营销风控的创新实践及安全之道

腾讯云安全-周斌

new trend
new technology
new application

Cloud + community
Developer conference

面对黑产攻击，安全应该思考什么

每年因为安全事件导致巨额损失

国内每天恶意流量影响 **600万+**用户	国内每天新增病毒影响 **1000万+**用户	每天因病毒暗扣话费 **1000万+**人民币	暗夜DDoS攻击团伙 **流量峰值达462G**
		国内“黑产”从业人员 **100万+**	移动APP漏洞超 **60%** 中高危风险
国内恶意推广影响超 **1000万+**人次	国内手机恶意应用每天影响 **100万+**人次	流氓行为手机病毒 **16.98%**	资源消耗手机病毒 **32.26%**
		恶意扣费手机病毒 **28.29%**	隐私获取手机病毒 **20.4%**
国内每天发生流量劫持 **2000万+**次	国内“黑产”每天影响用户 **2000万+**人次	每天新增广告病毒变种 **200+**个	每天新增病毒 **2000+**个

安全从不是一个点，而是一个面

全链路的智慧业务安全

全链路的智慧业务安全 产品和引擎

业务层

电商 | 智慧零售 | 游戏 | 直播 | 银行 | 支付 | OTA | O2O

链路协同

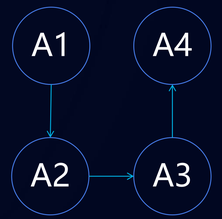
云端风控 ⇄ 威胁感知 ⇄ 移动安全

产品层

流量反欺诈 | 营销风控 | 金融反欺诈 | 身份认证 | 威胁感知 | 移动安全 | 图像识别 | 消息过滤

AI层

系统引擎

团伙挖掘	知识图谱	行为序列分析	威胁自动感知
			

策略

账号类别识别	身份识别
小号 盗用账号	自动机识别 社工平台 人脸交叉验证
养号 黑产用户	黑产挖掘

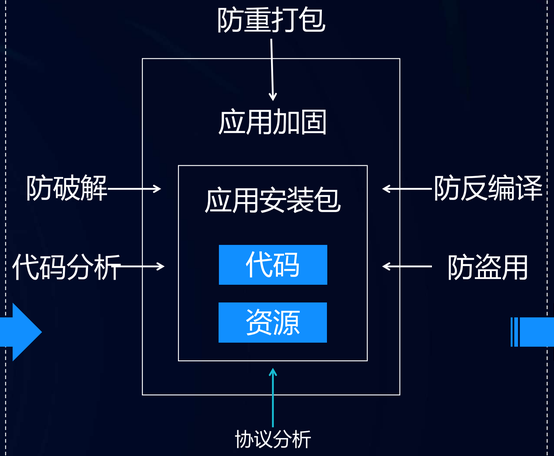
全链路的智慧业务安全 移动安全防护

移动安全组件

安全组件

- 白盒秘钥
- SDK安全沙箱
- H5应用与小程序安全沙箱
- 病毒扫描SDK
- 伪基站检测
- 恶意wifi检测
- 恶意URL检测

移动应用加固



移动应用加固

- 安卓APP加固
- 安卓SDK加固
- 安卓源码混淆
- SO库加固
- IOS源码混淆
- 手游防篡改加固

移动应用安全监测

- 应用代码风险检测
- 应用漏洞扫描
- APK包敏感信息检测
- 系统权限检测
- 应用功能测试
- 应用兼容性测试

可持续安全运营

- 移动应用质量监测
- 移动应用盗版监测

全链路的智慧业务安全 威胁情报

腾讯云 | 连接智能未来

威胁情报抓取

蜜罐系统

威胁情报分析

情报解析

- 猎狩人群
- 攻击链识别
- 团伙识别
- 攻击方法挖掘
- 身份识别
- 元数据抽取

黑产情报识别

人工智能

- 分类算法
- 实体抽取
- 聚类算法
- 无监督学习
- 深度学习
- 图挖掘算法

全链路识别

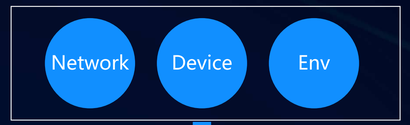
- 风险注册识别
- 风险账号识别
- 风险登录识别
- 风险交易识别

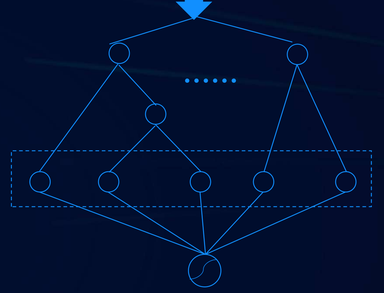
全链路拦截策略

- 注册保护
- 登录保护
- 限制权限
- 限制交易

全链路的智慧业务安全 云端风控

腾讯云 | 连接智能未来





多层专家系统

假机

云端联防

身份识别

设备关联

网络检测

网络分析

流量分析

终端监控

应用解析

系统分析

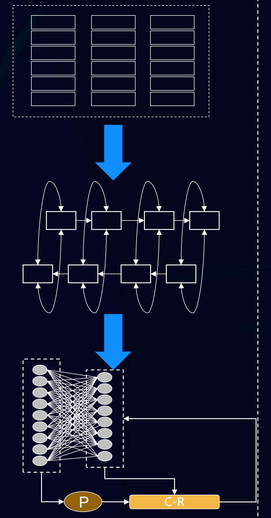
真假机用户

超维特征结构

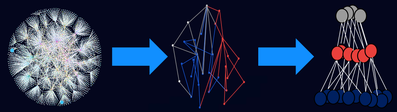
异常检测

染色跟踪

可信度识别



真用户假行为



黑产群体切分

黑产骨干识别

黑产角色识别

真行为假动机

CPM\CPC
- 虚假曝光
- 虚假点击

CPA
- 批量注册
- 批量登录
- 恶意刷券

CPS
- 众包下单
- 商家刷单

安全不是一成不变 而是“动静”辩证发展

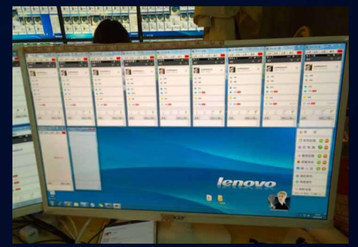
静：伪造正常流量，黑产在不断进化

黑产初阶手段

猫池　验证码识别器

模拟器批量挂机

自动接码平台



黑产中阶手段

手机墙——群控——伪造留存

黑产高阶手段

病毒木马

静默下载、安装

积分墙、网赚等众包

动静 辩证发展： 以 静 自动应对“动”的黑产伪装

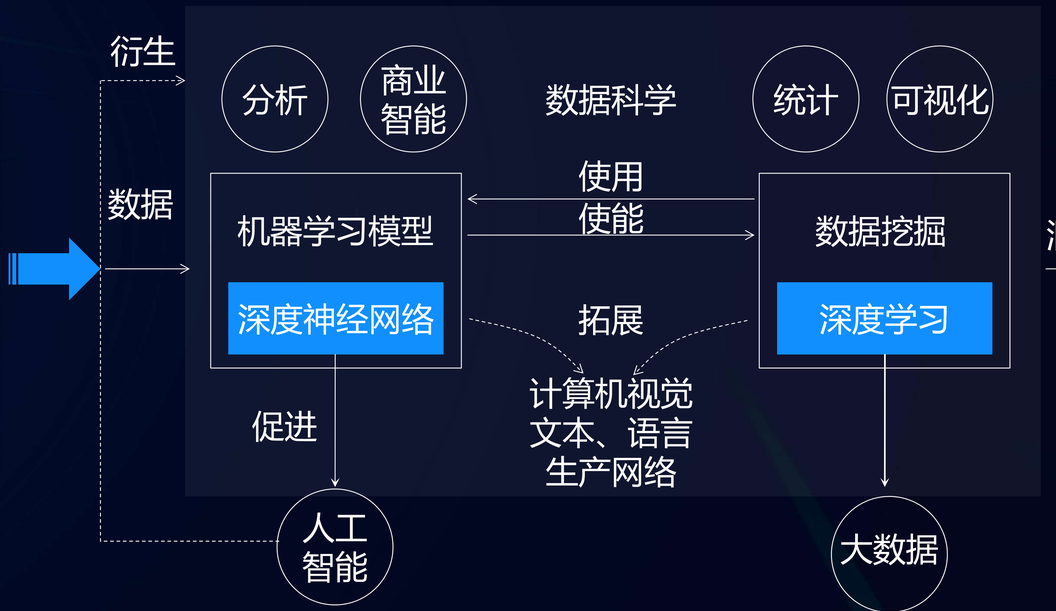
试图伪装成
分布式的正常用户

大量分散的IP

大量分散的设备

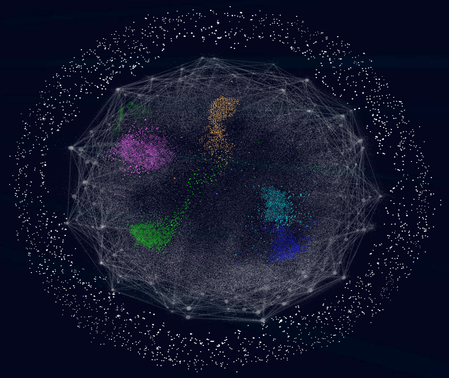
大量毫无相关的手机号

天御AI风控系统

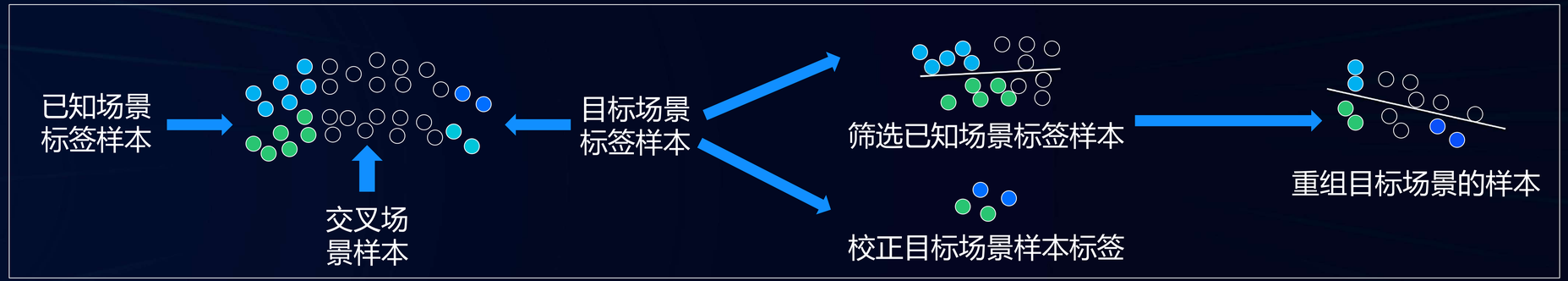


洞察

伪装终究难以完全拟人化
在行为和数据模型中呈现
区别正常的离散化



动静 辩证发展： 以 静 自动应对“动”的场景



安全在营销场景的实践

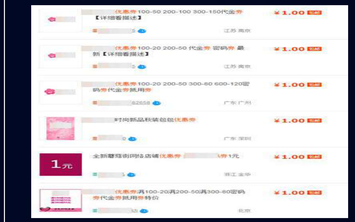
营销全链路安全服务

营销宣传

虚假曝光　虚假下载　恶意注册

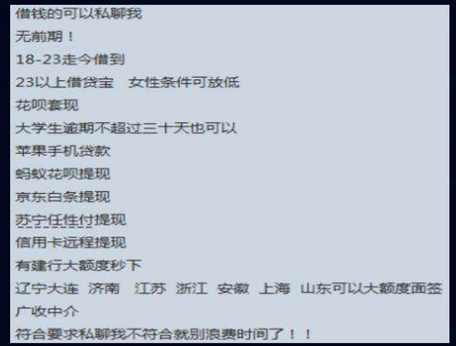
营销活动

薅羊毛　刷分享　黄牛订单



营销结算

资金盗用　消费贷欺诈

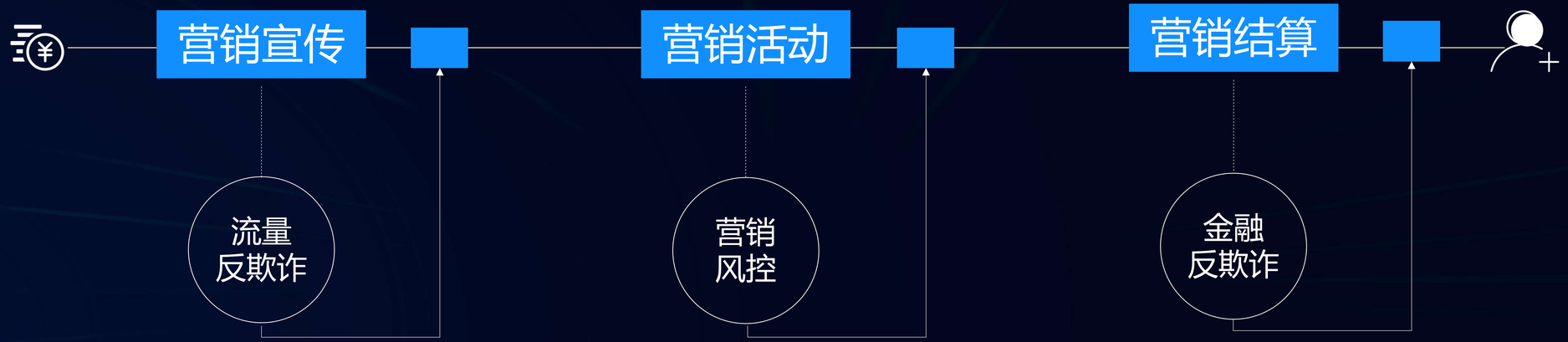


流量反欺诈　渠道反作弊

羊毛党防护　网赚防护　黄牛党防护

资金防盗刷　金融反欺诈

营销风控实践应用



•宣传阶段把采买的流量通过云API的形式，发送给天御，过滤虚假流量。

流量欺诈分

>80分 虚假

•防止营销资金被“牛马羊”薅取

•保证营销数据去伪存真

•防止客户资金被盗用

•防止消费贷逾期风险

金融欺诈分

>80分 欺诈

每年可为接入企业

节省超千万的营销资金

安全不仅是黑产对抗，更是云信心的基石

信心的基石

腾讯云 | 连接智能未来

国内首家

CISPE数据保护行为准则认证，中国第一家云服务商获得此认证；
能有效帮助提升云服务商遵循GDPR要求的合规程度。

国内首家获得ISO 27001:2013信息安全管理体系认证的云服务商

国内首家在云计算领域获得ISO9001 CNAS（中国合格评定国家认可委员会）和ANAB（美国注册机构认可委员会）双认可的云服务商。

国内权威认证

网络安全
等级保护

可信云
服务认证

ITSS云服务能力
增强级认证

大数据产品
能力认证

国际权威认证

CSA STAR
云安全
管理体系认证

ISO 27018
公有云
个人信息保护认证

ISO 27017
云服务信息安全管理
体系认证

ISO 20000
信息技术服务管理
体系认证

ISO 22301
业务连续性管理
体系认证

SOC 1&2&3 Type
II审计

PCI DSS
支付卡行业数据
安全标准

MPAA
美国电影协会
最佳实践标准

THANKS

new trend
new technology
new application

Cloud + community
Developer conference