C3安全峰会
CYBER | CLOUD | COMMUNICATION

百度安全能力及生态建设

韩祖利

百度安全产品中心

C3安全峰会
CYBER | CLOUD | COMMUNICATION

我们有一个安全生态的共识

开放心态、开放交流、开放合作

百度安全
Baidu Security

用户面临着更大的威胁

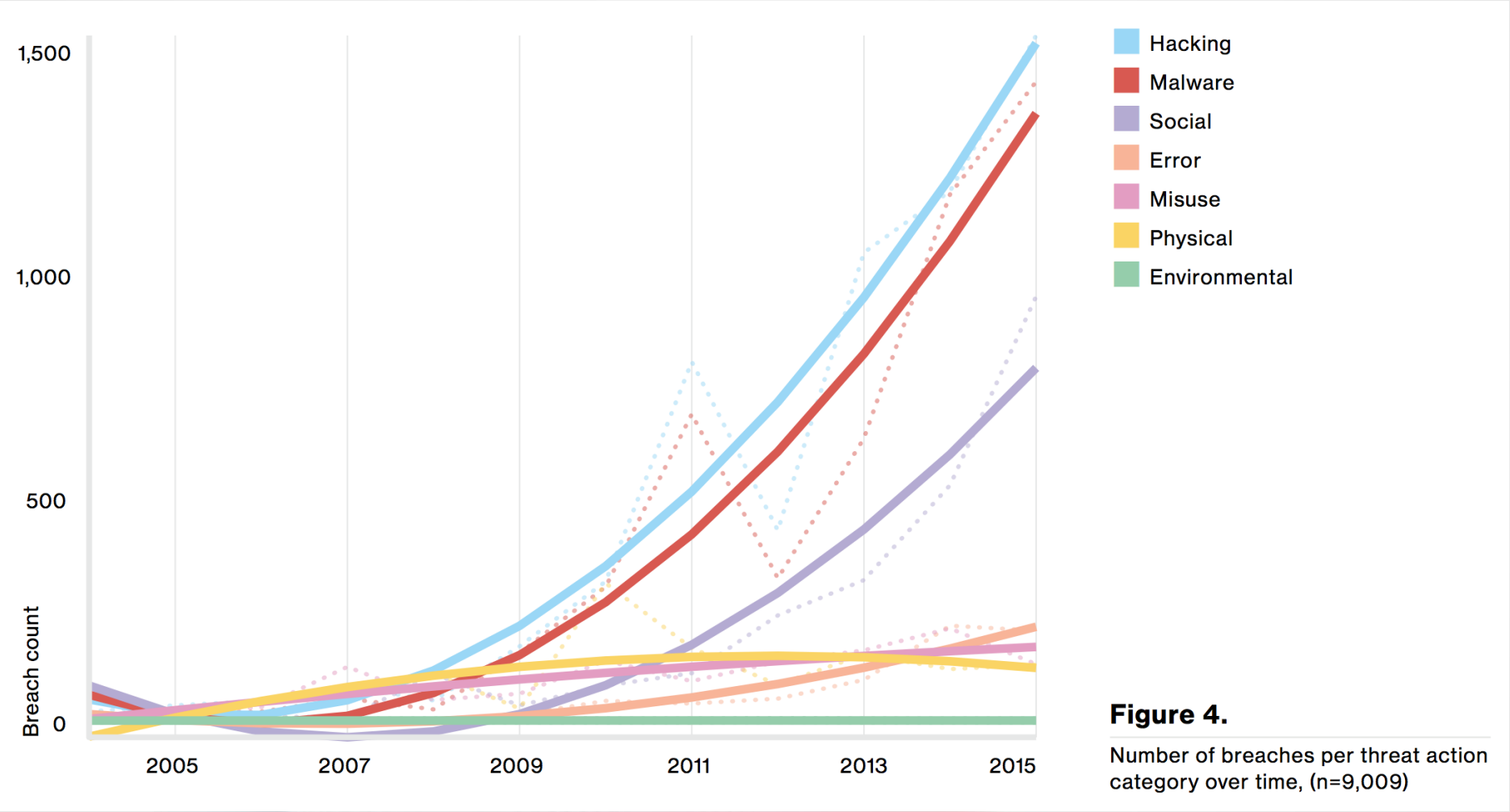


Figure 4.

Number of breaches per threat action category over time, (n=9,009)

数据来源：Verizon 2016 Data Breach Investigations Report

用户面临着严重的威胁

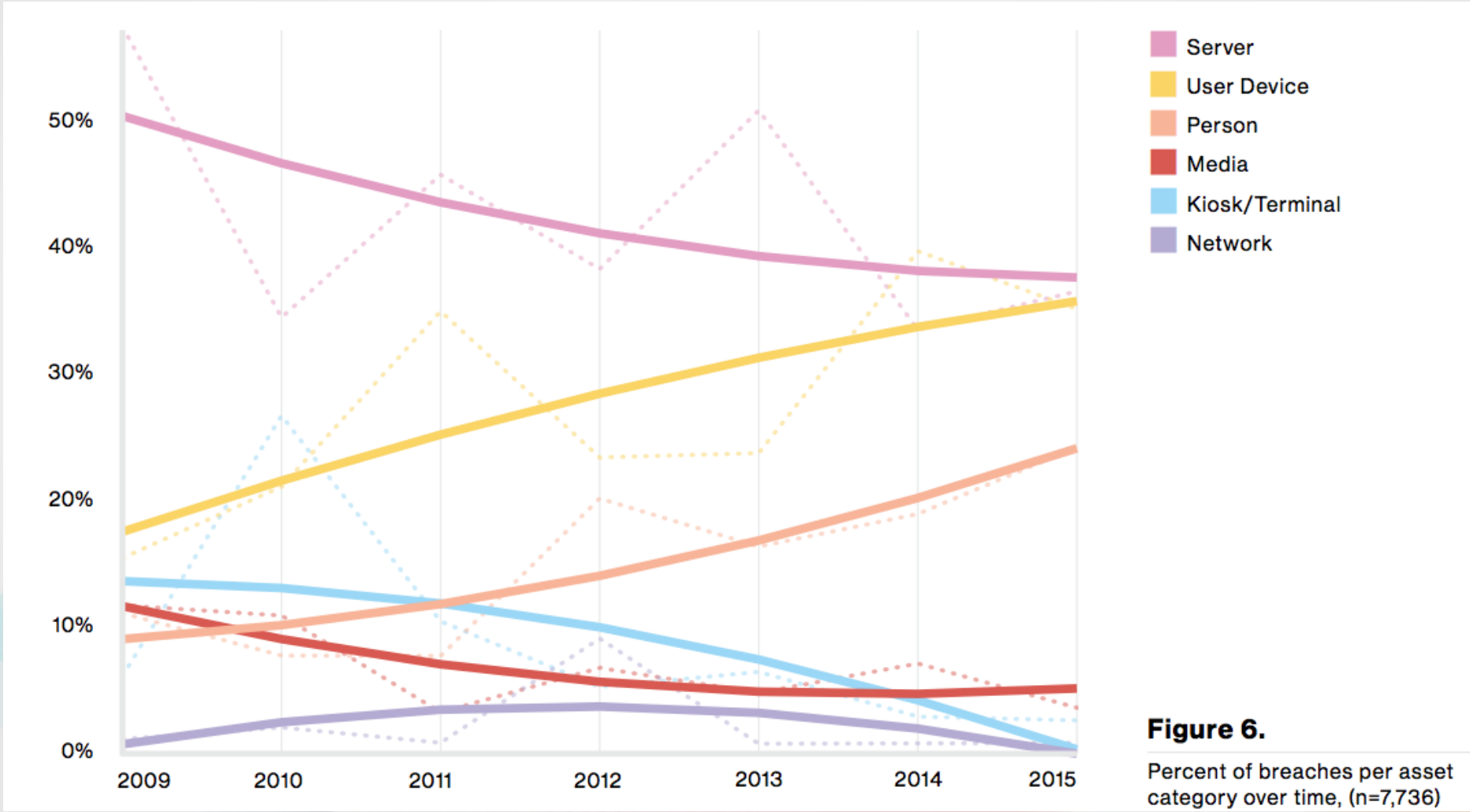


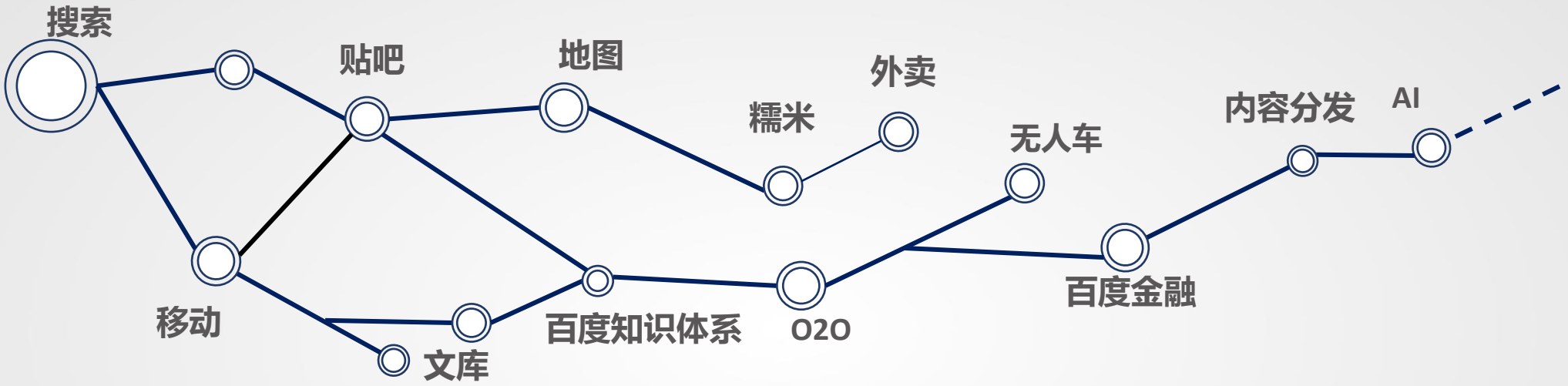
Figure 6.

Percent of breaches per asset category over time, (n=7,736)

数据来源：Verizon 2016 Data Breach Investigations Report

百度的安全现状

风险伴随百度业务发展



- 复杂的业务线
- 用户群体广泛
- 大规模敏感数据

→

- 试手的首选
- 黑灰产的首选
- 每个业务都被紧盯

→

- 网络与信息安全
- 业务&内容安全
- 企业&行业安全

复杂业务场景下的最佳实践

每天拦截无数次黑客攻击，每周拦截有组织的APT钓鱼邮件1.76万封，每年找到上千个内部安全漏洞。


威胁感知


漏洞扫描


内容监测


加固


手机模拟器识别


设备指纹


抗DDos


WAF


主机防护


DNS反劫持


反病毒引擎

ooo

- 网络
- 应用
- 系统
- 数据

基于业务的安全

搜索结果检查

百度索引的内容检测

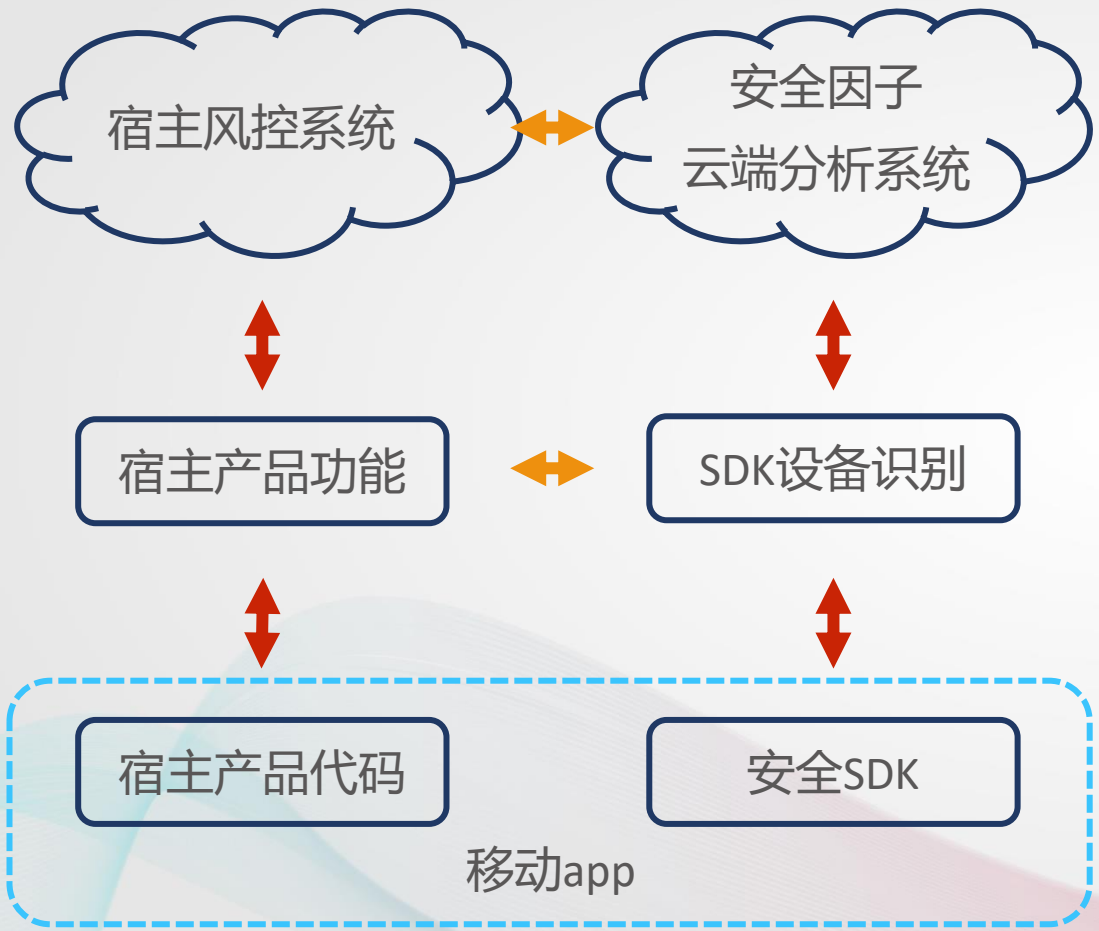
用户网络劫持

保证用户使用百度业务

业务风控

防止业务被非法利用

移动端反黑产引擎



- 实时分析系统，在云端风险评估
- 与云端安全通讯，防止窃取、劫持
- 本地通过安全因子的识别对业务行为进行决策
- 几十K的体积
- 资源占用率极低
- 仅仅采集安全数据

对外输出的安全产品

个人安全

百度杀毒、百度卫士、手机卫士等

累计保护亿级用户

企业安全

简单可依赖的云端安全

灵活健全的百度安全实践方案

公众安全

伪基站、危险WiFi、欺诈地图

帮助全国公安破获几百起电信犯罪

开放战略

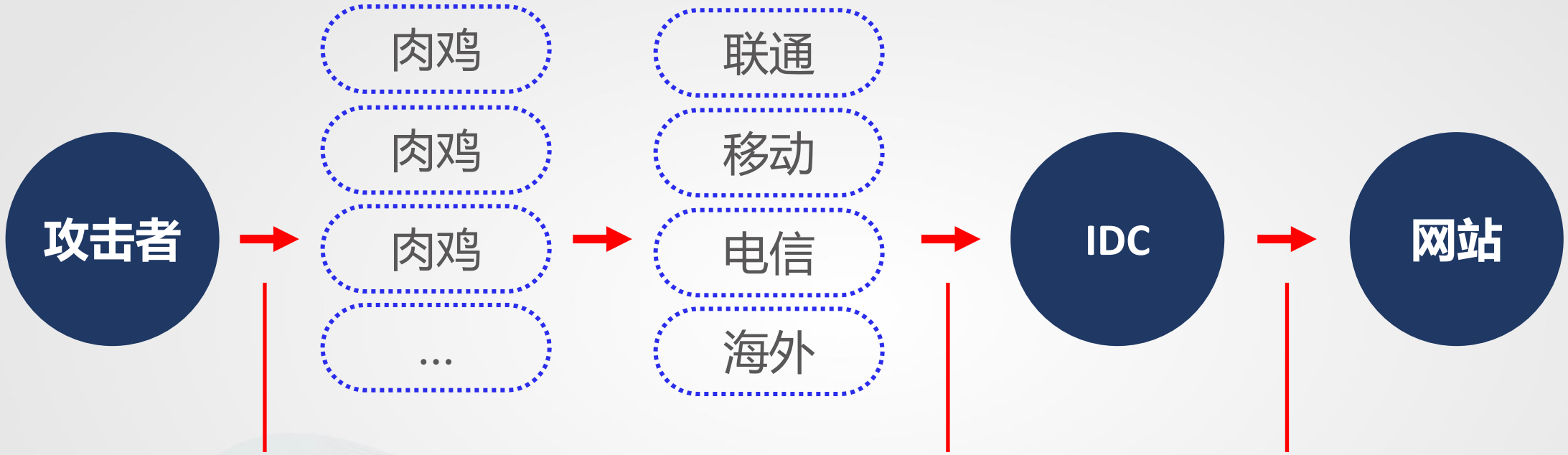
聚焦 + **开放** + **探索**

- 精简产品
- 必要的产品

- 输出&引入能力
- 赋能合作伙伴

- 基于AI安全
- 探索数据安全

优势能力 – 抗DDoS



- 攻击预警

有可能在大规模攻击前2分钟发现攻击

- 调度与清洗

1T调度能力，实施镜源封堵

400G云端清洗能力

- 本地清洗

本地清洗引擎

优势能力 – 移动杀毒

- **APP恶意代码扫描**
  - 针对Android应用扫描
  - 自动提取特征码，发现应用的恶意代码
- **支持多种插件扫描**
  - 广告插件
  - 支付插件
  - 敏感行为
- **仿冒App检测**
  - 网盘、论坛、企业网站
  - 钓鱼网站等非典型渠道

移动杀毒引擎

- **移动杀毒软件**
  - 多家AppStore内APP检测
  - 每日7W-9W新APP检测
- 连续几年AV-TEST满分
- 检测性能行业领先
- 检出率99.99%

C3安全峰会
CYBER | CLOUD | COMMUNICATION

比情报更重要的是分析能力

基于大数据与机器学习的实践

百度安全
Baidu Security

安全生态三步走

C3安全峰会
CYBER | CLOUD | COMMUNICATION

建立信任
交流分享

建立合作
合作共赢

建立生态
融合创造

百度安全
Baidu Security

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Thank You