卡巴斯基虚拟化安全解决方案

XXXX

2015 年 10 月 19 日

目 录

1. 概述

从世界范围来看，企业的 IT 负责人已经普遍接纳虚拟化技术。全球 2000 家大型企业每年花费超过 66 亿美元用于管理、维护数据中心，实现虚拟化后，这一成本会迅速下降。目前这 2000 家企业中有 90%正在讨论、研究服务器虚拟化；50%正在使用这项技术。从中国市场看，近三成大企业计划在一年内尝试虚拟化技术和产品。

我国正在大力推进节能减排战略，这也将极大推动虚拟化在中国的发展。当前，绿色 IT 的概念已经深入人心，工业和信息化部、国资委对通信行业节能降耗提出了明确的要求。一方面，虚拟化技术的应用将大大减少运营商电力浪费；另一方面，通过系统资源的优化整合，淘汰、替换旧有能耗低效的系统平台，将极大地节省能源，真正实现运营商极其关注的绿色节能指标。

在系统架构成本方面，新服务器硬件成本、电力和制冷成本、数据中心不动产成本居高不下，服务器虚拟化解决方案可将多台物理服务器整合至较少数量的物理服务器，并使之转变为动态数据中心，支持资源的灵活分配、调用，实时的应用程序部署等，从而可带来更高的灵活性和资源的高效利用。

从技术的发展历程看，尽管虚拟化的概念已经存在了 40 多年，软件行业才刚刚开始理解这一重要技术的全部意义。服务器虚拟技术把多台机器整合成一台服务器，这是如今最常见的一种虚拟化技术的应用，但是它仍处于接受周期的早期阶段。我们相信，在未来几年里服务器虚拟化技术将会无处不在。而其他虚拟化技术也才刚刚起步，其潜在价值在很大程度上仍未得到充分开发。毫无疑问，虚拟化技术的引入，将推动企业 IT 系统“动态扩展”，为他们降低成本和拓展新的业务空间带来极大帮助。

大多数的企业 IT 经理人希望在保证公司业务正常运转的情况下，各种应用服务器能够物尽其用，减少无谓的浪费，并且能够对所有的应用进行集中管理，减少雇用维护人员的开销。他们可以利用全部联合到一起的 x86 服务器。把 60%或 70%的服务器联合起来的公司可以动态地管理全部服务器上的资源。这些公司不仅硬件成本方面省下了一大笔资金，获得了有形的利益。同时在将来，他们还将获得虚拟化带来的无形的利益--更可操作性和灵活性。

2. 中国 XXXX 虚拟化搭建与安全需求

为适应 XXXX 信息化建设的需要，提高 XXXX 信息化设备的利用率，最大限度地减少资源浪费，增强系统运行维护的灵活性和可靠性，将基础资源平台构建成与具体应用相对无关，安全稳定、智能高效、易于扩展、便于管理、随需而动的统一的硬件支撑平台，即虚拟化资源整合基础架构平台。原有的一个物理设备承载一种服务或支持一类应用的状况，既不能完全使得物理设备的资源进行充分利用，而且对于电力消耗、日常监控、

故障维护、设备升级和总成本投入都不能做到优化节约。

虚拟化方案的最大优势是在不增加设备投入或少增加设备投入的前提情况下，将企业的多个服务或应用运行到一个设备上，这样能够使得企业对设备的利用率大大提高，并且还能够保证企业日常业务的快速增长需求。

虚拟化解决方案在为企业带来前所未有的具体效益和优势的同时，还带来了企业对于虚拟化安全风险的担忧，虚拟化作为企业现在和未来主要的发展趋势，势必会将替代现在的传统 IT 架构，而对于传统 IT 架构的防护，企业已经有了自己明确的规范，而对于虚拟化的特点，企业需要重新进行安全规划，业务的集中运行，全新的部署、管理和维护，这些都使得虚拟化的安全成为了企业更加关注的重点，一旦虚拟化安全出现了问题，更多、更集中的企业服务和应用将暴露在威胁面前，企业的虚拟化架构需要更加专业和专属的安全解决方案来进行全面的防护保证。

3. XXXX 虚拟化所面临的安全威胁

由于虚拟化技术和具体解决方案在企业中应用的时间并不长，而且其承担具体应用和服务又过于集中，这样就出现了虚拟化架构既要面临原有传统架构威胁的同时，还面临着全新的安全挑战，更多的网络犯罪份子将把注意力更加的集中在虚拟化上面。具体对虚拟化安全威胁进行统一可以进行以下分类：

- 来自外部网络的攻击行为：由于虚拟化平台中虚拟操作系统的高密度性，黑客一旦入侵到虚拟平台就可能获得大量的机密数据，因此，企业需要实时检测虚拟机上的网络流量，防护来自外部网络以及以一台虚拟操作系统作为桥梁向整个虚拟化平台进行的网络攻击活动。

- 虚拟机之间的互相攻击：由于目前 XXXX 对虚拟化安全的防护还没有明确的定义，这就使得在物理设备中各个虚拟机之间存在着互相攻击和互相入侵的安全隐患。

- 虚拟机启动与新增带来的防护断点：由于 XXXX 目前大量使用 VMware 的虚拟化解决方案，VMware 为 XXXX 提供了高效的负载均衡和灾难备份、迁移技术，这些随时由于资源动态调整关闭或开启虚拟机会导致防护间歇问题。如，某台一直处于关闭状态的虚拟机在业务需要时会自动启动，成为后台服务器组的一部分，但在这台虚拟机启动时，在其中部署的安全防护产品将会同时启动，但由于安全防护产品启动后并不具备最新的反病毒数据库和引擎，就使得这种防护措施不能对最新威胁进行相应和处理。

- 非专属的安全防护产品：由于在 XXXX 的 VMware 虚拟化解决方案中运行着大量的办公业务系统和应用服务系统，而且这些系统在日常工作中起到了至关重要的作用，如果被威胁进行了破坏会造成无法弥补的损失，在这样的前提情况下，非专属的安全防护产品因为不能完全与虚拟化环境进行紧密结合，所以既不能确保虚拟环境的安全，而且还可能做造成因安全防护产品自身带来的资源浪费。

- 防病毒风暴的出现：在 XXXX 的虚拟化环境中如果对每一个虚拟机都安装安全产品，这样当然可以保护每个虚拟化的安全，但是这种方式很可能会对物理机的资源占用带来问题，因为一旦所有安装在虚拟机上的客户端产品同时进行更新或扫描操作，就很可能会出现物理机资源占用过高的情况，这样就使得虚拟化环境造成一定的影响。

- 不能统一的管理：在 XXXX 的当今 IT 环境下 VMware 的虚拟化环境还处于承载部分应用与服务业务上，而一部分的应用和日常的办公系统还仍在继续使用传统的 IT 架构，在这种情况下对于虚拟化环境安全产品的管理与对传统环境安全产品的管理，如果采用两套管理方式，这样会对企业的日常管理带来额外的负担。

通过以上的分析对于 XXXX 中虚拟化架构的防护，不能依靠传统的防护方式，这样不能完全保证虚拟化环境中所有虚拟机自身和虚拟机之间数据传输及网络流量的安全，针对于当前 XXXX 的具体环境卡巴斯基实验室推荐使用卡巴斯基虚拟化安全解决方案，这套方案是为 VMware 虚拟化技术所开发的专属解决方案，集中卡巴斯基实验室最先进的安全防护技术和统一的管理平台，确保了 XXXX 虚拟化环境和传统环境的统一安全管理。

4. XXXX 虚拟化环境需要专业的安全防护

在对 XXXX 企业环境进行深入分析后，我们可以看到为了配合本企业快速发展的步伐和业务增长的趋势，对部分应用服务和业务系统进行了虚拟化改造，这样对于企业的整体规划和成本投入都起到了最为优化的效果。也是因为当前 XXXX 虚拟化环境中所承载的应用服务和业务系统是企业工作的重点环节，使得虚拟化环境也成为了 XXXX 安全防护的重点环节，当前的虚拟化环境不仅需要面临传统环境所要面临的各种恶意程序威胁及网络攻击活动，而且由于其自身环境的特殊性还需要面临着最新威胁的关注，这样就使得对于虚拟化环境的安全防护不能够完全依赖于传统的安全防护方式。XXXX 引入虚拟化环境的搭建就是为了在保证企业应用服务和业务系统正常运行的情况下，来降低总体成本的投入，而如果采用了传统的防护方式来对虚拟化环境进行防护，那么由于传统防护方式在对虚拟化环境防护上只能做到对每个主机的安全防护，而且对于主机的防护还会随着虚拟化技术各种技术的应用，如：高可用性、灾难备份、负载均衡、虚拟机克隆等，会出现防护间断、资源占用过多等问题，而且还会因为需要更多的人力和物理力来投入到对于虚拟机安全防护之中，这样就会造成企业总体成本的浪费。

通过以上的分析我们可以得出结论，虚拟化环境需要的是为虚拟化所专属设计的安全防护解决方案，这样的方案需要能够与虚拟化环境进行无缝集成，并且采用最先进的安全防护技术来对已有和未知的威胁进行防护，有效拦截典型网络攻击活动，最优化的资源使用方案来使得安全产品自身占用最少的物理资源，而且还能够去配合虚拟化的各种技术，保证每个虚拟机自身和虚拟机中数据的安全，这样就可以为 XXXX 的应用服务和业务系统正常运行做出保障。

5. 卡巴斯基虚拟化安全解决方案——物理环境与虚拟环境的完美兼容

Kaspersky Security for Virtualization 为虚拟架构提供倍受赞誉的反恶意软件及反网络攻击解决方案，结合最新的安全技术，涵盖了对服务器、工作桌面和数据中心等虚拟系统的保护。该方案还提供了用以管理多种设备——包括物理服务器、虚拟机和移动设备安全性的统一而简单控制平台。这种单一的安全管理控制平台模式从根本上简化了安全任务的实施，并使安全管理事项更显而易见。卡巴斯基虚拟安全集成 VMware vShield，将反恶意程序安全功能安装在独立的虚拟主机上。集成 VMware vCloud Networking and Security: vCloud Ecosystem Framework 组件提供 IPS/IDS 检测系统，从而提供最高级别的防护。

由于应用独特的无代理模式，Kaspersky Security for Virtualization 比所有的有代理的传统安全产品具有更佳的性能和更高的整合率。

5.1 灵活的安全措施

- 保护

程序将保护虚拟机的子操作系统的文件系统。程序将扫描由用户或其他应用程序在虚拟机上打开或关闭的所有文件，以查找病毒和其他威胁。如果文件未感染病毒或不存在威胁，Kaspersky Security 将允许用户访问该文件。如果发现某个文件包含病毒或其他威胁，Kaspersky Security 将执行其设置中指定的操作；例如，删除或阻止该文件。Kaspersky Security 发送有关虚拟机保护期间发生的所有事件的信息到 Kaspersky Security Center 管理服务器。

- 反网络攻击

对于部署了分布式虚拟环境的企业，卡巴斯基提供了一个入侵防御系统（IPS）/入侵检测系统（IDS）来保护企业的 hypervisor 的网络流量，查找典型网络攻击活动。当检测到对虚拟机的网络攻击时，Kaspersky Security for Virtualization 会拦截发起网络攻击的 IP 地址，并发送有关虚拟机反网络威胁保护期间发生的所有事件的信息到 Kaspersky Security Center 管理服务器。

- 卡巴斯基安全云网络

覆盖全球的卡巴斯基安全云网络能够更快的应对零日攻击。

- 全局扫描

可根据预定计划，执行在所有虚拟机上的日常扫描。自动避免在多个虚拟机上同时实施日常扫描，KSV 有助于实现负载均衡。

- 虚拟机扫描

管理员可以任意选择虚拟机、个别的文件或文件夹执行手动扫描。此项按需扫描的功能，在 IT 团队针对任意虚拟机上可疑迹象的检查时十分有用。

- 共享缓存

如果一个文件在虚拟机上被打开，扫描了该文件后，并且证明该文件是安全的，那么该文件的信息会被放入共享缓存。那么如果有一个完全相同的文件存储在其它虚拟机上，那么该文件将不会再次扫描。共享缓存能够有效的减少系统资源负荷。

5.2 高度整合

- 支持 VMware vMotion

由于完全支持 VMware vMotion，Kaspersky Security for Virtualization 能够确保当工作负载从一个 ESXi 主机移动到另一个 ESXi 主机时保护不会中断。如果新的主机有必备的许可，安全保护将伴随着工作负载迁移、所有安全设置保持不变。

- 与 VMware vCenter 集成

Kaspersky Security for Virtualization 从 vCenter 获取有关虚拟机的信息，其中包括所有虚拟机的列表和相关参数。除了提供 IT 团队更清晰的安全信息，KSV 与 vCenter 集成确保了一旦有新虚拟机在 vCenter 中配置，安全保护便自动生效。

- 经过了广泛的 VMware 环境中的测试

Kaspersky Security for Virtualization 在以下环境中测试并证实了其兼容性。

VMware vSphere Distributed Resource Scheduler (DRS)

VMware vSphere High Availability (HA)

VMware vSphere Fault Tolerance (FT)

5.3 实现传统物理环境与虚拟环境的统一管理

- 快速部署

仅一台安全虚拟设备便可以为同一物理服务器上的所有虚拟机提供安全保护。用户可以简单地创建他们的新虚拟机，然后仅仅需要复制一个文件镜像到新虚拟机，这台新创建的虚拟机立即自动地受到倍受赞誉的卡巴

斯基反恶意软件解决方案的保护。

- 灵活的安全配置文件

不同的安全设置可以很容易的应用到不同的虚拟机组。这样的的灵活性能帮助提高性能。即，允许排除不相关的指定程序不对其进行扫描。

- 报表功能

详细的报告为管理员更透明、更详尽地展现物理机和虚拟机上的事件和任务完成情况。

- 管理一系列的卡巴斯基安全解决方案

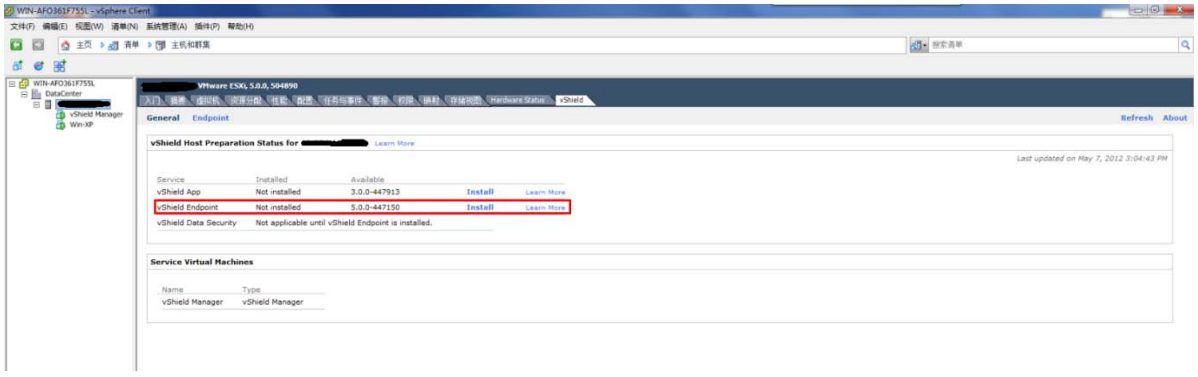
Kaspersky Security Center 也能管理卡巴斯基的其它安全产品，从而为您提供一个单一管理架构，使所有 IT 设备有了一致的安全策略。尤其是针对于卡巴斯基安全产品的原有用户，在部署虚拟化平台的安全防护时，只需将原有的管理服务器进行升级，就可以实现原有物理系统和新增 VMware 虚拟平台系统的统一管理，极大地减小 IT 管理人员的工作量，增加整体网络环境的兼容性和统一性。

6. 卡巴斯基虚拟化安全解决方案部署实施

6.1 VMware vShield Manager 部署

VMware vShield Manager 作为 VMware 虚拟化架构的安全组件，其负责对虚拟化环境进行安全防护，包括了虚拟防火墙和反病毒产品的 API 接口，卡巴斯基虚拟化安全解决方案可以与 VMware vShield Endpoint 进行完美结合，对 ESX 和 ESXi 上的所有虚拟机进行全面的反恶意程序安全防护。反网络攻击组件保护所有装有 VMware Tools 9.0.0 suite (版本 582409 或更新) 的虚拟机，无论其上装的是什么操作系统。

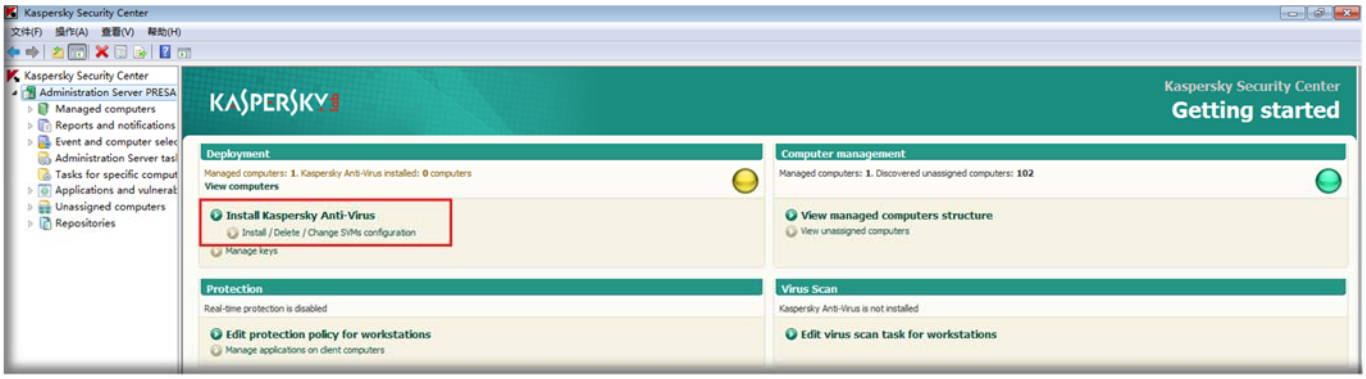
首先通过 XXXX 的 VMware vCenter 部署 vShield Manager，并安装 vShield Endpoint。



6.2 卡巴斯基虚拟化安全解决方案管理平台部署

卡巴斯基这套虚拟化安全解决方案可以通过 Kaspersky Security Center 10 来进行统一管理，而这个管理

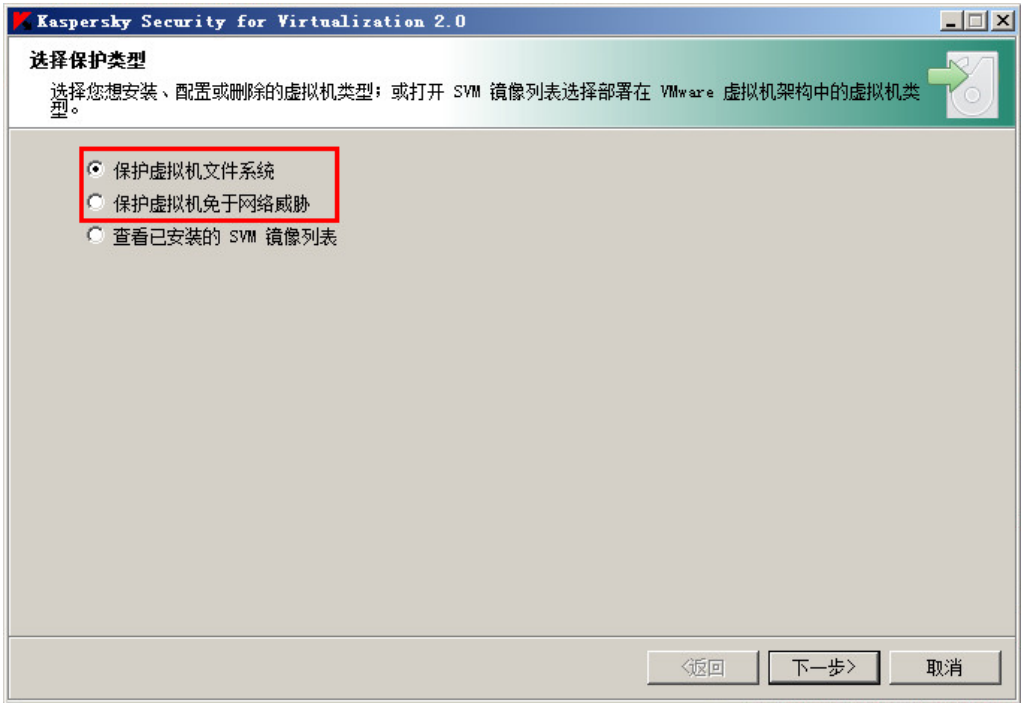
平台不仅可以对卡巴斯基虚拟化安全产品进行任务、策略、授权、扫描和更新等进行统一管理，还可以对卡巴斯基其他企业级产品进行统一管理，可以更加有效的为企业保证数据安全的基础上节省了总体成本。



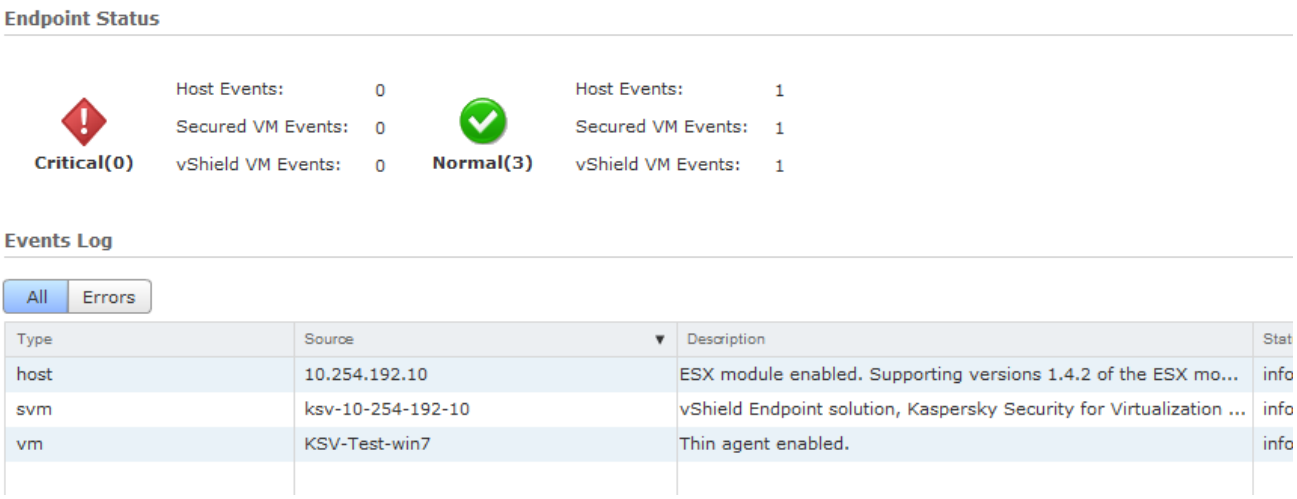
6.3 Kaspersky Security For Virtualization 部署

Kaspersky Security For Virtualization 为基于 VMware 平台的虚拟化环境提供无代理，反恶意程序和网络安全解决方案。结合最新的安全技术，可以接受 Kaspersky Security Center 的统一管理，卡巴斯基虚拟化安全有效地保护虚拟环境，提供 IT 管理员统一的管理平台以及可视化的界面。卡巴斯基虚拟安全集成 VMware vShield，将反恶意程序安全功能安装在独立的虚拟主机上。集成 VMware vCloud Networking and Security：vCloud Ecosystem Framework 组件提供 IPS/IDS 检测系统，从而提供最高级别的防护。

在卡巴斯基虚拟化安全产品的配置向导中，我们可以选择将要部署的产品功能，选择部署保护虚拟机文件系统时，该向导将帮助用户在基础架构中的 ESXi 主机上安装并配置 SVM。选择保护虚拟机免于网络威胁时，该向导将帮助用户安装和配置在基础架构的 VMware 集群上的装有反网络攻击组件的 SVM。

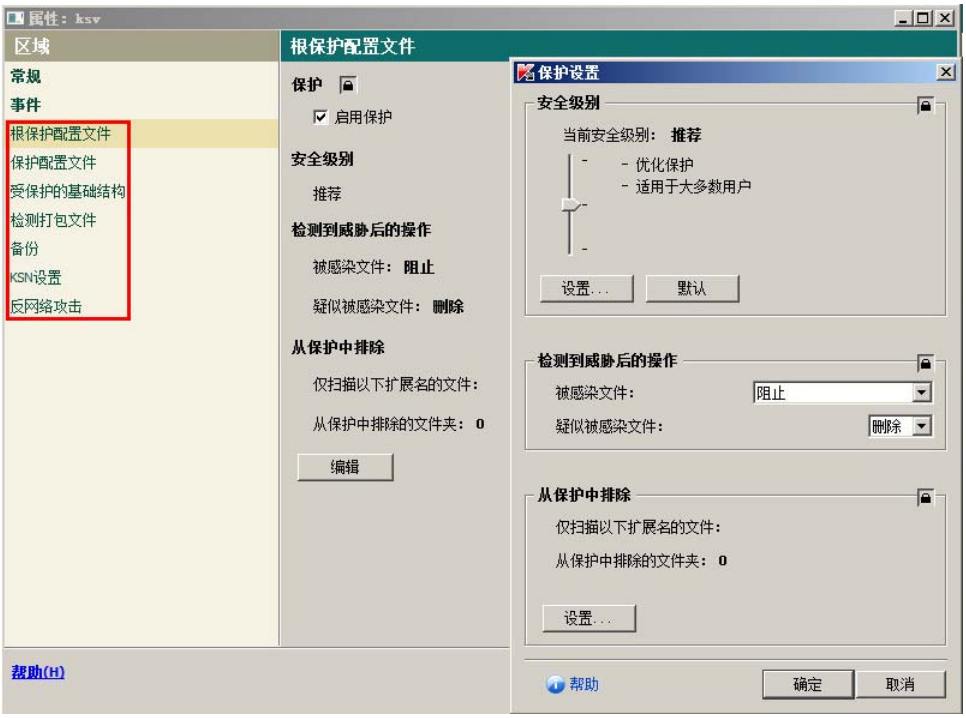


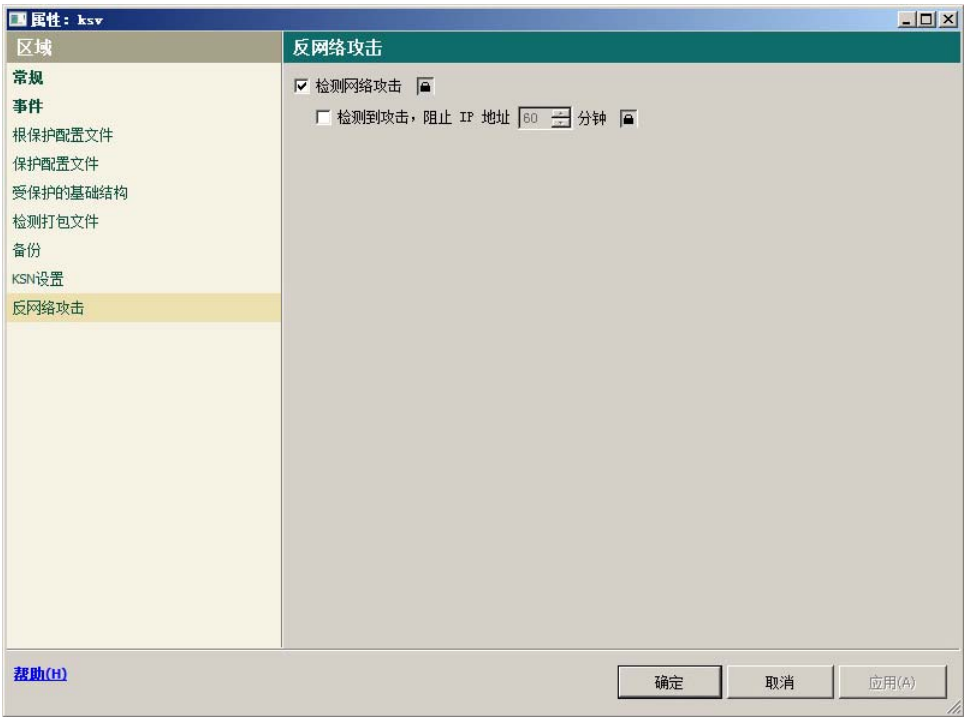
卡巴斯基文件反病毒组件会保护装有以下操作系统的虚拟机：Windows Vista（32 位）、Windows 7 (32/64 位)、Windows XP SP3 或更高版本(32 位/64 位)；Windows Server 2003 SP2 或更高版本（32/64 位）、Windows Server 2003 R2（32/64 位）、Windows Server 2008（32/64 位）、Windows Server 2008 R2（64 位）。



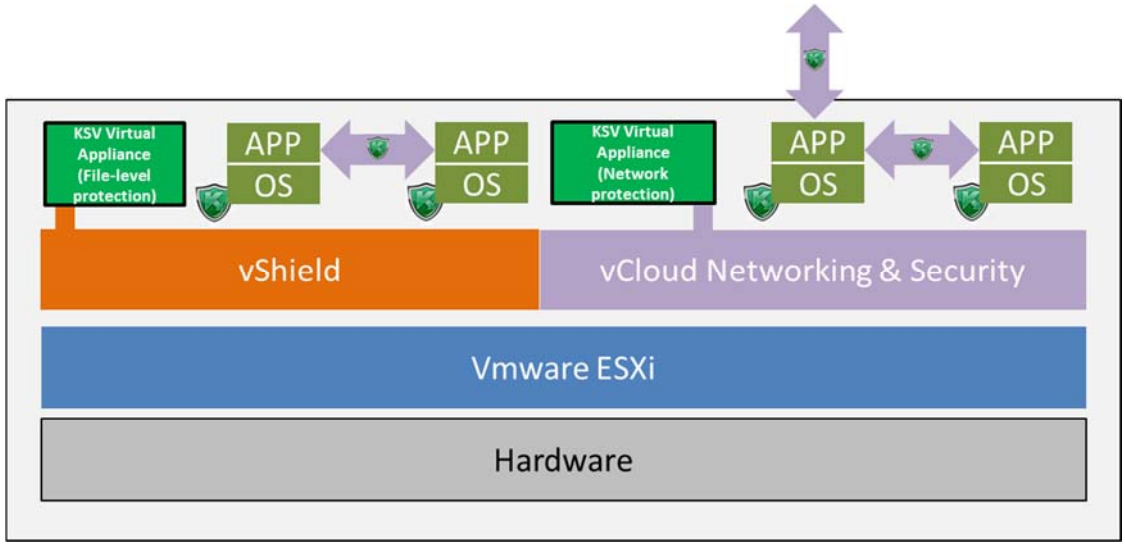
反网络攻击组件保护所有装有 VMware Tools 9.0.0 suite (版本 582409 或更新) 的虚拟机，无论其上装的是什么操作系统。

产品部署完成后，可以通过Kaspersky Security Center管理中心的策略窗口中详细设置虚拟化安全产品的各项功能参数。如下图所示：





卡巴斯基虚拟化安全解决方案的文件反病毒组件和反网络攻击组件完全部署完成后的防护架构如下图所示：



KSV 虚拟安全防护系统架构简图

7. 卡巴斯基虚拟化安全解决方案优势特点

事实上，虚拟机如同物理机一样容易受到恶意软件的侵害。因此，确保其系统得到最优秀的防护对于 IT 专业人员来说至关重要。但是，当企业开始扩大虚拟化软件规模时，安全软件可能会影响硬件的性能！此时，反病毒软件有可能“事与愿违”地逆转了虚拟化本应该给组织带来的好处。卡巴斯基实验室推出了针对虚拟环境的反恶意软件解决方案，该方案在保证性能最优化的同时还能提供强大防护，使组织免受当今威胁的侵害！

- 集中安全 – 为虚拟环境而开发安全方案

Kaspersky Security for Virtualization 允许为虚拟机执行各种策略。当使用 vMotion 将虚拟机从一台主机迁入另一台主机时，这些策略会跟随虚拟机一同移动。KSV 仅需要单一工作引擎和一份反病毒数据库就可以为运行在该物理主机上的所有虚拟操作系统提供完备的安全服务。管理员也可以通过卡巴斯基的管理控制台来查看逻辑及物理计算结构。

- 单一的管理工具

Kaspersky Security Center 是一个免费安全控制平台。使用这种单一平台式的安全控制工具来管理所有虚拟机、物理机和移动设备的安全。支持查看在 KSC 集群中的虚拟机列表，可以通过列表查看每一台虚拟机的受保护状态（是否受保护）。

- 高密度虚拟机

作为一个无代理模式的解决方案，Kaspersky Security for Virtualization 实现了高密度的虚拟化，消除了“更新风暴”、“扫描风暴”和“安全间隙”等代理模式的产品的弊端。

- 顶级的反病毒技术

卡巴斯基优秀的反恶意软件技，结合卡巴斯基的产品-实时的更新频率能及时阻止新的和快速传播的恶意威胁。启发式分析技术更能够有效地对抗多态的恶意软件。

- 卡巴斯基安全云网络

覆盖全球的卡巴斯基安全云网络能够更快的应对零日攻击

- 针对虚拟环境进行的优化

卡巴斯基的虚拟设备扫描主机上的所有子虚拟机，确保了最佳性能，因为没有多余的反病毒程序会来争夺系统资源，或产生反病毒风暴。一旦创建了新的虚拟机，Kaspersky Security for Virtualization 能迅速反应并自动提供保护，这消除了使用代理模式的解决方案会导致的防护间隙。

- 占用资源少

安全软件不会给主机硬件增加压力。因为卡巴斯基在有效扫描恶意软件上一直是行业领导者，我们的引擎是基于一个紧密集成的代码库，仅需要占用很少的资源。

- 共享缓存

如果一个文件在虚拟机上被打开，扫描了该文件后，并且证明该文件是安全的，那么该文件的信息会被放

入共享缓存。那么如果有一个完全相同的文件存储在其它虚拟机上，那么该文件将不会再次扫描，有效的减少系统资源负荷。

- 与 vShield 紧密集成

Kaspersky Security for Virtualization 允许为虚拟机执行各种策略。当使用 vMotion 将虚拟机从一台主机迁入另一台主机时，这些策略会跟随虚拟机一同移动。管理员也可以通过卡巴斯基的管理控制台来查看逻辑及物理计算结构。

- 第一个支持最新的 **VMware vCloud Networking and Security：vCloud Ecosystem Framework** 技术的安全厂商

该技术可以提供更有效的 IPS /IDS 功能。扫描虚拟机上的 HTTP 和 FTP 网络流量，检测和拦截典型的网络攻击活动。

8. 卡巴斯基技术支持服务

8.1 完善的反病毒服务体系

完善的产品服务

企业配备了先进的计算机反病毒产品，需要一个完善的服务体系来确保该系统的正常工作，并不断通过升级、更新使系统效能得到充分的发挥，才能确保企业的反病毒体系真正起到杜绝病毒进入内部网络的作用。

选择一个有丰富反病毒服务经验、了解最新反病毒状况、可及时获得使用反病毒产品使用中出现的问题解决方案、熟悉新病毒出现时的应急处理并能提供有效解决办法的专业反病毒服务商，并与之建立长期有效的服务关系，能从新产品新技术的采用、软件产品的升级换代、病毒事件的应急处理等多方面、全方位为企业提供全面反病毒技术支持，对保证企业的网络系统的病毒安全防护就显得非常重要。卡巴斯基技术开发（北京）有限公司是目前国内适合上述服务的领先公司之一，能够为企业提供完善的反病毒产品服务。

完善的安全管理服务

根据对目前国内外计算机病毒的发展现状和危害程度的分析，业界公认正确使用和快速反应成是病毒防范体系的重要内容，卡巴斯基技术开发（北京）有限公司将完善的计算机系统安全防范理念和长期积累的实践经验应用于企业的计算机反病毒体系，协助用户建立完善的反病毒安全管理体系。

8.2 快速响应的服务中心网络

卡巴斯基开放空间产品各地服务中心分布示意图

从多年反病毒服务中，卡巴斯基技术开发（北京）有限公司了解到，很多反病毒产品用户缺乏专业的反病毒知识，也不可能通过几次培训就能达到反病毒专业水平，另外用户也没有足够的精力跟踪反病毒的动态，无法独立解决每一次的病毒事件。特别是紧急情况下，用户迫切需要专业的反病毒上门服务，以解决燃眉之急，如果依靠反病毒厂商千里迢迢赶赴现场，可能给用户带来巨大的损失。因此，卡巴斯基技术开发（北京）有限公司公司根据多年反病毒服务的经验，在全国通过建立各地授权服务中心，直接提供本地化的专业反病毒服务。在这个专业化的服务体系中，卡巴斯基技术开发（北京）有限公司负责各地服务中心技术服务人员的专业认证培训，达到要求后给服务中心授权。得到授权的服务中心提供所在省市范围内所有卡巴斯基用户的维护和上门服务，以保证反病毒的快速响应。目前我们已在上海、杭州、广州、南京、石家庄、成都、沈阳、大连、济南、长春、郑州、乌鲁木齐、西安、南通等地建立了服务中心，其他省市的服务中心正在筹建中。各省市服务中心可自建各地市卡巴斯基反病毒二级服务中心，并经过培训获得卡巴斯基技术开发（北京）有限公司的认证。

此外，卡巴斯基技术开发（北京）有限公司还通过上班时间工作电话、电子邮件技术支持。在各地服务中心遇到无法处理的事件时，可随时联络卡巴斯基技术开发（北京）有限公司提供技术指导和现场服务。这样，通过组建全国的一级和二级服务中心，实现专业反病毒的快速反应，给广大卡巴斯基用户提供优质高效的反病毒专业服务。

8.3 服务内容

A. 卡巴斯基提供 5X8 小时的电子邮件与电话支持；

B. 免费提供一年反病毒软件版本升级及技术服务；

C. 技术支持响应时间保证：

✓ 对提交的可疑文件（包括新病毒），卡巴斯基技术开发（北京）有限公司在接到可疑文件的 24 小时内给予回复。

✓ 紧急情况下，如果可疑病毒开始在系统内大量扩散，卡巴斯基技术开发（北京）有限公司会在收到可疑程序后的一小时内向 XXXX 提供紧急应对方法。

✓ 在接到 XXXX 提出的问题后，卡巴斯基技术开发（北京）有限公司将跟据问题的种类和紧急程度以及先后顺序，保证在规定时间内向 XXXX 作出响应和提供相应的支持。问题种类和响应级别参照下表。

严重性	定义	反应时间	问题解决时间
最高级 Critical	软件死锁、没有反应。 病毒爆发、大量扩散。	**30 分钟**	**1 个工作日**
紧急 Urgent	系统主要功能无法执行。 系统性能突然严重降低。	**4 小时**	**2 个工作日**
重要 Important	系统出现错误，不过有变通方法可以暂时运作。 系统出现细微错误，不影响日常正常作业。 一般性的产品使用问题。	**1 个工作日**	**3 个工作日**
普通 Nor	索取产品更新（非电子数据方式）。 索取一般信息。	**1 个工作日**	**3 – 5 个工作日**

	mal			

注：以上解决问题的时间，是基于用户的良好配合

8.4 反病毒软件的更新

在服务期内，为 XXXX 提供免费的反病毒数据库更新服务和产品升级信息。至于是否升级产品，由 XXXX 提出要求。

免费紧急事件响应：

发生紧急事件（病毒爆发）时 XXXX 应立即通知卡巴斯基技术开发（北京）有限公司，卡巴斯基技术开发（北京）有限公司应了解病毒爆发状况，如病毒爆发地点、病毒感染现象等确定参与紧急事件响应技术人员和响应方式。

如果出现的紧急情况需要现场支持，卡巴斯基技术开发（北京）有限公司将提供现场支持服务，响应时间参照响应条例并加上路途所需时间。

对于出现的紧急情况，卡巴斯基技术开发（北京）有限公司将以最有效的方式处理出现的问题，并不限于 XXXX 所使用的产品，确保将损失降低到最低程度。

8.5 通过通讯方式提供技术服务

在服务期间内，卡巴斯基技术开发（北京）有限公司承诺免费 XXXX 提供计算机病毒防治技术咨询服务。服务方式可通过电话、电子邮件、传真等。

地址：中国北京市东城区青龙胡同 1 号歌华大厦 B 座 12 层（邮编：100007）

电话：010-84186111　　传真：010-84186222

5×8 小时技术支持电话：400-611-6633

技术支持邮箱：china-corp@kaspersky.com

病毒分析邮箱：viruslab@kaspersky.com.cn

升级续费邮箱：kaspersky@kaspersky.com.cn

官方论坛：bbs.kaspersky.com.cn

官方网站：www.kaspersky.com.cn

卡巴斯基病毒百科网站：www.securelist.com

9. 卡巴斯基公司介绍

9.1 公司介绍

卡巴斯基实验室是一个覆盖全球 100 多个国家和地区的国际集团。公司总部位于俄罗斯的莫斯科。目前，卡巴斯基实验室拥有超过 2300 名高素质专业人才，在全球 29 个国家均设立了区域办事处。我们的产品和技术为全球超过 3 亿的用户提供安全保护。

历经二十余年的磨砺，卡巴斯基实验室已经成为当今世界上增长速度最快的 IT 安全公司之一。今天，卡巴斯基实验室已稳居全球四大终端安全软件提供商之一，并不断提高其市场地位，在全球所有地区均呈现出显著增长。

从 1997 年 6 月卡巴斯基实验室公司正式成立以来，公司的首要任务是开发和完善保护计算机及计算机网络的软件来抵御计算机病毒的入侵，AVP Silver、AVP Gold 和 AVP Platinum 等主要产品很快受到国内外用户的好评。由于产品的可靠性及使用了革新的技术成果，1999 年，卡巴斯基实验室成为俄罗斯主要的反病毒软件提供商。

2000 年，卡巴斯基实验室宣布公司的反病毒解决方案将使用新商标卡巴斯基 AV 来代替 AVP（AntiViral Toolkit Pro）卡巴斯基实验室系列产品注册了雨伞形图形标志。

由于，Internet 和其他通讯手段的快速发展，卡巴斯基实验室开发了新的生产线，完全可以满足用户对新的数据保护的需要。公司为单机用户，中小型企业用户和大型企业用户提供了不同的产品和解决方案。在完善自己的反病毒产品的同时，公司开始开发新的项目——信息安全系统，扩充了产品的种类：网络屏蔽和内容过滤（防火墙类产品）。

2002 年 4 月，卡巴斯基实验室推出了自行开发的个人防火墙测试版。卡巴斯基实验室给美国的 Aladdin、Sybari、Deerfield、ITAmigo 以及其它公司发放了许可证，允许它们在自己的产品中使用卡巴斯基反病毒技术。

为了满足对现代化信息安全防护的需要，公司向用户提供了全套的信息安全防护解决方案，包括系统检测、开发、实施和维护等卡巴斯基实验室单机版产品使用的是与商业级产品同样的技术，但操作却非常简单，这使得它们在同级别产品中具有很强的可靠性及竞争力。

我们的产品持有许多全球最权威的认证和奖项。2003 年，卡巴斯基公司成为微软公司安全解决方案的金牌认证伙伴。卡巴斯基公司还是 SUSE 和 Red Hat 的荣誉合作伙伴，及 Intel 公司移动计算(CMT)项目的认证厂商。卡巴斯基公司的专家活跃在 CARO(Computer Antivirus Research Organization)、ICSA(International

Computer Security Association)等 IT 业高级协会中。

卡巴斯基实验室为了最大限度满足用户的需求，不断发展和完善自己的解决方案，在反病毒行业始终保持领先地位。卡巴斯基实验室对新的病毒能够快速做出反应；努力完善和发展新的产品，给客户提供最先进的信息防护体系。