数据中心安全

卡巴斯基
虚拟化安全解决方案

为虚拟服务器和VDI提供灵活、高效的出色保护

随着虚拟环境被越来越广泛地应用于企业IT领域，企业对虚拟化专用安全解决方案的需求也在日益加剧。但是要找到一款既能为快速成长的虚拟桌面基础架构（VDI）提供有效的安全保障，又能在保留虚拟化所有优势的前提下实现虚拟服务器环境安全的解决方案绝非易事。

虚拟和物理终端面临着同样的安全威胁以及同样的网络犯罪。虚拟基础架构一旦因安全漏洞而遭到破坏，企业将为之付出高昂的代价，因此安全问题不容懈怠。与此同时，企业还应确保最佳的性能。

卡巴斯基虚拟化安全解决方案为VDI和虚拟服务器环境提供出色且多层级的细粒度保护。我们独一无二的解决方案能够提供强大的保护，同时不占用系统资源，亦不会影响性能。相比传统的解决方案，卡巴斯基虚拟化安全解决方案能实现更高的整合率，完美兼顾虚拟化技术构架的性能与安全。

亮点

卓越保护

- **为主流平台上的所有虚拟机提供强大的实时保护，适用于VMware vSphere、Citrix XenServer、KVM和Microsoft Hyper-V。**
- 包含应用程序控制以及Web和设备控制等增强功能，保证VDI用户的安全性与高效性。
- 屡获殊荣的高级漏洞防护（AEP）技术保护企业虚拟化环境远离复杂威胁和安全漏洞。
- 集成基于云的卡巴斯基网络安全（KSN），主动防御新兴威胁。
- 强大的入侵检测系统与入侵防御系统（IDS/IPS）识别与拦截已知、未知和高级的漏洞利用型威胁。

更出色的性能

- **采用创新专利设计[1]确保最低的资源占用，从而优化整合率，实现最高密度。**
- 专为虚拟化设计的安全解决方案，节省宝贵的管理资源。
- 强大的轻量级保护可减轻文件扫描任务的负载，使用智能化的流程保障平台的整体效率。
- 为VMware Horizon和Citrix XenDesktop提供多层级保护，不影响VDI终端用户的体验，同时确保平台性能和响应速度。

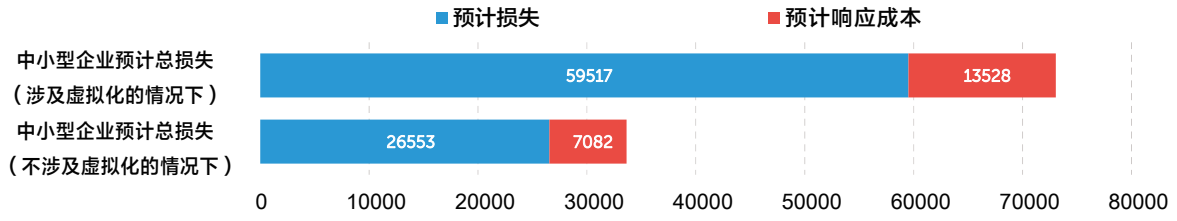
vmware PARTNER TECHNOLOGY ALLIANCE
vmware READY NETWORKING AND SECURITY
CITRIX READY
VBLOCK READY
VCE VALIDATION READY

1 美国专利号9009836及9088618

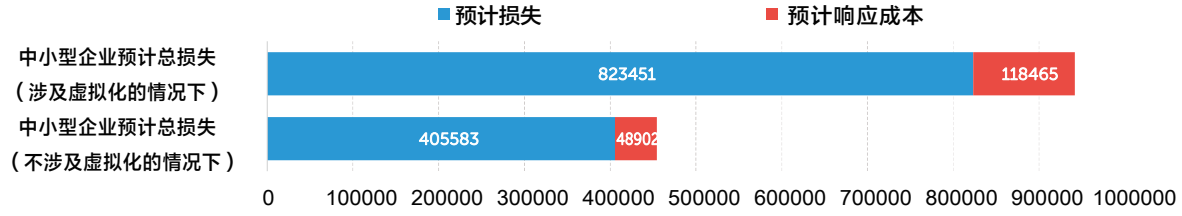
2015年，卡巴斯基实验室联合B2B International公司对5564位来自全球35个国家不同规模企业的IT专家就虚拟化安全相关问题进行了调查。

调查发现：

- 若安全事故涉及到虚拟基础架构，**企业的修复成本会增加一倍。**
  - 中小企业修复每起安全事故的平均直接成本约为6万美元。

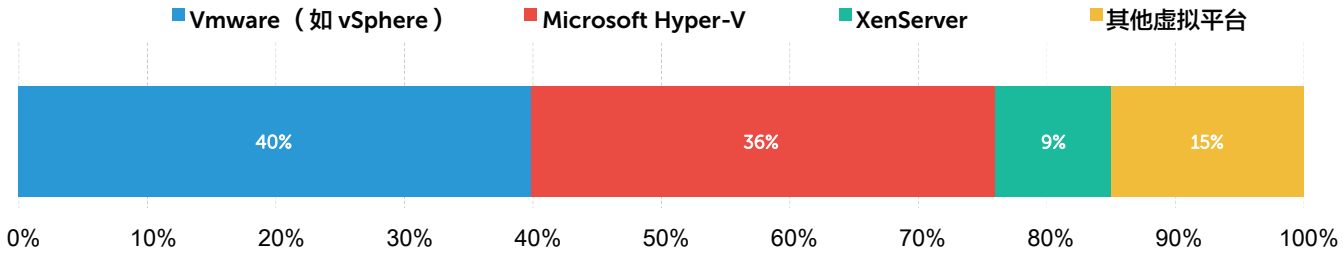


  - 企业在安全修复方面的花费超过$800,000。



- 成本增加的三大原因：
  - 安全的复杂性：仅有56%的受访企业表示做好了应对虚拟环境安全风险的充分准备。
  - 企业有必要加深对虚拟环境安全风险的认识：仅有52%的受访企业代表表示对风险有充分的认识。
  - 将虚拟设施广泛应用于关键任务操作。

- 62%的受访企业正在使用某类虚拟基础架构。
- 受访企业使用最多的三大虚拟平台：VMWare（40%）、Microsoft（36%）及Citrix（9%）。



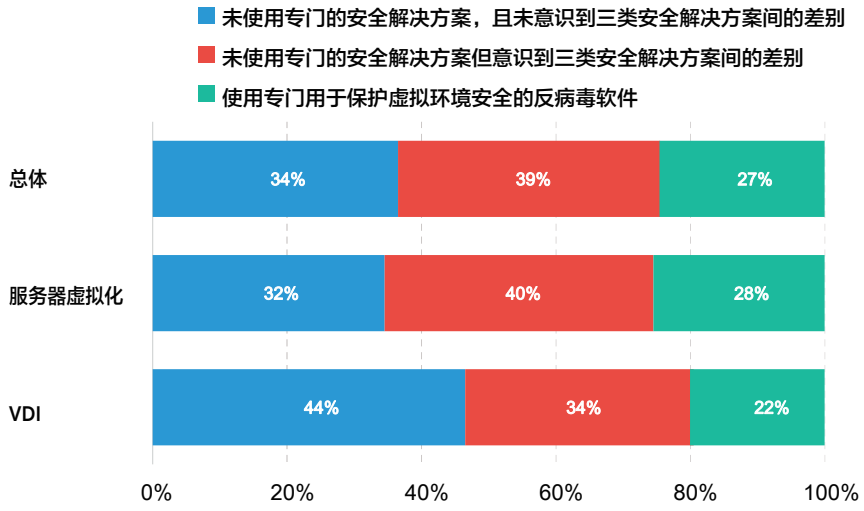
- 有9%的受访企业使用开源虚拟平台：Xen(6%)与KVM(3%)。
- 42%的受访企业仍认为虚拟环境比物理环境更为安全。
- 鲜少受访企业采用专门的虚拟环境安全解决方案：
  - 有73%的受访企业未使用专门的IT安全解决方案。
  - 有34%的受访企业甚至尚未意识到使用安全解决方案的好处。

虚拟基础架构安全

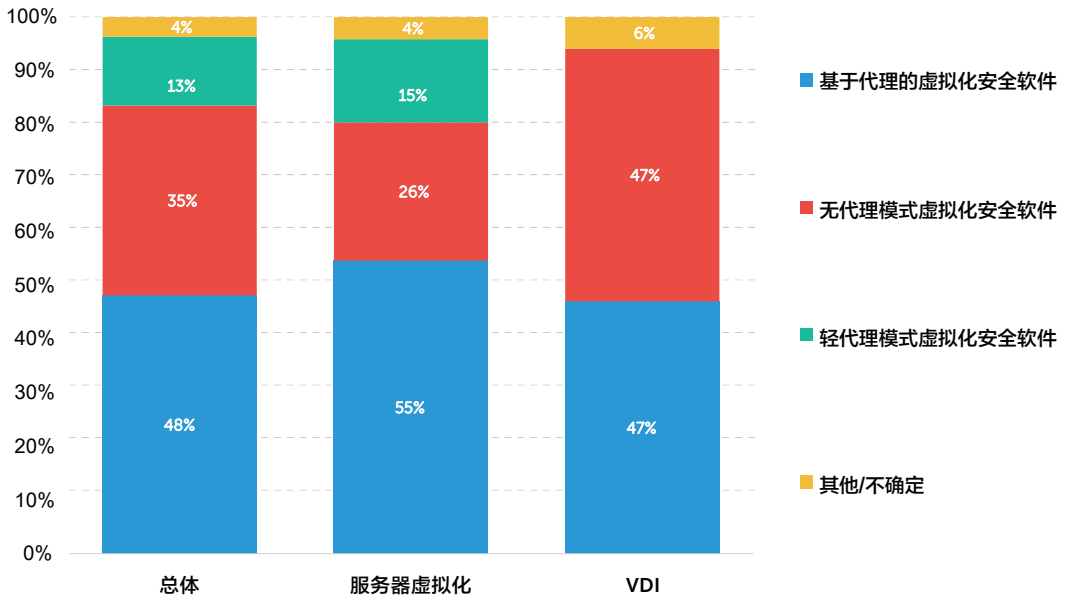
目前市场上主要有三种虚拟环境安全解决方案：

- 基于代理的安全解决方案：需在每台虚拟机上安装安全代理（这种安全解决方案有丰富的安全功能，占用较多资源）
- 无代理模式安全解决方案：将虚拟机安装在另一台物理服务器上，通过专门的虚拟平台界面实现对所有虚拟机的安全保护（这种安全解决方案资源占用量小，但功能与支持的平台有限）。
- 轻代理模式安全解决方案：一种两全其美的安全解决方案（相比无代理模式，这种安全解决方案功能丰富且对性能影响小）

研究表明，很多公司并未真正意识到上述三类安全解决方案的差别。事实上，仅有27%的企业表示部署了专门用于虚拟环境防护的安全解决方案。



在使用专门的IT安全解决方案的企业中，有48%的受访企业使用基于代理的安全解决方案，使用无代理模式和轻代理模式安全解决方案的企业仅分别占35%和13%，所占比例远低于基于代理的安全解决方案。



更高的效率

- **卡巴斯基实验室的安全虚拟设备（SVA）可集中扫描主机环境中的所有虚拟机。只需在每台虚拟机上部署一个轻代理，即可享受更深层次的保护。简单直接，无需重启。**
- 杜绝更新、扫描“风暴”、漏洞窗口与“即开即用”漏洞的出现。
- 反网络攻击、应用程序防火墙、基于主机的入侵防御系统（HIPS）和反钓鱼技术的强大组合可保护虚拟机免遭网络威胁。
- 支持VMware NSX和vCNS，完美适应基础架构和网络拓扑的变化。

一流的灵活性和可视化

- **专为虚拟服务器和虚拟桌面设计的首选安全方案充分满足企业的需求。**
- 灵活的授权许可选项——可基于虚拟机（桌面或服务器）或硬件资源（内核数）的数量选择授权许可。
- 通过单一控制台统一管理物理机、虚拟机和移动设备。
- 功能多样的报告和监测使组织内部安全的管理与监督更加简便易行。

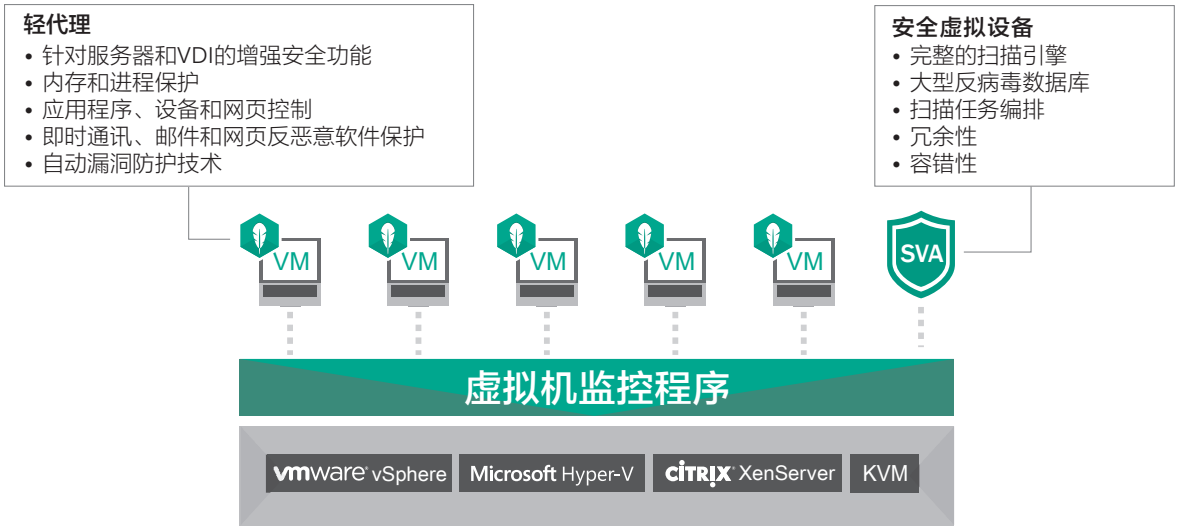
使用无代理技术

卡巴斯基虚拟化安全解决方案同vShield Endpoint和NSX等VMware技术紧密整合。由于无需在每台虚拟机上额外安装代理，系统对虚拟平台性能的影响近乎于零，管理任务轻松简洁，并且每一台运行的虚拟机均处于实时保护之中。

无代理技术适合需要强大的文件级安全保护和网络保护的、基于VMware的基础架构。对于业务关键型虚拟服务器和桌面，在虚拟机上安装一个代理能够实现更高级的安全功能。

独家轻代理技术

原理与作用



每台主机上的安全虚拟设备（SVA）可集中扫描所有虚拟机。同时，部署在每台虚拟机上、强大的轻量级代理可以激活高级安全保护功能，包括应用程序、设备和网页控制，即时通讯、邮件和网页反恶意软件保护以及先进的启发式分析技术。

卡巴斯基虚拟化安全解决方案与包括VMware vSphere、Microsoft Hyper-V、Citrix XenServer和KVM在内的主流平台紧密整合，因而可充分利用管理程序自有的核心技术，并在此基础上完善及增强虚拟环境（如VMware Horizon和Citrix XenDesktop VDI）的安全性，优化业务关键型基础架构的性能。

卡巴斯基的虚拟化安全解决方案将轻代理和无代理两种模式合二为一，在为虚拟环境提供强大保护的同时，还确保高效的性能。

如需详细了解卡巴斯基虚拟化安全解决方案，请访问 http://www.kaspersky.com.cn/business-security/。

KASPERSKY lab