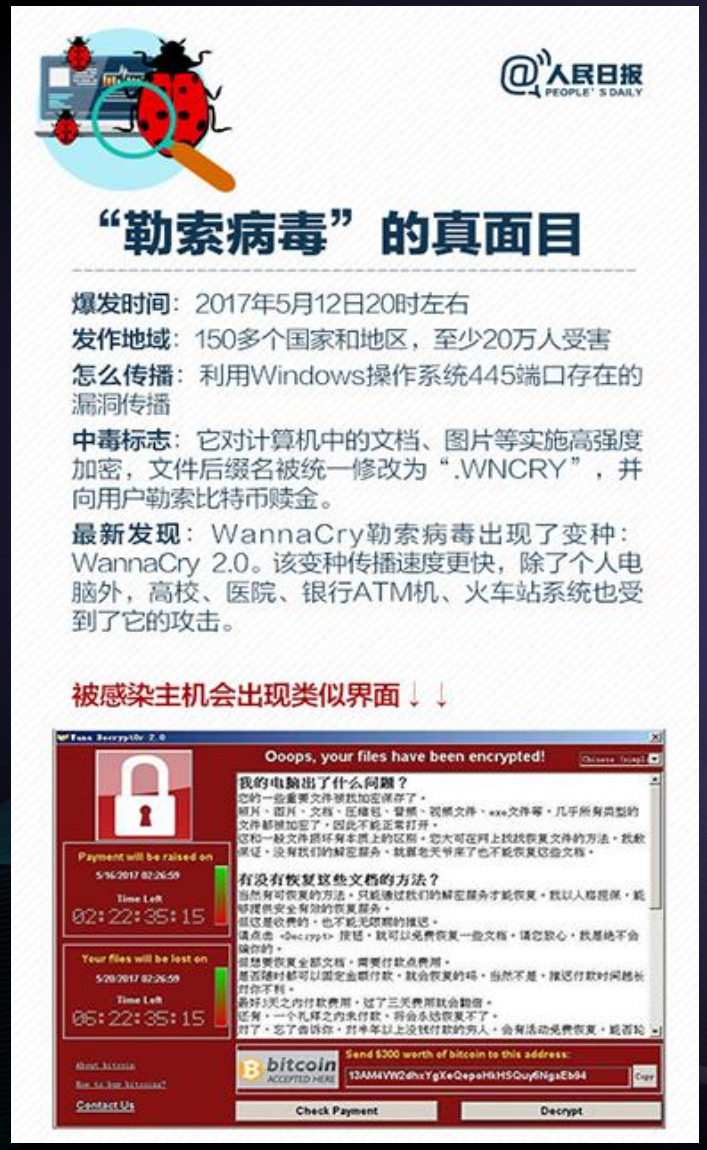
C3安全峰会
CYBER | CLOUD | COMMUNICATION

从永恒之蓝勒索攻击看高级威胁调查取证的创新价值

徐江明
亚信安全产品管理部产品总监

C3

“想哭”蠕虫勒索病毒带来了安全新挑战



- 2017年5月12日起，Wannacry 蠕虫勒索软件袭击全球网络，几小时内，全球**超过100个国家**，**近万家组织和企业**遭受攻击

- WannaCry是一种蠕虫变种勒索软件，利用NSA黑客武器库泄露的“**永恒之蓝**”发起病毒攻击，利用Windows SMB 服务器漏洞（CVE-2017-0147）渗透到Windows机器中，其中严重的漏洞**允许远程执行代码传播迅速**

- 当更多的零日漏洞和未知威胁**穿透当前的安全防御体系**后，如何**尽快地做出响应**，**锁定攻击范围**，**最大程度地减少损失**，将成为最有价值的创新

“想哭”蠕虫勒索攻击的溯源分析

C3安全峰会
CYBER | CLOUD | COMMUNICATION

仪表盘 | 调查 | 监控 | 管理

XX公司XX服务器（高危）

IP address：10.42.162.78

可疑行为

深入调查

高级威胁治理模型

制定治理策略，执行补救措施清除威胁、实施联动保护，适应防护变化的要求

通过数据发掘、加密、防泄漏、应用控制、APT追踪等技术，防止信息资产被非法访问或外泄

确认威胁是否发生，分析威胁，判断攻击和攻击者的本质，回溯攻击场景，评估威胁的影响和范围

调查取证/高级审计技术

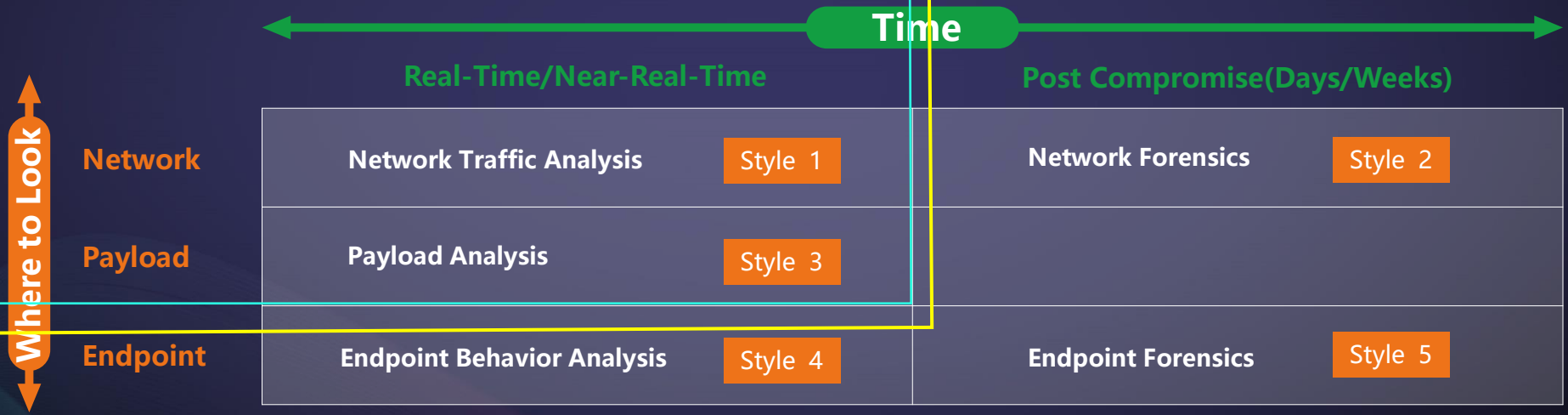
检测攻击者所使用的，传统防御无法识别的恶意对象、通讯及行为等威胁

Gartner推荐的高级威胁防御模型

C3安全峰会
CYBER | CLOUD | COMMUNICATION

深度威胁发现设备
TDA 威胁情报分析系统

Figure 1. Five Styles of Advanced threat defense



Source:gartner(August 2013)

主机取证设备

高级网络安全调查取证设备

Cyber Threat Deep Investigation

主机取证设备 -- 取证黑匣子（飞行数据记录仪）

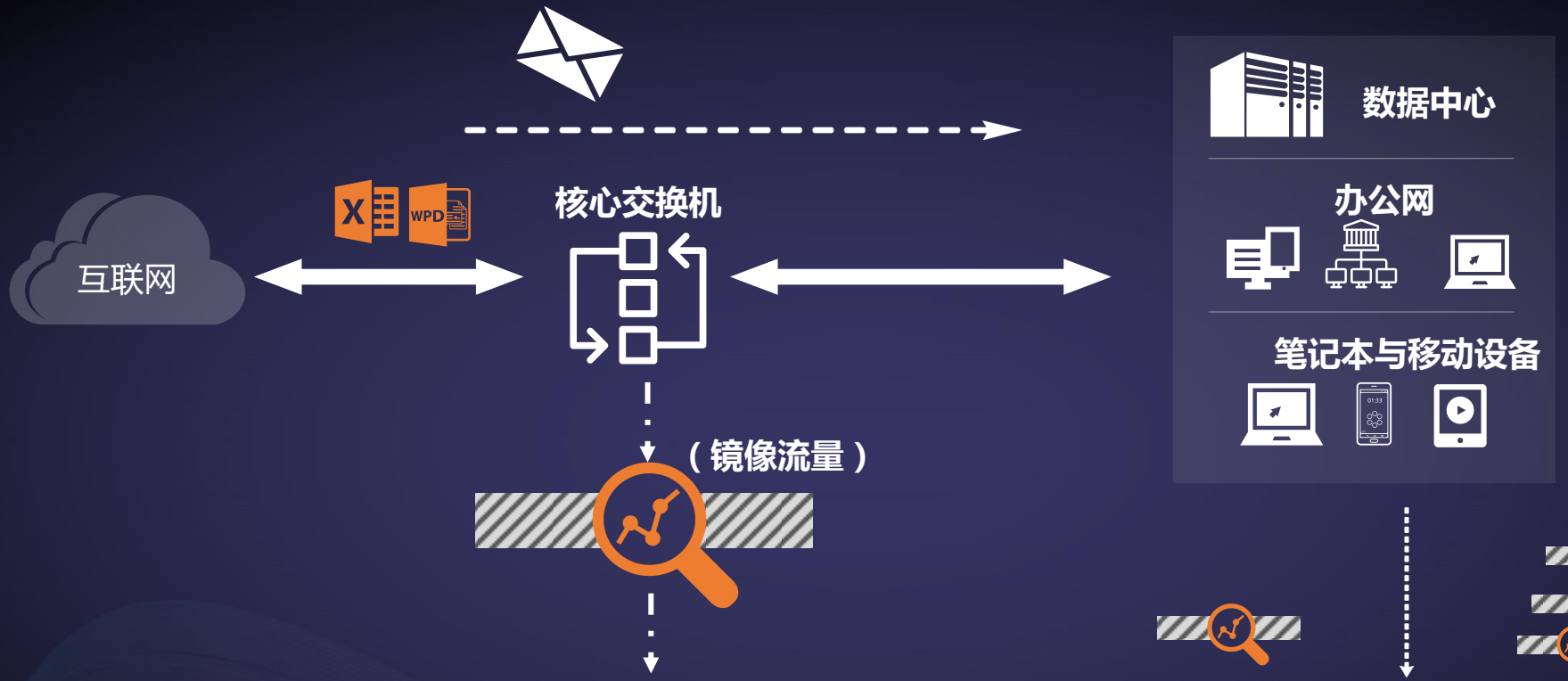
服务器端收集日志并进行关联分析

- 硬件一体机
- 日志集中存储
- 20/40/60TB
- 关联分析和查询

轻量级客户端记录系统行为

- 文件读写
- 进程起停
- 网络连接
- 注册表改动

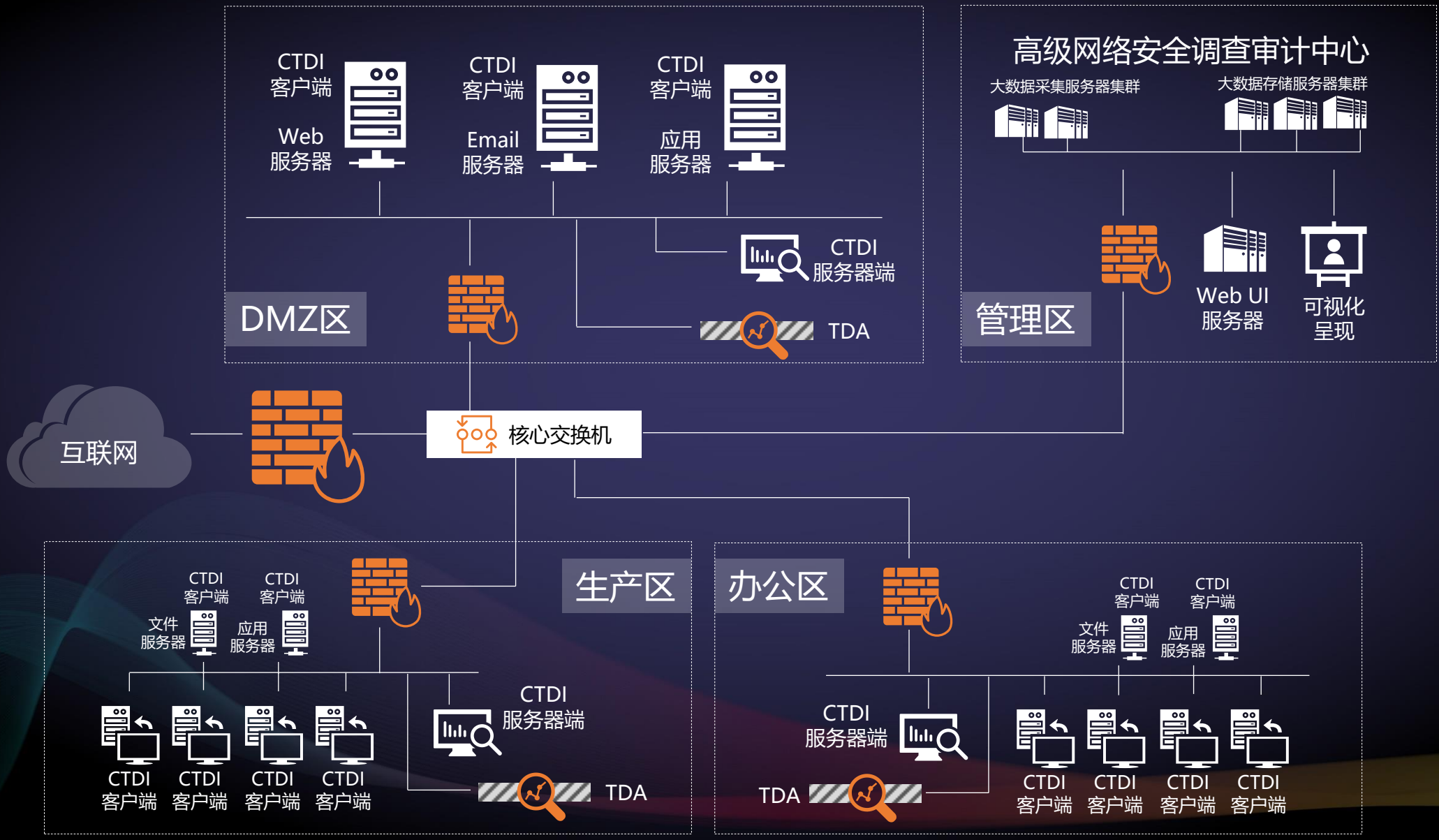
高级网络安全调查取证/高级审计解决方案



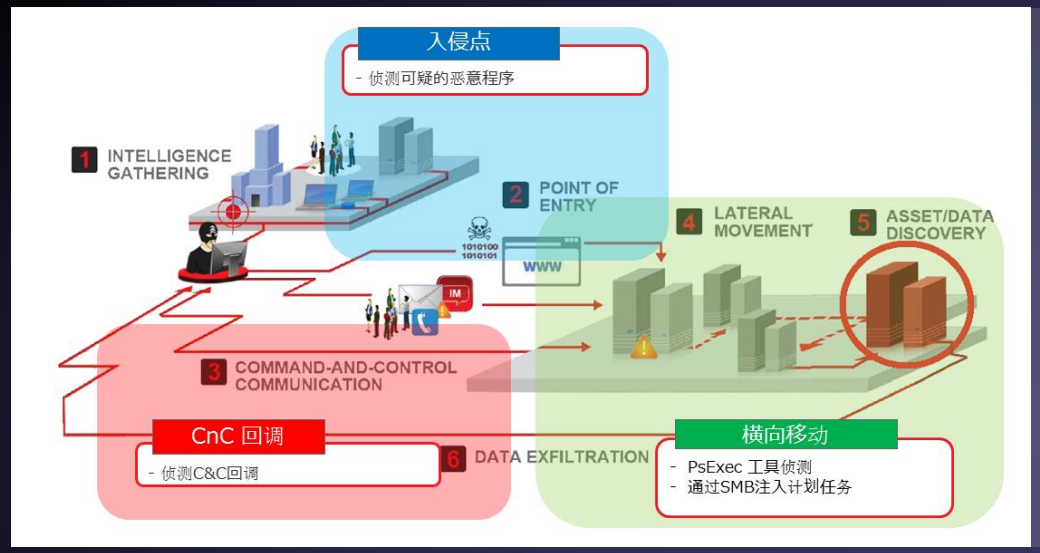
依托云端威胁情报和本地沙盒分析侦测到安全事件的调查线索

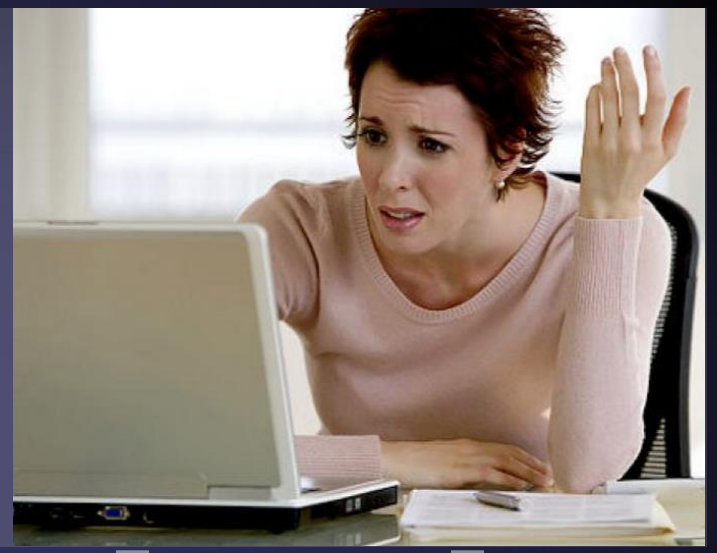
根据威胁情报分析系统提供的安全事件线索，
在主机取证设备上进行关联分析，还原出攻击场景

调查取证/高级审计解决方案部署架构



方案价值1 -- 解答困扰安全管理人员的4个问题





01 哪些主机遭到入侵?

02 哪些账号遭到入侵？

03 攻击是如何发生的？

04 哪些数据被泄露？

方案价值2

调查取证
高级审计
打击震慑网络犯罪

从内核层面详细记录：
文件操作
进程起停
模块加载
网络连接

部署网络威胁情报分析系统
和主机取证设备监控并侦测
“已知”和“未知”威胁

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Thank You