

从甲方到乙方

腾讯

云安全实践之路

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
UETUE

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
UETUE

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



旧金山 伦敦 北京 圣保罗 东京 纽约 上海
San Francisco London Beijing Sao Paulo Tokyo New York Shanghai

QCon

全球软件开发大会

2016年4月21-23日 | 北京·国际会议中心

主办方 **Geekbang** & **InfoQ**
极客邦科技

7折 优惠 (截至12月27日)
现在报名, 节省2040元/张, 团购享受更多优惠

www.qconbeijing.com



扫描获取更多大会信息

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

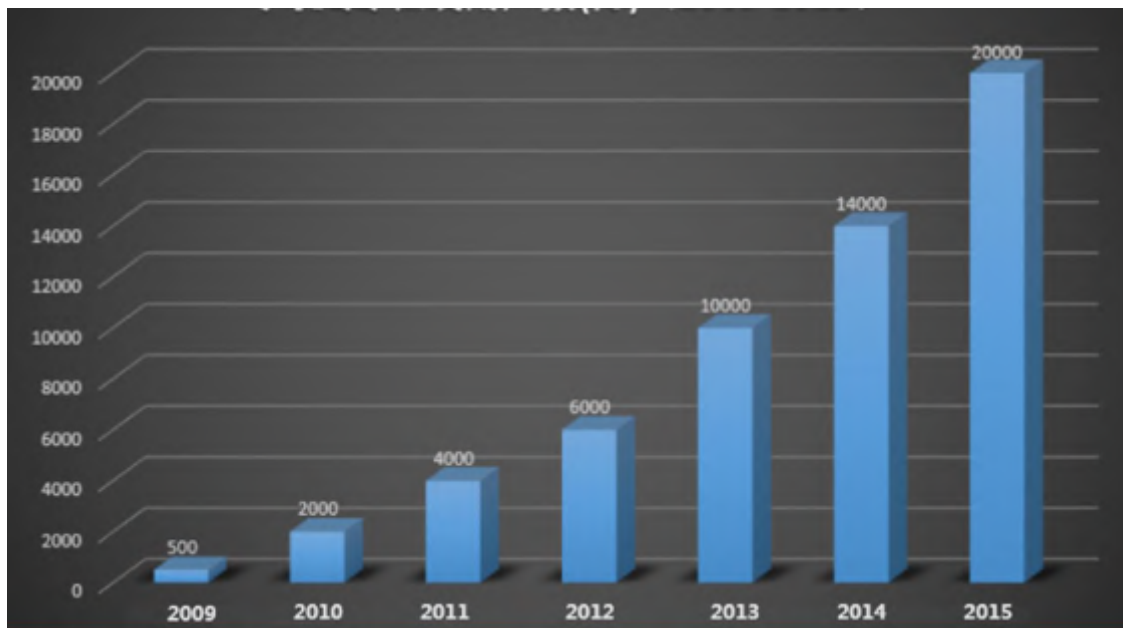
- 面临的挑战
- 云上的安全风险
- DDoS对抗
- 业务安全对抗
- 总结



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](#)

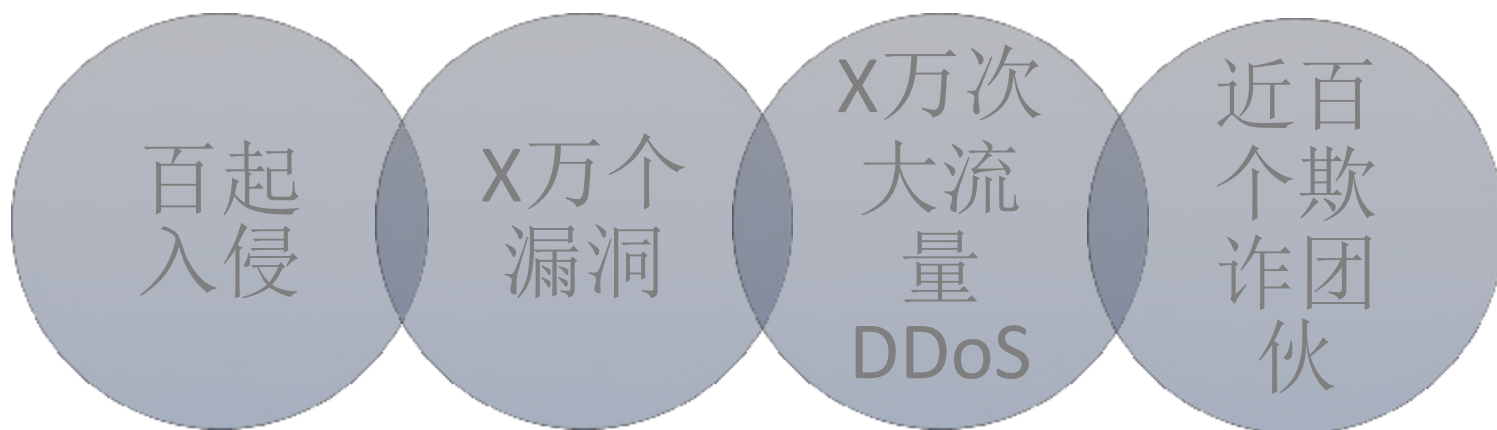
↑ 收起 | 🔍 查看大图 | ↶ 向左旋转 | ↷ 向右旋转

```
https://[redacted]
https://[redacted]/js/pan/base/base-init.js/a.php

/*! * PAN Management UI * Copyright(c) Palo Alto Networks, Inc. */ // re
blank image Ext.BLANK_IMAGE_URL = 'imgget.php?Ext.namespace('Pan.ba
(function() { var msgCt; function createBox(s, t) { return [
:
:
: //
:
: t,
:
: s,
:
: ].join(''); } // we need it in each of the top level esp files so that
called from the // save.esp file after a commit is done. Johnny said to
instead of // in each of the top level index.php files. If we put it her
accessible everywhere. window.checkPendingConfigChanges = function() {
```

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



QQ安全中心

AQ.QQ.COM 在线生活,安全护航



云安全

提供多重可靠防护

免费安全保护

您在购买腾讯云服务后,只需开启想要的安全服务,即可免费享受相应的安全保护。

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



反欺诈——保
用户利益

抗DDoS——保
障服务可用

云上的风险——DDoS对抗

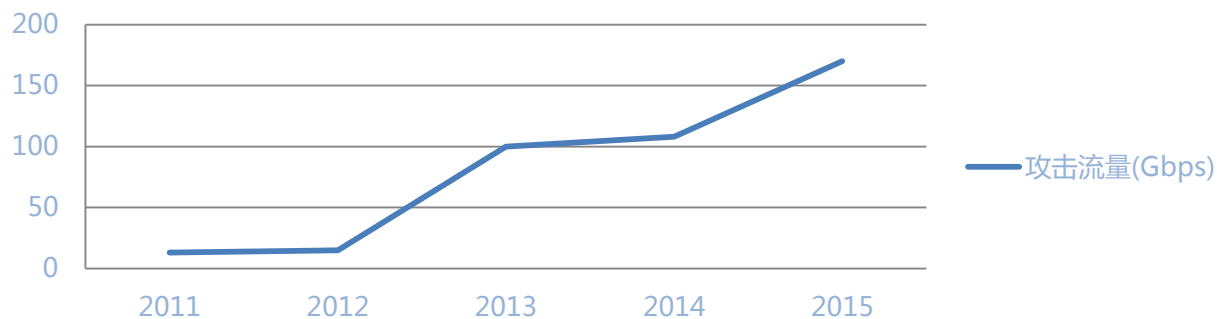
DDoS对抗

DDoS愈来愈频繁

- 低成本
- 高收益



最大攻击流量趋势



DDoS对抗

自研检测防护能力——宙斯盾

规模：机架级<1G
对手：内部作恶
单机版，检测能力有限，无清洗能力

规模：机房级10G
对手：小流量
Syn / udp
流量镜像，分布检测，购买清洗设备

规模：机房级20G
对手：中等流量攻击
单机多核处理 + 自研清洗设备

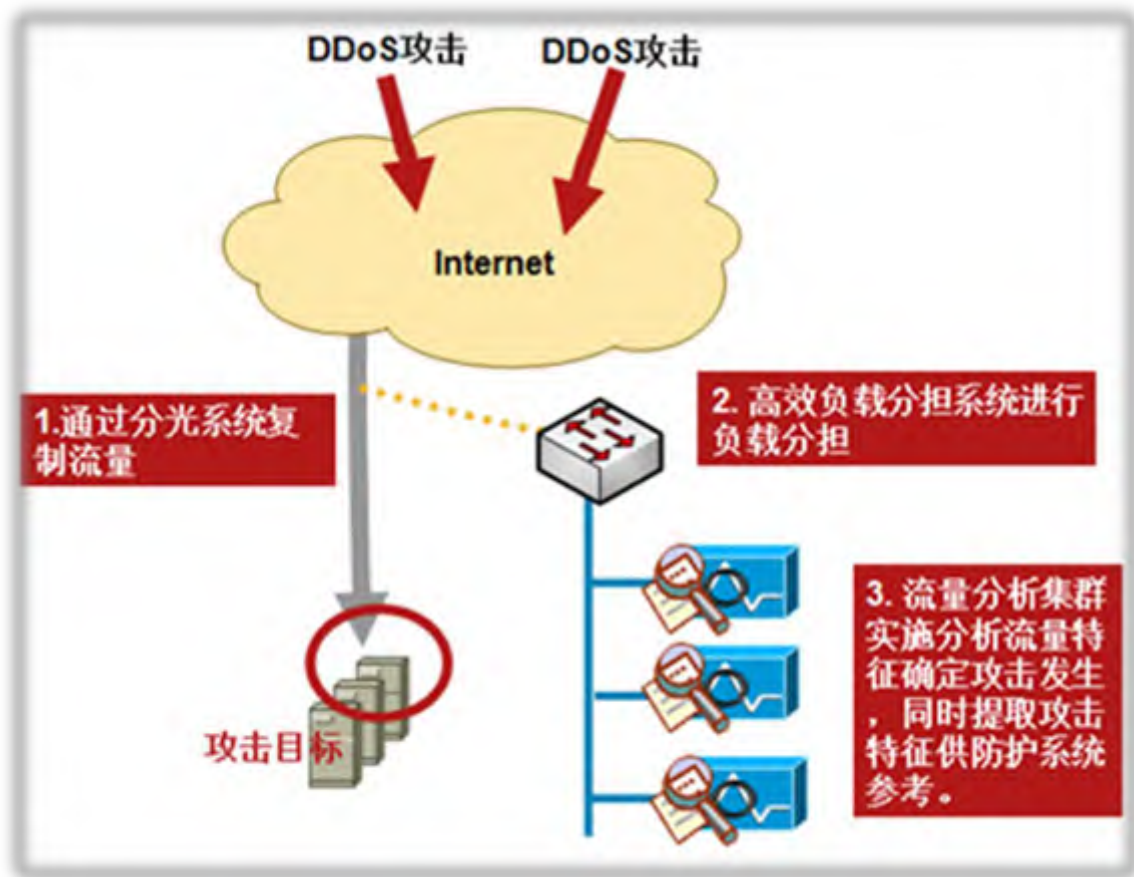
规模：地区级>100G
对手：大流量攻击
应用层防护能力

DDoS对抗

1.0版本——基于机房的对抗

- 带宽瓶颈
- 防护短板

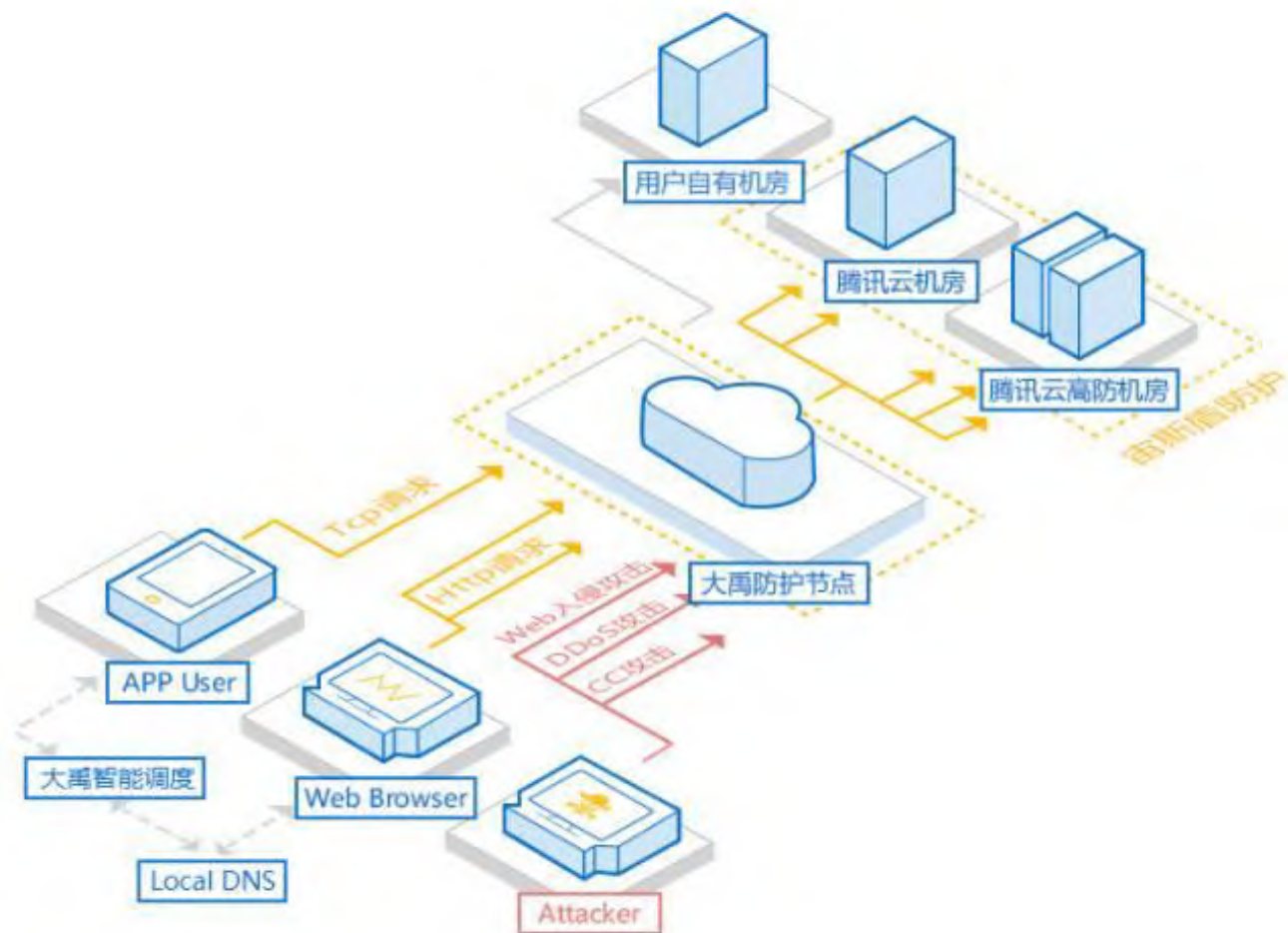
不能满足需求！



DDoS对抗

2.0版本——分布式防御

- DNS调度
- CDN抗流量攻击



DDoS对抗



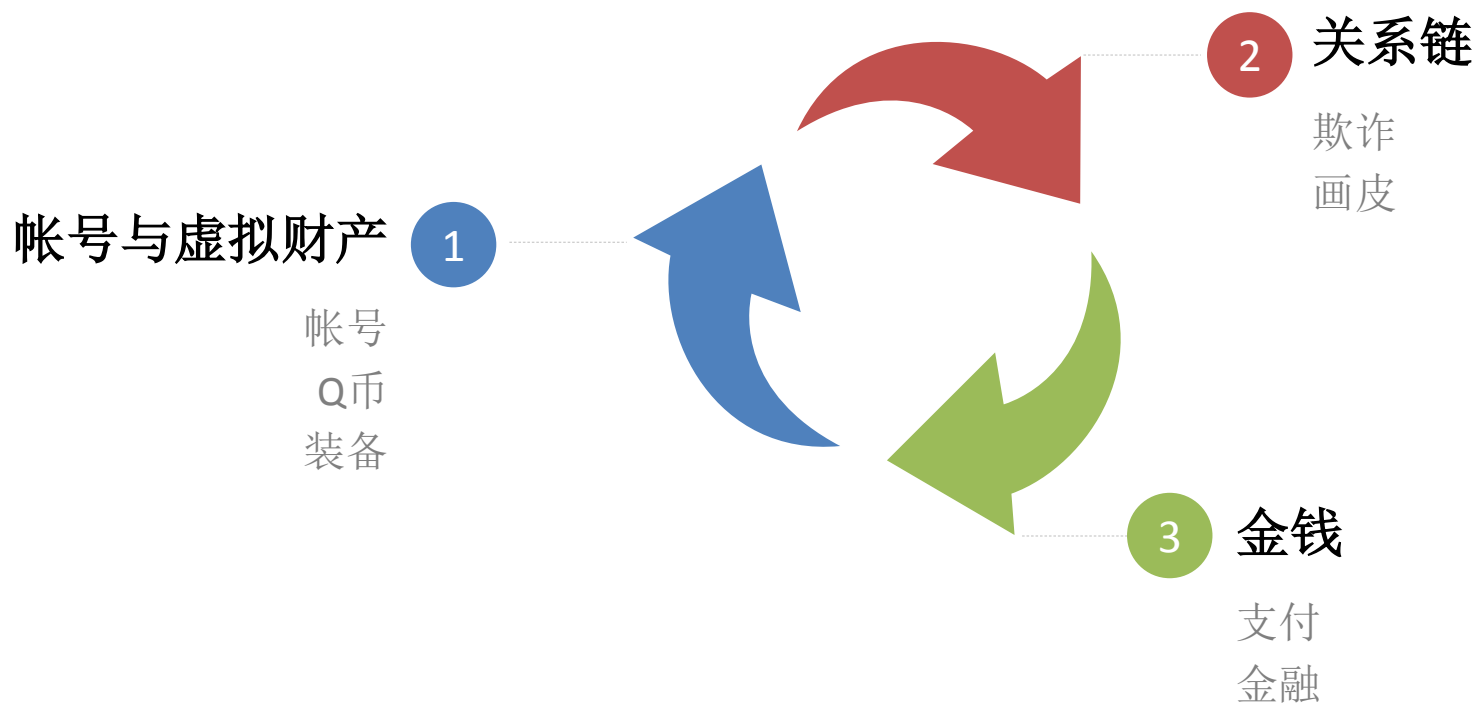
防护总带宽**xT**

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



业务安全对抗

一个案例

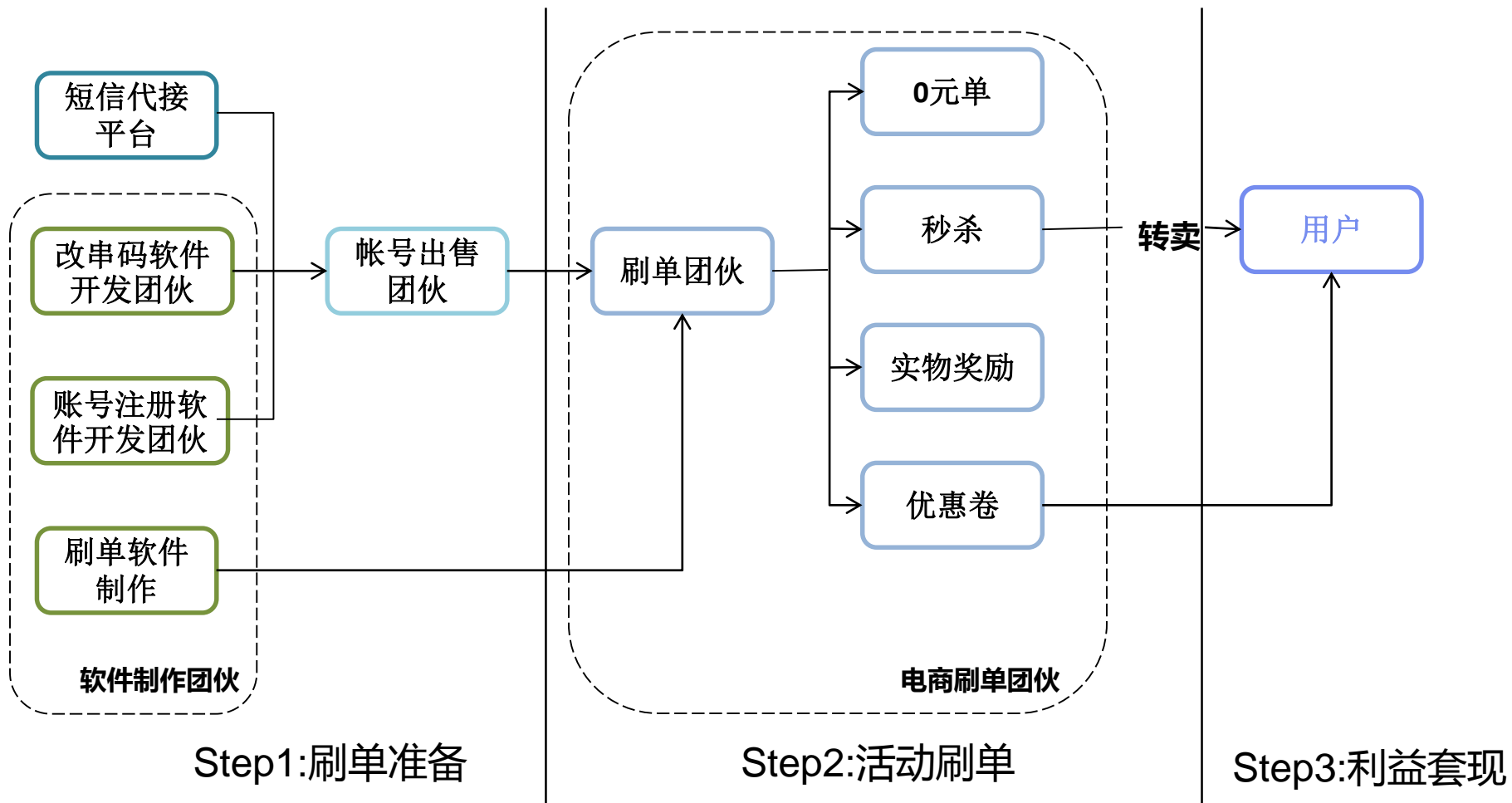
某电商平台为提升品牌口碑，斥巨资筹办一次0元抢购活动。就在活动刚开始时，大批羊毛党利用自动化软件开始批量刷取活动资源，导致正常用户无法打开网页，持续30分钟以上。待用户可以正常访问网页时，发现优惠商品已被羊毛党抢购一空。一时间论坛、微博吐槽声一片。

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

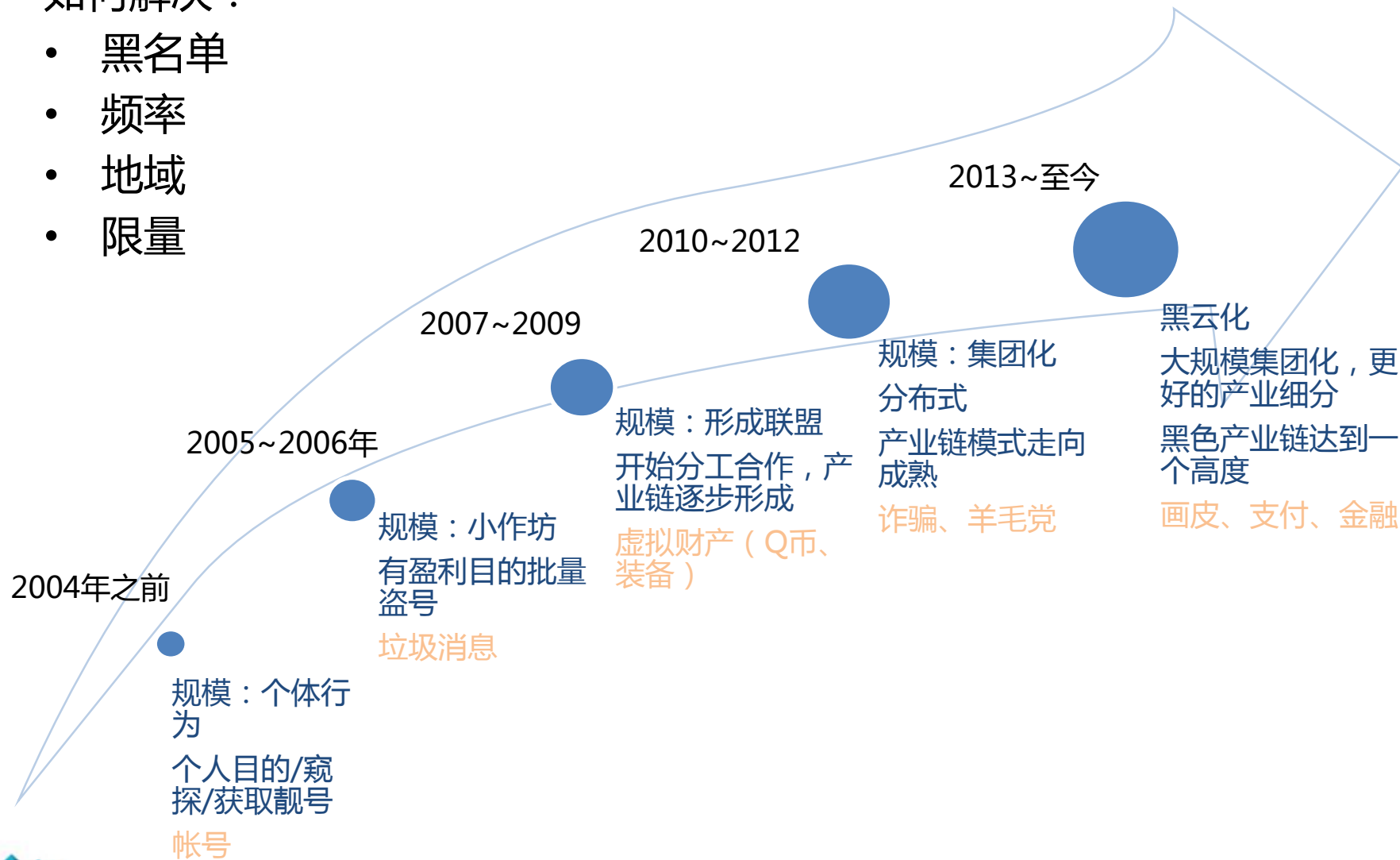


细化的产业分工，让刷单门槛低、专业化

业务安全对抗

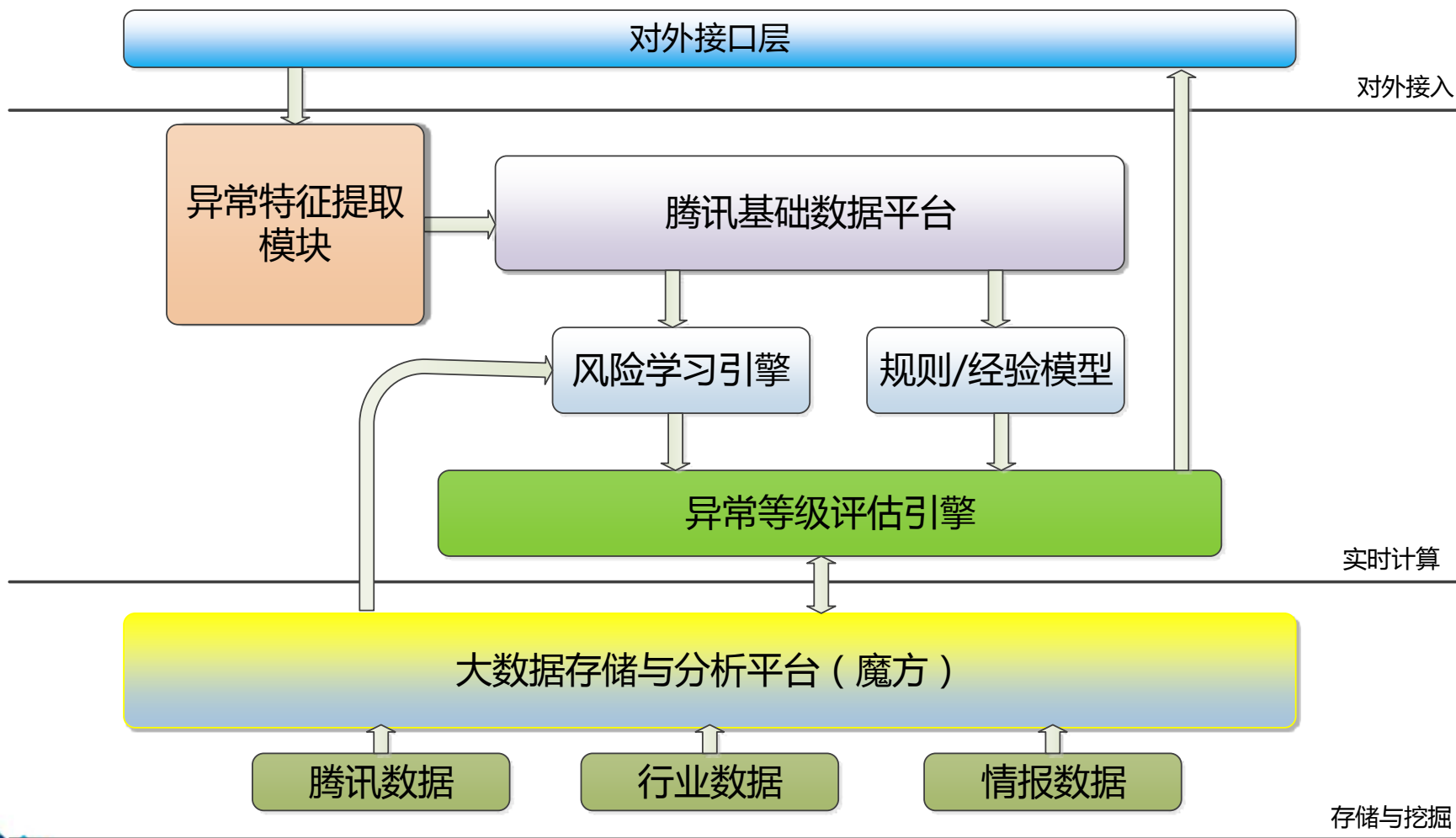
如何解决？

- 黑名单
- 频率
- 地域
- 限量

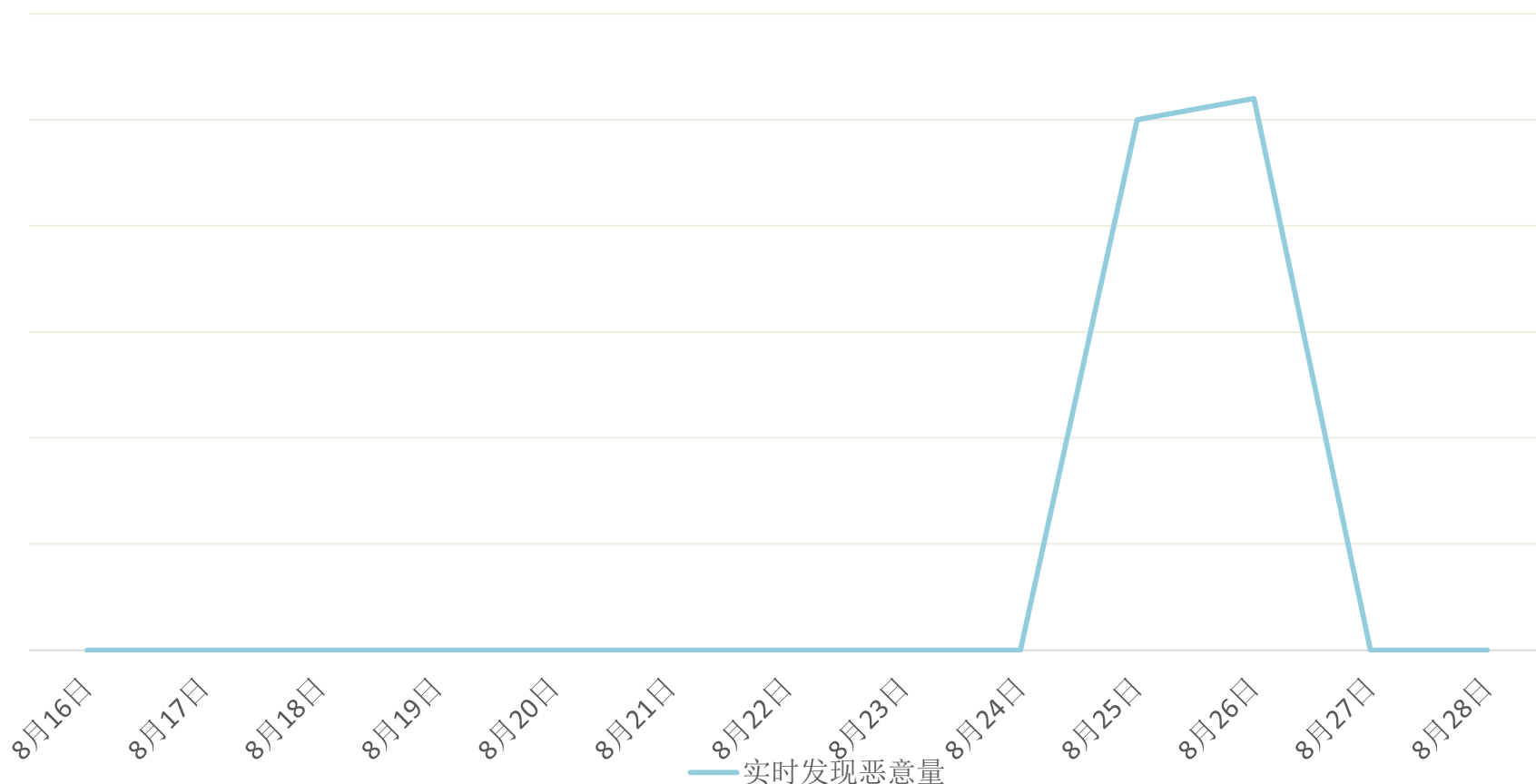


业务安全对抗

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!

