Threat Intelligence
重塑安全边界

演讲人：谭晓生

职务：奇虎360 副总裁，首席隐私官

日期：2014年9月24日

什么是Threat Intelligence？

- 中文翻译：威胁情报
- “背景”
  - 谁在攻击你？
  - 为什么攻击你？
  - 什么时候攻击的？
  - 怎么攻击的？
  - 攻击是否成功？
  - 损失了什么？
  - 有关联攻击么？
  - 还攻击了谁？

威胁情报对用户的价值

- 发现攻击
- 分析攻击
- 快速响应
- 掌控全局
- 节省成本

威胁情报的基础技术

- 大数据的收集与分析能力
- 攻防知识

威胁情报的分享

- 与谁分享？
- 如何匿名化？

威胁应对

- 如何应对？
- 如何快速应对？

威胁情报商业化服务举例

- FireEye DTI
  - 检测与拦截攻击，匿名交换Web、邮件、文件数据
- FireEye ATI
  - +攻击者的信息与恶意软件的信息，可能的动机，恶意软件的特征
- FireEye ATI+
  - +综合档案、趋势、新闻，攻击目标的有关信息，社区信息共享

威胁情报需要突破的障碍

- 传统信息安全边界造成的信息共享障碍
  - 保密要求
  - 安全考评要求
  - 信任问题

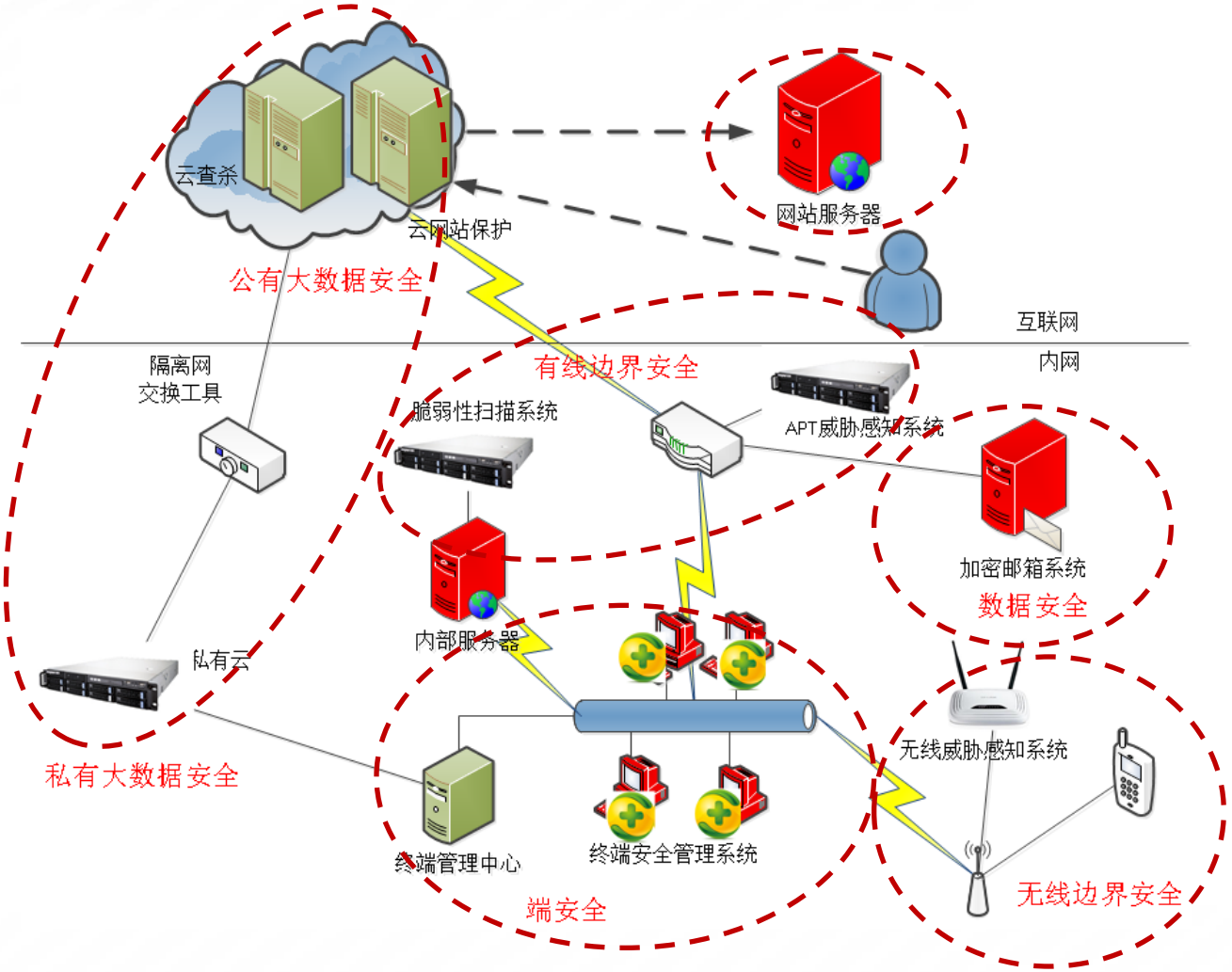
企业信息安全边界在哪里？

- 企业网站
- 企业Wifi
- BYOD
- 智能硬件设备
- 供应链
- 互联网路由
- ……

企业信息安全的新挑战

- 这些安全产品是否可以有效保证企业的信息安全？
  - 防火墙
  - IPS
  - IDS
  - UTM
  - VPN
  - 扫描器

新的安全边界在哪里？


云查杀
云网站保护
网站服务器
公有大数据安全
互联网
内网
隔离网
交换工具
有线边界安全
脆弱性扫描系统
APT威胁感知系统
加密邮箱系统
数据安全
内部服务器
私有云
私有大数据安全
无线威胁感知系统
终端管理中心
终端安全管理系统
端安全
无线边界安全

新的安全边界在哪里？

- 端
  - PC机
  - 手机
  - 智能终端
- 网络（边界、管道）
  - 出口路由器
  - 核心交换机
  - 各种网络安全设备
- 云计算基础架构

中国的威胁情报服务前景

- 中小企业使用基于公有云的威胁情报服务
- 政府与大型企业的外网建立私有云与公有云相结合的行业威胁情报服务中心
- 涉密网建立涉密网内部的威胁情报服务中心
- 威胁情报服务是SAAS（安全即服务）的一个绝佳案例

Thanks!