McAfee Management for Optimized Virtual Environments AntiVirus

适用于私有云且不会降低服务器性能的安全保护

传统防病毒软件无法与虚拟化基础设施有效整合。McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) 可为您的虚拟化桌面机和服务器提供优化的高级恶意软件防护。可以跨多个虚拟机监控程序实施，或者对于 VMware NSX 或 VMware vCNS，也可以选择经过调整的无代理选项。总之，您不仅可以获得即时威胁检测的顶级安全保护，虚拟机 (VM) 的性能也几乎不会受到影响。McAfee MOVE AntiVirus 可释放虚拟机监控程序资源，同时确保根据策略运行最新的安全扫描，从而优化了针对虚拟化部署的防恶意软件保护功能。

优化的扫描控制

来宾桌面机和虚拟服务器的动态特性要求必须谨慎操作。当用户发起会话时必须确保映像未感染恶意软件。这可能有一定难度，因为用户往往以团队形式开展工作，这会导致对“防病毒风暴”的峰值需求，进而消耗资源并阻止用户获取会话。

为了消除扫描瓶颈和延迟，McAfee MOVE AntiVirus 将扫描、配置和 .DAT 更新操作的工作从单个来宾映像转移到卸载扫描服务器。我们构建并维护一个已扫描文件的全局缓存，以确保当文件经过扫描并确认未受感染时，访问该文件的后续虚拟机无需等待扫描。这样就可以减少分配给每台虚拟机的内存资源，从而将这些多出来的资源释放回资源池，以便实现更有效的利用。

McAfee MOVE AntiVirus 允许为按访问扫描和按需扫描设置单独的策略，从而让您精确调整安全执行活动。例如，对于实时扫描和按访问扫描，管理员可以合理地假设它们具有一定程度的风险级别，从而避免在扫描时降低服务器性能，随后，当操作对服务器性能影响不大时，可以利用更严格的策略来执行按需扫描。

跨所有云的全面端到端监控

掌握的信息不全会导致难以为虚拟化环境实施正确的安全策略。McAfee Cloud Workload Security (McAfee CWS) 涵盖本地、私有云和公共云环境（包括 VMware 和 OpenStack），可提供对虚拟数据中心的全面监控能力，并将服务器、虚拟机监控程序和 VM 等关键属性导入 McAfee ePO 控制台。如果管理员可以全面掌握所有虚拟机的安全状态，并近乎实时地监控虚拟机监控程序与虚拟机之间的关系，那么保护您的虚拟数据中心就会容易得多。可自定义的信息显示板会显示有关资产的安全扫描状态、执行概况，以及历史安全数据。

McAfee CWS Essentials 和 McAfee CWS Advanced 扩展了对 Amazon Web Services (AWS)、Microsoft Azure 公共云和物理服务器的监控和控制能力。

主要优势

- **减轻恶意软件扫描的负担：**提供即时保护，对内存和处理过程的影响较小
- **防范防病毒风暴：**选项包括按访问扫描和按需扫描
- **启用灵活部署：**多平台（所有主流虚拟机监控程序、Windows VM）或无代理（VMware、Windows 和 Linux VM）
- **改进资源优化：**脱机扫描程序的弹性配置，并提供事件通知（多平台）
- **几秒钟内阻止未知的零日威胁：**在沙盒环境中将本地信誉情报与行为分析相结合（多平台，单独出售的附加模块）
- **利用 McAfee® ePolicy Orchestrator® (McAfee ePO™) 控制台：**端到端监控，以及跨物理、虚拟和云部署进行控制

精细的策略管理

这个常用的 McAfee ePO 控制台允许您配置 McAfee MOVE AntiVirus 的各项策略和控制。您可以将来自物理系统和公共云的虚拟数据汇总在一起，从而提供统一的信息显示板和报告。管理员可以通过 McAfee Cloud Workload Security，按照虚拟机、群集或数据中心配置单独的策略，从而让它们的安全保护能够专门适应数据中心的构成。

McAfee MOVE AntiVirus 的其他功能

管理和监控：

- 立即对一台或一组虚拟机安排按需扫描。
- 利用针对性按需扫描提高扫描精度。
- 通过集成 VMware NSX Service Composer，自动在每个虚拟机监控程序中部署卸载扫描程序。
- 随时掌握信息显示板、报告和电子邮件警报中暴露的问题。

简化的部署和配置过程：

- 在多个虚拟机监控程序（无代理）上部署和配置卸载扫描程序。
- 使用 McAfee ePO 控制台（多平台）还原被隔离的文件。
- 为防病毒软件优化进行详细的诊断。
- 无缝无代理和多平台策略管理。

适用于 VMware 的无代理选项

McAfee MOVE AntiVirus 可以利用 VMware NSX 或 VMware vCNS 来实现更高的效率。在无代理部署中，它们利用虚拟机监控程序作为高速连接，以允许 McAfee MOVE AntiVirus 安全虚拟机 (SVM) 扫描来自来宾映像外部的虚拟机。执行扫描时，SVM 将指示 VMware NSX 或 VMware vCNS 缓存正常文件，或者删除、拒绝访问或隔离恶意文件。

在 VMware ESX 服务器上安装和配置 SVM 和 VMware NSX 或 VMware vCNS 组件，并且在来宾虚拟机上安装 VMware NSX 或 VMware vCNS 终端驱动程序后，无需在每台客户端虚拟机上安装 McAfee 的软件，每个映像就可以自动受到保护。我们的 vMotion 感知实施意味着虚拟机可以从一个主机转移到另一个主机，并能得到目标主机上 SVM 的严密保护，同时还不会影响扫描或用户体验。

McAfee 产品与 VMware vCNS 集成可让您在 VMware vCenter 中监控 SVM 状态，并在 SVM 断开连接时收到警报。McAfee ePO 控制台会在虚拟机受到感染时收到事件数据，详细说明受到感染的虚拟机的状况。与 VMware NSX 的深度集成可同步在 McAfee ePO 控制台中创建的策略和在 VMware NSX 中分配的规则。对于没有防恶意软件保护或已遭到恶意软件入侵的计算机，通过将其标记为存在漏洞的计算机，则可以利用 VMware NSX 防火墙立即隔离相应的虚拟机。

我们支持为 VMware vCNS 和 VMware NSX 同时部署无代理 McAfee MOVE AntiVirus，这进一步简化了难度，让 VMware vCNS 客户可以无缝过渡到 VMware NSX。

适用于所有主流虚拟机监控程序的多平台

在包括 vSphere、Hyper-V、KVM 和 XenServer 等在内的多平台安装中，McAfee MOVE AntiVirus 代理（一种轻型终端组件）会与 SVM 进行通信，代表每个虚拟桌面机安排防病毒处理。McAfee MOVE AntiVirus 代理会维护一个本地缓存，并管理各项策略和扫描功能。用作清理大师时，可以指定和扫描参考映像。使用未受感染的映像预先填充本地缓存可实现最快速的虚拟机启动。

当访问文件时，McAfee MOVE Offload Scan Server 会执行按访问扫描，向虚拟机提供反馈。用户可以通过弹出式警报接收问题通知，随后可以执行删除、拒绝访问或隔离恶意文件等操作。

McAfee MOVE AntiVirus 配置

McAfee MOVE AntiVirus for Virtual Servers

- McAfee MOVE AntiVirus：
  - 多平台部署
  - 无代理部署
- 适用于私有云的 Cloud Workload Security（VMware 和 OpenStack）
- McAfee ePO 软件

McAfee MOVE AntiVirus for Virtual Desktops

- McAfee MOVE AntiVirus：
  - 多平台部署
  - 无代理部署
- 适用于私有云的 Cloud Workload Security（涵盖 VMware 和 OpenStack）
- McAfee Host Intrusion Prevention System
- McAfee SiteAdvisor® Enterprise
- 内存保护、Web 应用程序保护
- McAfee ePO 软件

在多平台部署中，扫描需求可能会上下波动，因此，可以自动向资源池中添加 SVM 或从资源池中删除 SVM，从而增强或减弱能力，实现无限制的扩展和高效资源利用率。事件通知可以帮助管理员了解利于优化资源管理的 SVM 使用情况。

利用 McAfee Threat Intelligence Exchange 的本地数据（一个单独出售的附加模块），多平台部署下的 McAfee MOVE AntiVirus 可以从 McAfee Global Threat Intelligence (McAfee GTI) 增强全球信誉情报，从而即时识别和应对不断增长的独特恶意软件样本数量。利用 McAfee Threat Intelligence Exchange，McAfee MOVE AntiVirus 会与 McAfee Advanced Threat Defense 相互协调，在沙盒环境中对未知应用程序的行为进行动态分析，以及让所有终端自动免受新检测到的恶意软件的威胁。McAfee MOVE AntiVirus 通过 McAfee Threat Intelligence Exchange 与 McAfee Network Security Platform 集成，为统一的周边和虚拟机保护提供分层安全保护方法。

适用于无代理和多平台部署的统一策略管理

许多组织可能希望利用 McAfee MOVE AntiVirus 的能力来同时支持无代理和多平台部署。凭借 McAfee MOVE AntiVirus，安全管理员可以使用 McAfee ePO 中的一个扩展点定义和管理一致的安全策略，因此，这些不同方法的管理既无缝又简单。

了解更多

McAfee 解决方案不仅可以让您拥有所需的安全防护，而且还能让您享用操作上的灵活性。

请访问 www.mcafee.com/cn/products/move-anti-virus.aspx 了解更多信息。

体系结构	多平台部署	无代理部署
支持虚拟机监控程序/平台	所有主流虚拟机监控程序，包括 VMware、Citrix、Hyper-V 和 KVM	VMware
扫描平台	Windows 2008、Windows 2012 R2、Windows Server 2016、Windows 10 R4 和 RS5	Linux Ubuntu 16.04
部署可扩展性	一个 SVM 可以通过多个虚拟机监控程序保护虚拟机。SVM 可以采用弹性方式进行配置。	每台 ESX 主机一个 SVM
与虚拟机通信	通过网络	通过虚拟机监控程序
虚拟机保护	Windows	Windows 和 Linux

北京市东城区北三环东路 36 号
北京环球贸易中心 D 座 18 层，100013
电话：8610 8572 2000
www.mcafee.com/cn