Trend Micro Enterprise Security

即时防护，化繁为简。

改变虚拟数据中心防病毒领域的游戏规则

趋势科技白皮书 | 2010 年 9 月

I. 简介

虚拟化的早期实验应用始于二十世纪六七十年代，随后作为一种通过服务器整合控制 IT 资本和运营支出的方式首次正式实施。2005 年，Intel 和 AMD 推出专门支持虚拟硬件芯片集，虚拟环境开始扩展到业务范围应用，在此应用中，虚拟环境继续通过资源整合提高 IT 生产的成本效率。现在，降低 IT 成本在 CIO 最关心的问题中始终位列三甲，权威分析公司高盛的调查证实，虚拟化是降低技术成本的关键促成因素之一。 [1]

由于虚拟化在节约成本方面的作用已得到了广泛证实，人们把更多目光转向了虚拟化服务的质量，希望能在服务水平协议、速度和稳定性方面有所作为。但是，由于对虚拟化利益的追求过于急功近利，企业在虚拟化环境中仓促实施了传统架构的安全解决方案。尽管企业对此方法驾轻就熟，但遗憾的是，其结果并不尽如人意。采用此方法造成的最轻微影响是复杂性增加和性能受到影响，最坏的结果则是引发新的安全风险并降低服务器整合的成本效率。

“我们现已对 90% 左右的环境进行了虚拟化，这在降低成本和提高灾难恢复能力方面效果显著。”

Corporate Express 公司 CIO Gary Whatley 在 2009 年 1 月接受 Gartner 采访时的讲话

此白皮书对在虚拟化环境中使用端点安全所面临的挑战进行了评论，这些挑战包括动态虚拟机的固有风险，以及多个虚拟机中的安全软件（如病毒扫描程序）对单个物理主机的资源影响。[2] 为应对这些挑战，我们提供了一种新的虚拟数据中心安全标准；此标准结合了经验证的威胁防护技术以及一种创新性体系结构以在虚拟化环境中提供防病毒保护。

II. 虚拟数据中心内的安全挑战

以下两个因素使确保虚拟化进程的安全变得比较复杂：(1) 物理数据中心内存在的风险 (2) 虚拟化环境特有的风险。

企业安全和虚拟化领域的两个领军企业 — 趋势科技和 VMware® 强强联手，力图将这些挑战准确地呈现给客户，并在特定领域展开合作，帮助客户寻求解决之道。上述挑战对企业虚拟化能力的直接影响集中在从成本效率到服务质量，最终到业务灵活性的环节。只有经过这一最后阶段，IT 才可以真正作为服务（或通过云）交付，企业才可以根据需求请求这些服务。

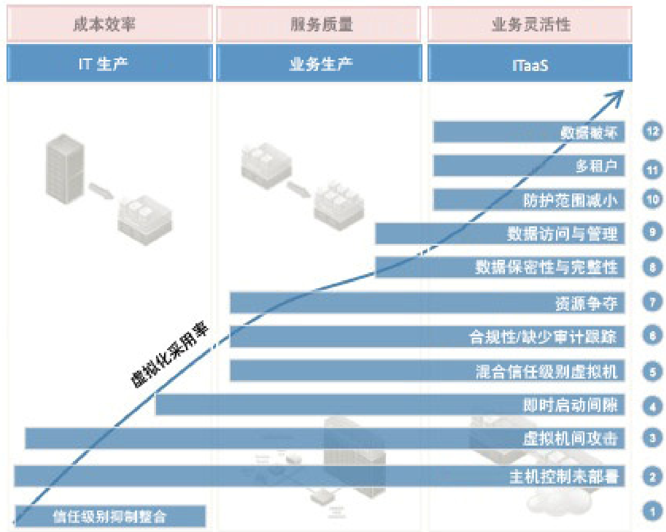

图 1：伴随虚拟化进程的安全挑战

虚拟数据中心内的传统方法

随着企业进入虚拟化的业务生产阶段，安全问题凸显出来，物理主机的大量整合带来的忧虑迅速超过喜悦。为应对虚拟机面临的风险，关注安全的企业将现有的终端安全解决方案部署到其虚拟化环境中的各个虚拟机。一个关于如何在虚拟化数据中心中，如何处理防病毒问题的实际“标准”因此而产生。

- **物理 v.s. 虚拟：** 物理体系结构与虚拟体系结构之间的固有区别不容忽视。例如，物理环境中的每个操作系统 (OS) 实例都直接在专用硬件平台上运行。与此相反，虚拟环境中的每个 OS 实例都在虚拟机上运行，多个虚拟机在“虚拟监控程序”层上运行。此虚拟监控程序是虚拟机和底层硬件之间的一个抽象层，通过该层可对系统资源进行动态分配。由于这些根本区别，文件扫描和软件更新的网络请求等常规处理措施的表现肯定会存在差异。

- **繁琐的防病毒管理：** 虚拟化基础架构 (VI) 管理员可以使用模板加快部署速度，进而提高效率。安全管理员可以采用集中式防病毒管理。但即使借助一定级别的自动化，每个虚拟机上的防病毒部署和持续管理也是不可扩展的。在物理环境中，这一过程非常繁琐，虚拟环境的动态性只能使繁琐加剧。

传统防病毒管理

1. 安装、配置客户端
2. 运行过程中细度配置客户端（如果需要）
3. 补丁/升级客户端
4. 病毒码更新

此传统方法使虚拟化环境面临三个关键挑战：

- 即时启动的防护间隙 （快照、还原的威胁和安全风险）
- 资源争夺
- 合规性 / 缺少审计跟踪

即时启动防护间隙

除服务器整合之外，企业通过按需配置和取消配置虚拟机，将其动态性用于测试环境、定期维护、灾难恢复以及用于支持需要按需计算资源的“任务工作者”。因此，当以较快频率激活和停用虚拟机时，无法快速、一致地为这些虚拟机配置安全措施并使其保持最新。休眠的虚拟机最终偏离引入大量安全漏洞这一简单的基线。如果不配置客户端和病毒库更新，即使是使用包含防病毒功能的模板构建的新虚拟机也无法立即对客户机起到防护作用。简言之，如果虚拟机在部署或更新防病毒软件期间未处于联机状态，它将处于不受保护的休眠状态，一旦激活、联机后将会立即受到攻击。

资源争夺

常规防病毒扫描和病毒码 更新等占用大量资源的操作将在很短的时间内导致过量系统负载。如果防病毒扫描或定期更新在单个物理系统的所有虚拟机上同时启动，将会引起“防病毒风暴”。此“风暴”就如同银行挤兑，其中的“银行”是由内存、存储和 CPU 构成的基本虚拟化资源池。此性能影响将阻碍服务器应用程序和虚拟桌面 /VDI 环境的正常运行。

传统体系结构还将导致内存分配随单个主机上虚拟机数量的增加而呈现线性增长。在物理环境中，每一操作系统上都必须安装防病毒软件。将此体系结构应用于虚拟系统意味着每个虚拟机都需要多占用大量内存，从而导致对服务器整合工作的不必要消耗。

IT 合规性挑战

行业规章和企业安全策略必须与虚拟化技术保持同步，这对合规性工作提出了一系列特殊的挑战。由于传统的基于主机的安全软件和网络安全设备未集成到内视层中，

“PCI DSS 2.0 将对系统组件的定义进行扩展，将虚拟组件加入其中。”

PCI DSS 2.0 和 PA-DSS 2.0

更改摘要 - 要点，2010 年 8 月

因此，在虚拟环境中，系统和网络活动的可视性和控制甚至更复杂。解决此问题的最有效方法是，使用虚拟监控程序内视功能（监视和控制进出虚拟监控程序层的功能）将防病毒功能直接集成到虚拟化平台中。实现上述高效率需要与虚拟化平台提供商合作。

III. 需要新方法

由于未考虑虚拟环境与物理环境的固有差异，在虚拟环境中实施专为物理环境设计的解决方案可能产生新的挑战，其效果与将当今的恶意软件检测用于物理环境相同。

弥补传统方法的缺陷：必须确定在虚拟化环境中引起最大问题的防病毒操作，并开发简化这些操作的解决方案。对于即时启动的防护间隙，此解决方案必须在完全防护状态下配置并管理虚拟机，这样就可以确保虚拟机的持久安全，而无需考虑上次进行病毒库更新或预设扫描的时间。对于资源争夺问题，此解决方案必须补偿上述防病毒活动导致的资源使用峰值。

确保新方法切实有效：这一新方法还必须有效利用现有投资，不仅是出于成本效率的考虑，还是出于员工培训需求的考虑。此外，此方法不得破坏其他业务领域的现状；必须继续满足所有安全策略、行业规章和合规性要求，还必须通过审计跟踪和其他深入报告满足可见性要求。

IV. 平台 — VMWARE VSHIELD ENDPOINT

VMware 是虚拟化和云基础架构领域的全球领军企业，向超过 190,000 家客户提供了经客户证实有效的解决方案，这些客户中有超过 97% 的财富 1000 强公司和 94% 的全球 500 强公司。通过在虚拟化数据中心领域不断创，VMware 借助 VMware vShield Endpoint 对其平台进行了扩展，使该平台支持优化虚拟化环境中的安全功能所必需的虚拟监控程序内视功能。

VMware vShield Endpoint 强化了虚拟机及其主机的安全，同时根据端点保护强度的需求改进了性能。可以通过 vShield Endpoint 将防病毒处理的任务转交给由趋势科技提供的专用安全强化虚拟机。vShield Endpoint 还可以大幅降低虚拟主机上的安全程序所占用的内存，方法是清除虚拟机上的防病毒软件并把这些功能集中于专用的安全虚拟机。VI 管理员可以通过集成在 VMware vCenter™ Server 中的 vShield Manager 控制台集中管理 VMware vShield Endpoint，进而管理趋势科技防病毒解决方案平台。

工作方式

以主机为单位部署的 vShield Endpoint 直接插入 VMware vSphere™ 平台，它由以下三个组件构成：

- 强化的安全虚拟设备（由趋势科技提供）
- 虚拟机驱动程序，用于转交文件事件
- VMware Endpoint Security (EPSEC) ESX 模块，链接虚拟监控程序层的前两个组件

vShield Endpoint 驱动程序针对基于 vSphere 的受保护虚拟机启用，只需几兆 的内存即可运行。[3] 此驱动程序监控虚拟机文件事件并向防病毒引擎发出通知，该引擎扫描这些文件并返回处置方式。它还支持由虚拟安全设备中的防病毒引擎启动的预设全盘扫描和部分文件扫描。需要进行补救时，管理员可以使用现有的防病毒管理器指定要采取的处理措施，而 vShield Endpoint 会在各自虚拟机中自动执行补救措施。

V. 解决方案 — 趋势科技™ Deep Security

可通过 VMware vShield Endpoint 平台在虚拟化环境中对防病毒解决方案进行优化。在此平台的基础上，作为战略合作伙伴的趋势科技首先提供了应对上述挑战的解决方案，即通过趋势科技™ Deep Security保证虚拟化环境的安全。

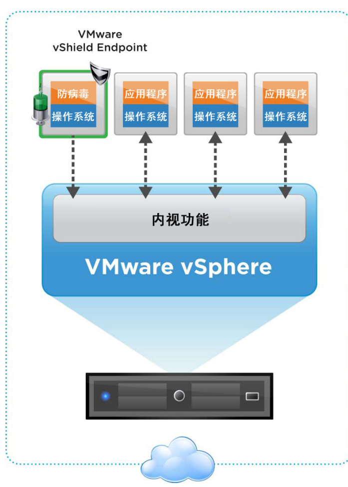

图 2：VMware vShield Endpoint 和趋势科技Deep Security

通过结合使用二者，企业可以有效应对虚拟数据中心内的即时启动防护间隙和资源争夺挑战。这项前所未有的创新改变了虚拟数据中心防病毒领域的游戏规则。

趋势科技 Deep Security 提供的防病毒引擎有能力执行定时（和访问时）文件扫描、病毒库更新、检查文件内容（已知或未知恶意软件）等常见处理措施的“安全虚拟设备”，以及关于强制处理措施（例如隔离、删除）的说明。强制处理措施的实际执行由监控虚拟监控程序和虚拟机文件活动的 VMware vShield Endpoint 技术执行。

始终启用安全来应对即时启动防护间隙

在受趋势科技 Deep Security 和 VMware vShield Endpoint 连动式保护的环境中，虚拟机在其整个生命周期内都将受到保护，这确保了所有文件访问都会被自动扫描，以排除最新的已知威胁。部署趋势科技 Deep Security 安全虚拟设备时对其进行了必要的安全强化，可确保防病毒引擎始终存在并适用于执行上述任务。

防病毒转交解决了资源争夺问题

通过这一创新型新技术，组织现在可以将防病毒扫描等活动从单个虚拟机转交给各受保护 vSphere 主机上的单个趋势科技安全虚拟设备，从而达到改进性能和保持整合率的目的。

- **回收内存以提高整合率：**通过降低每个虚拟机的内存分配，管理员可以显著提高服务器的整合率。现在，组织无需再向物理计算机上的每个虚拟机部署占用数百兆空间的防恶意软件软件，而只需向虚拟设备部署一个单独的防病毒引擎，并在每个虚拟机上用一个占用空间非常小的驱动程序 (vShield Endpoint) 执行必要的转交。在 200:1 的整合率比较常见的 VDI (VMware View™) 环境中，此技术的效果非常明显。[5] 内存分配的大幅降低可以实现成本节约，企业可以更充分地发掘其物理服务器的使用价值，并实现更高的服务器整合率。

- **集中扫描和更新以避免防病毒风暴：**趋势科技 Deep Security 使用这一新的体系结构处理占用大量 CPU 和 I/O 资源的文件扫描和病毒库更新，这将使虚拟机拥有更多用于执行业务关键功能的资源。通过跨给定主机上的多个虚拟机进行序列化操作，此解决方案可防止与这些同步扫描和更新关联的防病毒风暴和瓶颈。

可视性和控制可以简化合规性工作

趋势科技 Deep Security 解决了除安全性之外的多个其他合规性方面的问题：

- **各服务器的特有功能：**PCI DSS 2.0 最近的一项更新表明，即使在需求2.2.1（“每个服务器都有一项主要功能”）必须得到满足的情况下，虚拟化技术也是可以接受的。根据此观点，安全虚拟设备可以是一台只提供防病毒保护这一单纯功能的虚拟机。

- **通过内视实现可视性：**此解决方案使用强大且安全的虚拟监控程序内视功能（通过 vShield Endpoint）确保防病毒扫描期间可以了解到最深层的文件活动。大多数行业规章和企业数据安全策略需要主动监控系统对恶意软件采取的措施，趋势科技则更进一步，在虚拟系统上执行这些扫描。

- **记录 vSphere 和趋势科技事件：**趋势科技和 VMware 解决方案提供了对相关安全事件的详细日志记录功能，可帮助满足管理需求以及可能需要取证数据以便进行调查的企业策略。

- **职责分离：**这一新的体系结构使安全管理员可以通过趋势科技 Deep Security 管理控制台（与确保物理环境安全使用的界面相同）实施和管理虚拟环境的防病毒策略。同样，VI 管理员可以使用 vCenter，随趋势科技安全虚拟设备一起部署 vShield Endpoint。由于设计原因，任何个人都无法管理其他基础架构。VI 管理员与安全管理员的这一职责分离，以及活动的详细信息记录可帮助企业证明合规性并满足审计要求。

VI. 优势远超出解决方案本身

通过直接在虚拟监控程序层上执行操作，趋势科技针对资源争夺和即时启动防护间隙问题提供了一种强大的解决方案，可在不影响性能的情况下简化 IT 管理并提高资源效率。

简化管理

在物理数据中心内，防病毒程序的初期部署和持续管理是非常困难的。新解决方案解决了虚拟数据中心内的这些挑战。

- **简化防病毒管理：**通过 VMware vShield Endpoint 和趋势科技 Deep Security，管理员只需向趋势科技 Deep Security 安全虚拟设备部署企业防病毒引擎和病毒库更新即可。这从根本上消除了传统方法中执行许多繁琐任务的必要：

  1. 安装时无需配置客户端
  2. 运行过程中无需重新配置客户端（根据需要）
  3. 无需安装补丁/升级客户端
  4. 无需大量的病毒码更新

- **无需重新培训管理员：**通过与趋势科技管理控制台集成在一起的 VMware vCenter 进行基于角色的访问控制，使用户可以持续进行其日常操作，将中断时间降到最低。管理员可以在 vCenter 上定义一个角色，该角色只允许授权管理员向虚拟主机部署趋势科技 Deep Security 安全虚拟设备。还可以将趋势科技控制台配置为限制访问趋势科技 Deep Security 策略和安全操作（以实现重要更新的最佳预设），从而避免资源争夺。

安全性更高

趋势科技 Deep Security 在很大程度上提供了更高的安全性，因为它具体实现了一种在虚拟化数据中心环境中有效保障安全的方法。过去二十年间，安全行业的一贯做法是在需要防护的相同系统上运行防病毒软件，不经意间就可能对攻击敞开门户。

- **消除攻击目标：**由于未在虚拟机上安装防病毒软件，趋势科技 Deep Security 解决方案减少了安装客户端的必要性。如上所述，防病毒技术部署在经过强化的安全虚拟设备中。此外，每个虚拟机上的 VMware vShield Endpoint 驱动程序只允许与趋势科技Deep Security 安全虚拟设备进行特定的通信。对防病毒产品的大多数攻击都假设会在虚拟机上遇到一个全方位的客户端防病毒安装程序，但此类攻击将对这一全新解决方案束手无策。

- **消除常见攻击方法的漏洞：**防病毒引擎在其上运行的趋势科技 Deep Security 安全虚拟设备针对常见攻击方法（如 Conficker 蠕虫，又称飞客病毒使用的方法）进行了强化。只有与恶意软件防护相关的特定处理措施可以在安全虚拟设备和虚拟机之间存在。由于此设备始终处于开启状态，不存在即时启动防护间隙；虚拟机始终受到保护。

常见攻击方法

1. 卸载防病毒程序
2. 停止防病毒程序
3. 修改防病毒程序需要的注册表项

VII. 为什么选择趋势科技

自 20 年前创立之初开始，趋势科技专注于内容安全，在内容安全方面具有核心竞争力和专业经验。趋势科技通过趋势科技云安全智能防护网络不断提供创新，此网络可关联新的未知威胁的实时数据，并在环境中提供持续更新保护，非常适合保护物理和虚拟环境。云安全智能防护网络基础架构可从云端提供高级防护，可以在威胁到达公司网络前将其实时阻止。借助独特的云客户端体系结构，云安全智能防护网络综合运用威胁情报传感器全球网络、电子邮件、Web 和文件信誉技术显著降低了病毒感染的几率。

趋势科技将云安全技术直接用于趋势科技 Deep Security 防病毒技术，以降低病毒库占用的内存空间。趋势科技 Deep Security 安全虚拟设备是最近提供的虚拟化就绪解决方案，可帮助企业集中管理物理和虚拟环境的防病毒资源，从而进一步降低运营成本。

趋势科技年度收入超过十亿美元、拥有 1000 多名威胁研究人员和 4000 多名员工 — 在全球范围内，趋势科技具有足够的规模、速度和独一无二的云端核心技术基础架构，我们有足够的信心为当今的企业安全保驾护航。

VIII. 结论

企业在应对虚拟数据中心的安全挑战时会理所当然地选择熟悉的方法，但物理与虚拟基础架构的固有差异使传统解决方案的表现差强人意。趋势科技与 VMware 联合推出了通过趋势科技 Deep Security 对 VMware 虚拟数据中心进行防病毒保护的创新方法。这一前所未有的方法不仅解决了传统方法所面临的关键挑战，而且轻松实现了简化管理、满足 IT 合规性要求和改进解决方案整体安全性的目标。

虚拟化环境中 的安全挑战	解决方案的优点
即时启动防护间隙	• 在 IT 可以安装防病毒软件之前自动保护 • 通过在安全虚拟设备集中部署使防病毒特征码保持最新
资源争夺	• 通过回收内存保持高整合率 • 通过集中扫描避免防病毒风暴
IT 合规性挑战	• 服务器的特有功能符合 PCI DSS 和其他规章 • 通过内视实现可视性 • 记录 vSphere 和趋势科技 Deep Security 事件 • 支持职责分离

虚拟化环境中 的安全挑战	解决方案的优点
管理复杂性 传统防病毒措施的安全风险	• 简化安全管理 • 无需重新培训管理员 • 消除攻击目标 • 消除常见攻击方法的漏洞

请通过 http://www.trendmicro.com.cn 了解有关趋势科技 Deep Security 的详细信息。

请通过 http://www.vmware.com/products/vshield-endpoint/ 了解有关 VMware vShield Endpoint 的详细信息。

IX. 参考

[1] “直面挑战：2009 CIO 议程”，2009 年 1 月，32 和 45 页

[2] 检测和清除病毒、特洛伊木马和其他形式的恶意软件的软件通常被称为防病毒软件或防恶意软件软件。在此页我们将称之为防病毒软件

[3] 必须使用现有的虚拟机配置方法（如模板）对驱动程序进行初始部署。VMware 正在考虑将其用作 VMware Tools 的虚拟机驱动程序。源：VMware

[4] 源：VMware® ROI TCO Calculator http://roitco.vmware.com/vmw/