KASPERSKY lab

虚拟基础架构安全

IT安全风险专题系列报告

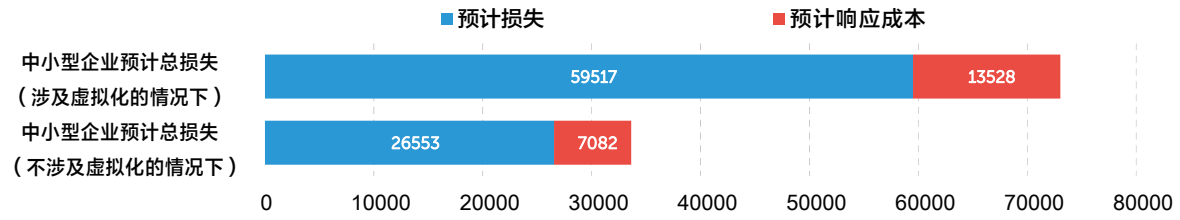
卡巴斯基实验室

企业IT安全风险调查情况：

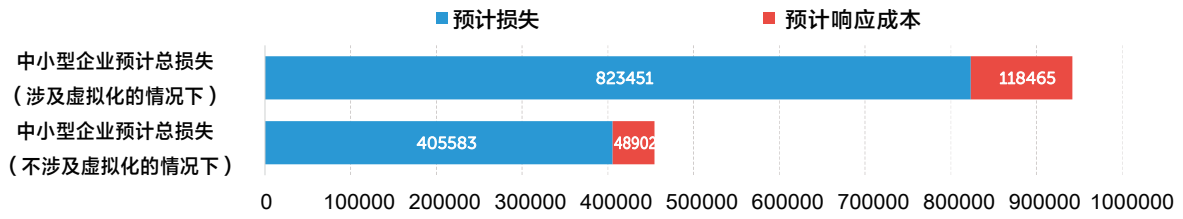
- 调查对象包括来自全球超过25个国家的5500余家企业。
- 企业高层管理人员与IT专业人员接受了调查，回答了安全、IT威胁及基础架构相关的调查问题。

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。

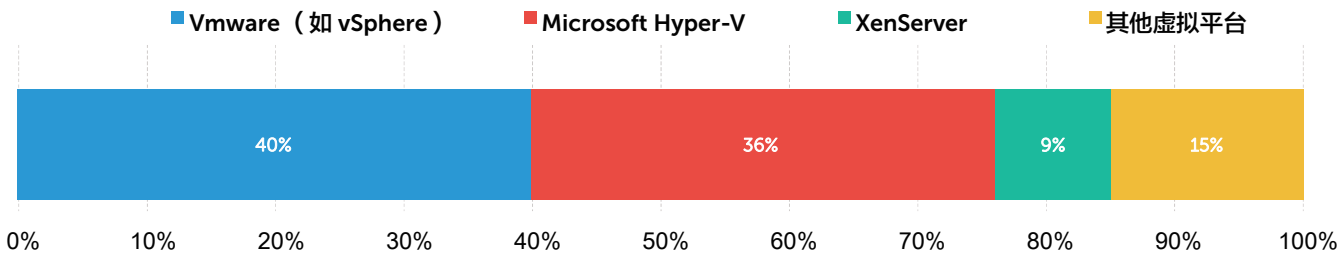


  - 企业在安全修复方面的花费超过$800,000。



- 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。

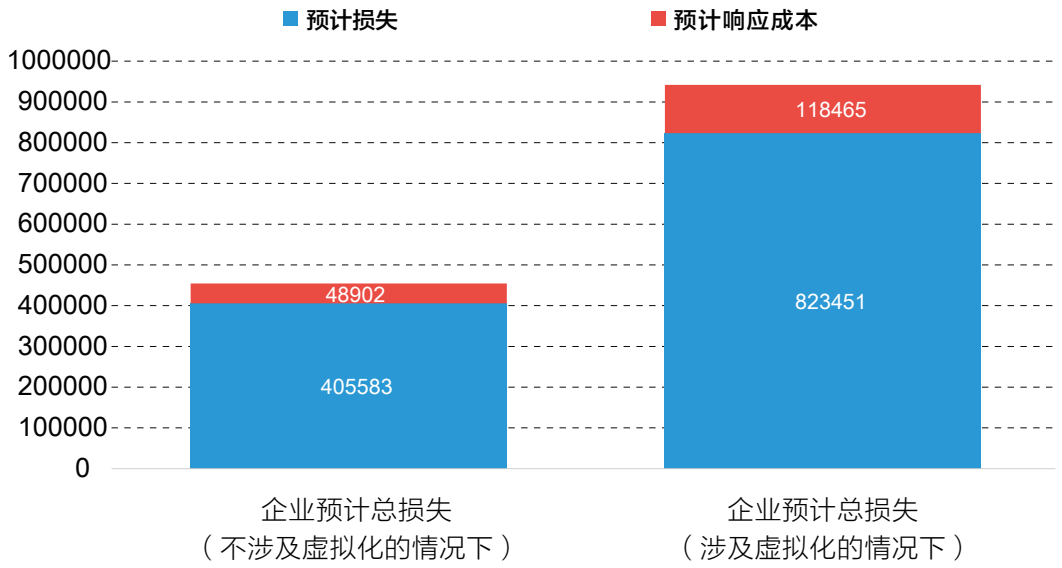
- 62%的受访企业正在使用某类虚拟基础架构。
- 受访企业使用最多的三大虚拟平台：VMWare（40%）、Microsoft（36%）及Citrix（9%）。



- 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。

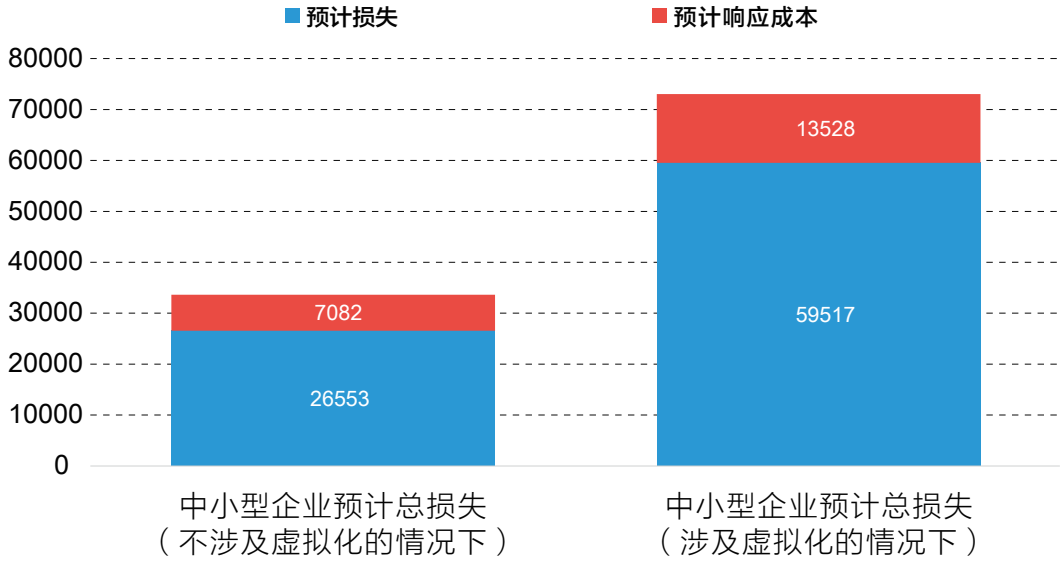
关键调查结果：
虚拟基础架构使得安全事故修复成本增加一倍

此次调查中，最有意思的发现是受访企业所提供经济损失间的差异性。若企业的虚拟基础架构受到安全事故的影响，企业的安全事故修复成本会增加一倍。大型企业（员工多于1500人的企业）修复一起安全事故的平均直接成本超过80万美元。若将企业遭受攻击后，进行员工培训以减轻日后风险损失所产生的成本等间接成本也计算在内，总修复成本将接近一百万美元。



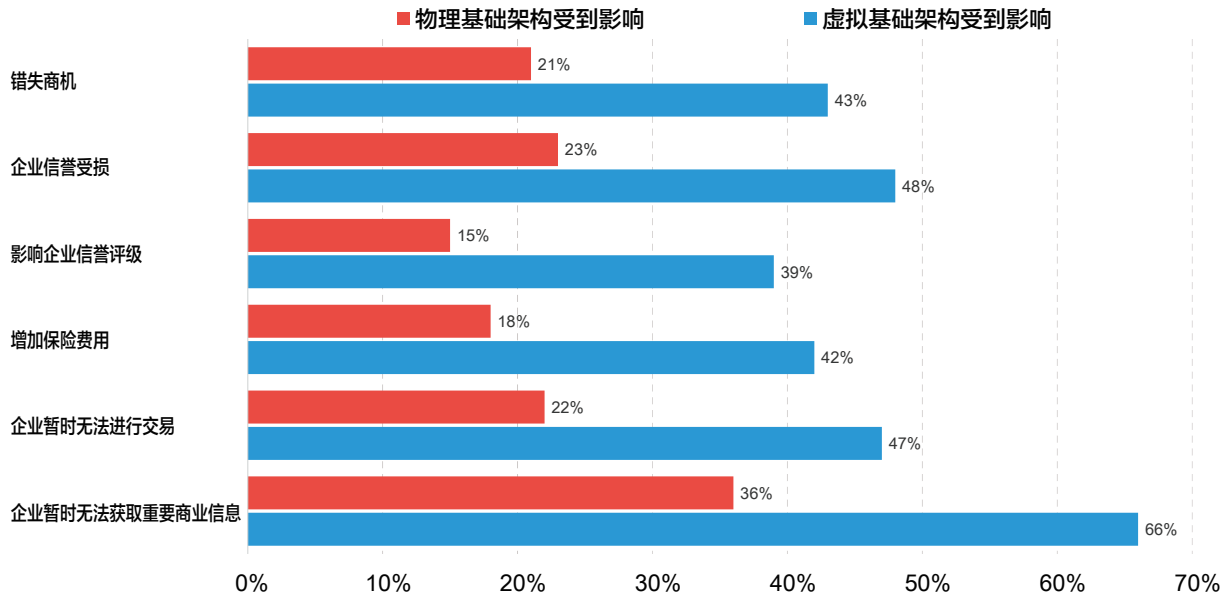
数据外泄对企业造成的总体经济损失（单位：美元）

据受访中小型企业反映，因物理基础架构环境遭到攻击而产生的平均损失超过2.6万美元。若虚拟基础架构受到安全事故的影响，企业的损失金额将增至约6万美元（不含响应成本）。



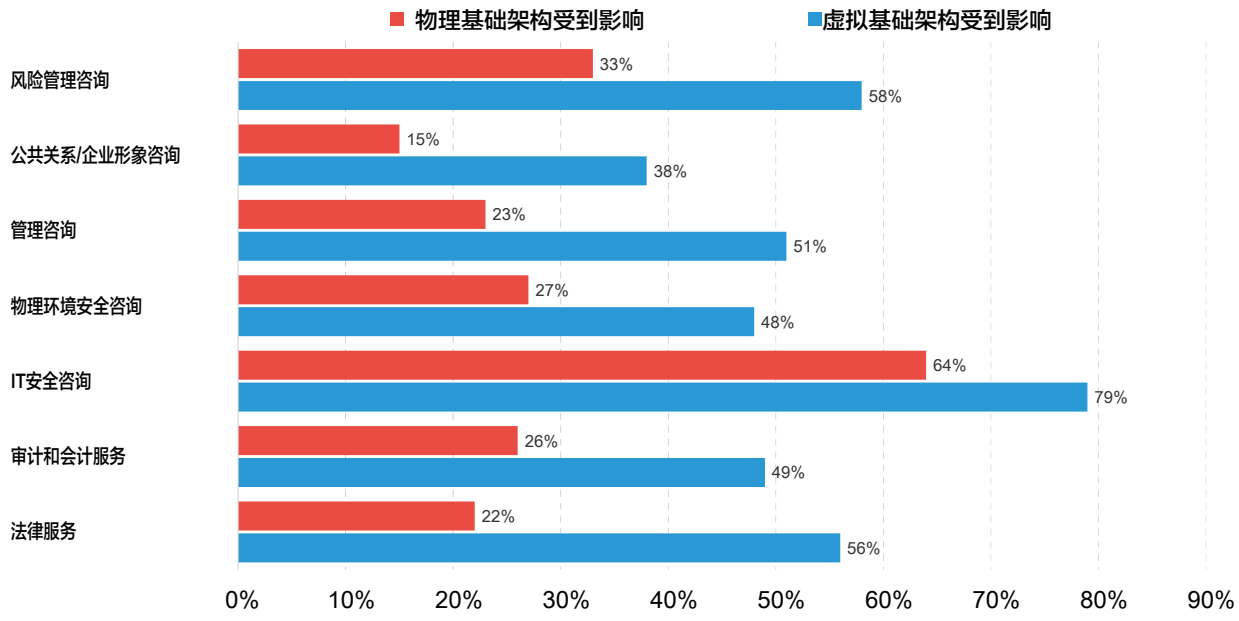
数据外泄对中小型企业造成的总体经济损失（单位：美元）

为什么会产生这部分额外的修复成本？虽然我们可清楚地认识到虚拟环境的IT安全对许多企业而言都是一项复杂的工作（详情见下文），但主要原因在于虚拟基础架构更常被用于进行关键任务操作与/或储存关键敏感的数据。以下对涉及/不涉及虚拟基础架构的安全事故后果的比较足以证明这一观点。



影响虚拟基础架构（蓝色）与只影响了物理基础架构（红色）的安全事故后果比较。
上图表示遭受上述不良后果的企业所占比例。

企业虚拟环境遭受攻击更易造成企业短时间内无法获取重要数据，丧失核心服务能力并使企业信誉受损。我们还发现，虚拟基础架构遭受到攻击的企业在IT咨询和法律服务方面支出的修复成本更高：

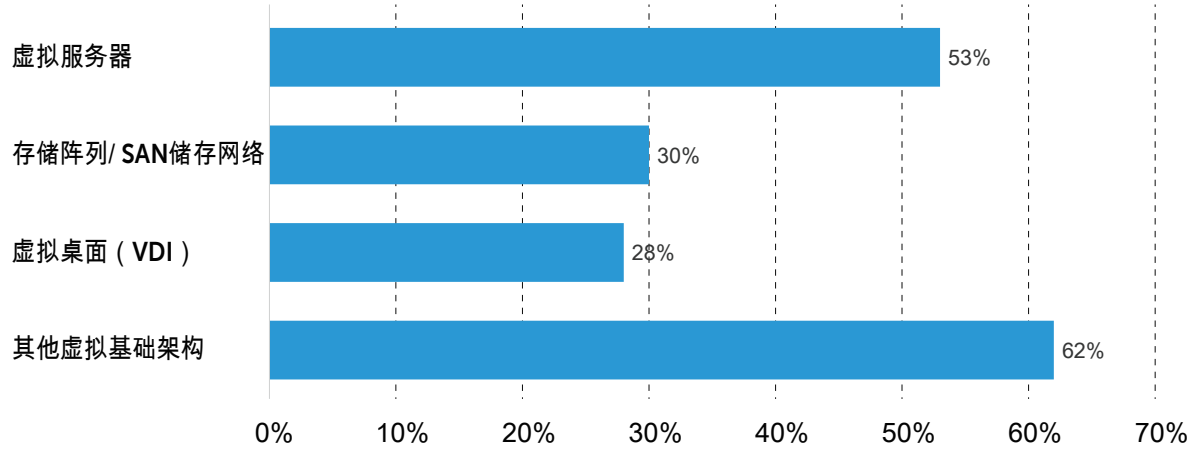


影响虚拟基础架构（蓝色）与只影响了物理基础架构（红色）的安全事故后果比较。
上图表示遭受上述不良后果的企业所占比例。

法律服务与IT安全咨询成本同时大幅增加表明，涉及虚拟基础架构的安全事故更易被公众、客户及合作伙伴知晓。

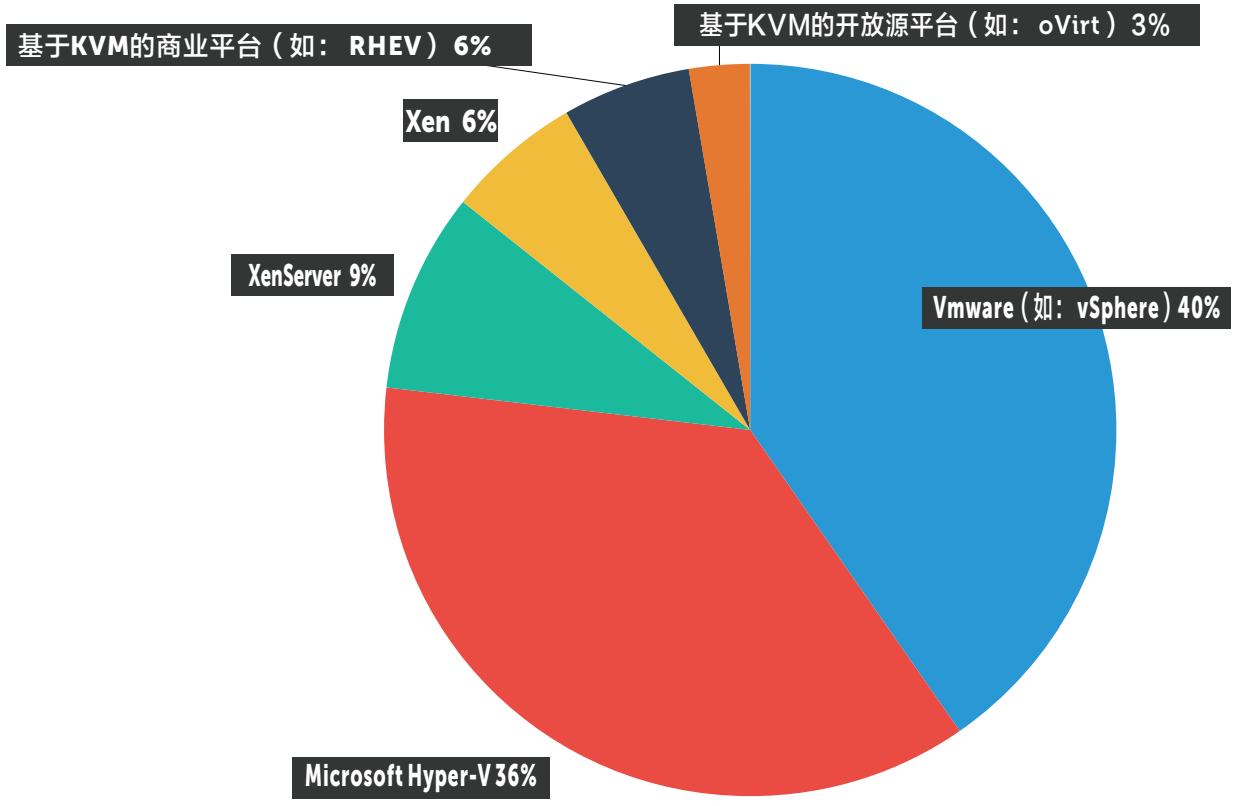
虚拟基础架构详情

实现虚拟化已不再是潮流，早已成为了商业惯例。62%的受访者表示其公司正使用某类虚拟基础架构。

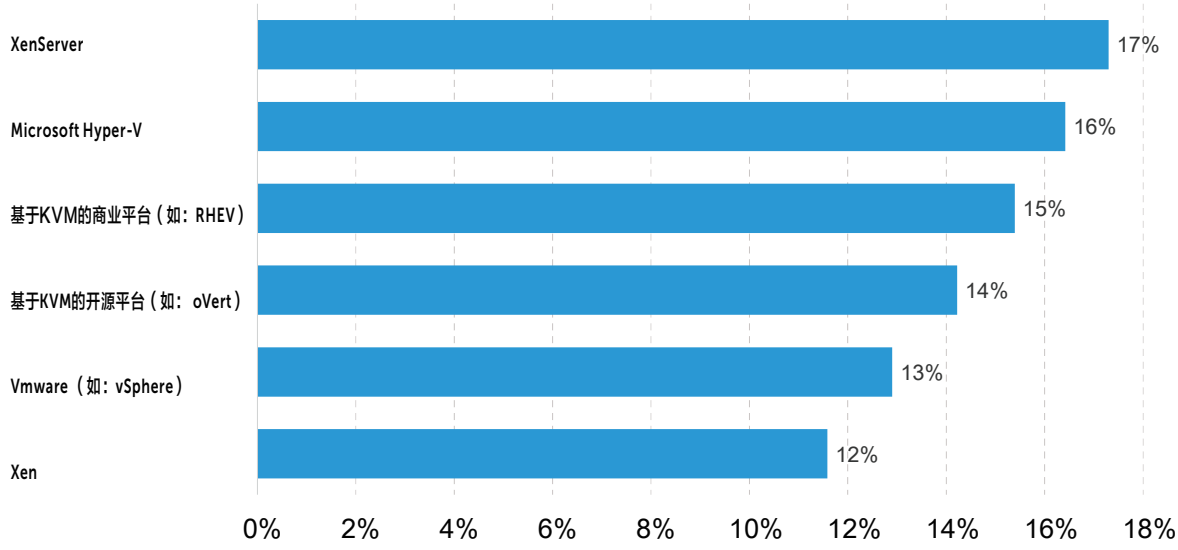


受访企业采用的各类虚拟基础架构及使用上述各类基础架构的企业所占比例

随着企业的发展，企业对虚拟基础架构的需求也随之增加。在员工人数超过1500人的受访企业中，77%的企业都有使用某类虚拟基础架构。



据虚拟化专家（企业版虚拟化解决方案专家）表示，最受欢迎的虚拟机管理程序为VMware与Microsoft，KVM对用户的吸引力也正逐渐增加。在企业的虚拟基础架构愿望清单中，(商业和开源)KVM是企业最期待使用的平台之一。



未来两年企业可能选用的虚拟平台

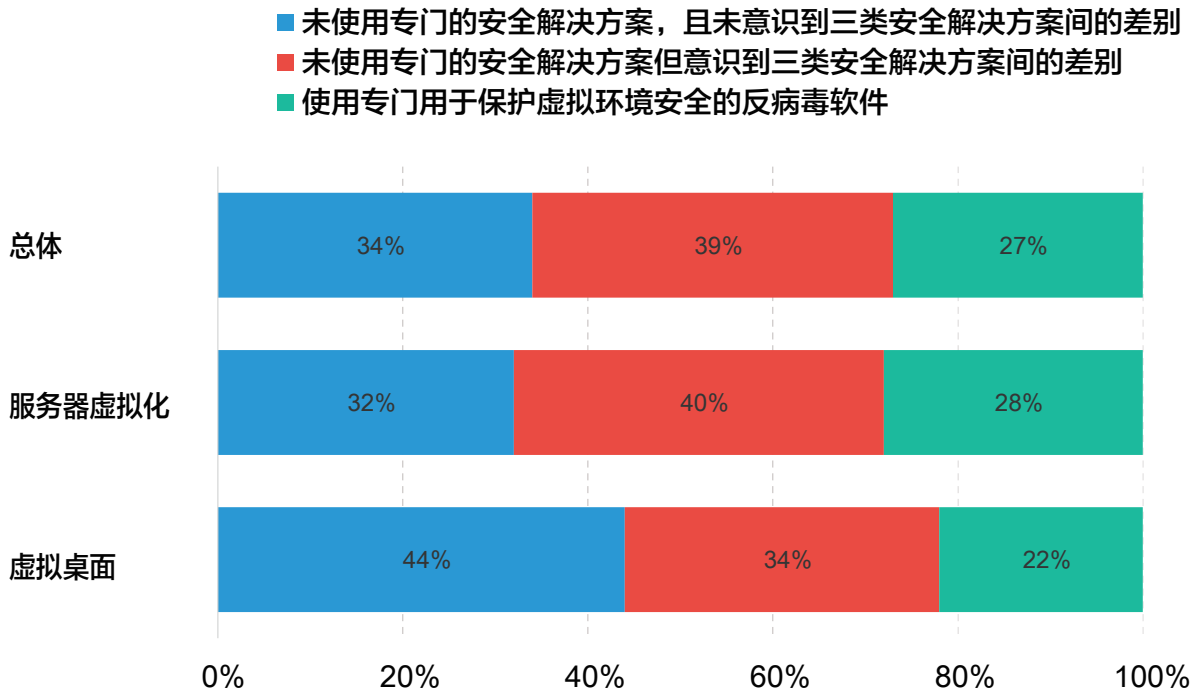
超过三分之二的受访者表示，他们在使用Microsoft和VMware的虚拟平台。在企业近来希望选用的虚拟平台排名中，微软公司的Hyper-V位列第二。从这些数据中可看出，尤其是商业及免费开源平台被提上日程后，KVM将有望成为目前市场领导者们最有力的竞争者。

虚拟基础架构安全

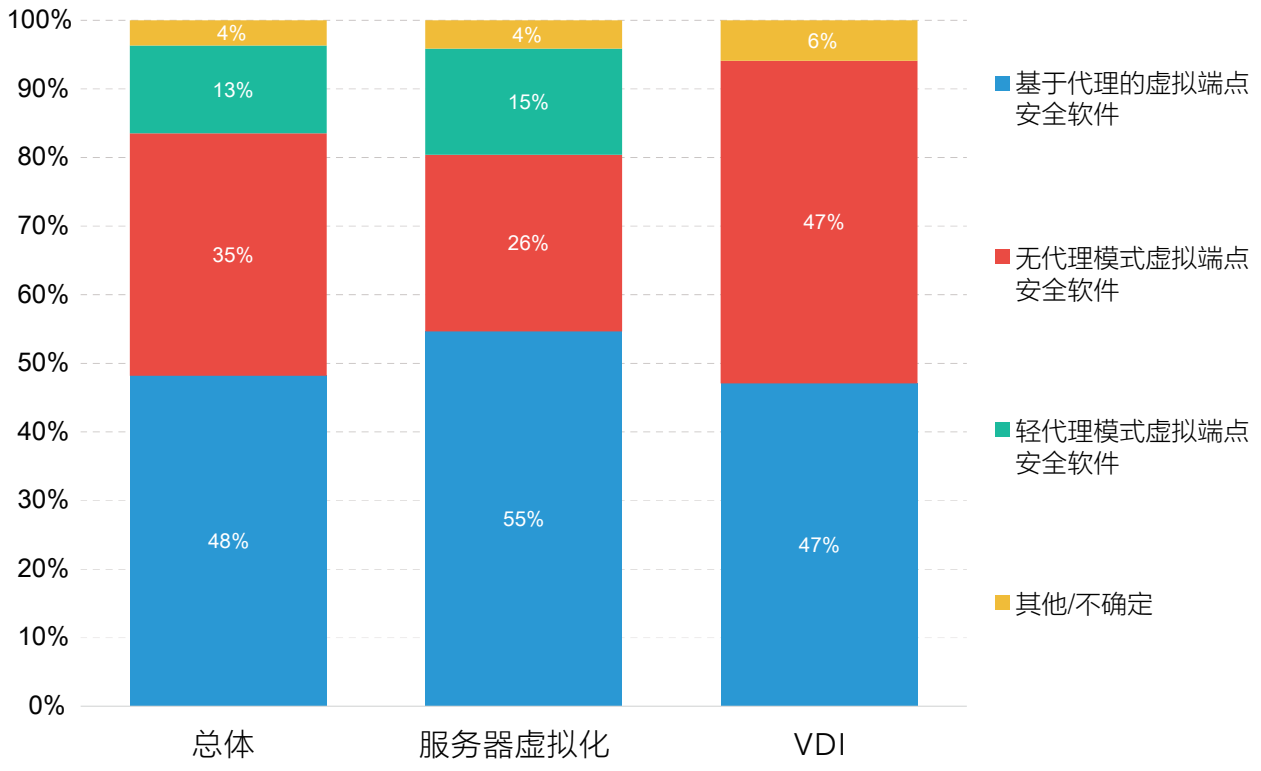
要保护物理端点与服务器的安全，企业需选择一位安全软件供应商，但在实现虚拟桌面或服务器防护前，企业则必须先选择一种安全解决方案。目前市场上主要有三种虚拟环境安全解决方案：

- 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）

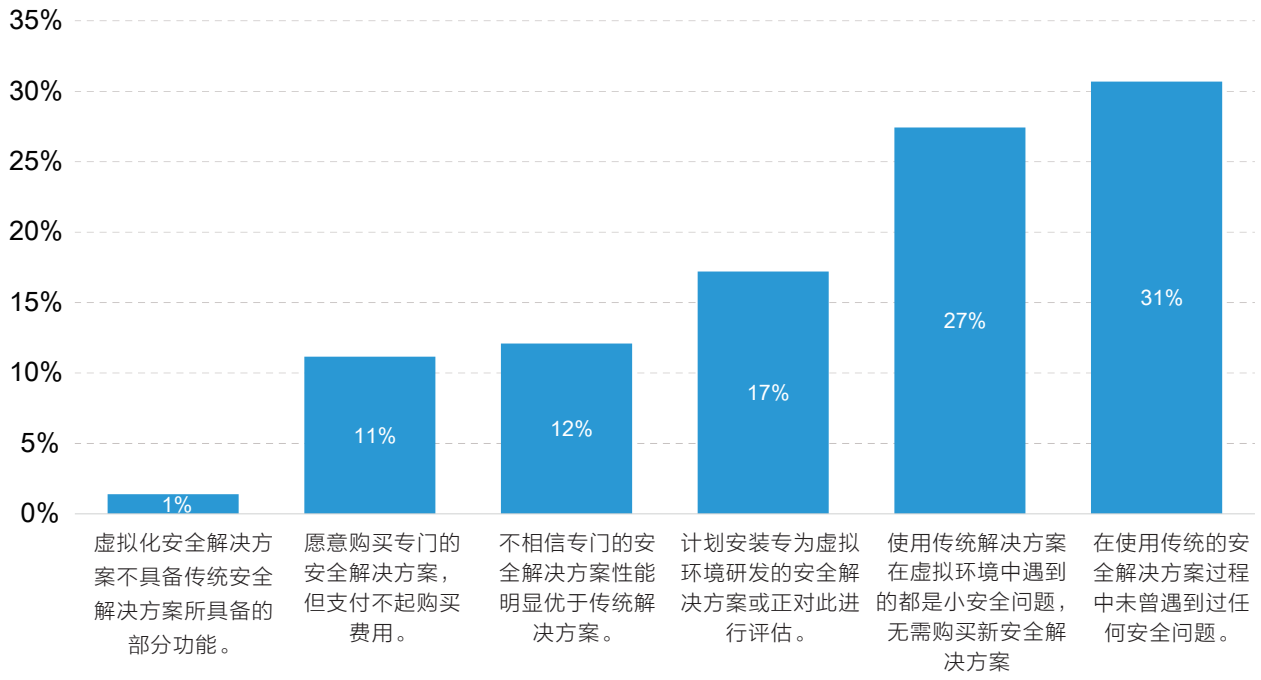
研究表明，很多公司并未真正意识到上述三类安全解决方案的差别。事实上，仅有27%的企业表示部署了专门用于虚拟环境防护的安全解决方案。



在使用专门的安全解决方案的受访企业中，多数企业仍在使用会影响集成比例与虚拟化性能的基于代理的安全软件。

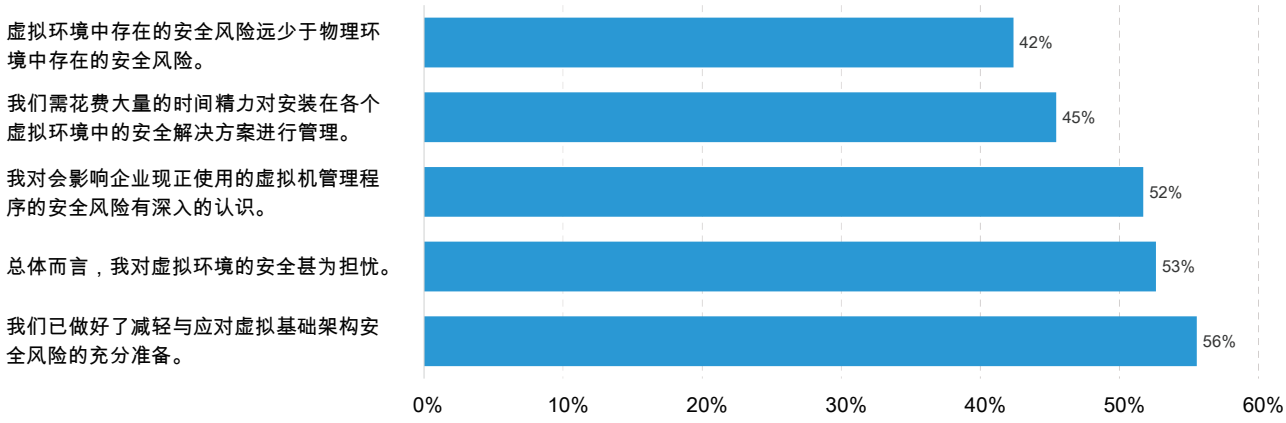


更多的企业则未使用任何虚拟化安全解决方案。其中，仅有31%的企业在使用传统的安全解决方案过程中未曾遇到过任何安全问题。



的确，在多数情况下，传统的安全解决方案可用于虚拟环境防护。但在多台虚拟机上进行部署时，会稍稍影响物理端点的性能，这又被称之为性能代偿，从而大幅降低成本效能。而这也印证了为什么影响虚拟基础架构的攻击造成的损失会是仅影响物理端点与服务器的攻击的两倍。我们由此可得出如下结论：IT威胁是影响虚拟基础架构总拥有成本（TCO）的重要因素。一起安全事故，甚至是选择错误的安全解决方案都可让实现虚拟化的预计成本效能化为乌有。

仅有53%的受访企业对虚拟环境防护表示担忧，只有半数受访者表示对会影响企业虚拟机管理程序的安全风险有深入的认识。同时，有56%的受访者认为他们已做好了减轻与应对相关威胁的充分准备，但这可能只是一种因受到误导而产生的错误认知。



许多虚拟环境防护相关问题产生的根本原因都在于过时的错误观念——认为虚拟环境中存在的安全风险远少于物理环境中存在的安全风险。42%的受访者仍然相信这种错误的观点。

结论

正如我们在调查中所发现，企业对使用虚拟基础架构抱有积极的态度。但行业对这项技术，尤其是虚拟环境的安全问题却明显不足。虚拟环境较之物理服务器更加安全可靠，在残酷的安全环境中，并没有什么是绝对安全可靠的。虚拟基础架构会增加漏洞修复成本，影响所部署的安全解决方案的效能。相反，不合理的决策也会影响投资回报（ROI），导致实现虚拟化的预期成效无法在日后得以实现，甚至会让您觉得虚拟基础架构不值一试。

企业IT安全风险调查情况

2015年，卡巴斯基实验室与B2B International公司共同对5564位来自35个国家不同规模企业的IT专家进行了调查，其中包括3465位小微企业（员工人数不超过250人）IT专家代表，1074名中型企业（员工人数介于251-1499人）IT专家代表以及1025位大型企业（员工人数超过1500人）IT专家代表。但该份报告主要列载了与虚拟技术用户（62%）相关的调查问题。

我们在35个国家展开了这项调查，包括巴西、中国、法国、德国、印度、意大利、日本、俄罗斯、西班牙、英国、美国、墨西哥、沙特阿拉伯、南非、土耳其、阿拉伯联合酋长国（阿联酋）、澳大利亚、加拿大、印度尼西亚、马来西亚、新加坡、智利、哥伦比亚、捷克共和国、希腊、匈牙利、哈萨克斯坦、秘鲁、丹麦、瑞典、泰国、越南、荷兰、比利时和以色列。

Securelist 卡巴斯基实验室
专家的技术研究、
分析和观点汇总。

卡巴斯基实验室中文网站

尤金•卡巴斯基官方博客

卡巴斯基实验室B2C博客

卡巴斯基实验室B2B博客

卡巴斯基实验室安全信息服务网站

卡巴斯基实验室学术网站

卡巴斯基技术开发（北京）有限公司

地址：北京市东城区青龙胡同1号
歌华大厦B座12层
网址：www.kaspersky.com.cn

联系电话：010-8418　6111
5x8技术服务热线（天津）：400-611-6633

KASPERSKY lab