The 8th China Cloud Computing Conference
第八届中国云计算大会
技术融合 应用创新

企业网络环境主机安全威胁云预警平台建设思路

安天实验室 李柏松

提纲

- 重点行业网络面临的APT威胁
- 中小企业网络面临的勒索威胁
- 企业终端安全威胁的应对策略
- 建设终端威胁预警云平台思路

重点行业网络面临的APT威胁

APT攻击的动机、手段、目标

攻击动机

- 政治
- 军事
- 经济
- ……

Advanced 高级性

- 相对被攻击一方面而言
- 使用较新的攻击手段
- 利用0-Day漏洞、通信加密、U盘摆渡……

Persistent 持续性

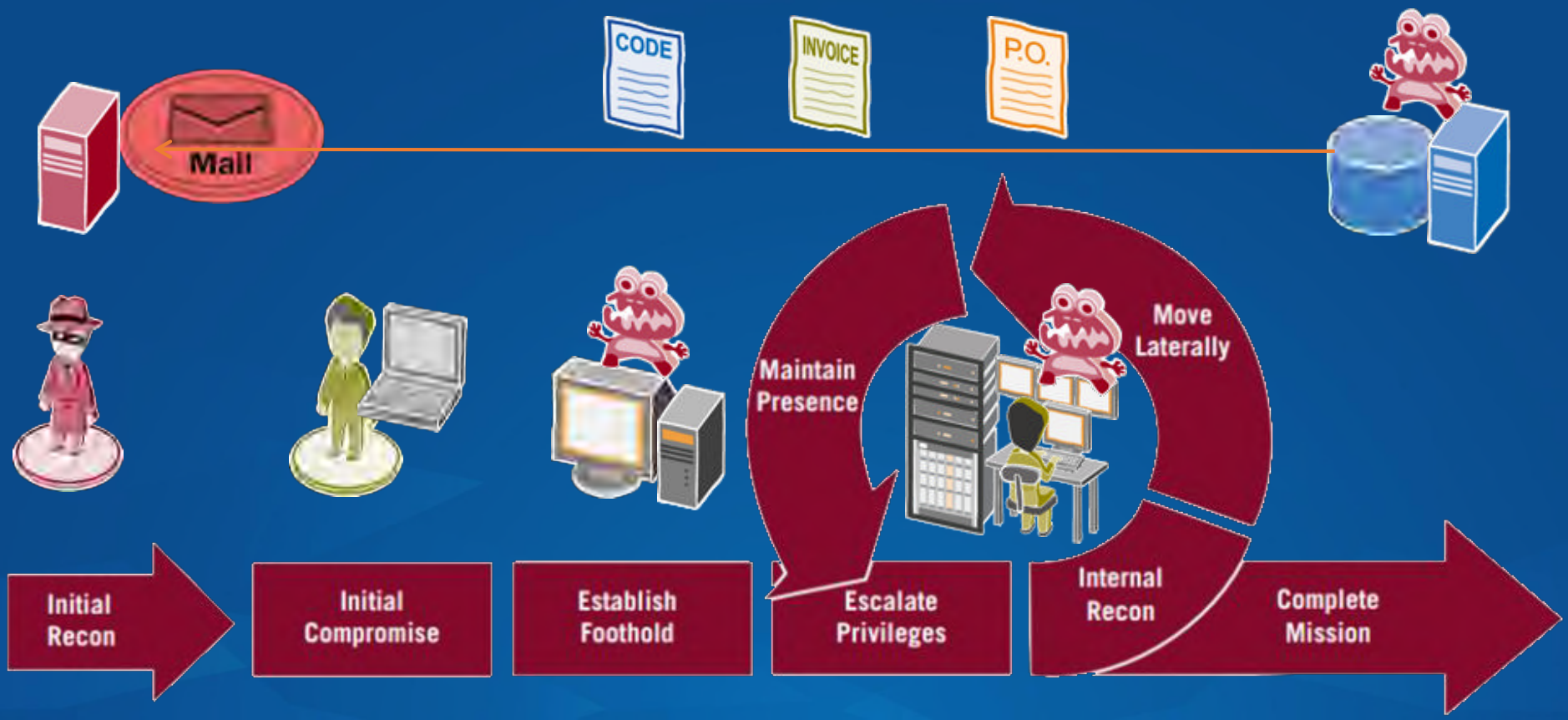
- 相对普通攻击时间而言
- 攻击时间较长
- 隐蔽通信、横向移动、条件触发……

Threat 威胁

- 具有针对性
- 造成敏感信息泄露
- 长期被攻击者控制

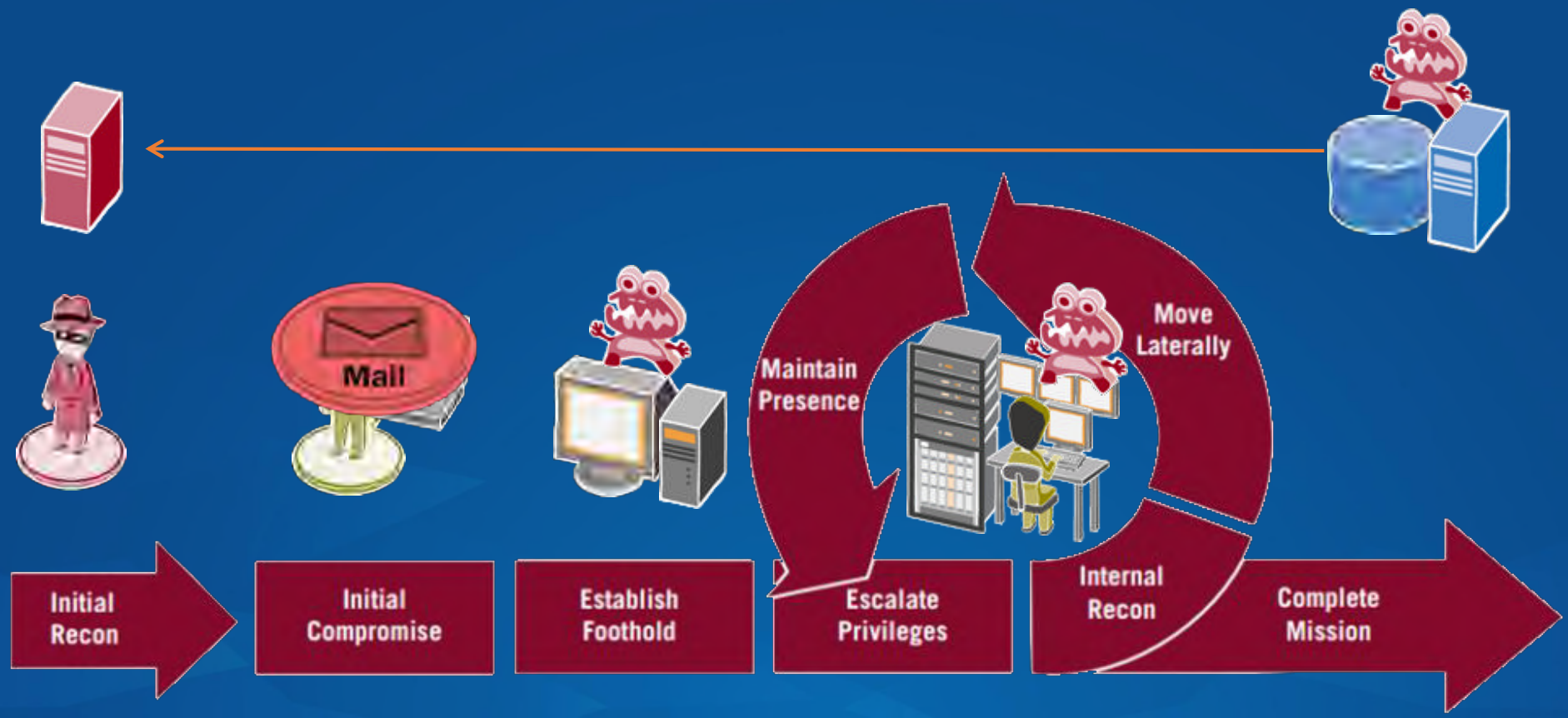
重点行业网络面临的APT威胁

APT攻击一般过程



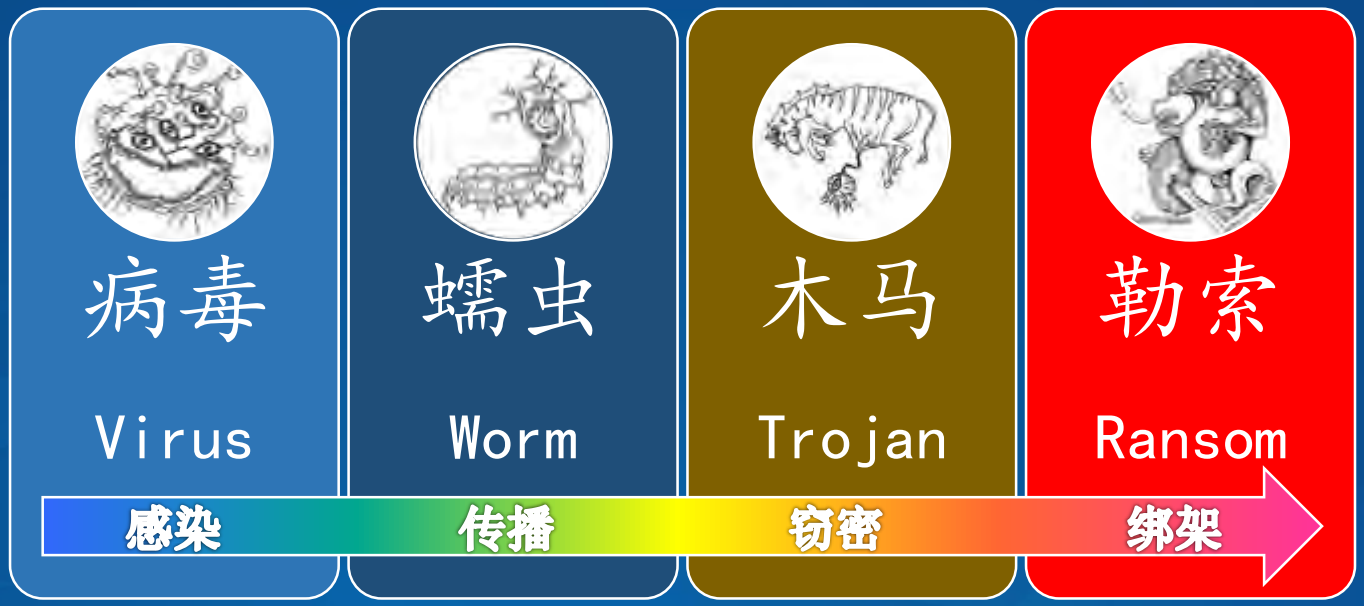
重点行业网络面临的APT威胁

APT攻击的检测



中小企业网络面临的勒索软件威胁

- 病毒、蠕虫、木马到勒索软件

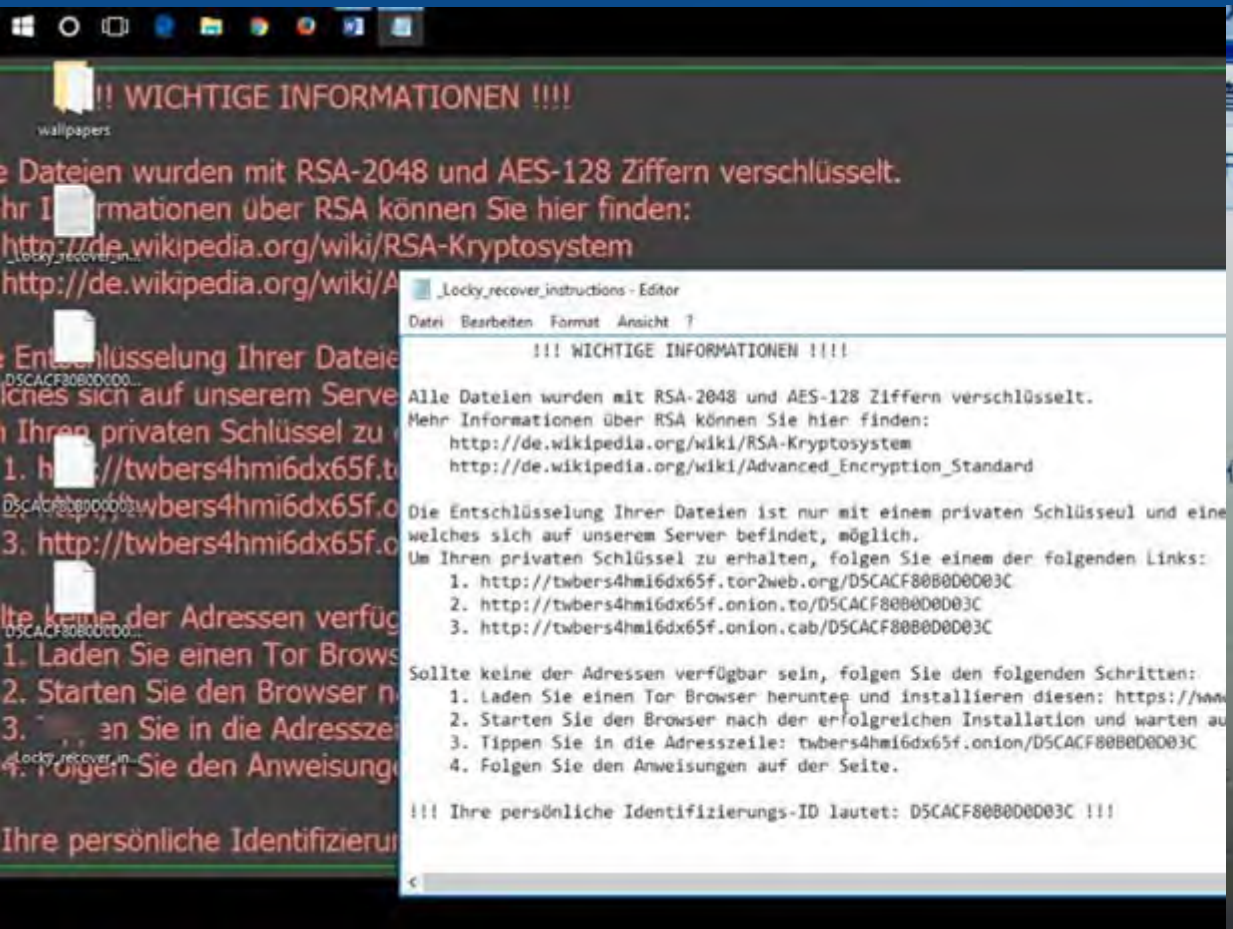


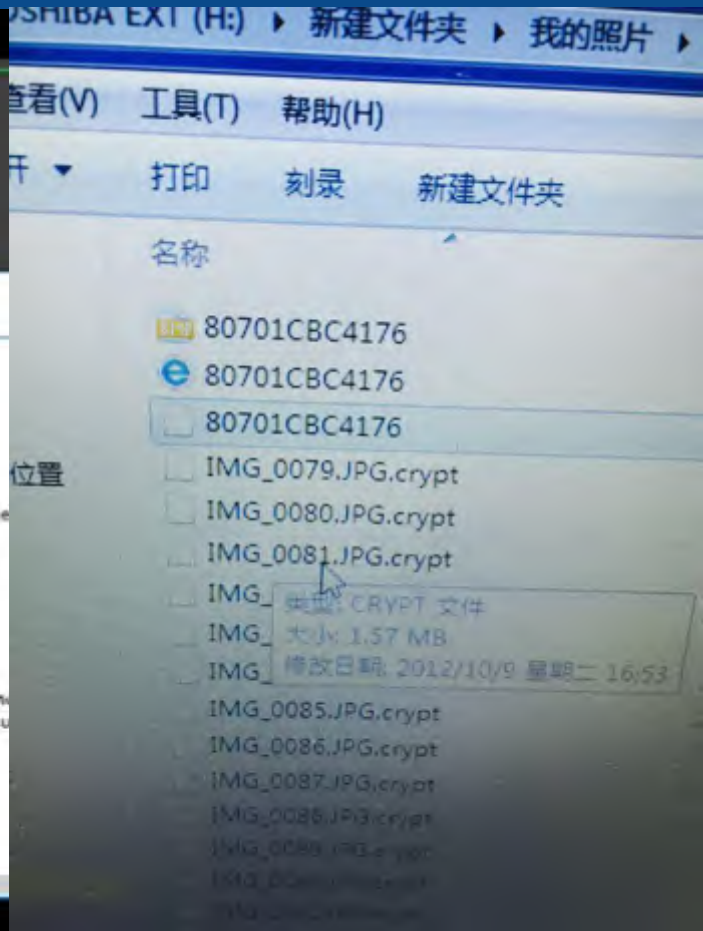
中小企业网络面临的勒索软件威胁

- 感染过程

中小企业网络面临的勒索软件威胁

感染现象

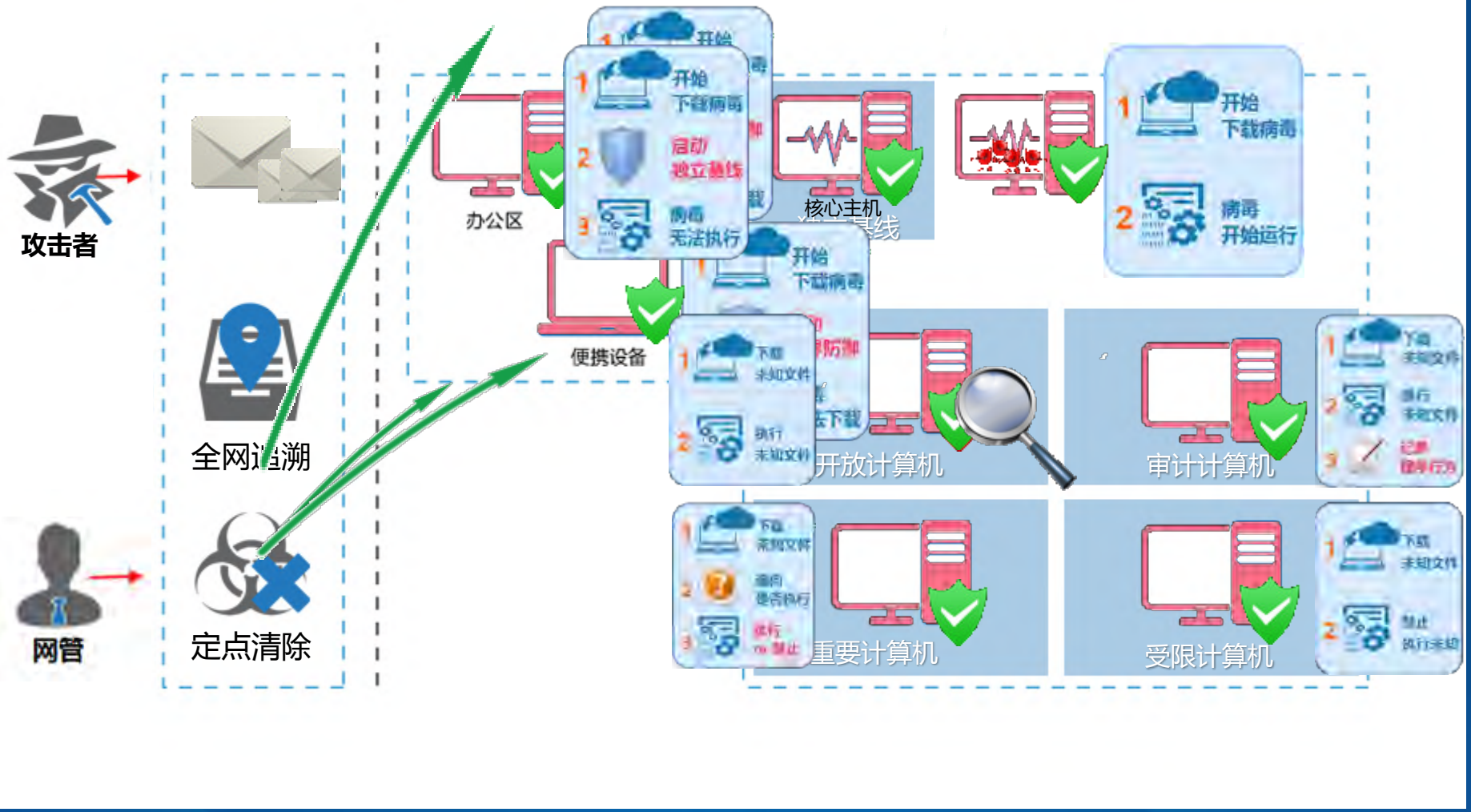




企业终端安全威胁的应对策略

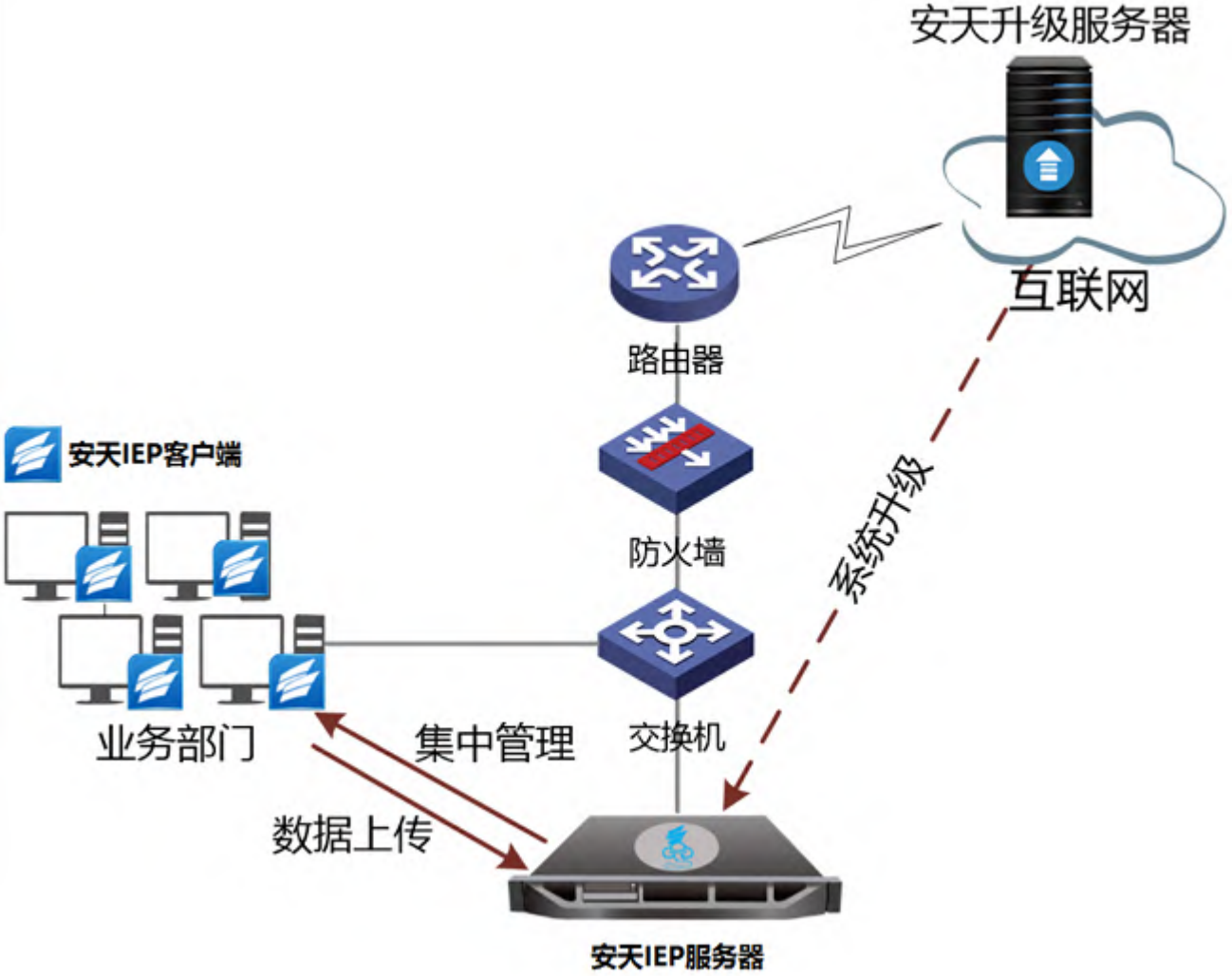
- 防范已知威胁
- 发现未知威胁
- 了解威胁影响
- 保护主机资产
- 掌握威胁态势
- 防范未知威胁

未知防御 -> 全网追溯 -> 定点清除



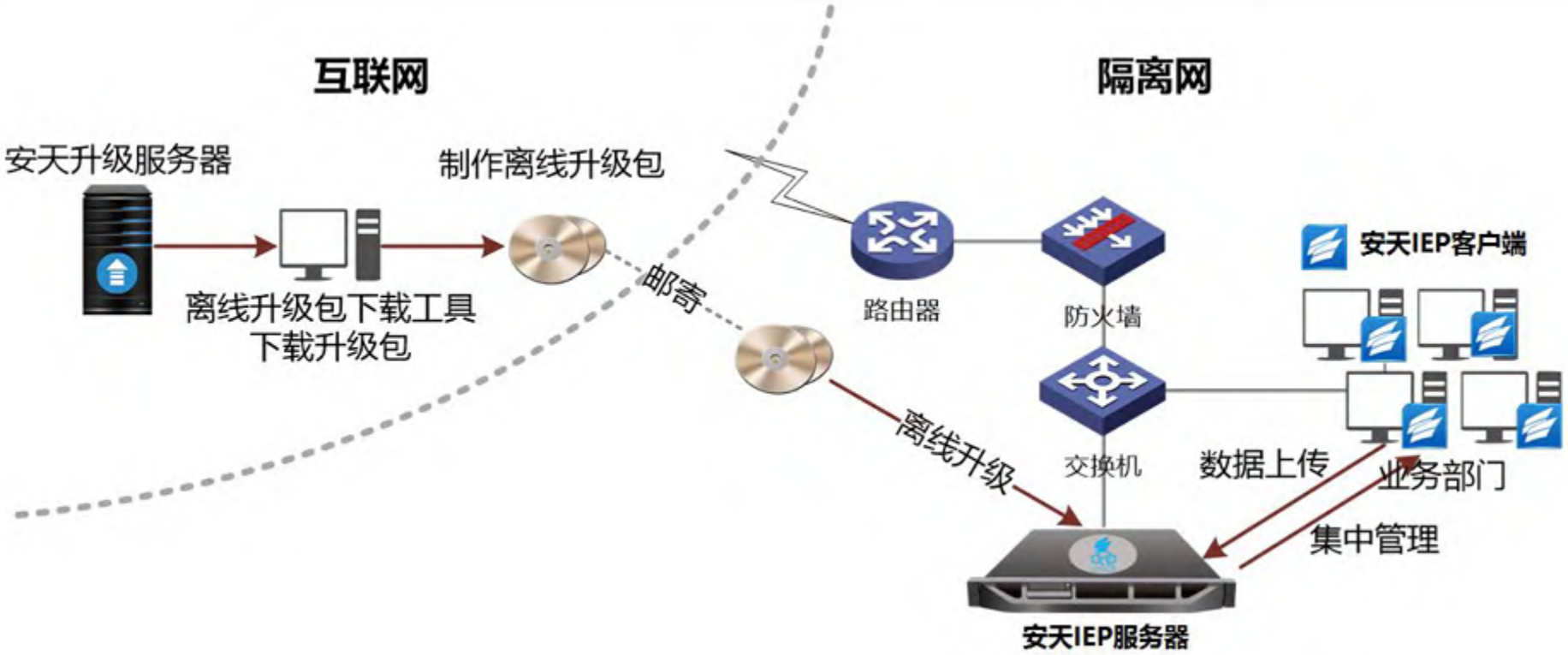
企业终端安全威胁的应对策略

- 云+本地服务器



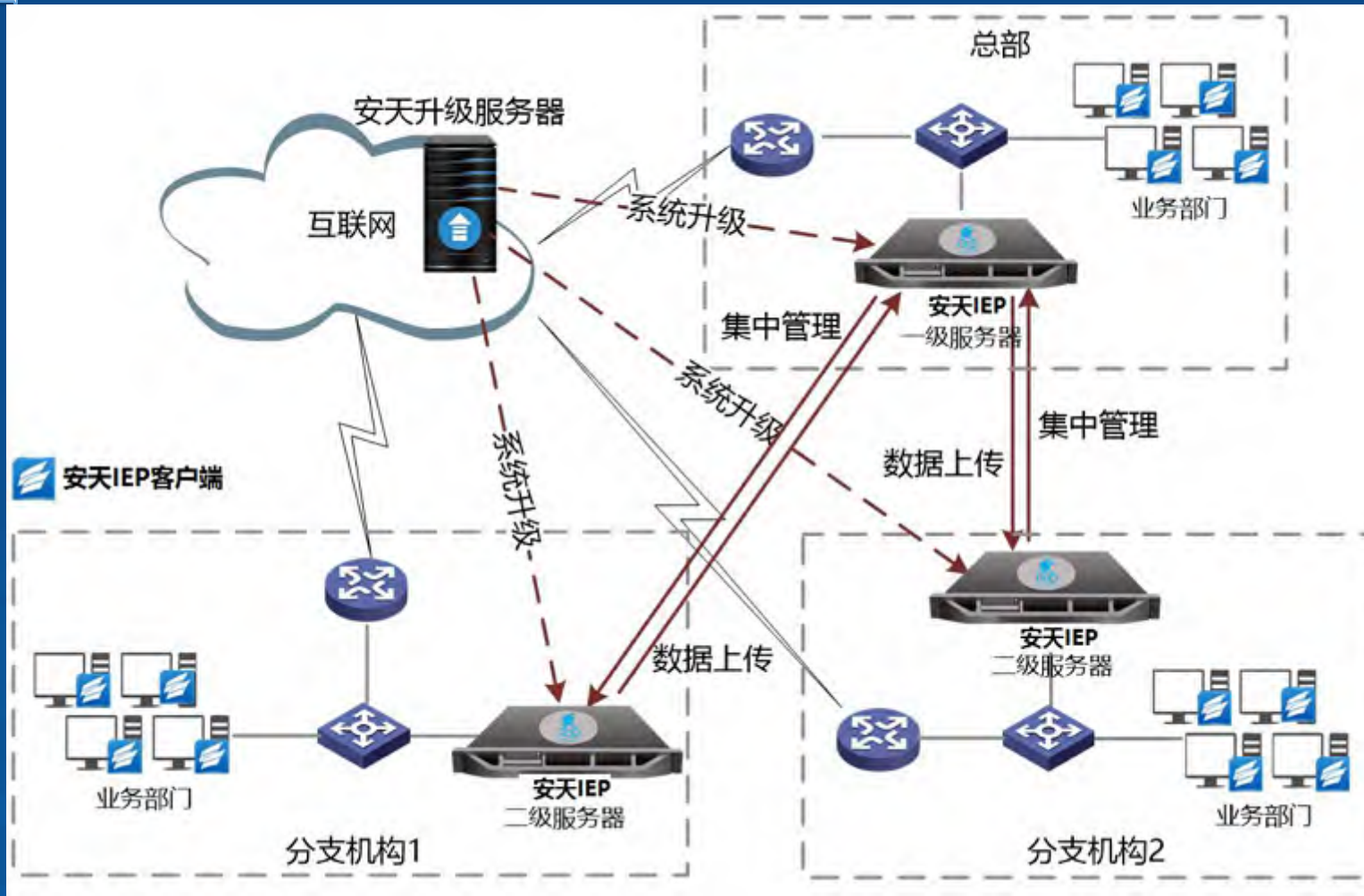
企业终端安全威胁的应对策略

- 隔离网环境



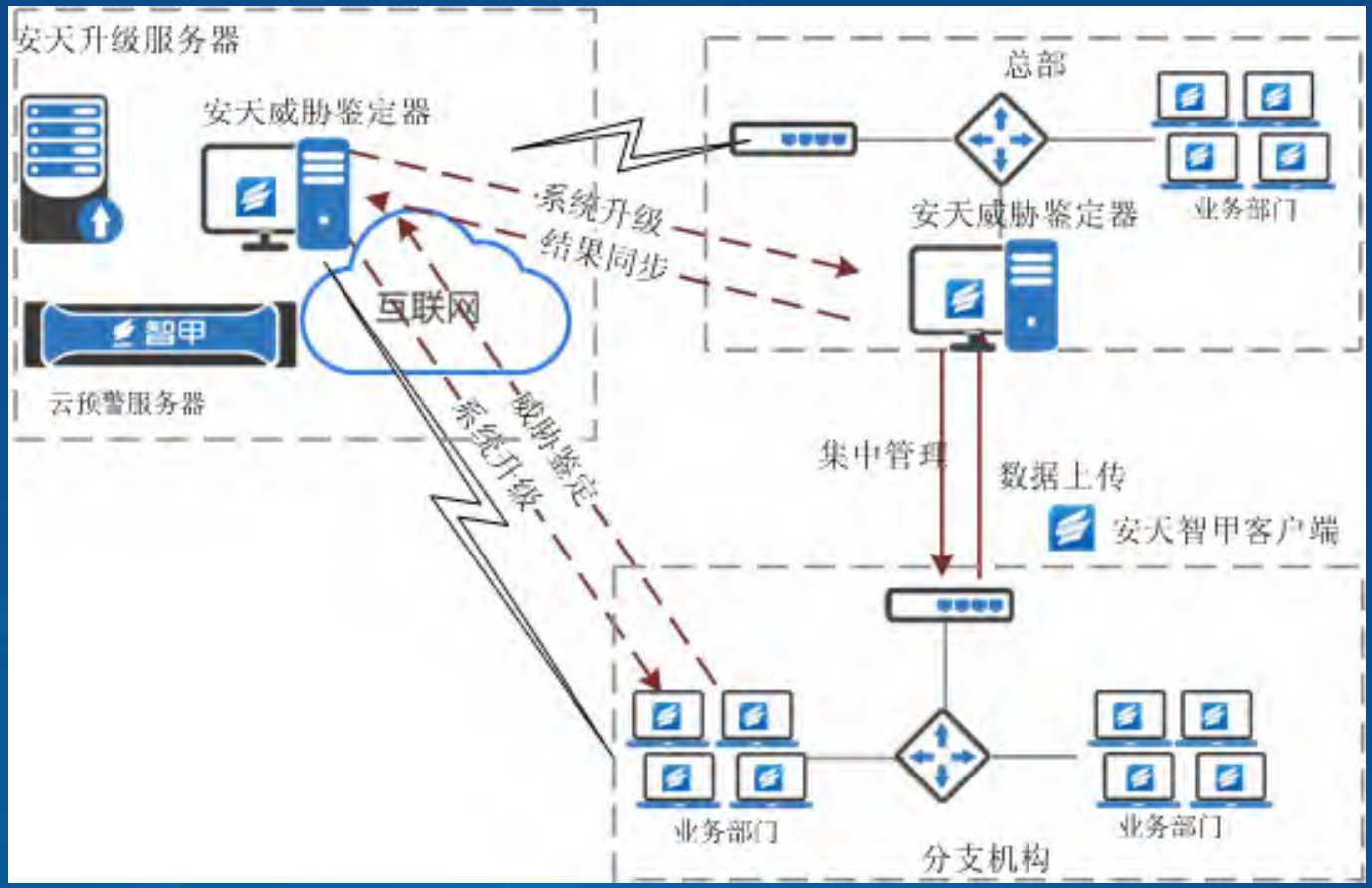
企业终端安全威胁的应对策略

- 云+多级部署



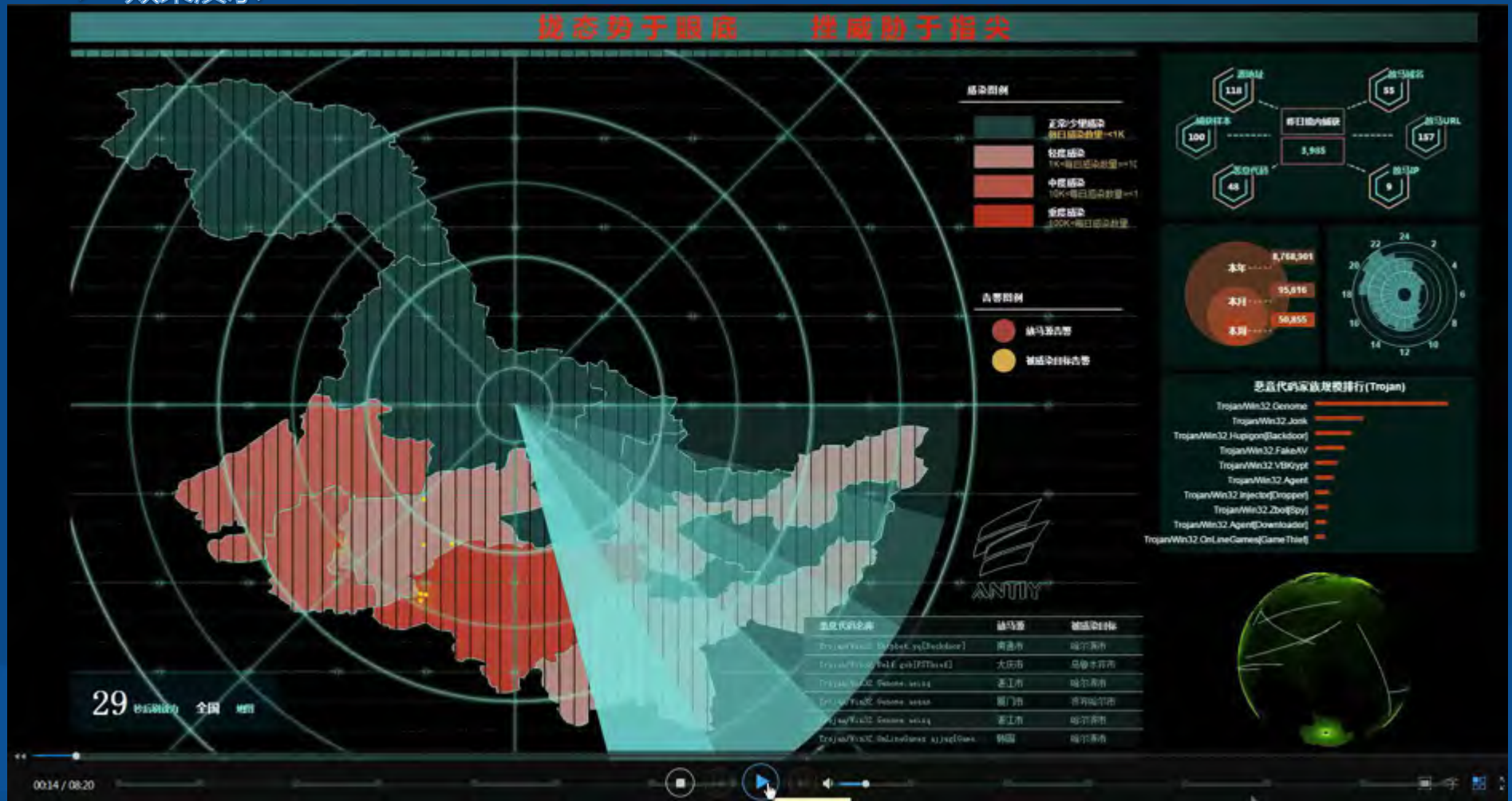
建设终端威胁预警云平台思路

- SaaS模式



建设终端威胁预警云平台思路

- 效果演示



建设终端威胁预警云平台思路

- 效果演示

The 8th China Cloud Computing Conference

weibo.com/libaisong75

libaisong@antiy.cn

Thank you