RISING 瑞星

虚拟化系统环境下的安全防护

郑斌

瑞星虚拟化产品开发总监

1 虚拟化环境的快速发展

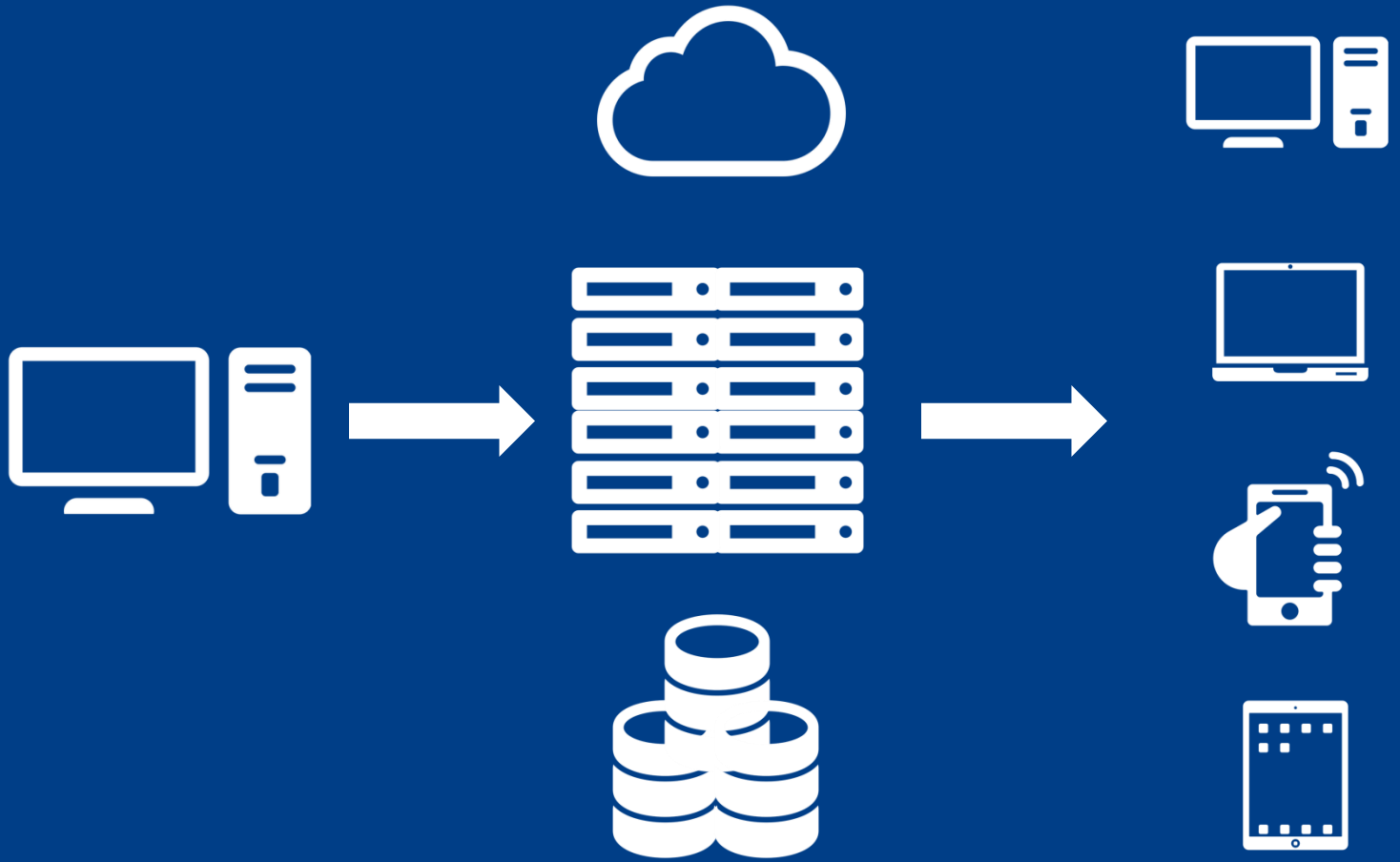
2 虚拟化环境的安全问题

3 虚拟化环境的安全防护

1

虚拟化环境

快速发展




MODEL X


Intelligents

2

虚拟化环境

安全问题

虚拟化环境面临的风险

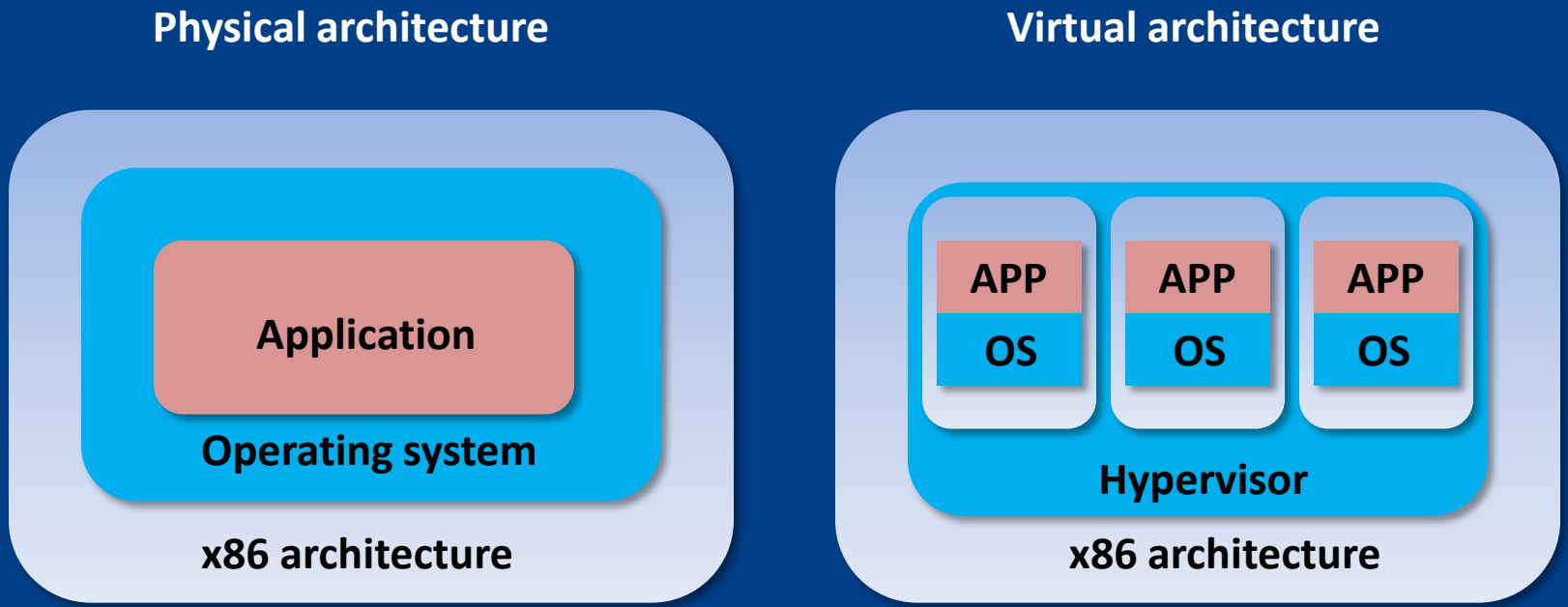
传统环境下的安全风险

Hypervisor自身的安全漏洞

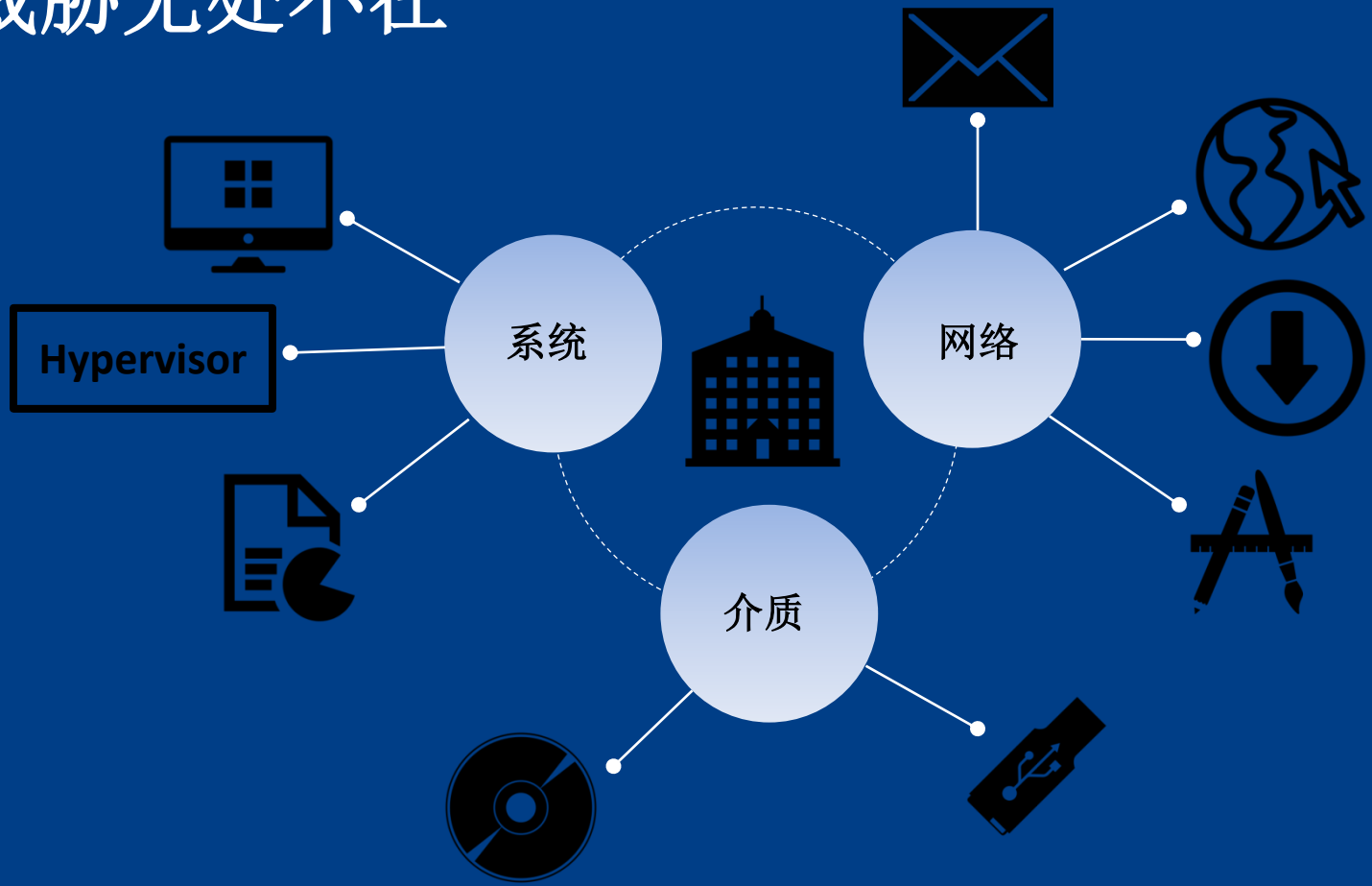
APT攻击问题

防护间隙问题

物理与虚拟体系结构对比



威胁无处不在



什么是APT攻击

APT（Advanced Persistent Threat）

--------高级持续性威胁

Advanced

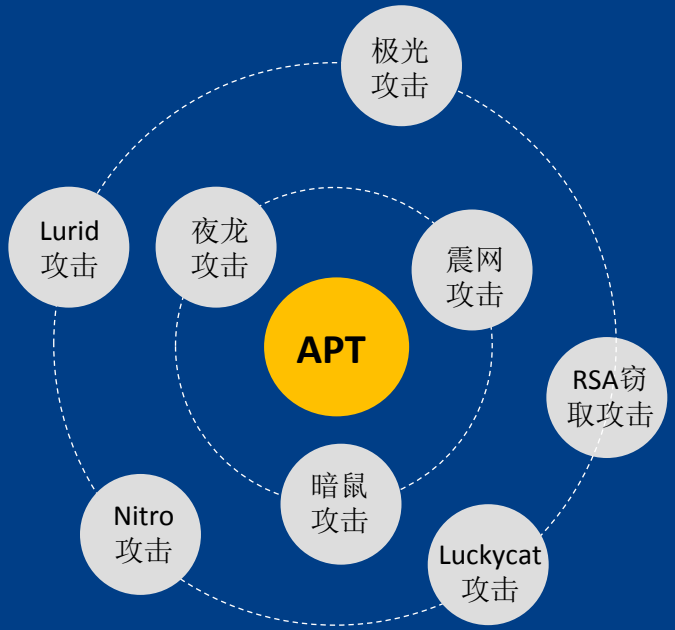
攻击手段，攻击技术相对普通攻击更加高级和先进。

Persistent

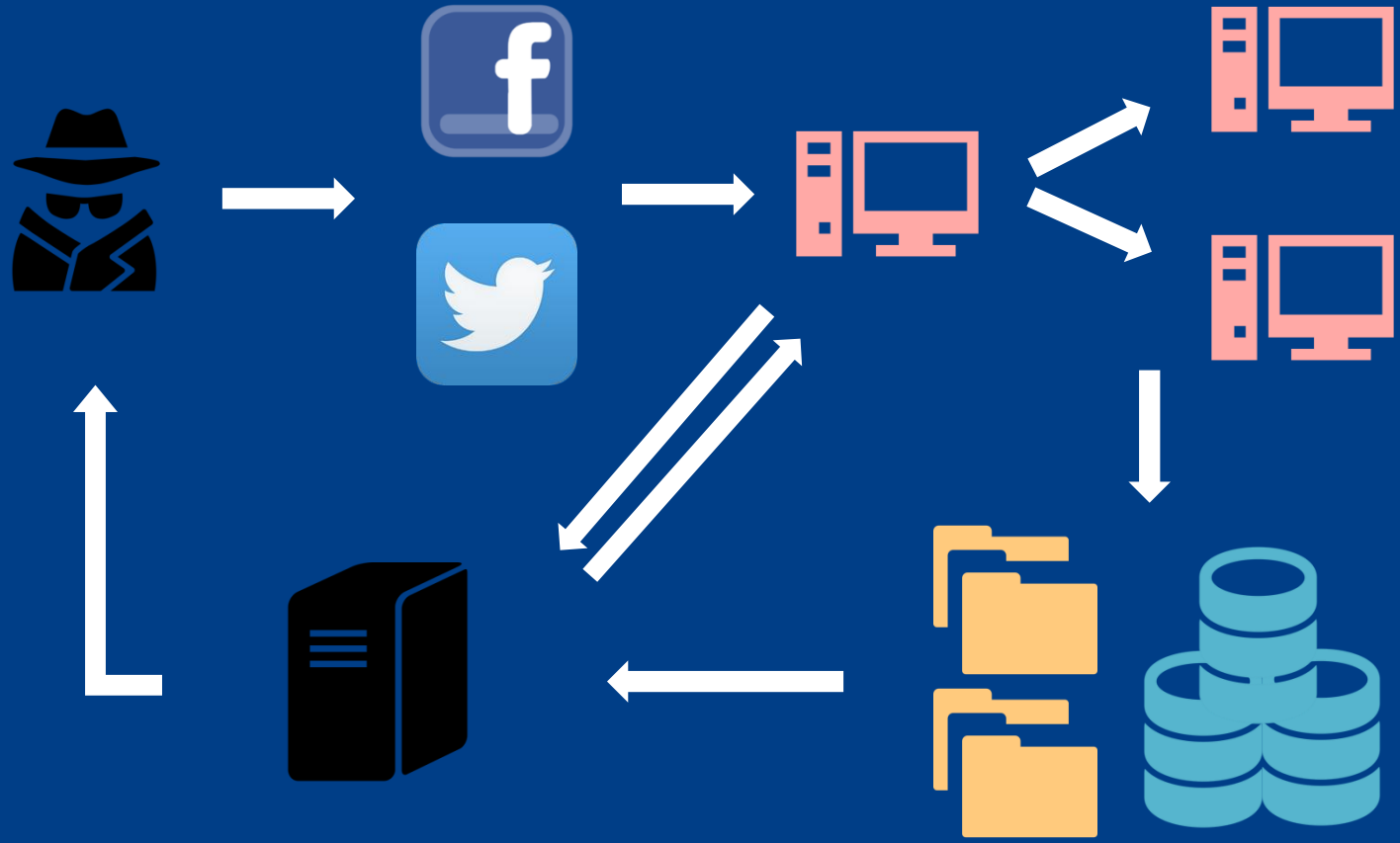
对特定目标进行长期，持续性的网络攻击。

Threat

针对特定目标，特殊群体的重要数据和隐私的持续威胁。



APT攻击步骤



Stuxnet

发现时间2010年6月

截止到2010年09月全球已有约45000个网络被该蠕虫感染，其中60%的受害主机位于伊朗境内。伊朗政府已经确认该国的布什尔核电站遭到Stuxnet蠕虫的攻击。

Duqu

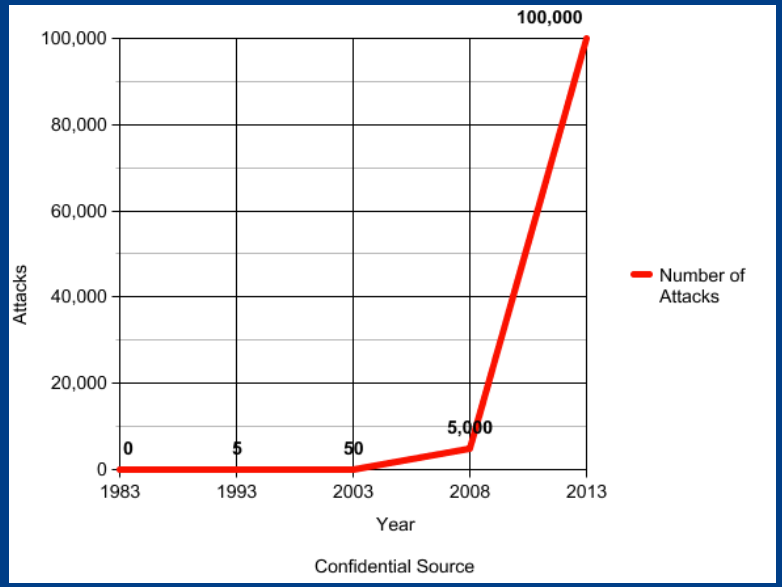
发现时间2011年9月

它采用了一种从来没有人看过的编程语言来编写，这意味着开发这款蠕虫的人士有着相当纯属的编程功底，可以自创编程语言。安全研究人员在一些DLL样本中发现了这种面向对象的未知的语言。

Flame

发现时间2012年5月

其构造十分复杂，危害性巨大，可以通过USB存储器以及网络复制等多种方式传播，并能接受来自世界各地多个服务器的指令，堪称目前世界上最复杂、最危险的病毒。



3

虚拟化环境

安全防护

RISING 瑞星

失去防护的风险

病毒交叉感染

数据泄漏

黑客入侵

系统漏洞

传统防护软件的弊端

过度的存储占用

- 每一个客户端都有一份独立的引擎和病毒码
- 病毒码不断的更新，相同的病毒码重复占用存储空间

定时查杀风暴

- 定时查杀同时启动导致“查杀风暴”
- CPU资源，磁盘I/O资源大量被同时占用

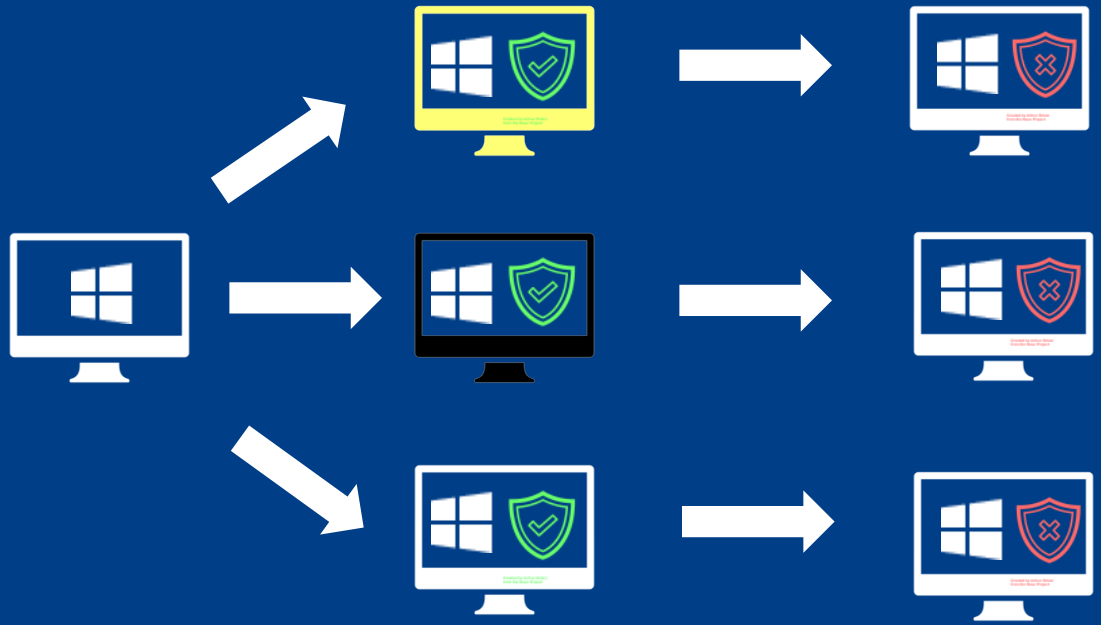
定时更新风暴

- 定时更新同时启动导致“更新风暴”
- 病毒码以及防护软件更新导致大量网络资源被占用

RISING 瑞星

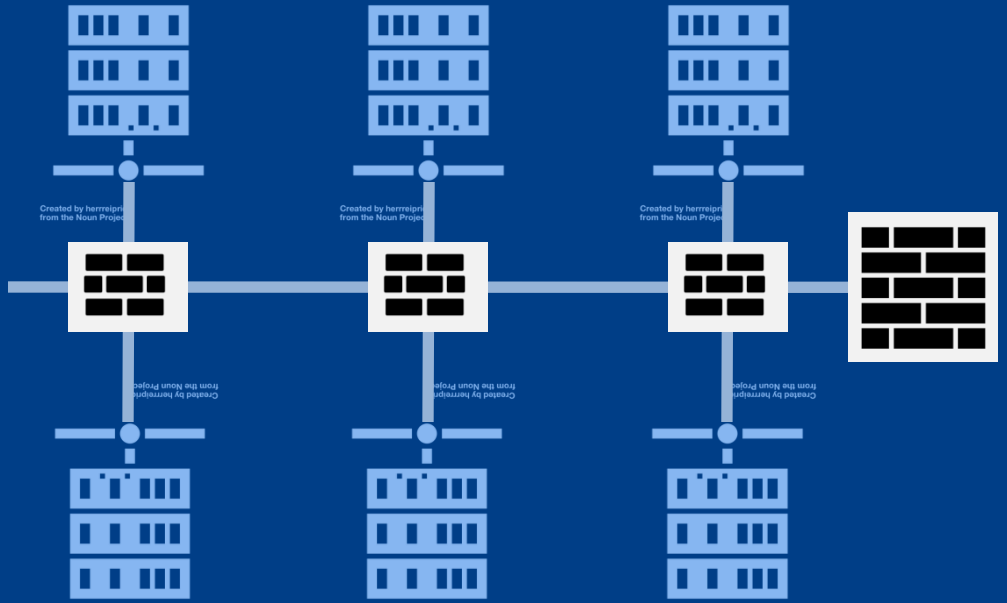
时刻存在的防护间隙

- 模板分发
- DPM
- 恢复快照



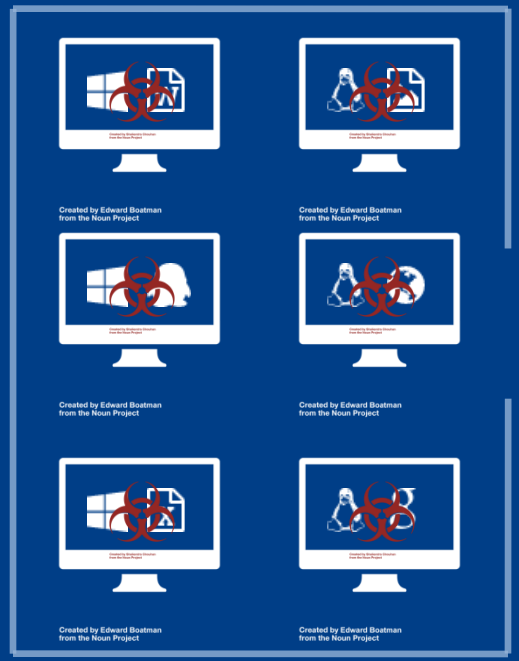
RISING 瑞星

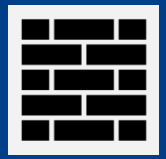
时刻存在的防护间隙



RISING 瑞星

时刻存在的防护间隙





大量的成本消耗

资源压力上升

工作内容增多

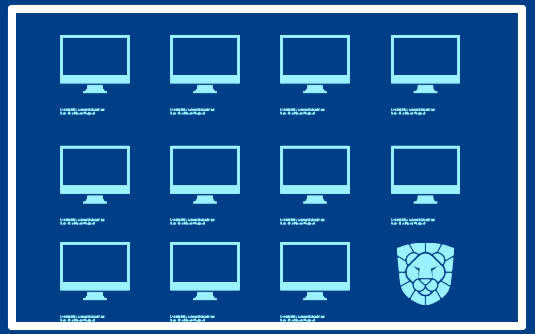
资金成本增加

无代理安全防护的优势

RISING 瑞星

RISING 瑞星

无代理安全防护的优势



两种防护方式对比

	传统安全产品	无代理安全产品
物理服务器 (100台VM)	开启虚拟机 安装安全软件 配置网络 重启虚拟机 **x100** 更新病毒码 划分管理组 设置安全策略	导入设备 配置网络 **x1** 开启设备
虚拟服务器	开启虚拟机 安装安全软件 配置网络 重启虚拟机 更新病毒码 划分管理组 设置安全策略	

RISING 瑞星

无代理安全防护的优势

无需客户端 大幅提高性能

完美兼容 摆脱防护间隙

智能识别 提高访问效率

智能分析 阻断网络攻击

阻断挂马、钓鱼网站的侵害

有效防护各类针对漏洞的攻击

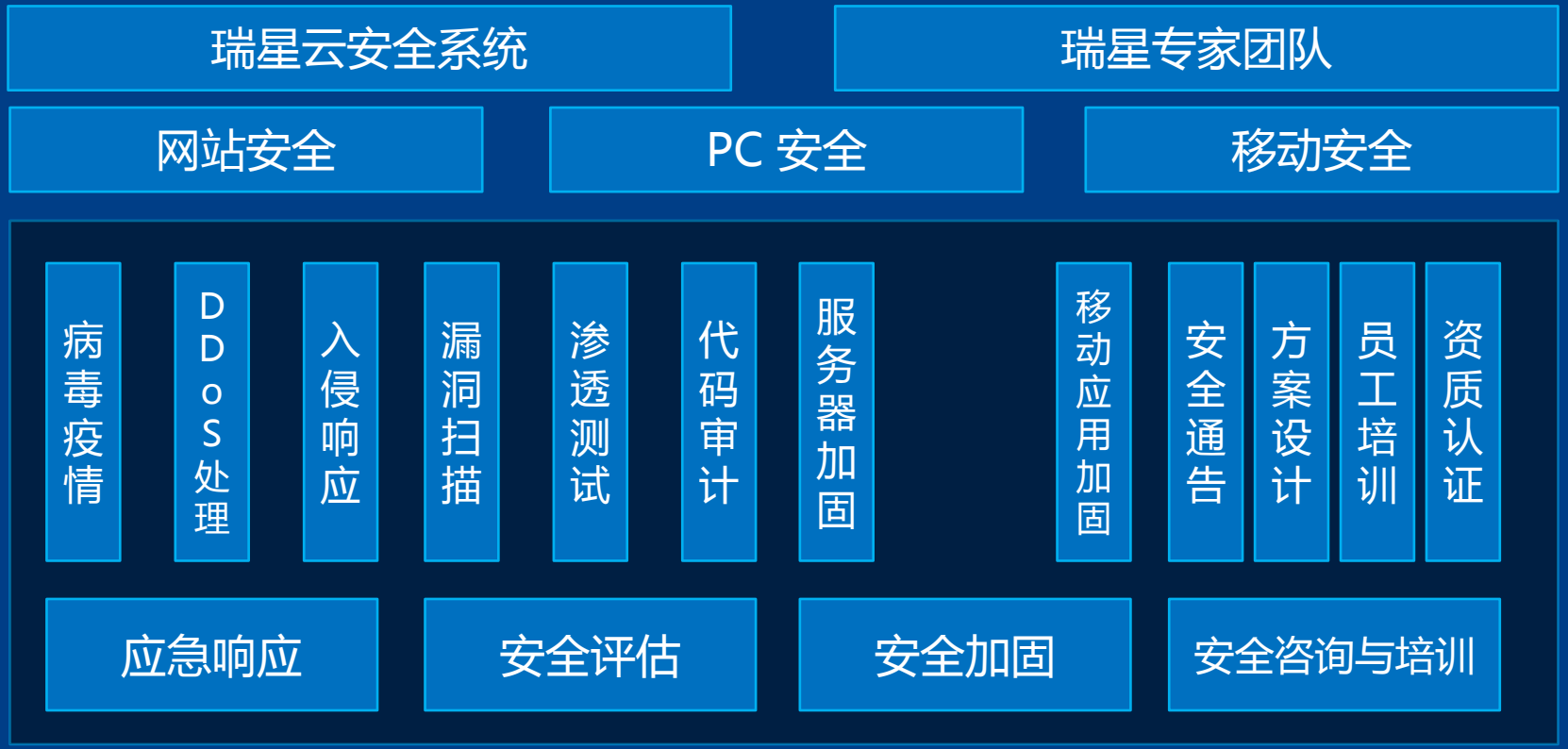
瑞星虚拟化系统安全软件FOR华为

完美结合 降低成本

部署快捷 简易扩展

功能完善 全面防护

虚拟化环境下的全面防护



RISING 瑞星

谢谢