评测 报告

Tolly.

2011 年 2 月

受趋势科技股份有限公司委托

趋势科技 Deep Security 7.5 与 McAfee 和 Symantec 比较

VMware ESX 虚拟环境中的防病毒性能

摘要

对于旨在降低资本和运营开支的任何 IT 战略而言，服务器和桌面虚拟化已成为不可或缺的一部分。由于急于实施虚拟化技术，许多组织仅部署了与其物理服务器和桌面系统完全相同的防病毒解决方案。由于这些传统的防病毒解决方案不是专为虚拟环境而设计的，因此它们会引起严重的运营问题，如防病毒风暴、资源浪费、管理开支增加并影响组织的目标 — 最大化虚拟机密度。

趋势科技股份有限公司委托 Tolly 对趋势科技 Deep Security 与 McAfee Total Protection for Endpoint 和 Symantec Endpoint Protection 11.0 在虚拟环境中的性能进行比较评测。具体地讲，此测试用于评估每种解决方案对主机系统（物理服务器）资源的影响，尤其是当密度高达 100 台虚拟机同时在 VMware ESX 4.1 环境中运行时。

测试要点

趋势科技 Deep Security 虚拟设备：

1. 证明对系统 CPU、内存和磁盘 I/O 的资源需求比传统的基于客户端的解决方案始终更低，即使在非病毒扫描时也是如此
2. 借助于预设扫描和特征码更新成功避免了防病毒风暴问题（该问题使其他解决方案测试时无法超过 25 台虚拟机）
3. 证明在测试状态下，密度提升为 29% 到 275%，优于 McAfee 和 Symantec

测试表明，趋势科技 Deep Security 提供的无客户端、基于虚拟设备的病毒防护方法最适用于虚拟化，并且与不具有虚拟化感知能力的实施方案（防病毒客户端和处理位于每台 Windows 7 虚拟机中）相比，趋势科技 Deep Security 消耗的 CPU、内存和磁盘 I/O 资源更少。

在正常工作状态下的测试中，传统的防病毒解决方案的资源消耗比趋势科技解决方案高出 1.7 到 8.5 倍，除此之外，当在 25 台虚拟机上同时触发操作来测试峰值活动（例如，运行按需扫描和病毒库更新）时，传统的防病毒解决方案还会面临防病毒风暴挑战。具体而言，，由于传统的解决方案不具有虚拟化感知功能，因此管理站会请求 25 台虚拟机运行按需扫描或更新病毒库，这触发了所有虚拟机同时执行功能，从而导致对 CPU 和内存等主机资源的需求出现瞬间激增。

最终，趋势科技 Deep Security 在资源消耗方面的节省使得组织可以提升虚拟机密度，即增加每台物理机上可运行的虚拟机数量，从而降低了企业的资本支出 (CAPEX) 和运营支出 (OPEX)。在峰值状态测试中，趋势科技在防病毒风暴规避和资源消耗方面远胜于 McAfee 和 Symantec，最低节省为 29%（当运行的工作负荷重点不在于防病毒时），最高达 275%（在防病毒风暴期间），这使得改善虚拟机密度成为可能。

Tolly 工程师们通过在多达 100 台虚拟机上同时运行各种工作负荷来对安全系统资源利用率进行评测。基线是通过运行模拟某些系统（未安装端点安全解决方案）上各种最终用户功能的工作负荷并测量资源消耗来制定的。

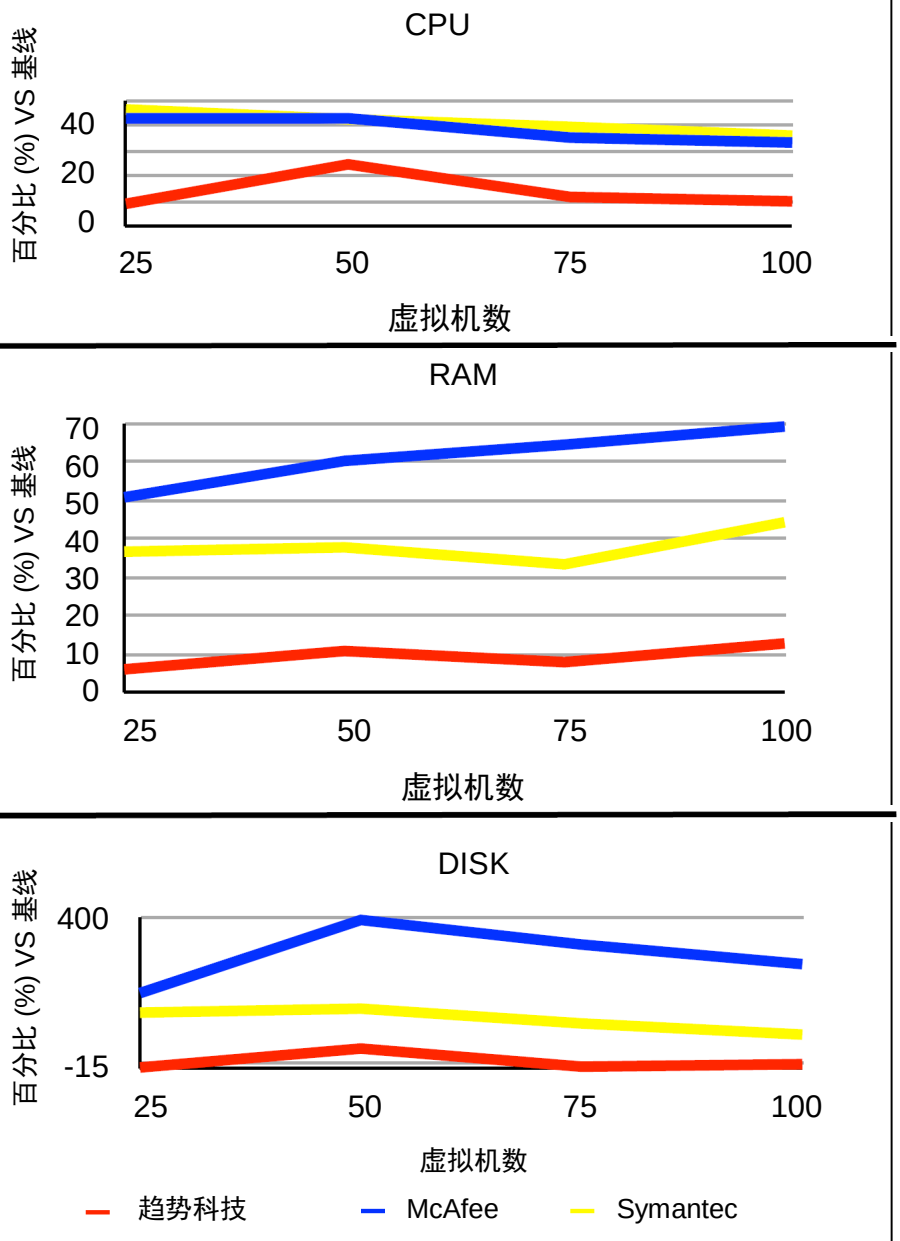
测试内容包括评测运行特定防病毒任务（按需扫描和病毒库更新）时的资源消耗以及每台虚拟机上存在防病毒防护时的常规用户工作负荷。

模拟工作负荷（25 至 100 台虚拟机）条件下的防病毒资源利用率

图 1 说明了在多达 100 台虚拟机上同时运行测试工作时 VMware ESX 服务器上的关键系统资源平均利用率水平。（有关各个数据点的信息，请参阅表 4。）
这些图包括由各个虚拟机使用的资源以及由趋势科技 Deep Security 虚拟设备使用的资源。有关工作负荷和环境的详细信息，请参阅“测试方法和测试平台设置”部分。

McAfee 和 Symantec 解决方案均需要一个单独的防病毒客户端运行于每台虚拟机上。趋势科技 Deep Security 仅需要在每台主机上运行一个虚拟设备客户端。该图说明了在各个虚拟机密度上 Symantec 和 McAfee 在三种资源（CPU、内存和磁盘使用）的消耗上是趋势科技所需资源的 1.7 到 8.5 倍的。[1]

vCenter 报告： VMware ESX 4.1 主机资源消耗
在 100 台 Microsoft Windows 7 虚拟机平台下运行病毒扫描
（数值越低越好）



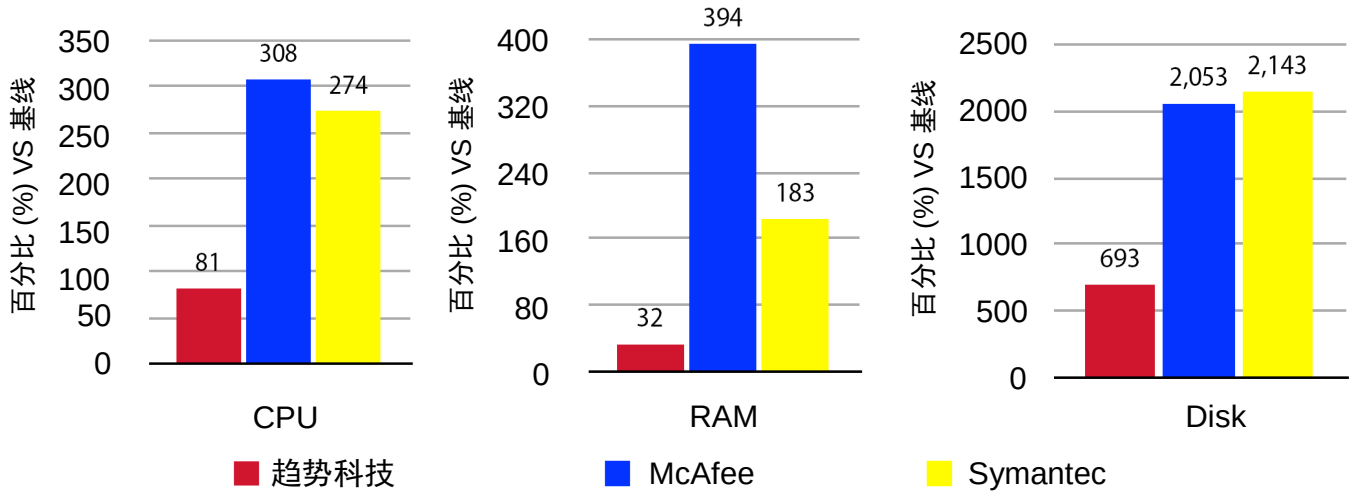
注意：除扫描之外，所有系统还都运行了专有工作负荷。基线指未安装端点安全解决方案运行时的专有工作负荷。有关基线值和详细结果的信息，请参阅报告主体。基于基线的利用率是由结果减去基线，除以基线，再乘以 100 计算得到的。由于 McAfee 无法完成包含 100 台虚拟机的测试，针对 100 台虚拟机的结果是从包含 25、50 和 75 台虚拟机的测试结果推断而来。平均运行时间为 30 分钟。磁盘使用率结果变化范围达 30%，包含在此处仅供参考。

数据来源：Tolly，2010 年 10 月

图 1

[1] 尽管多次尝试并重新运行，McAfee 解决方案仍然无法完成 100 台虚拟机的测试。Tolly 工程师基于包含 25、50 和 75 台虚拟机的测试结果推断得出 McAfee 在 100 台虚拟机的结果。

vCenter qude 报告： VMware ESX 4.1 主机资源消耗
25 台 Microsoft Windows 7 虚拟机执行按需扫描
（数值越低越好）



注意：除扫描之外，所有系统还运行了专有工作负荷。基线指未安装端点安全解决方案运行时的专有工作负荷。基线值：CPU 平均值 = 4,109.76 MHz，内存平均值 = 7,893.28 MB，磁盘平均值 = 1,741.23 KBps。趋势每次只会运行单个扫描。其他供应商则同时触发 25 个扫描。每个供应商均建议了各种方法（如随机选择法）来调整按需扫描。有关详细信息，请参见报告主体。基于基线的利用率是由结果减去基线，除以基线，再乘以 100 计算得到的。平均运行时间为 30 分钟。

数据来源：Tolly，2010 年 10 月 图 2

防病毒按需扫描测试（25 台虚拟机）

工程师们评估每种解决方案如何响应安全管理系统请求以对 25 台虚拟机执行完整扫描。由于扫描本身需要耗费较多的资源，因此同时扫描会降低整体用户体验。

趋势科技 Deep Security 能够感知到它运行在这样的环境中：资源在所有虚拟机之间共享，并且自动化预设扫描逐次运行 — 每次最多有一台虚拟机在运行。因此，趋势科技 Deep Security 可以成功在 25 台和 50 台虚拟机上进行测试。基于在这些测试中观察到的资源利用，Tolly 推断趋势科技解决方案可以支持包含 100 台以上虚拟机的环境。

缺省情况下，其他解决方案（无法感知共享虚拟环境）尝试启动所有 25 台虚拟机的并发扫描。图 2 提供了这些测试；McAfee 资源消耗方面，CPU 比趋势科技高 2.8 倍，内存比趋势科技高 11 倍的平均资源结果。在 Symantec 资源消耗方面，CPU 比趋势科技高 2.4 倍，内存比趋势科技高 4.7 倍。

另外，Symantec 和 McAfee 的 25 台虚拟机数据集不提供有关可靠性和用户体验的完整情况。McAfee 和 Symantec 解决方案中的资源需求激增降低用户系统的性能。尤其是，Symantec 和 McAfee 解决方案均无法在超过 25 台虚拟机的情况下接受测试。在 Symantec 测试中，2 个客户端在测试期间与管理服务器失去连接，并且磁盘读写时间（未在图中说明）记录的平均值为 31 毫秒。在 McAfee 执行按需扫描环境中，磁盘读写时间记录为 80 毫秒。在测试中，有 14 名（共 25 名）用户无法访问各自的桌面。有关其他说明，请参阅表 2。

传统的解决方案通常建议两种方法（随机选择法和分组）来避免虚拟环境资源竞争。这两种方法均不提供虚拟化感知功能，因此，不属于本测试的范畴。

使用随机选择法时，管理员可以设置随机选择周期以允许端点在随机开始时间运行任务。对于诸如完整扫描等耗费时间较多的任务，此时间周期需要非常长（超过一天或一周，根据主机的虚拟机密度而定），以增加客户端任务避免彼此重叠的可能性。因此，当遇到严重安全威胁时，企业管理员可能无法立即修复系统。而且，如果当系统使用率已经很高时运行随机任务，它们可能会降低用户体验。

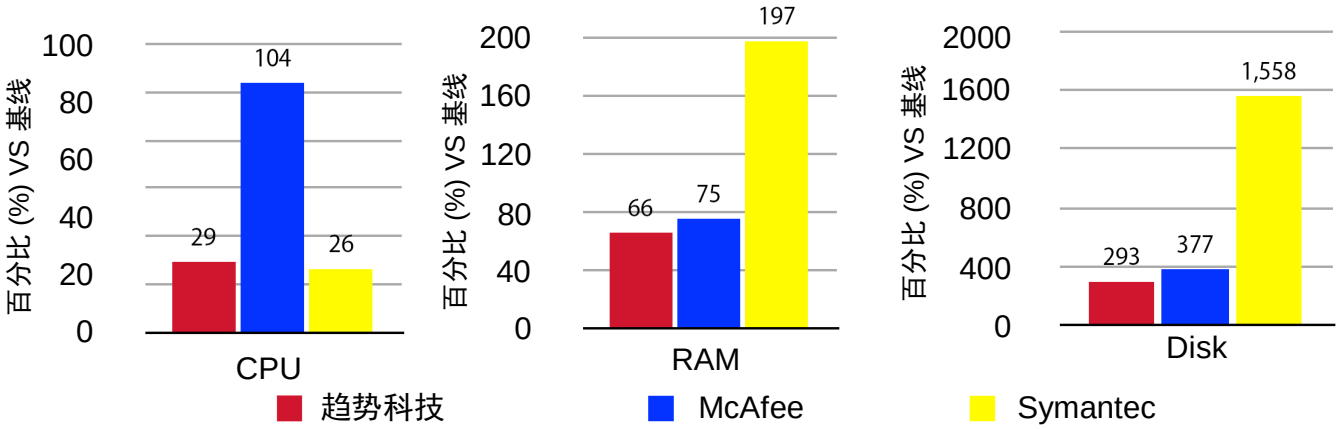
VMware ESX 4.1 下防病毒解决方案比较
在 Microsoft Windows 7 平台上的虚拟机运行按需扫描

供应商	产品	用于进行按需扫描的虚拟机数			
		25	50	75	100
趋势科技	趋势科技 Deep Security 7.5	是，完全稳定	是，完全稳定	是（预计， 无测试）	是（预计，无测试）
McAfee	Total Protection for Endpoint	是，但存在稳定性问题	由于同时进行 25 个扫描存在不稳定性问题，因此 Tolly 工程师未尝试更大数量测试。McAfee 在其客户端任务中提供了随机选择选项，该选项可以为预设触发任务和手动触发任务提供负荷分布功能。		
Symantec	Endpoint Protection 11.0	是，但存在稳定性问题	由于同时进行 25 个扫描存在不稳定性问题，因此 Tolly 工程师未尝试更大数量测试。Symantec 建议为随机选择方法配制预设任务。缺省情况下，这会将 100 台虚拟机的按需扫描请求扩大到大约 160 个小时。手动触发预设任务无法随机选择开始时间。		

注意：趋势科技方案是唯一经测试的具有虚拟化感知功能的解决方案，该方案自动错开按需扫描的时间以使扫描逐次执行。

数据来源：Tolly，2010 年 10 月 表 1

vCenter 报告： VMware ESX 4.1 主机资源消耗
在 50 台 Microsoft Windows 7 虚拟机上运行病毒库更新请求
（数值越低越好）

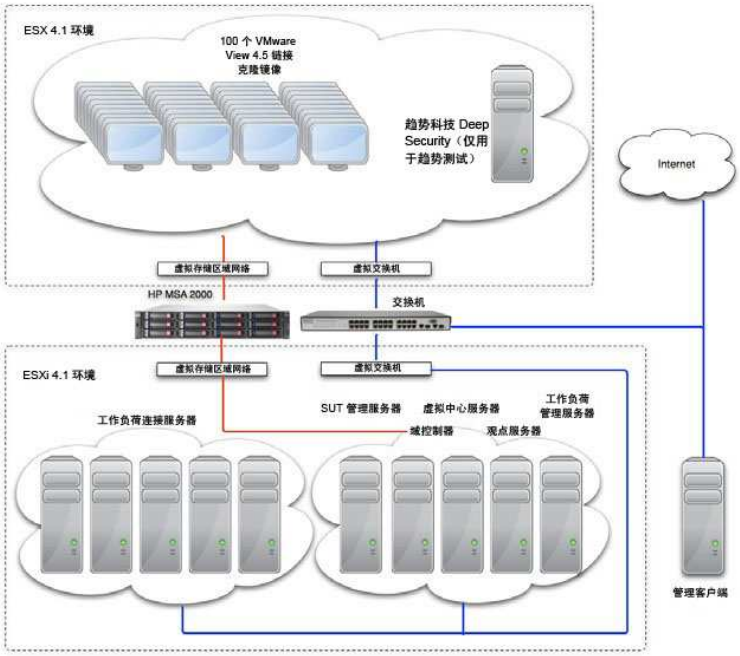


注意：除扫描之外，所有系统还都运行了专有工作负荷。基线指未安装端点安全解决方案运行时的专有工作负荷。基线值：CPU 平均值 = 8,434.91 MHz，内存平均值 = 14,119.62 MB, 磁盘平均值 = 2,341.41 KBps。趋势仅需将病毒库下载到其单个虚拟安全设备。其他供应商则同时触发 25 个更新。每个供应商均建议了各种方法来调整更新。有关详细信息，请参见报告主体。基于基线的利用率是由结果减去基线，除以基线，再乘以 100 计算得到的。平均运行时间为 30 分钟。

数据来源：Tolly，2010 年 10 月 图 1

借助于分组方法，管理员可以按组将虚拟机分配到不同的组并预设客户端任务。此方法需要执行管理工作并使得企业 IT 管理变得更加复杂。需要手动将新的虚拟机分配到组，并且如果由于负载平衡或其他原因虚拟机从一台主机迁移到其他主机，管理员则必须相应地更新组分配。

虚拟化防病毒测试环境



数据来源：Tolly，2010 年 10 月

图 4

测试中的系统

供应商	产品	组件	虚拟机感知功能	实现
趋势科技	趋势科技 Deep Security 7.5	Trend Micro Deep Security Manager 版本 7.5.1378；Trend Micro Security Virtual Appliance 7.5.0.1600；过滤器驱动程序 7.0.0.894；缺省配置。配置了预配置的 Windows 防恶意软件安全策略。	是	自动的、单个虚拟设备。无客户端方式通过 VMware vShield API 进行通信
McAfee	Total Protection for Endpoint	McAfee ePolicy Orchestrator 4.5；McAfee Agent for Windows 4.5.0 Minor Version 1270；McAfee VirusScan(R) Enterprise 8.7.0 Minor version 570 with Hot Fix 2；McAfee AntiSpyware Enterprise 8.7 Minor version 129；McAfee Host Intrusion Prevention 7.0.0 minor Version 1070；McAfee SiteAdvisor(R) Enterprise Plus 3.0.0 Minor version 476 均保留缺省策略。取消了预配置的完整扫描和更新客户端任务。	否	传统端点客户端
Symantec	Endpoint Protection 1.0	版本 11.0.6100.645	否	传统端点客户端

数据来源：Tolly，2010 年 10 月

表 2

防病毒特征码更新（50 台虚拟机）测试

工程师们评估了每种解决方案如何响应系统范围内的防病毒库更新请求。尽管病毒库更新比完整扫描需要的资源要少，但仍会降低性能和增加运营挑战，特别是在常规运营时间更为突出。

工程师们在 50 台虚拟机上运行病毒库更新。传统的解决方案要求更新每台虚拟机上的病毒库，而趋势科技解决方案仅需要单独复制一份位于趋势科技 Deep Security 虚拟设备上的病毒库，然后将该病毒库文件用于受趋势科技监控的所有虚拟机。因此，在资源消耗方面，传统的解决方案在 CPU 或内存方面显著较高，而趋势科技在资源消耗方面始终较低。请参阅图 3。

标准虚拟机密度（防病毒空闲）

此处的重点主要在于防病毒解决方案处于空闲时的资源足迹，尽管主要的工程师们还注意到，实施趋势科技解决方案的网络安全管理人员无需在病毒库更新发生期间为虚拟机“脱机”担忧。在传统的实施方案中，虚拟机必须处于联机状态才能接收更新。

在同时按需扫描测试中，McAfee 和 Symantec 解决方案在所有 50 台虚拟机上立即处理更新要求会对整体系统级别的资源和性能产生影响。

使用 Symantec 解决方案时，大多数虚拟机会在 VMware 的 vCenter 管理系统中触发内存警报，因为 Symantec 的病毒库更新任务完全消耗了分配给每台虚拟机的 1GB 内存。在本测试期间，50 名用户中有 10 名用户的 VMware View 桌面的连接发生中断。

工程师们注意到，McAfee 解决方案包括一个为空闲虚拟机每天更新一次病毒库的任务，尽管这并非本测试的目的。尽管工程师们取消了此任务，但值得注意的是，该任务仍会自动启动。

在 Symantec 解决方案中，同时更新 50 台虚拟机时耗费的资源是巨量的，并且工程师们注意到，在运行某些测试时 VMware ESX 系统的 CPU 使用率超过 10 分钟维持在 100%，并且整个虚拟化系统的性能严重下降。

虚拟机密度（整合）比较

大多数虚拟化尝试会主要基于主要的虚拟机工作负荷来计算规模，而忽略了会造成破坏的传统防病毒工作负荷。作为本测试的一部分，Tolly 评估防病毒效率对虚拟机密度的影响。可以通过各种方法计算密度改善 — (a) 防病毒处于空闲时，和 (b) 防病毒解决方案立即执行客户端任务（如按需扫描和病毒库更新）时。

趋势科技
Deep
Security 7.5
VMware
防病毒
性能

Tolly. Certified

测于
2010 年
10 月

VMware **性能主机测试平台组件**

组件	版本/Build
VMware ESX	4.1.0
VMware vCenter Server	4.1.0 build 258902
VMware View Composer Server	2.1 build 277387
VMware View Connection Server	4.5.0
VMware vShield Manager	4.1 build 310451
服务器硬件	2x Xeon x5680（六核心），运行频率为 3.33GHz，内存为 192 GB DDR 3（共 24 个逻辑核心））
存储区域网络	HP StorageWorks MSA，通过 4GB 光纤通道进行连接
子虚拟机资源	1GB 内存和 1 个虚拟 CPU
子操作系统	Microsoft Windows 7 Enterprise

数据来源：Tolly，2010 年 10 月 表 2

工作负荷仍在运行，但尚未触发特定防病毒任务。借助于趋势科技解决方案，虚拟机密度改善在 CPU 和内存方面分别高出 Symantec 34.5% 和 29%。类似地，虚拟机密度改善在 CPU 和内存方面分别高出 McAfee 31.4% 和 42.4%。请参阅表 5。

真实虚拟机密度（完整扫描）

使用防病毒空闲标准密度不会将高峰防病毒活动考虑在内，这也是为什么虚拟化部署越来越注重“防病毒风暴”（使得 ESX 主机和虚拟机工作负荷变得过大）的原因。从本测试中可以看出，防病毒扫描和更新对 CPU、内存和磁盘使用三方面的资源消耗较多，且这种资源消耗会随着系统和工作负荷而变化，从而导致资将成为瓶颈。

使用趋势科技解决方案时，虚拟机密度改善在 CPU 和内存方面分别高出 Symantec 106% 和 114%。类似地，虚拟机密度改善在 CPU 和内存方面分别高出 McAfee 124.9% 和 273.5%。

趋势科技 Deep Security

趋势科技已将 Deep Security 7.5 架构设置为为具有“虚拟机感知功能”。与传统的基于客户端的解决方案不同，趋势科技 Deep Security 将重点放在减少运营安全性问题（如防病毒风暴、资源浪费和管理开支）上。趋势科技 Deep Security 以无客户端方式提供了适用于虚拟化的防病毒防护，用于为虚拟化资产提供更快的性能、更高的虚拟机整合率、更为方便的管理以及更快的“保护响应时间”。

数据来源：趋势科技，2010 年 10 月

vCenter 报告： VMware ESX 4.1 主机资源消耗
在 100 台 Microsoft Windows 7 虚拟机上运行专有工作负荷
（数值越低越好）

虚拟机数量	防病毒解决方案		ESX 主机基线资源利用百分比增加（相对基线）		
			CPU (GHz)/%	RAM (GB)/%	磁盘 KBps)/%
25	基线			6.306 GB	1.705 KBps
	趋势科技	增加百分比（相对基线）	8.86%	5.94%	-13.26%
	McAfee		43.04%	50.83%	191.82%
	Symantec		46.58%	36.63%	138.05%
50	基线			11.908 GB	2.592 KBps
	趋势科技	增加百分比（相对基线）	24.65%	10.7%	38.98%
	McAfee		43.02%	60.34%	393.09%
	Symantec		42.73%	37.78%	148.91%
75	基线			17.325 GB	3.381 KBps
	趋势科技	增加百分比（相对基线）	11.61%	7.79%	-11.03%
	McAfee		35.33%	64.57%	325.32%
	Symantec		39.61%	33.33%	108.22%
100	基线			22.468 GB	5.417 KBps
	趋势科技	增加百分比（相对基线）	9.86%	12.7%	-4%
	McAfee		33.33%	69.31%	271.43%
	Symantec		36.14%	44.31%	77.61%

注意：基线值表示在未安装防病毒/端点安全解决方案的情况下运行为时 30 分钟的专有工作负荷测试。资源消耗的百分比增加越小越好。在很多情况下，由于测试窗口过期，测试运行未完成。尽管多次尝试并重新运行，McAfee 解决方案仍然无法完成 100 台虚拟机的测试。Tolly 工程师基于包含 25、50 和 75 台虚拟机的测试结果推断得出 McAfee 包含 100 台虚拟机的结果。磁盘使用率结果变化范围达 30%，包含在此处仅供参考。

数据来源：Tolly，2010 年 10 月

表 4

测试方法学和测试平台设置

所有测试均使用相同的硬件基础架构，因此，针对每个系统的测试是逐个进行的。表 2 提供了测试中的解决方案和虚拟机子系统的详细信息，表 3 提供了性能主机的虚拟机主机环境的详细信息。

值得注意的是，物理服务器 CPU 包括 24 个逻辑核心，这表示为 100 台虚拟机配置的系统以大约 4:1 的比例超额预订了物理 CPU 资源。测试人员注意到，在测试过程过，CPU 资源并非瓶颈。

VMware ESXi 主机用于运行测试所用的其他基础架构，包括测试中的系统所需的各种管理服务器以及负载生成器系统。

趋势科技解决方案为虚拟设备进行实施，并使用 VMware API 与子虚拟机进行通信。此 API 通过虚拟网络接口传导通信。

其他解决方案不具有“虚拟机感知功能”，因此，不会按照已部署了 100 台物理 Windows 计算机的相同方式来实施。

在测试环境最终确定时，适用于虚拟化环境中端点安全的 McAfee 的解决方案，McAfee Management for Optimized Virtual Environments (MOVE) 尚未上市。

所有测试中的产品均带有各自缺省防病毒策略。预先配置的预设完整扫描和更新任务已被取消。

主工作负荷

主要测试使用专有的工作负荷，该工作负荷进而被划分为三种级别的活动：

高：55% 的子虚拟机使用 Microsoft Outlook、Word、Excel、Powerpoint、Internet Explorer 和 Adobe Reader 应用程序运行脚本。
低：35% 的子虚拟机使用 Microsoft Outlook、Word、Excel、Powerpoint、Internet Explorer 和 Adobe Reader 应用程序运行脚本。
空闲：将 10% 的子虚拟机引导至 Windows，并允许它们保持空闲状态。

此工作负荷用于所有测试，并作为按需扫描和病毒库更新测试的后台工作负荷。所有子虚拟机上的 Windows 防火墙和 Windows Defender 均已关闭。

对于主工作负荷测试，Tolly 工程师们启动了自动登录所有带有 VMware View 客户端的用户的工作负荷，并运行应用程序脚本。

脚本活动包括编辑电子邮件和 Microsoft Office 文档，浏览 Adobe PDF 文档和上网。工作负荷不包括耗费 I/O 较多的任务或文件复制任务。运行时间为 30 分钟。

按需扫描和病毒库更新测试

Tolly 工程师启动主工作负荷作为后台负荷，然后从管理服务器向测试中的所有子虚拟机分配一个完整扫描或更新任务。运行时间为 15 分钟。

所有性能结果是以 20 秒的时间间隔从 VMware vCenter 捕获的。

虚拟机密度改善 — 专有工作负荷：趋势 vs. 竞争对手
（标准密度）

	CPU	内存	磁盘
McAfee	31.4%	42.4%	236%
Symantec	34.6%	29%	174%

虚拟机密度改善 — 按需扫描：趋势 vs. 竞争对手
（真实密度）

	CPU	内存	磁盘
McAfee	124.9%	273.5%	171.6%
Symantec	106.0%	114.1%	183%

注意：根据资源消耗，表中的图形表示趋势科技 vs. 竞争对手的潜在比例/密度改善。
标称密度指系统运行的负荷重点不在于防病毒。
真实密度指驱动防病毒解决方案的工作负荷。

数据来源：Tolly，2010 年 表5

关于 Tolly

Tolly Group 公司二十年来一直致力于提供顶级的 IT 服务。Tolly 是一家为 IT 产品、组件和服务供应商提供第三方验证服务的领先的全球提供商。您可以通过电子邮件 sales@tolly.com 或致电 +1561.391.5610 与该公司联系。

可以通过以下 Internet 地址访问 Tolly：
http://www.tolly.com

与竞争对手之间的交互

按照我们进行比较性测试的流程，Tolly Group 联系了处于竞争地位的供应商并邀请他们在正式公布之前查看测试方法和各自结果。McAfee 未进行回复。Symantec 进行了回复并配合 Tolly 工程师的工作。Symantec 建议使用其随机选择功能来在持续的时间周期内分散占用资源较多的工作负荷。

有关 Tolly Fair Testing Charter 的更多信息，请访问：

http://www.tolly.com/FTC.aspx

使用条款

本文档为免费提供，旨在帮助您了解特定产品、技术或服务是否值得您针对自己的特定需求进行进一步调查。您必须基于您的需求来评估适用性，从而决定是否购买产品。本文档不应该作为从权威 IT 或商业专业机构获取建议的替代品。本次评估的重点在于说明产品的具体功能和/或性能，并且在受控的实验室条件下进行。可能对某些测试进行了调整以使其反映理想条件下的性能；性能会因真实条件的差异而不同。用户应当基于真实环境来运行测试，才能验证自身网络的性能。

我们已尽力确保此处包含数据的准确性，但错误和/或疏漏仍可能出现。此处所记录的测试/审计可能还依赖于各种测试工具，这些工具的准确性超出我们的控制。而且，本文档依赖于赞助商的某些论述，我们无法对其进行验证。尤其是当软件/硬件属于量产产品或测试阶段产品，已经或将会以同等级或更高等级的形式销售给客户的情况下。本文档按“现状”提供，对于此处所含任何信息的正确性、完整性、用处或适用性，不论是明示或暗示、直接或间接的保证、陈述和许诺，Tolly Enterprises,LLC（简称 Tolly）均不提供任何担保。在阅读本文档时，您已同意对使用此处包含的任何信息承担风险，并对因此处信息或材料直接或间接造成的丢失、损坏、费用和其他后果承担所有风险和责任。Tolly 将概不负责，而您亦同意不追究 Tolly 将其相关子公司因您使用或依赖本文档提供的任何信息所导致的任何损失、损害或损伤的责任。

Tolly 并未宣称此处说明的任何产品或公司适合您投资。在进行本文所述的任何信息、产品或公司相关的任何投资或项目之前，无论法律、会计或其他方面，您均应获取独立的专业建议。当外文翻译与英文内容存在不同时，请以英文文件为准。为了确保准确性，请只使用直接从 Tolly.com 下载的文档。未经 Tolly 明确的书面允许，不得对任何文档的任何部分进行整体或部分复制。您已同意不得在不属于本公司的活动、产品或服务中，与您本身的完整或部分商标一起使用本公司的任何商标，或以任何有可能造成混淆、误导或欺诈的形式，或诽谤本公司或本公司的信息、项目或开发结果的形式使用本公司的任何商标。