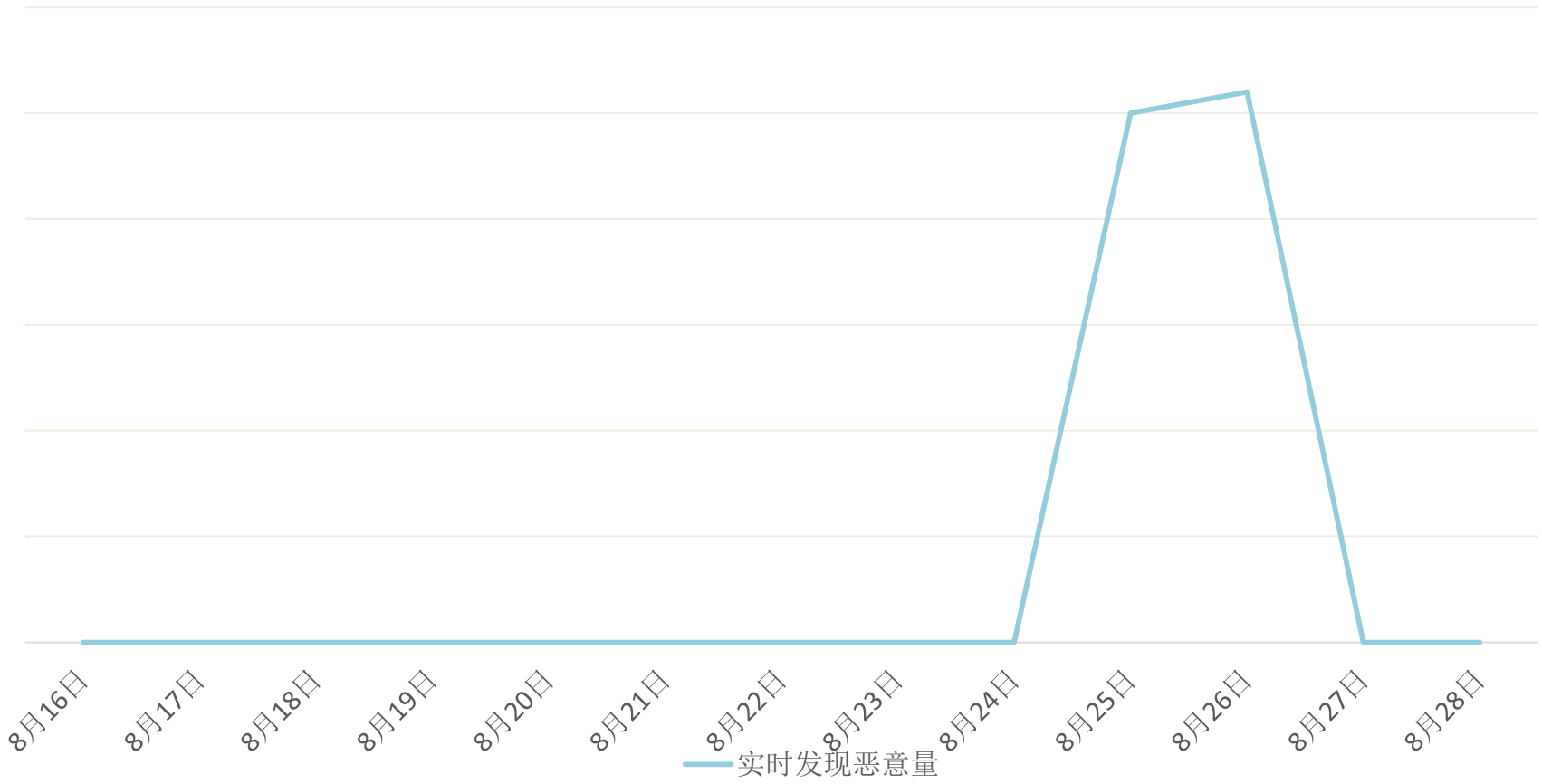


业务安全对抗

解决方案——安全大数据



业务安全对抗



从25日活动开始，到27日活动结束，帮助聚美优品成功**拦截20万恶意**帐号，挽回经济损失**800万**

总结

大禹4.0

久经考验的网站安全防护专家

天御

为业务安全保驾护航

运维安全

- DDoS防护
- DNS劫持监控
- 应急响应
- 漏洞扫描
- 入侵检测
- APP漏洞审计
- 情报
- WAF
- 数据保护
- 黑客画像
- 威胁感知

业务安全

- 黑名单库
- 高危用户识别
- 实时身份确认
- 用户画像
- 设备指纹
- 监控雷达
- 多维风控体系
- 信息修复
- 关系网络
- IP地址检测
- 人脸识别

Thanks!