vmware

化繁为简，让“终端”走向“云端”

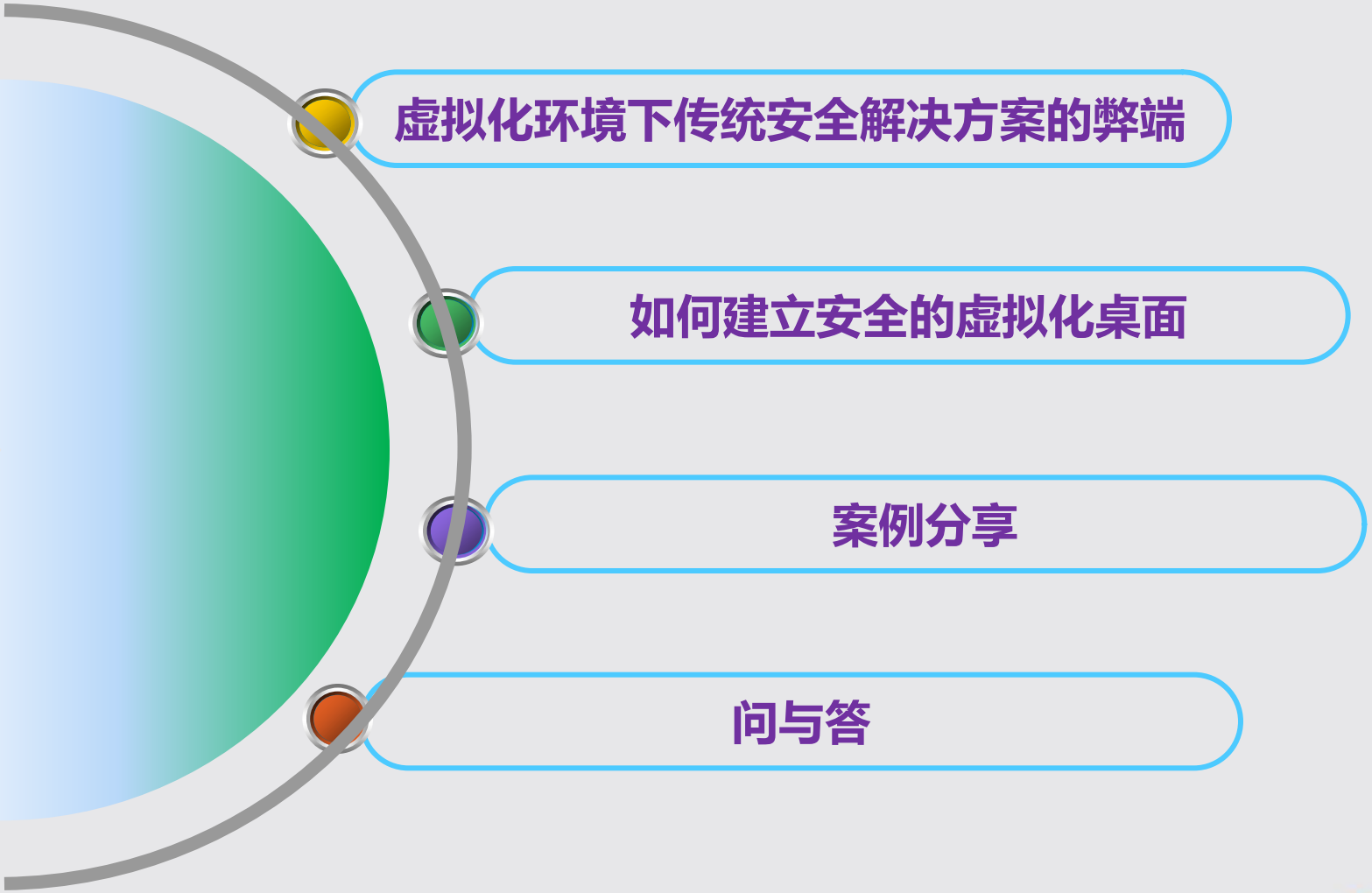
2013“桌面云”技术与应用研讨会

2013年5月9日 青岛中心假日酒店

如何建设安全的虚拟化桌面

罗海龙

趋势科技高级产品经理

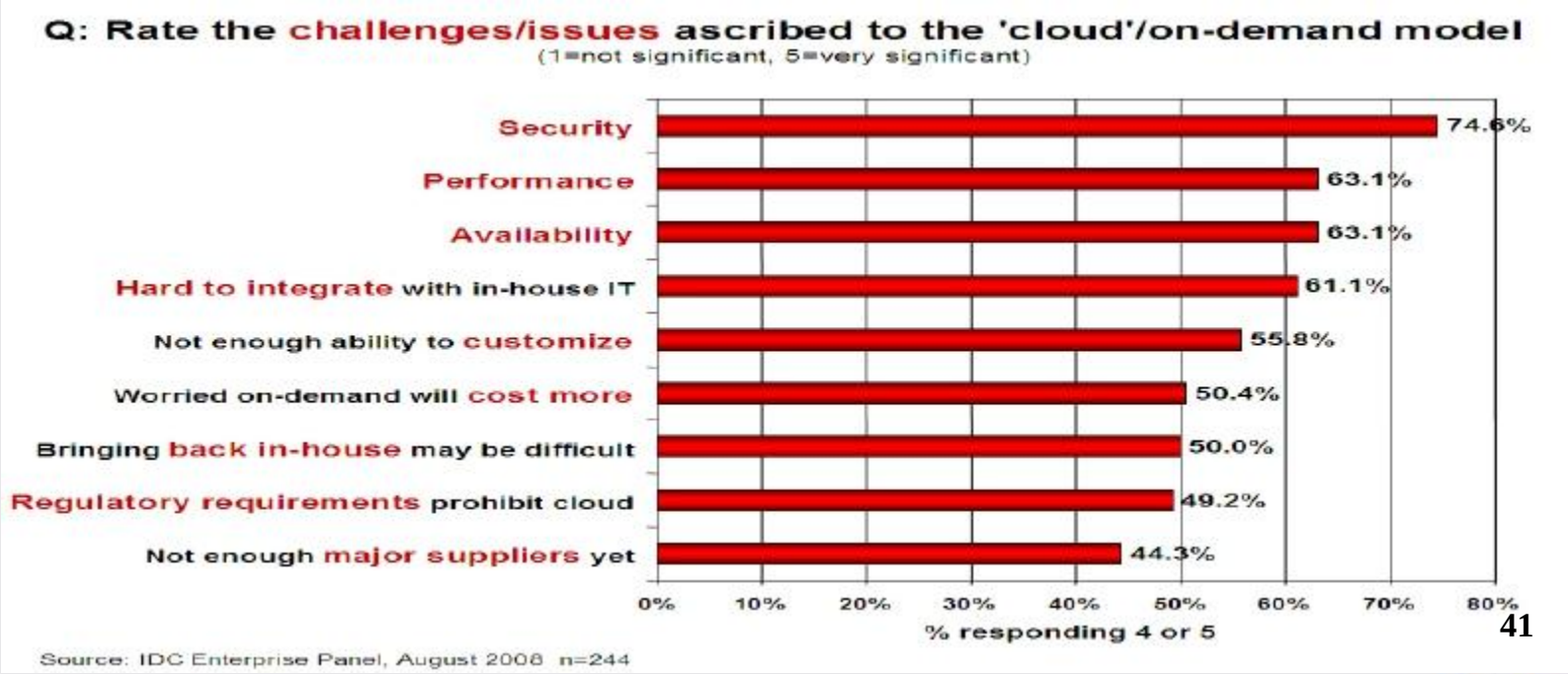


云安全

安全性是广大用户权衡是否使用云计算服务的重要指标之一，是云计算健康可持续发展的基础

IDC 调查报告显示，云计算服务面临的前三大市场挑战分别为服务安全性、性能和稳定性

Forrester Research 调查结果显示，有51%的中小型企业认为安全性和隐私问题是他们尚未使用云服务的最主要原因



云安全的内容

云安全：云计算应用安全+安全云服务

云计算应用安全

- “云上的安全”：云计算应用自身的安全
  - **主要包括如何保障云计算应用的服务可用性、数据机密性和完整性、隐私权的保护等内容**
  - **云计算应用健康可持续发展的基础**

安全云服务

- 云计算技术在安全领域的具体应用，是云计算应用的一个分支
  - **即基于云计算的安全解决方案，通过采用云计算技术在对安全系统进行云化的基础上，实现安全资源的池化，从而提升安全系统的服务效能**

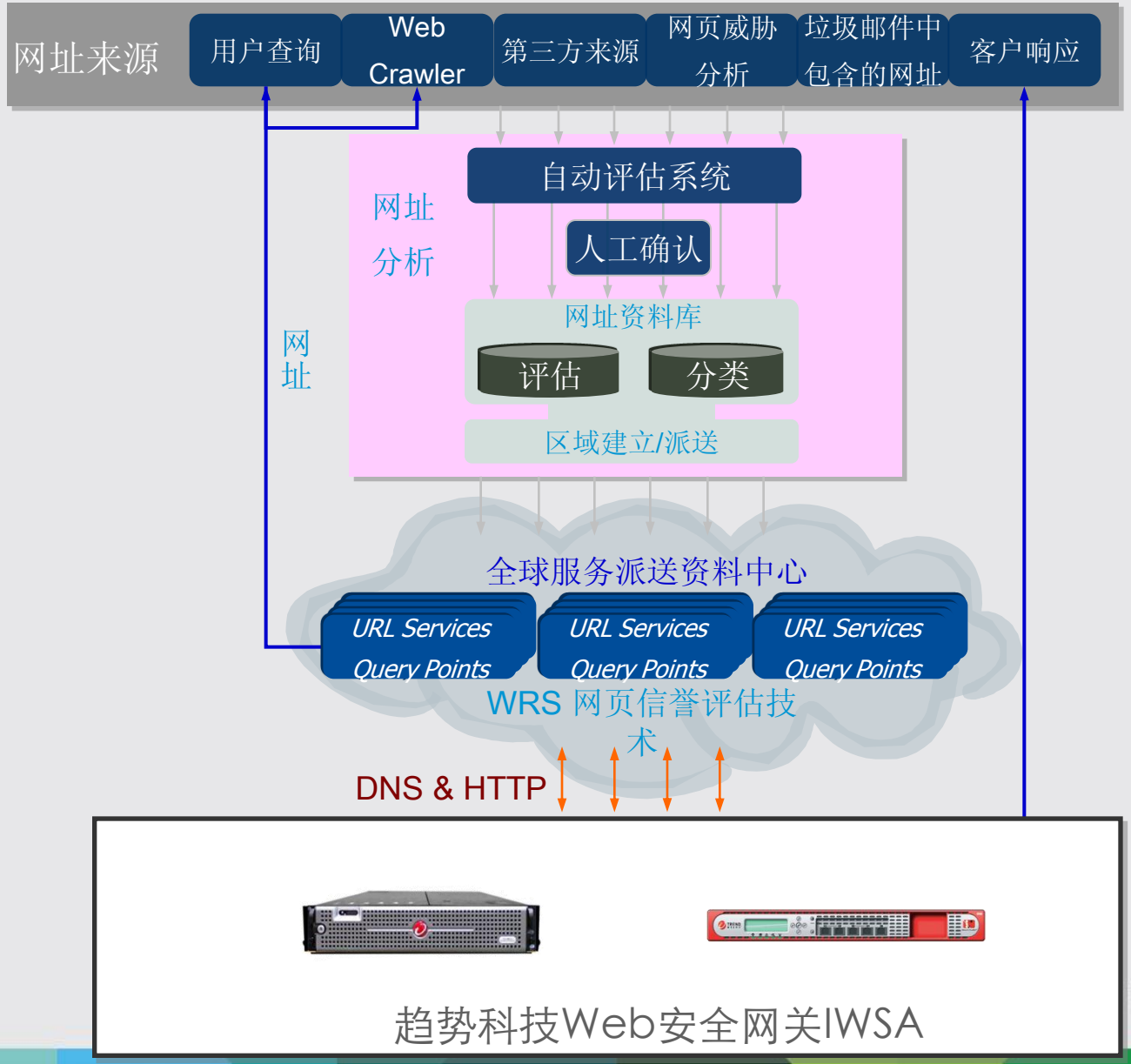
安全云服务

1、智能威胁收集系统

2、计算云

3、服务云

4、安全子系统



6

云计算应用安全

虚拟化

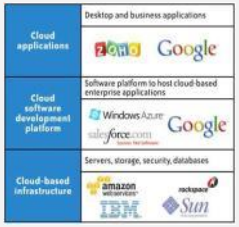
动态的数据中心包含
共享的系统，共享的存储

云终端

普及的, 无界的数据访问,
无处不在的数据

全面性云计算
安全管理

云中数据



数据所有权 vs. 运算保密 & 访问控制

云端应用

新应用的新平台. 例如,
网页篡改, SQL 注入

数据中心的发展

物理环境

Windows/Linux/Solaris

虚拟化环境

服务器虚拟化

桌面虚拟化

云平台

公有云

私有云

混合云

虚拟化

挑战

- 如何减少硬件资产的总成本
- 如何提高IT管理效率
- 过低的服务器利用率（3-5%）
- 不断增长的能源和制冷的成本
- 有限的机房空间

解决方案

- 通过服务器虚拟化技术，实现可管理的整合的数据中心

传统安全应用在虚拟化系统

虚拟化实践逐步深入，“免罪金牌”不再适用

防病毒风暴

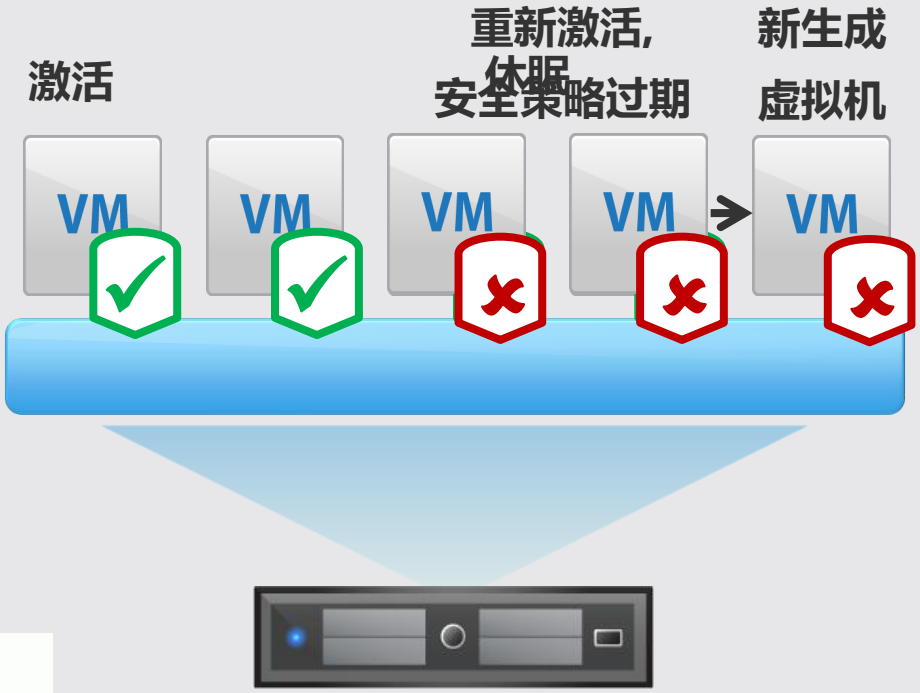
1 资源争夺

传统安全软件如何造成
- 定期扫描
  - **CPU + IO**
  - **网络**硬盘
- 病毒库更新
  - **网络**
  - **IO**
- 病毒库于内存所常驻
  - 重复的**内存**使用

传统安全软件
造成资源冲突
降低虚拟机密度

快照、还原的威胁和安全风险

1. 资源争夺
2. 随时启动的防护间隙

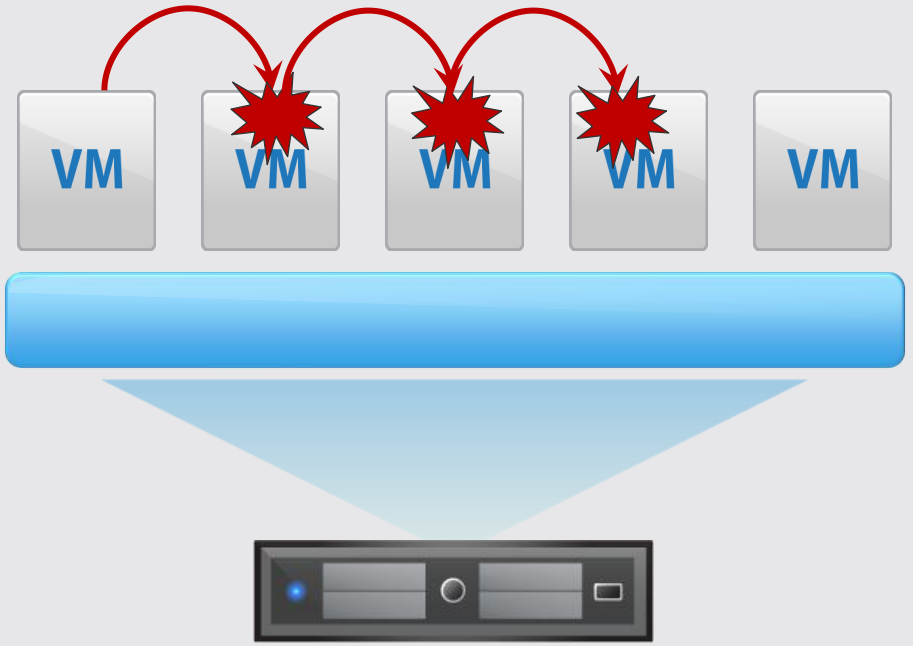


虚拟机必须带有

已配置完整的客户端和最新的病毒库

每个虚拟机都是安全漏洞

1. 资源争夺
2. 随时启动的防护间隙
3. 虚拟机之间攻击 / 防护盲点



攻击在虚拟器之中发生

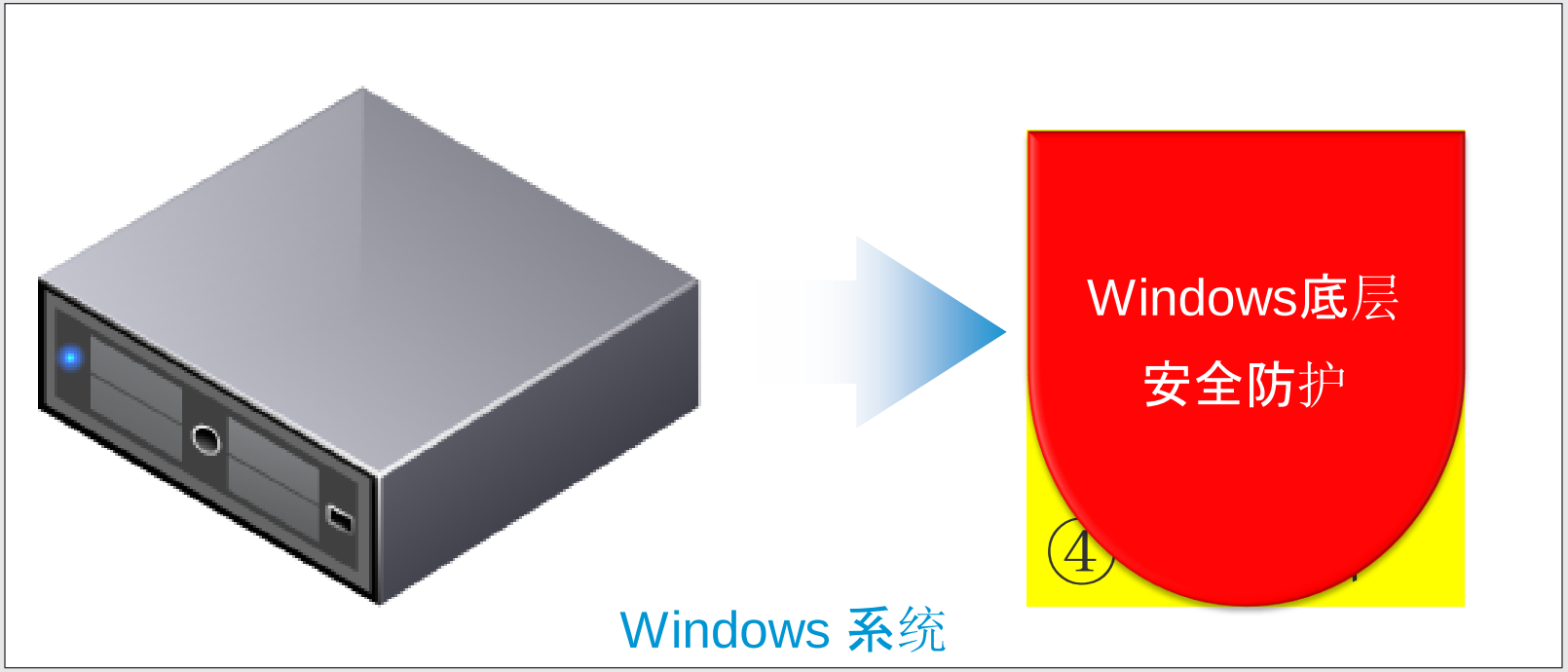
需要管理的终端数量增长

1. 资源争夺
2. 随时启动的防护间隙
3. 虚拟机之间攻击 / 防护盲点
4. 虚拟机个别管理复杂

管理成本随着系统总量上升

14

如何解决虚拟化的安全问题

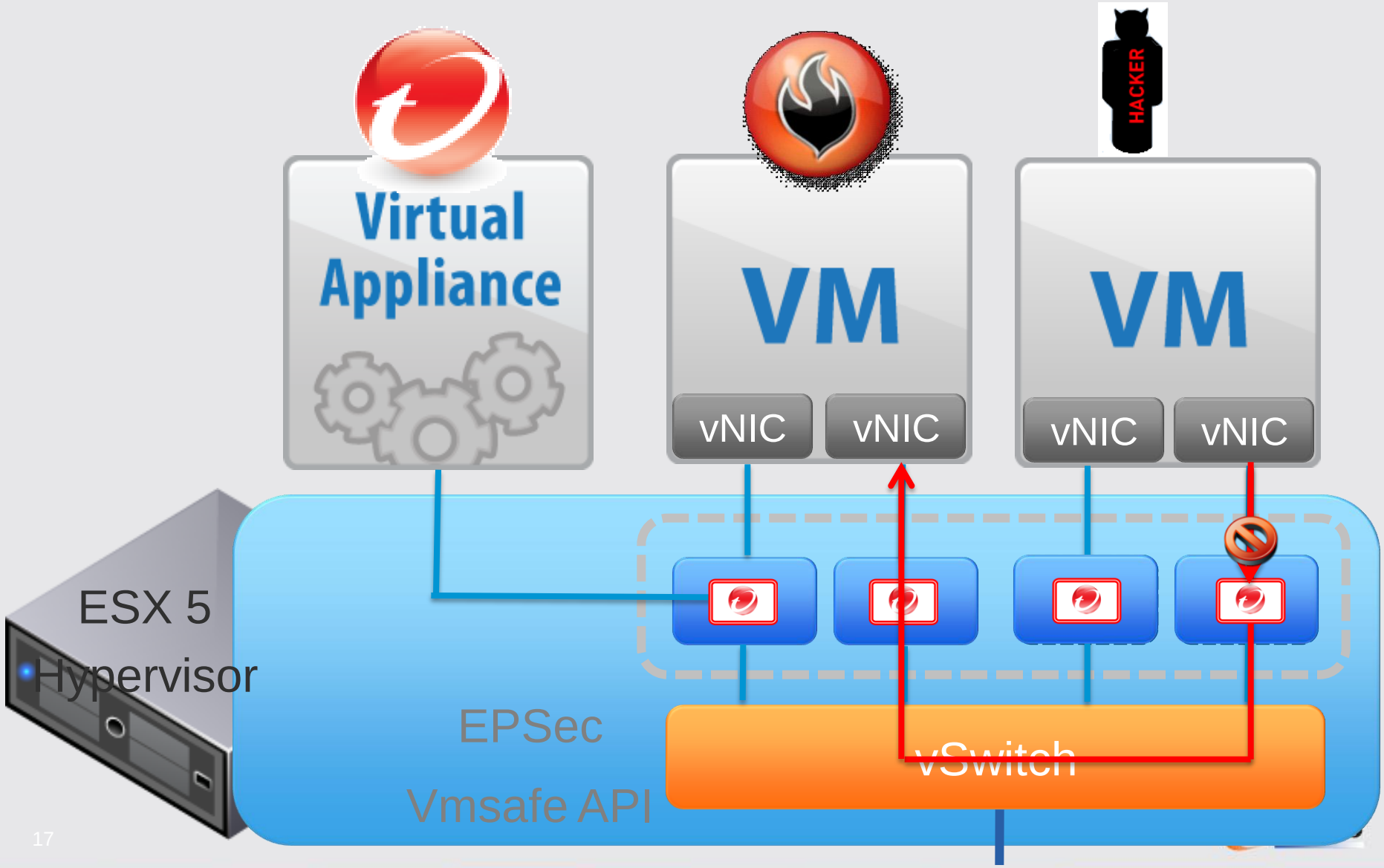


应在虚拟化系统底层解决安全问题

无代理工作原理一

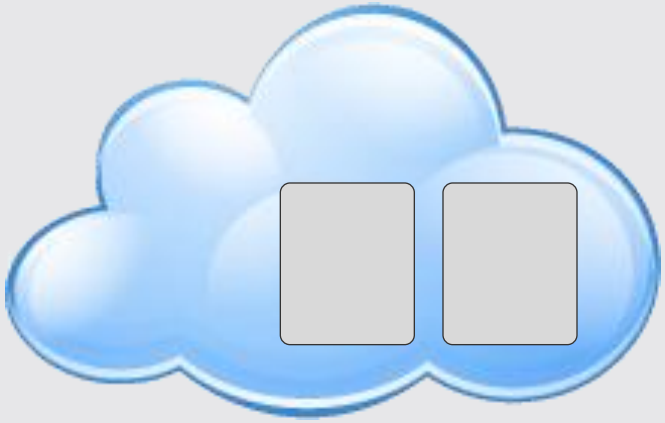

安全管理员
集中管理接口
安全虚拟机
Partner
Agent
EPsec
Interface
vShield Endpoint
预设扫描接口
实时扫描接口
清除、修复接口
缓存 & 过滤
状态监控
REST
Guest VM
APPs
OS
Guest Driver
VI Admin
vShield Manager 5.1
vCenter
ESX 5.1
vSphere 平台
vShield Endpoint
ESX Module
图例
安全产品提供商
DSVA组件和API接口
vShield Endpoint组件
Vmware平台
VMware
内部接口
安全产品接口

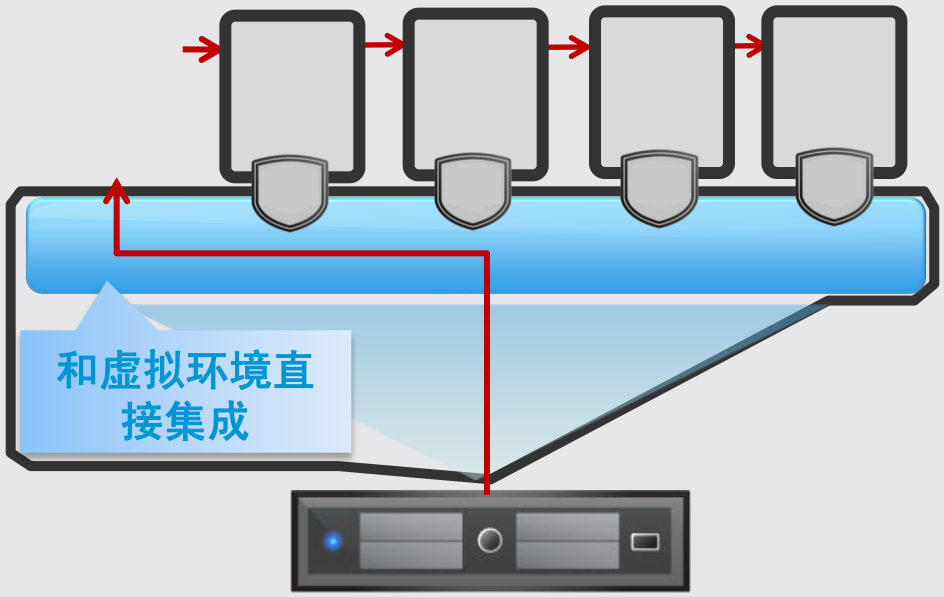
无代理工作原理二

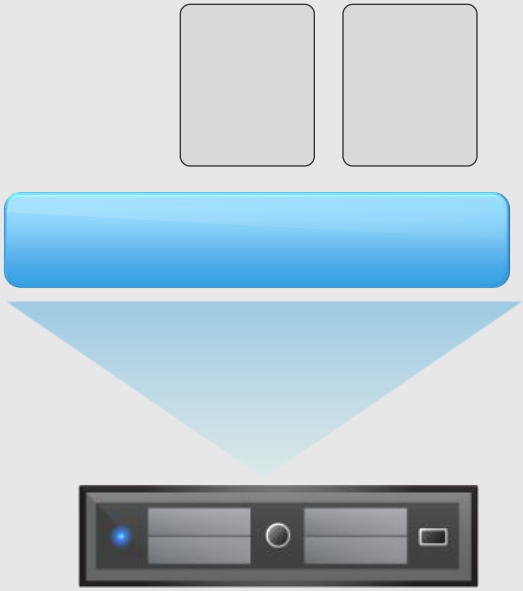

Virtual Appliance
VM
vNIC
vNIC
HACKER
VM
vNIC
vNIC
ESX 5 Hypervisor
EPSec
Vmsafe API
vSwitch

实现方式

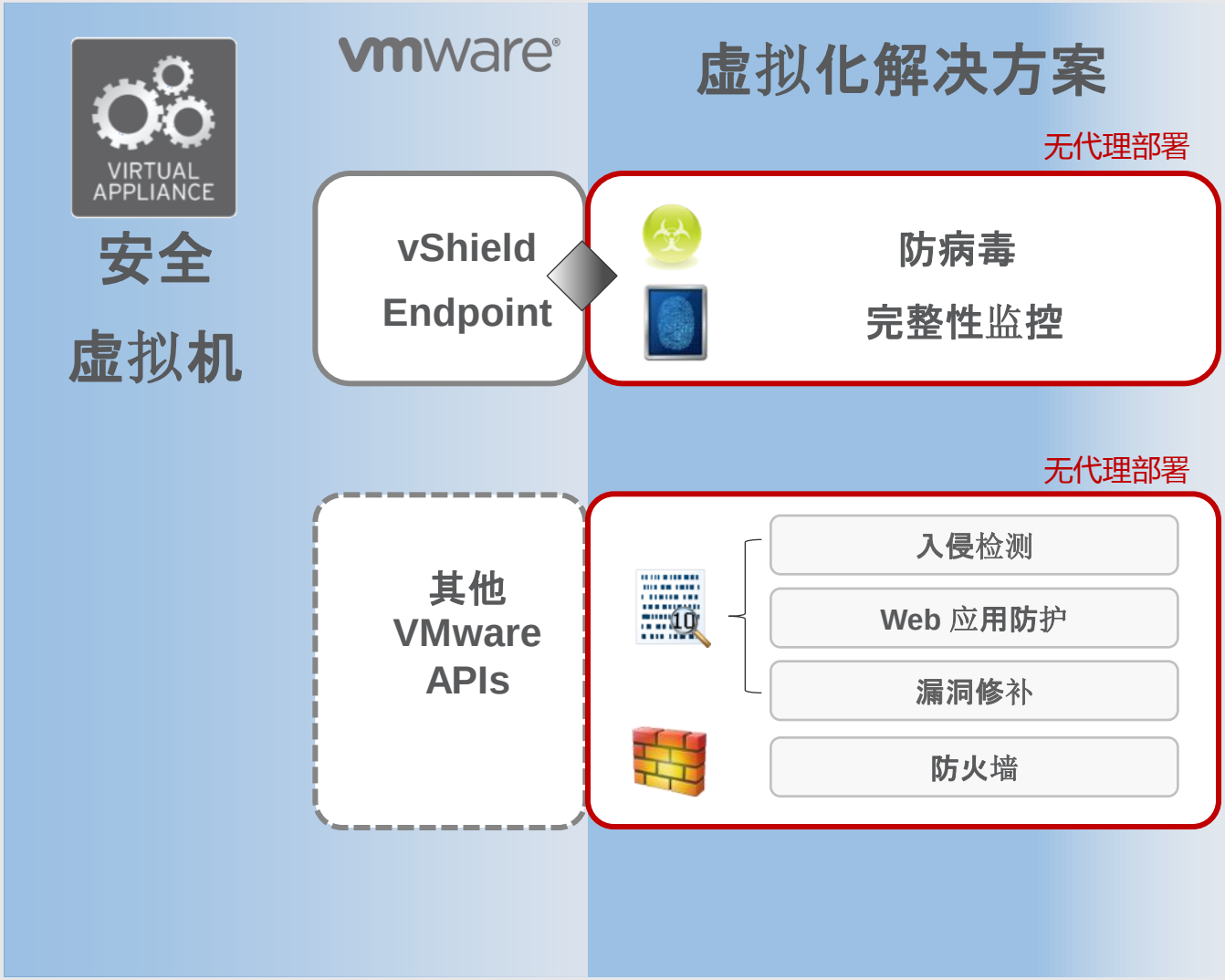
杀毒模块	系统监控	入侵防护
防火墙	应用保护	虚拟补丁







趋势科技为虚拟化构架的安全—Deep Security



虚拟环境的解决方案

1. 资源争夺

解决方案：无代安全具备虚拟环境感知能力，基于虚拟器整体资源所分发的安全任务有效避免资源争夺

2. 随时启动的防护间隙

解决方案：基于虚拟器部署的安全虚拟机实时使用最新威胁特征库

3. 虚拟机之间攻击 / 防护盲点

解决方案：与虚拟化平台所集成的虚拟环境感知安全解决方案

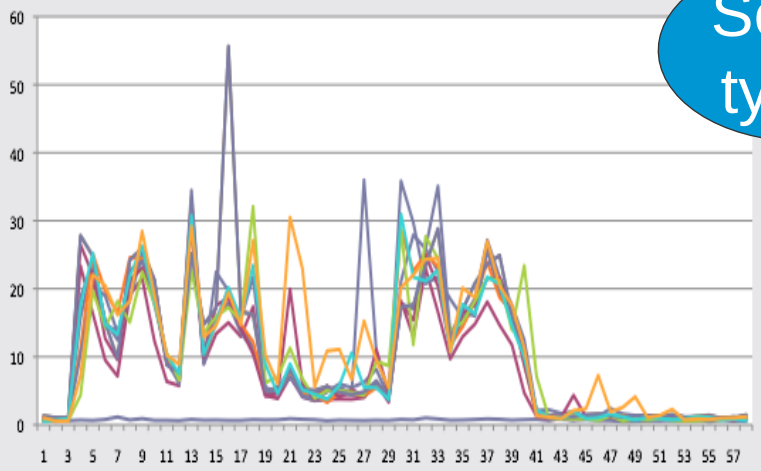
4. 虚拟机个别管理复杂

解决方案：与虚拟环境管理平台 VMware vCenter 集成，自动侦测安全层级不足的虚拟器

Deep Security特性---高性能

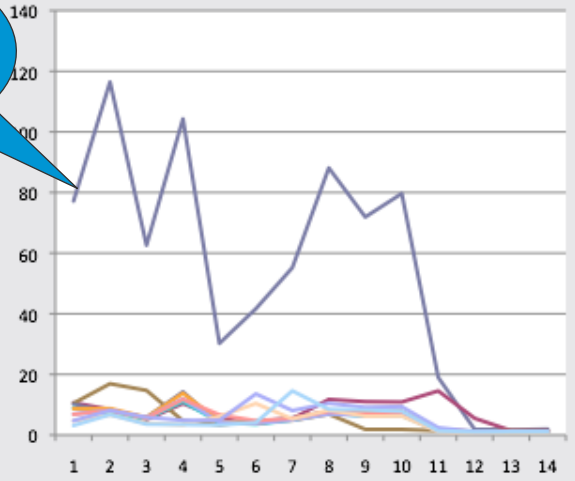
- **可以实现底层与虚拟系统所打造的安全软件，每台物理服务器安装一次**
  - 提升硬件服务器使用率
  - 简化安全管理
  - 具备自动继承的保护
- **性能状况：有客户端 VS 无客户端**

VM CPU Rate（有客户端）



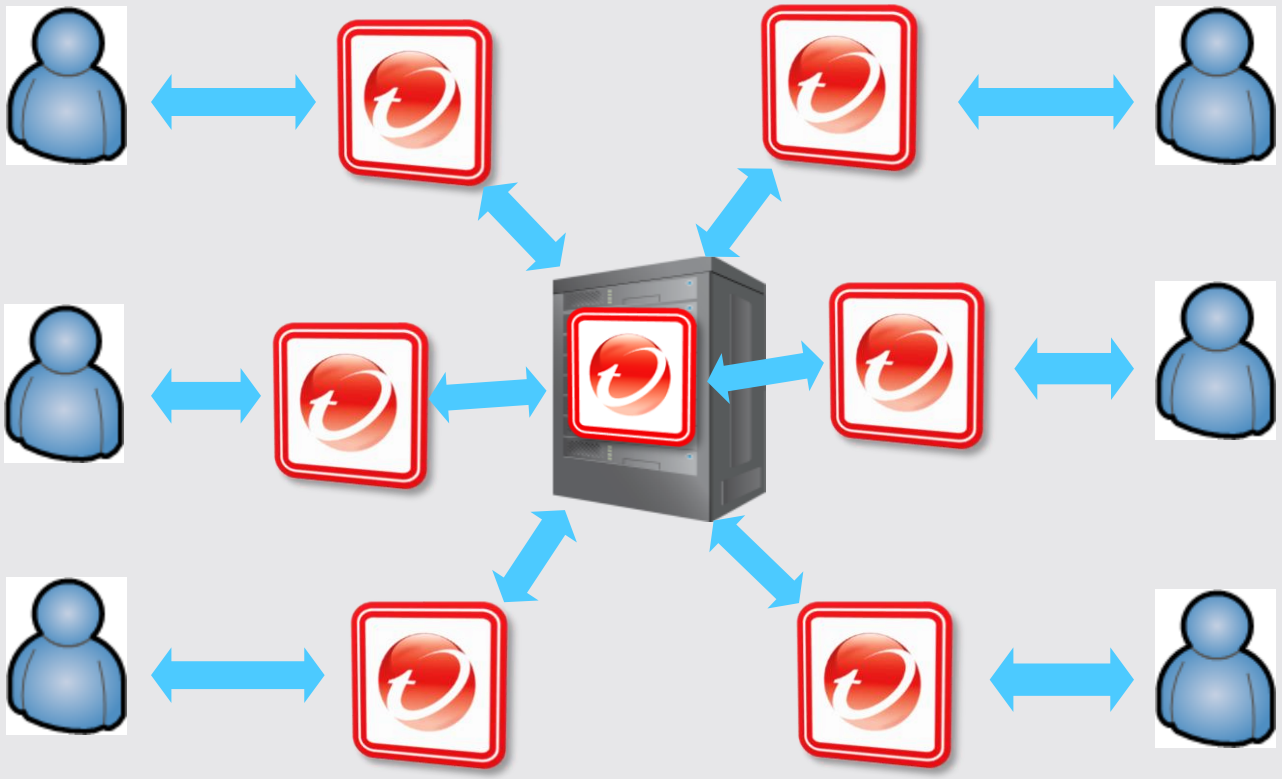
Security VM

VM CPU Rate（无客户端）



Deep Security特性---多租户

多租户功能实现安全即服务(Deep Security as a Service)，每一个租户都有一个虚拟的Deep Security 管理端

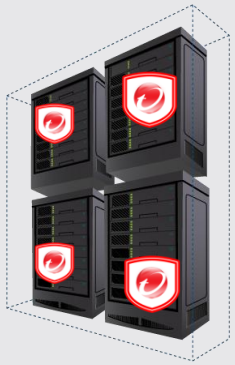


Deep Security特性---多平台

Deep Security

物理机

虚拟机



云

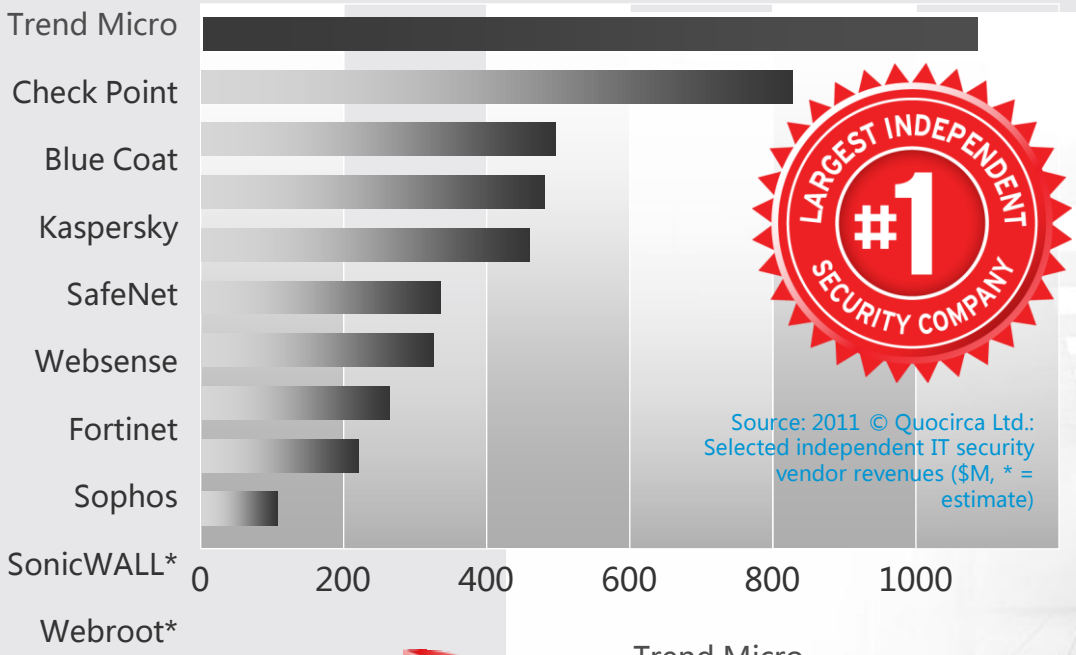
灵活适应各种环境

防护超过22种平台

保护超过56种应用/服务系统

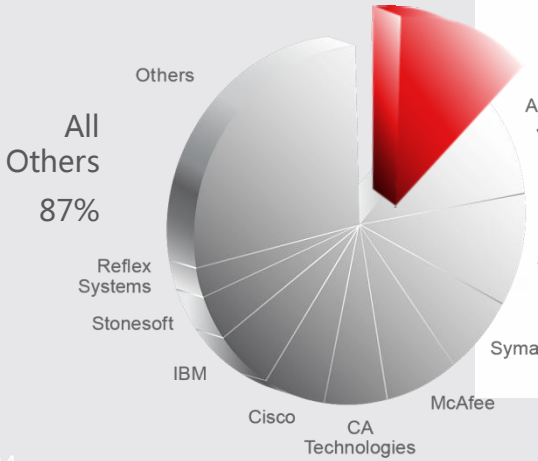
Microsoft
solaris
vmware
CITRIX
suse
redhat
AIX
hp
HP-ux
Microsoft Hyper-V Server 2008
ORACLE
IPSWITCH File Transfer Simple. Secure. Managed.
Microsoft Office
Microsoft SQL Server 2008
www.sj33.cn
Windows Internet Explorer 7
Microsoft Exchange Server 2010
Certified for IBM Lotus e-business software
Mozilla Firefox
Adobe PDF
QuickTime
e-works

Deep Security特性---各界的认可



LARGEST INDEPENDENT #1 SECURITY COMPANY

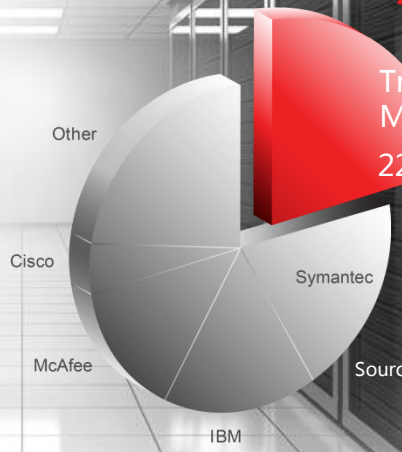
Source: 2011 © Quocirca Ltd.: Selected independent IT security vendor revenues ($M, * = estimate)



Trend Micro 13%

GLOBAL VIRTUALIZATION #1 MARKET LEADER

SERVER SECURITY #1 MARKET SHARE



All Others 77.1%

Source: Worldwide Endpoint Security 2010-2014 Forecast and 2009 Vendor Shares, IDC

Source: 2011 Technavio – Global Virtualization Security Management Solutions

中国区各大行业用户

金融行业

君龙人寿 KING DRAGON

中国出口信用保险公司 China Export & Credit Insurance Corporation

海通证券

中信证券 CITIC SECURITIES

信诚基金管理 满载诚信 全力以富

政府行业

宁波市公安局 WWW.NBSGAJ.GOV.CN

揭阳市国家税务局

长春民政

制造行业

中国烟草 CHINA TOBACCO

长春客车厂

上海大众

TSINGTAO 青岛啤酒

BRIDGESTONE 普利司通轮胎

企业及其他

中国南方电网 CHINA SOUTHERN POWER GRID

中国移动通信 CHINA MOBILE

中国电信 CHINA TELECOM

B&Q 百安居

新华社 XINHUA NEWS AGENCY

成功案例 – 云基础设施安全

美国国际集团:整合 29 个数据中心

业务需求

– 降低硬件成本

– 全球29个数据中心整合为2个 (第三个为灾难)

– 项目命名为 Next Generation Data Center (下一代数据中心)

–有效“整合服务器” 是战略目标

问题&挑战

– 在虚拟环境上所碰到的新挑战
  * 网关无法透视虚拟器

– 传统安全不适应新环境
  * 整合率

– 虚拟环境构架的解决方案和管理优势
  * 平滑升级
  * 物理、虚拟混合部署
  * 管理简化

应用场景

– vSphere v5

– 每个物理 ESX 部署一个 DSVA (安全虚拟机), 以主机为单位的管理

–次部署、多层防护:
  * 无代理防病毒
  * 虚拟补丁
  * 完整性监控

– 不仅整合数据中心、同时整合多个安全软件

成功案例 – 桌面虚拟化

国际零售业:整合 57 个分店和数据中心

- 中国第一大 DIY 零售店，欧洲第二大
- 将57个分店，数万台的终端转换为 VDI 架构
  - 巨大的终端管理成本
- 简化管理
  - 硬件整合
  - 多个解决方案集成
  - 综合的安全
  - 终端补丁管理

成功案例 – 虚拟资源优化

- 中国第二大酿酒厂
- 过上百个虚拟终端后，为虚拟环境优化的安全需求持续增加
  - 近耗尽的虚拟资源池
- 虚拟化构架的安全释放虚拟资源，同时提升安全性

vmware

提升安全性

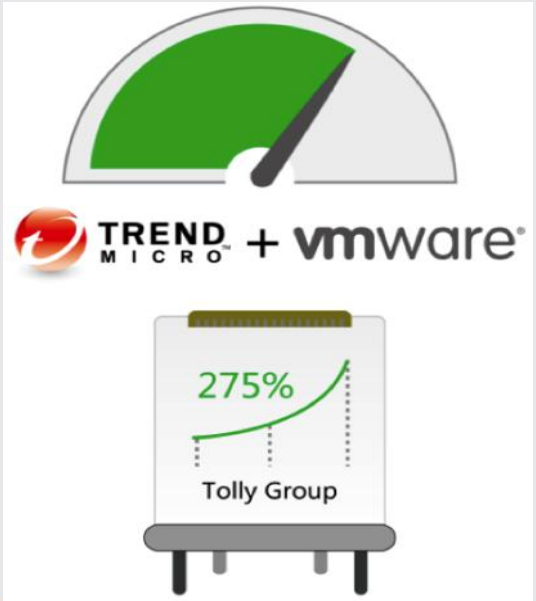
通过提供最安全的虚拟化基础设施，与API和认证计划

提升虚拟化

通过基于VMware平台提供安全解决方案，以充分发挥其效率

更强的安全

更高投资回报率



简化管理

vmware

化繁为简，让“终端”走向“云端”

2013“桌面云”技术与应用研讨会

2013年5月9日 青岛中心假日酒店