
ISC
2015
数据驱动安全
2015 中国互联网安全大会
China Internet Security Conference
互联网+时代下
新的数据安全防护思路
谭伟基
亚太区技术总监
Raytheon | Websense

网络空间安全上升到国家层面


中国共产党新闻网 www.cpcnews.cn

高层 组织结构 干部 新闻 人事 反腐 原创 基层 动态 典型 机关 学习 理论 评论 特稿 互动 网评 对党说
动态 中央部门 论坛 报道 宣传 统战 外联 党建 国企 非公 学校 参考 党史 缅怀 资料 交流 专题 云平台

以史正听 系列策划 纪念中国人民抗日战争暨世界反法西斯战争胜利70周年 人民网 中国共产党新闻网 cpc.people.cn

中国共产党新闻 >> 专题报道 >> 学习路上

学习路上

学者观察：习主席访美利于推动两国网络空间治理共识

2015年09月24日08:43 来源：人民网－中国共产党新闻网

中国共产党新闻网北京9月24日电 （万鹏）“中国是网络安全的坚定维护者”，习近平主席昨日在美国华盛顿州西雅图市出席欢迎宴会并发表演讲指出，国际社会应该本着相互尊重和相互信任的原则，共同构建和平、安全、开放、合作的网络空间。他指出，中国愿同美国建立两国共同打击网络犯罪高级别联合对话机制。多位学者分析指出，在中美关系各领域当中，网络空间治理议题在短短几年里受到了双方非常高度的重视。这不仅源于现实世界两国的国际政治地位，还源于二者在网络空间所占据的份额。中美两国应利用双方元首会面的良好契机，探寻网络空间合作共赢的健康之路。

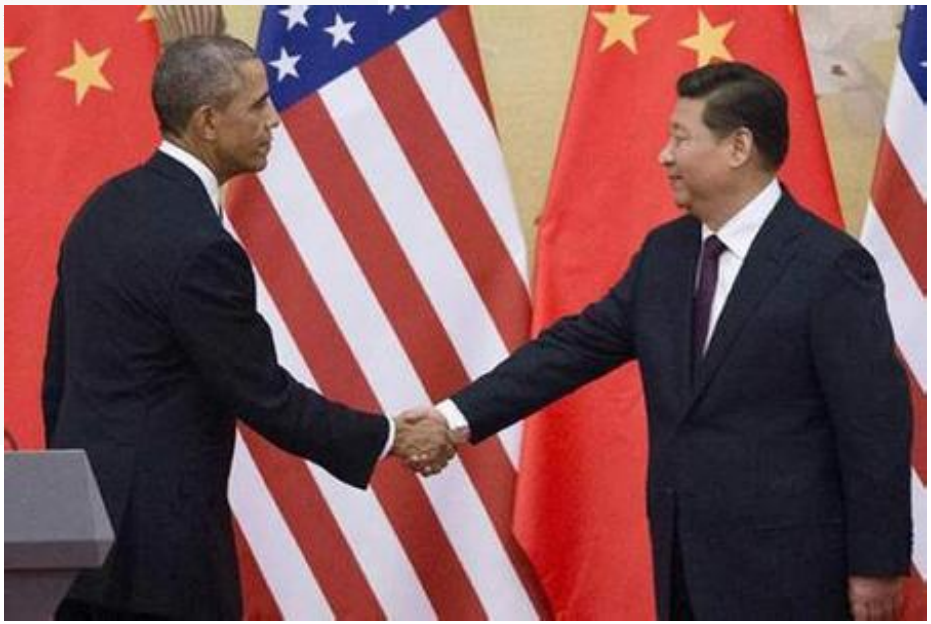
互联网不是“法外之地”：

既要充分尊重网民的权利，也要构建良好的网络秩序

热点关键词

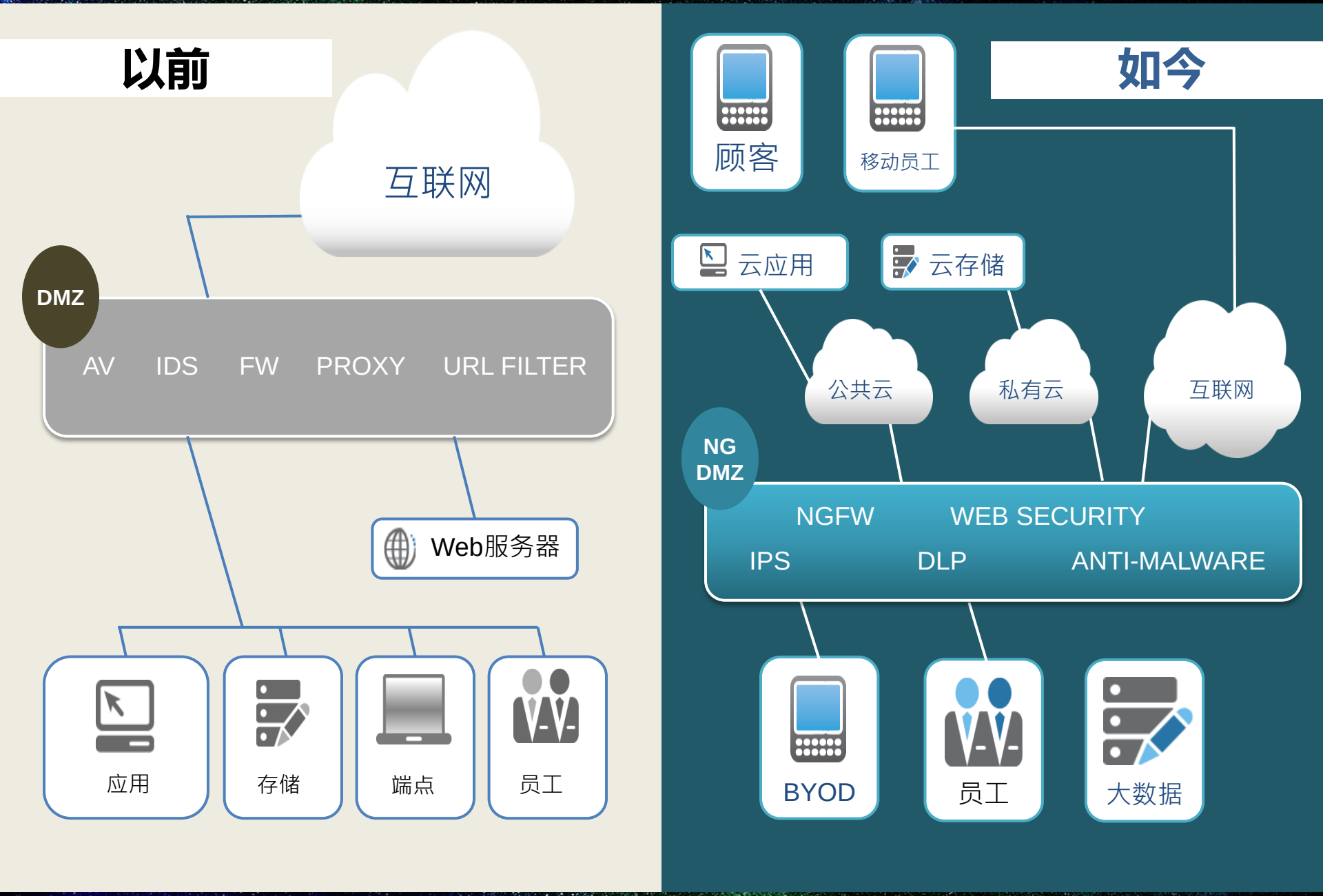
学习路上 中国政要资料库 “四个全面”布局
三严三实 以正史听 云平台 习大大 加油

互联网加意味着传统业务与互联网结合形成新的业务模式将成为今后几年的趋势



网络空间安全是这次习主席访问美国的几个重要话题之一，说明国家现在对于网络安全的重视程度

业务模式的改变导致IT架构的变革

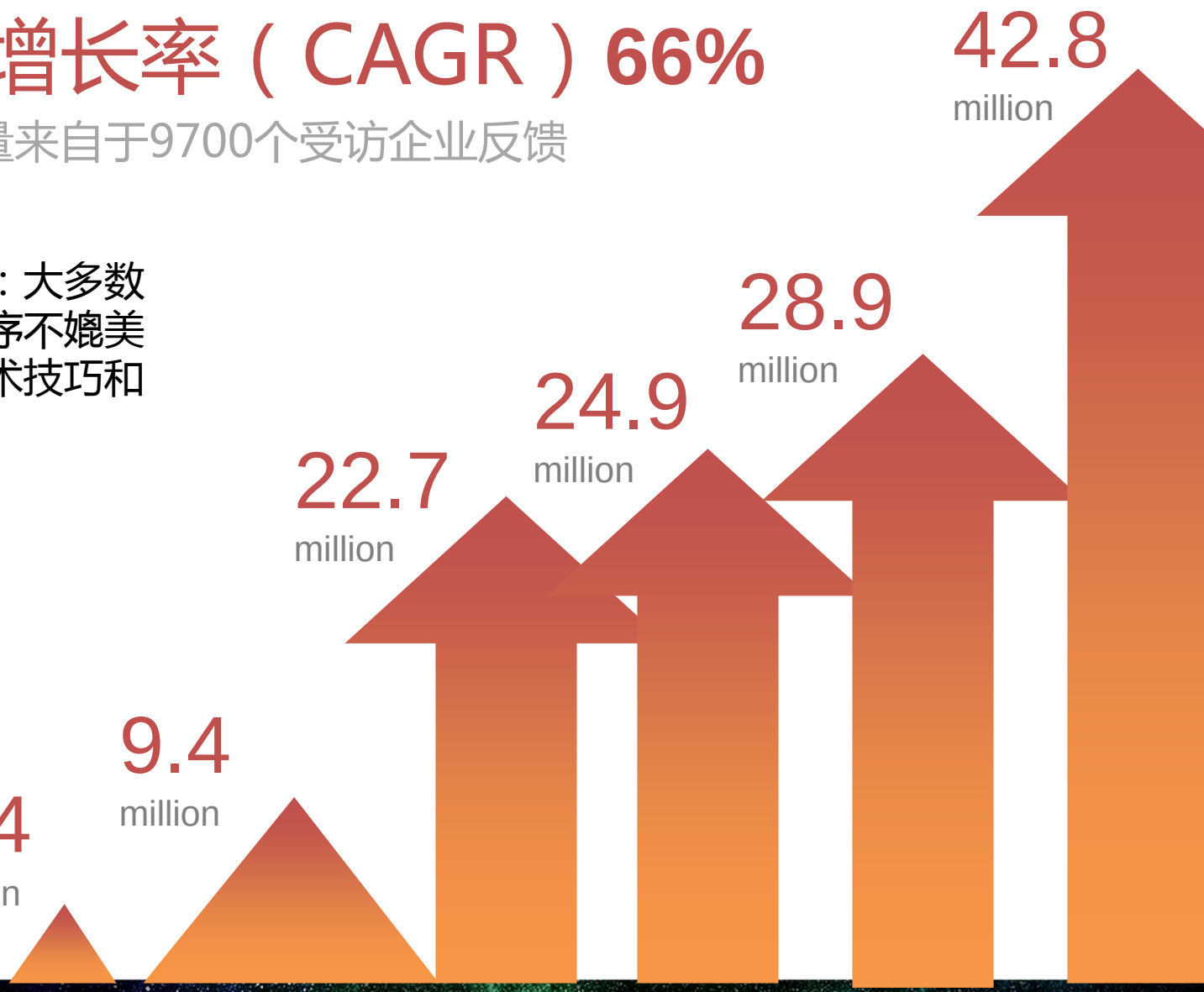


当前安全现状

复合年均增长率（CAGR）66%

安全事件统计数量来自于9700个受访企业反馈

有一点是很清楚的：大多数机构的网络安全程序不媲美当今的持久性，战术技巧和技术实力网络对手。



PwC - The Global State of Information Security® Survey 2014 & 2015

网络安全人才缺失

网络空间安全技能缺口持续增长

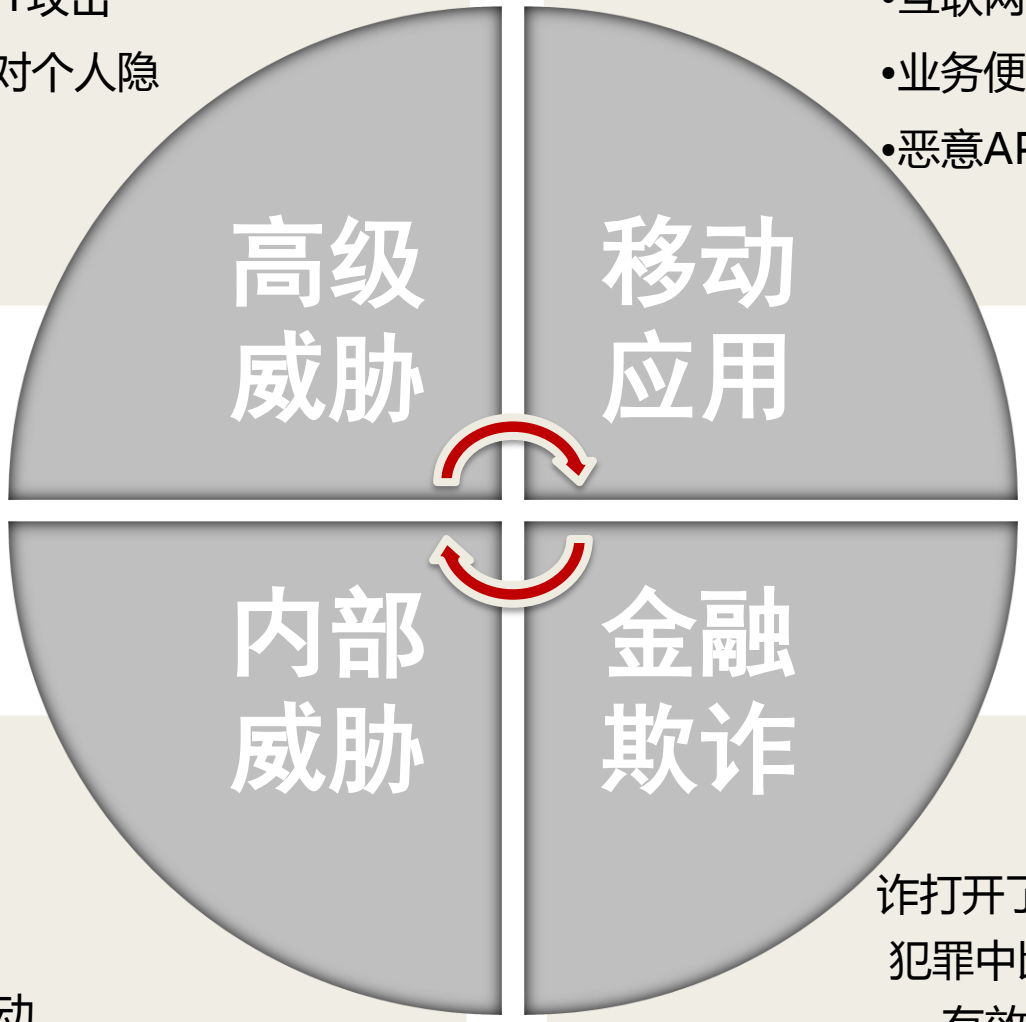
市场指标显示到2017年,
全球可能缺乏多达425万安全人员，
占人才需求47%

= 250,000

2013 (ISC)2 Global Information Workforce Study

近期四大信息安全热点

- 企业持续关注APT攻击
- 攻击目标更多针对个人隐私

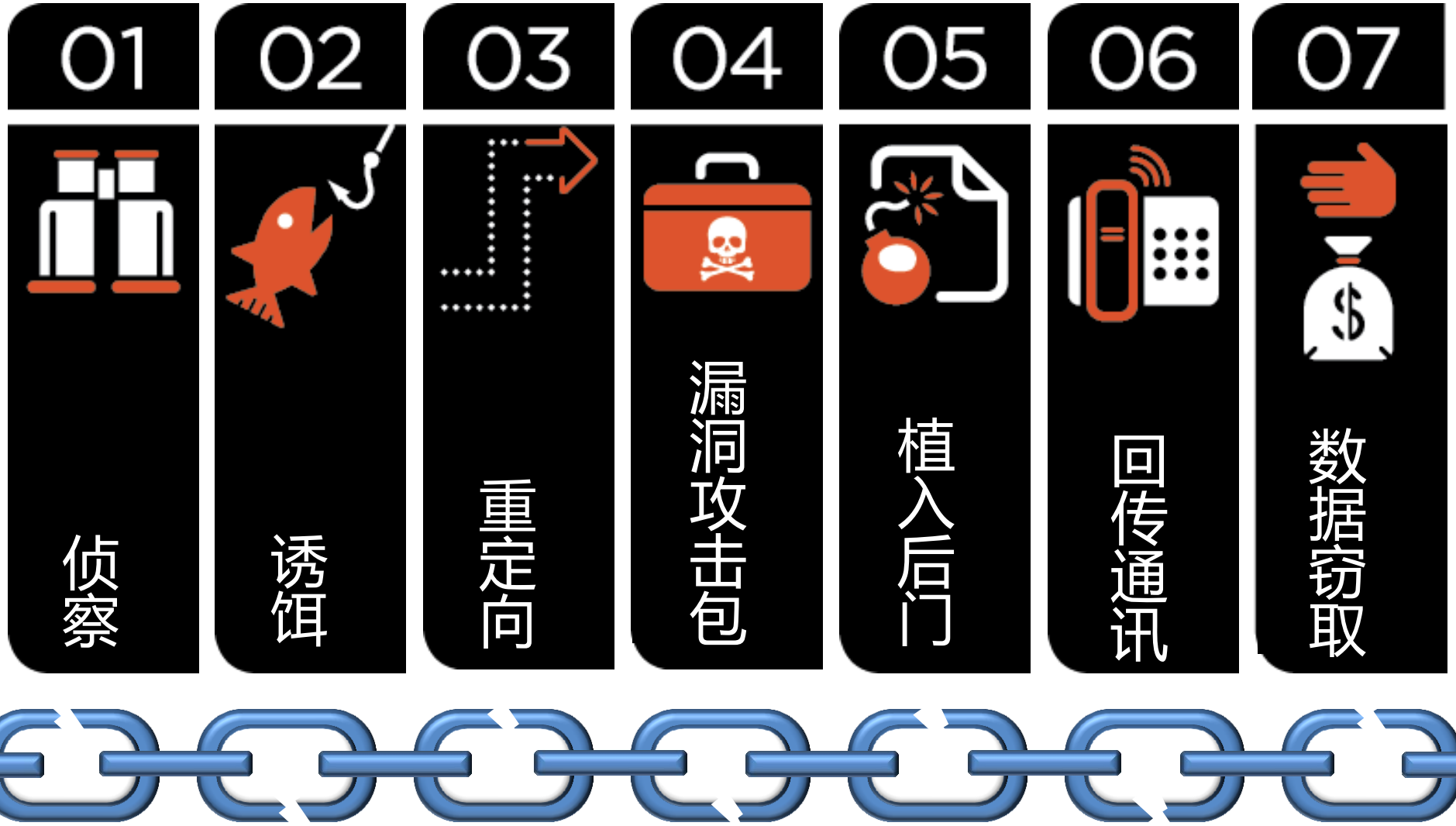


- 互联网 + 时代
- 业务便捷与数据风险共存
- 恶意APP威胁用户隐私

- 数据窃取
- 内部破坏
- 安全威胁横向移动

- 互联网为金融欺诈打开了便利之门, 在金融犯罪中比例不断增长,缺乏有效手段识别此类风险

高级威胁 - APT攻击



当前防御技术四大失败理由

1 单靠特征码和信誉

历史并非未来表现的可靠指标。特征码制作无法跟上威胁的动态创建

2 缺乏实时在线内容分析

收集利用后台进程的样品进行实验室分析，产生新的特征码和声誉

3 只检查请求，缺乏对外发资料的保护

没有数据感知，缺乏上下文分析，最小没有证据和事件分析能力

4 忽略SSL死角

UTM，NGFWs，IPS监控SSL严重影响性能，还是视而不见

移动应用 - 引出新的风险

数据泄露

平台复杂

BYOD

恶意APP

欺诈入口

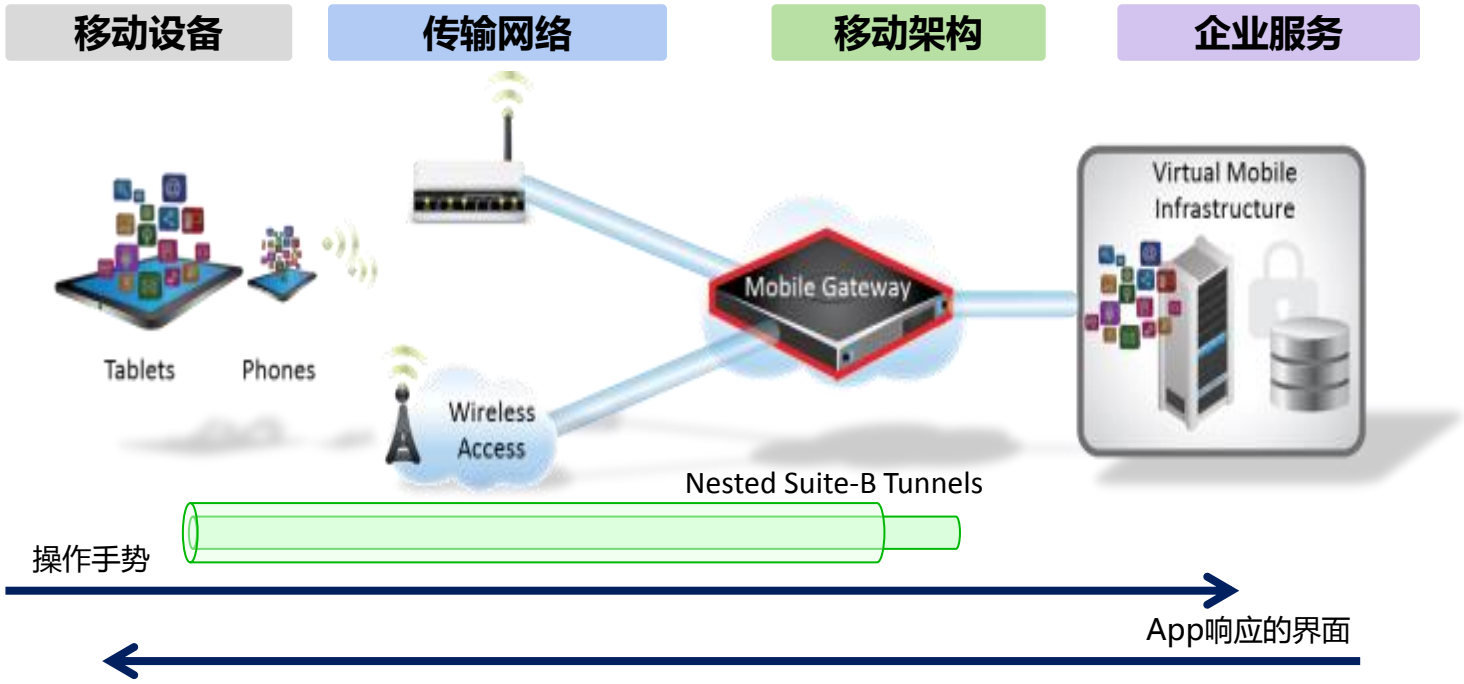
应用漏洞

开发维护

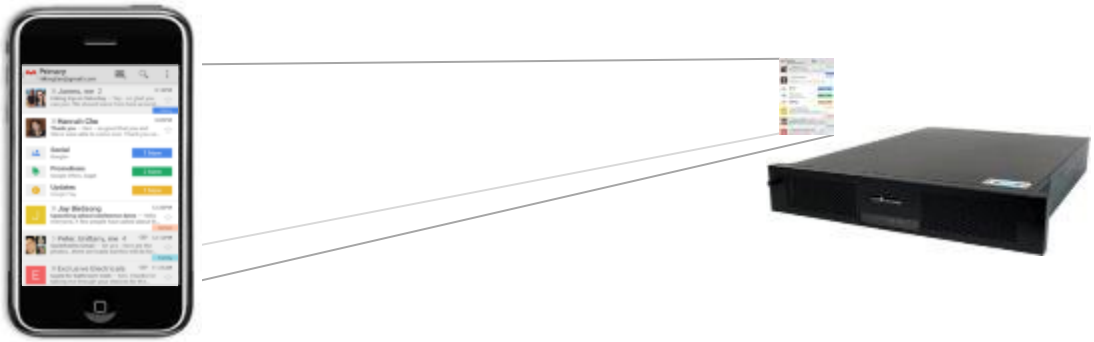
移动终端数据安全新思路

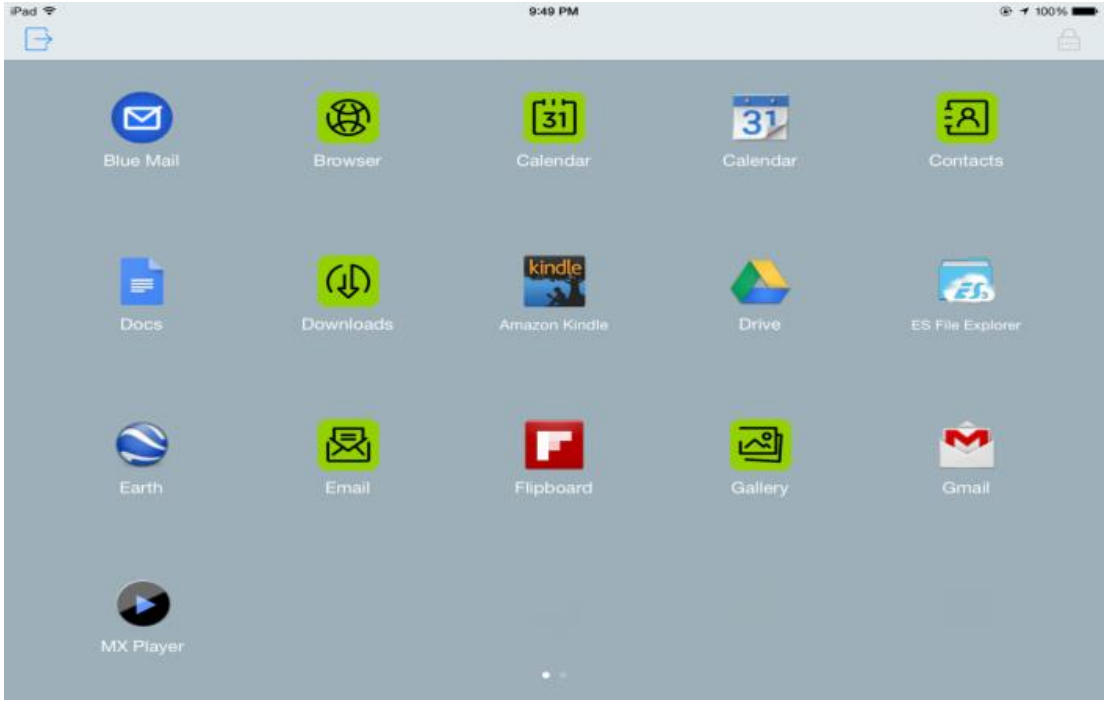
MDM v.s. **VMI**

移动设备管理　　虚拟移动基础设施



根本上控制移动终端安全风险





敏感数据不保留

操作习惯无变化

软件升级免干预

平台安全有保障

我们一直在关注“他”...

黑客和有组织犯罪集团是网络安全的坏人，每个人都了解

但是.....

* PwC - The Global State of Information Security® Survey 2014 & 2015

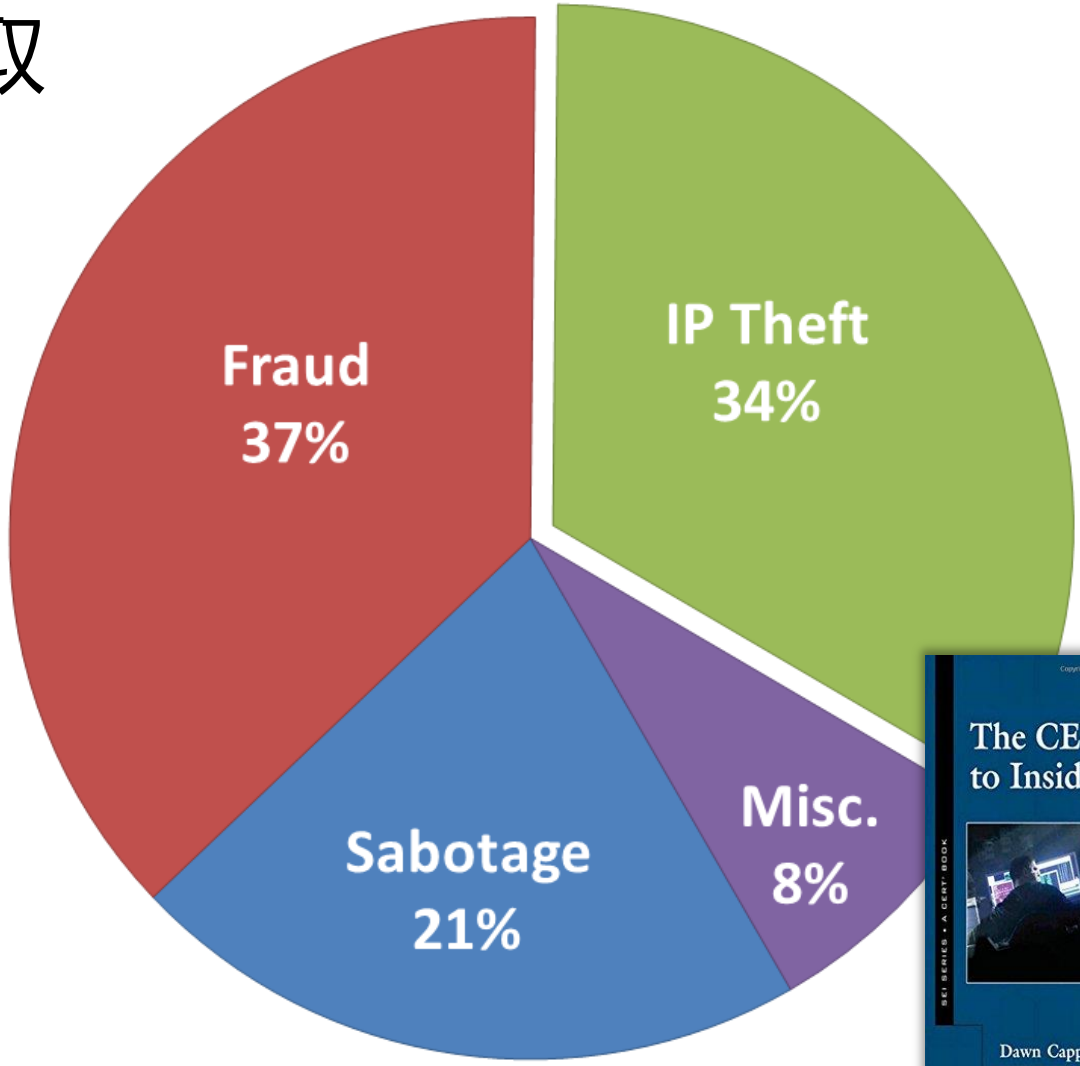
但“他”呢……？

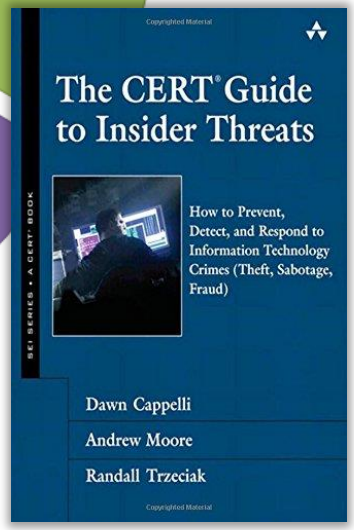
32%的受访者反馈内部威胁所带来的危害远高于来自于外部的攻击

* PwC - The Global State of Information Security® Survey 2014 & 2015

内部威胁 - 需要重点关注的威胁

- ✓ 知识产权窃取
- ✓ 金融欺诈
- ✓ 蓄意破坏
- ✓ 非故意行为
- ✓ 其他
  - ✓ 渎职行为
  - ✓ 暴力行为





Source: *The CERT Guide to Insider Threats*, 2012

准确识别内部威胁

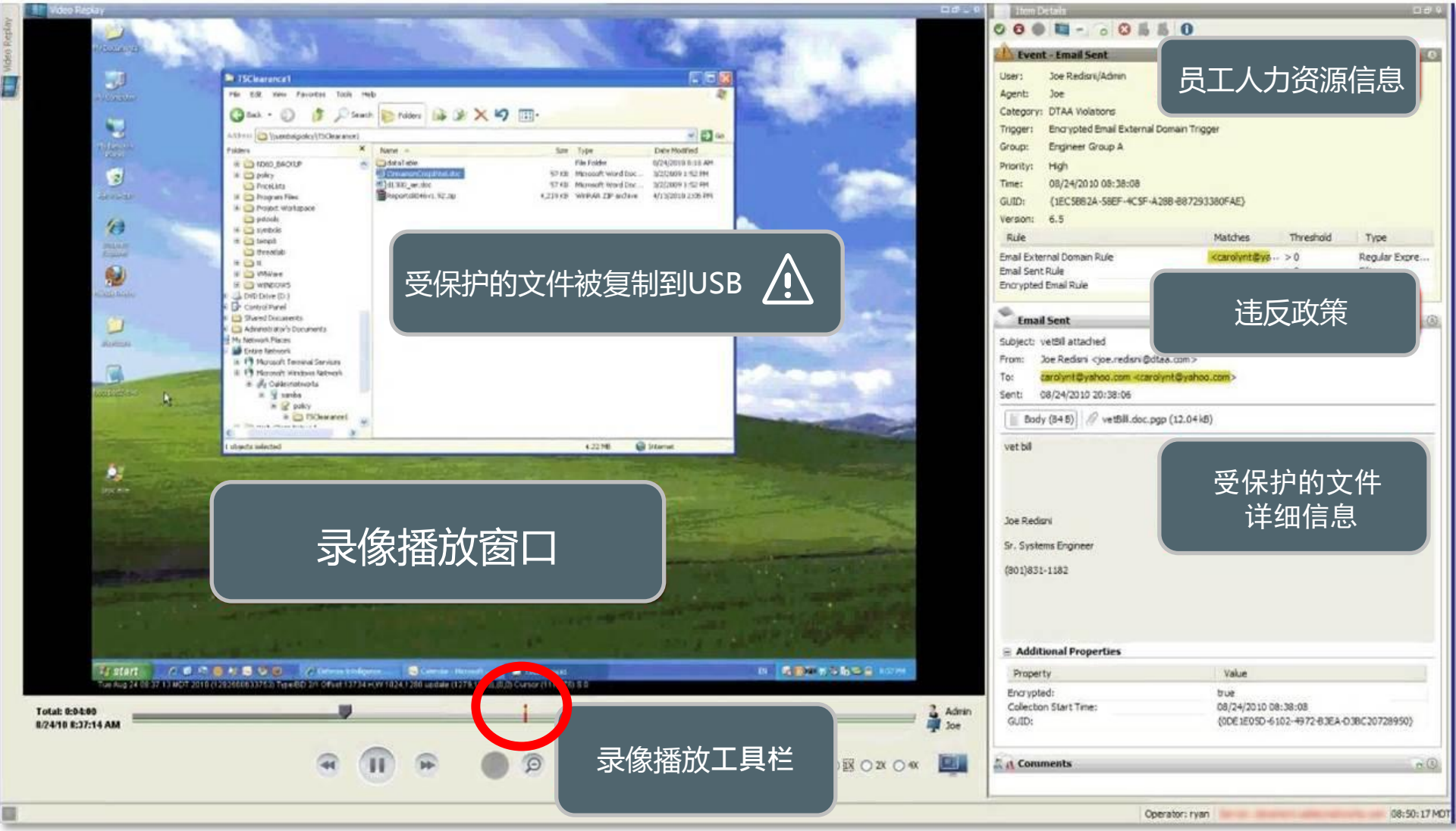
Visibility + Context

异常行为识别 → 上下文关联分析 → 完整复现操作过程 → 前瞻性定位风险

用户行为监控准确识别内部威胁

- 发现并记录:
  - 键盘输入
  - 聊天记录
  - 文件和文档内容
  - 截屏操作
  - 视频录像屏幕显示的操作
  - 捕获用户编辑的文件的不同版本
  - 针对移动介质操作
  - Web浏览器操作
  - 剪贴板操作（复制 / 剪切 / 黏贴）
  - 文件访问
  - 内核进程
  - 用户执行的应用程序
  - USB 端口操作
  - 邮件内容

具备DVR回放违规行为证明能力



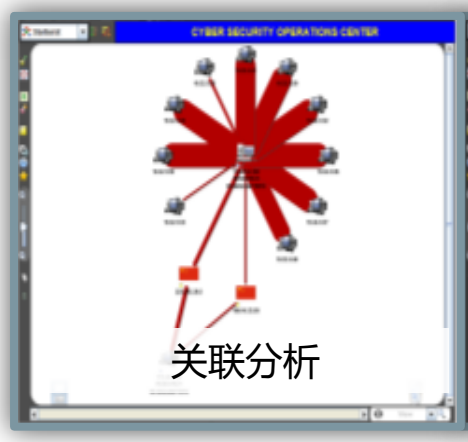
如何快速定位各类风险和威胁，包括金融欺诈

关联分析

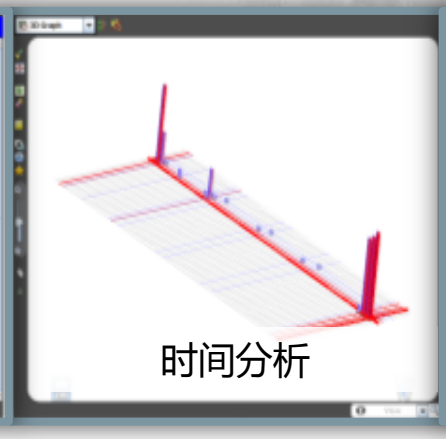
快速定位

化繁为简

从四个纬度定位各类风险



关联分析


时间分析


地理位置分析

统计分析

联合查询搜索

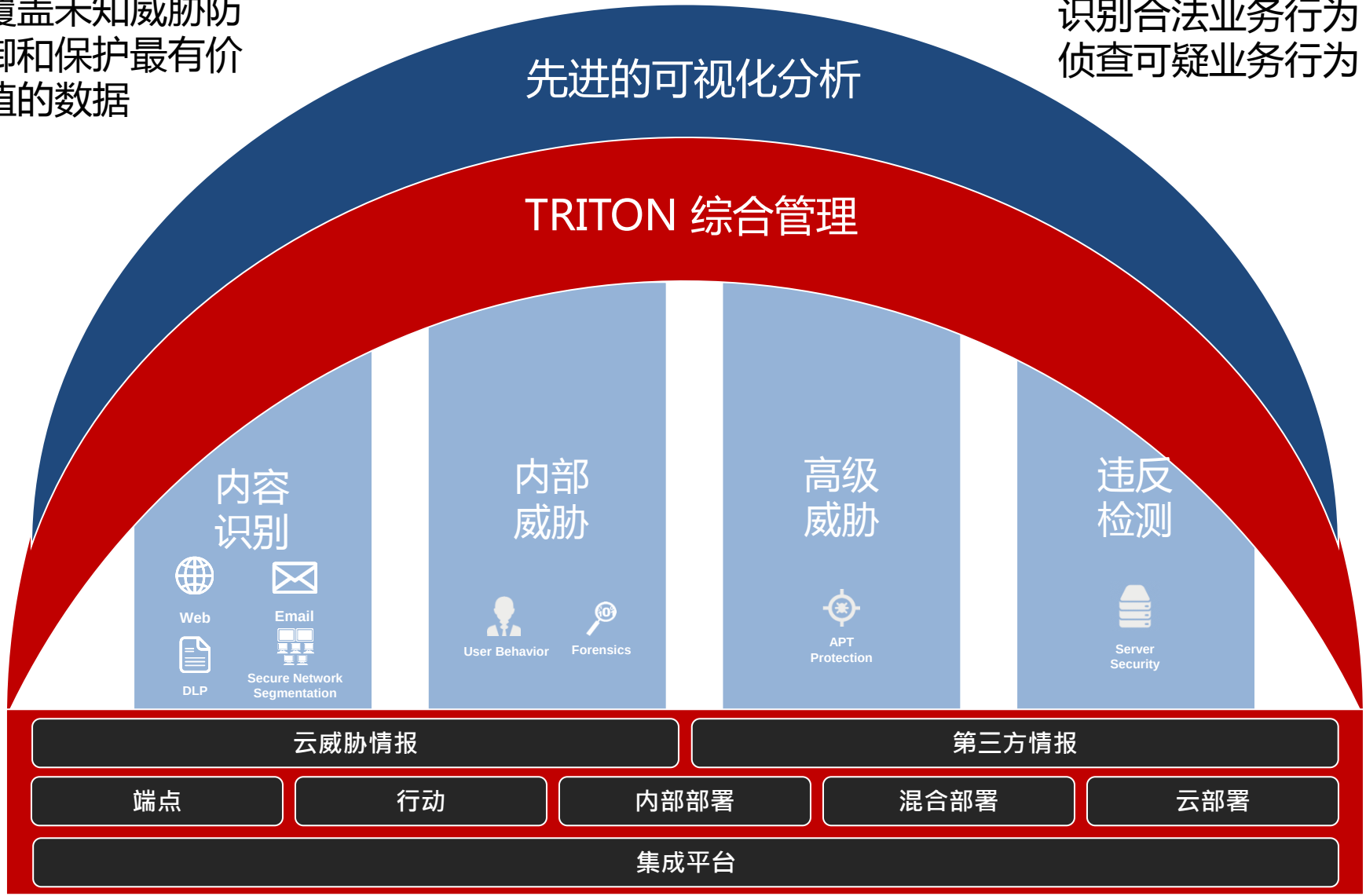
联合查询搜索技术采用建立一个虚拟的数据仓库，
并保持数据不被转移及复制

SIEM/数据仓库	联合查询搜索
• 静态数据库模式 • 数据的可扩展性低	• 按要求连接到数据源上 • 高度可扩展的数据层
• 需要数据的所有权 • 重复数据	• 数据仍然留在原地 • 不用复制数据 • 保留数据的所有权
• 需要摄入数据 • 数据延迟和过时	• 直接查询数据源 • 新鲜数据
可以连接到现有的数据仓库或SIEM	

以业务为核心建立预测性数据安全防御

内容和对话识别
覆盖未知威胁防御和保护最有价值的数据

阻挡恶意和违规行为
识别合法业务行为
侦查可疑业务行为



谢谢