

McAfee Endpoint Security 套件

以低廉的成本和简化的法规遵从提供的强大安全保护

为企业打造一个安全终端环境可能是一项复杂的工作。复杂的恶意软件 and 没有边界的工作场所使网络犯罪分子可以很容易地窃取信息和设备。相关法规迫使企业提高对数据的安全保护和验证法规遵从。日益增多的各种安全单点产品提高了管理成本和响应复杂性。McAfee® Endpoint Security 套件结合业界领先的终端安全和数据防护功能，利用可靠的安全集中管理，简化了运营并减轻了法规遵从压力。

主要优势

- 适用于所有终端的可靠保护
- 借助集中式管理降低运营成本
- 借助标准模板轻松实现合规性

“NSS Labs 创建了各种 Operation Aurora 的变体并对防恶意软件杀毒软件进行了测试，考查了七种产品在阻止利用漏洞攻击和恶意代码载荷方面的性能。在给定攻击可见性级别和自从首次发现攻击所经过的时间的情况下，大多数（如果不是全部）产品都能涵盖漏洞。但是，在七种经过测试的产品中只有一种产品正确阻止了多种漏洞和恶意代码载荷，显示了基于漏洞的保护功能（该产品就是迈克菲）。”

—NSS Labs 发现大多数终端安全产品缺乏“基于漏洞的保护”功能

<http://nsslabs.com/nss-labs-in-the-news/nss-labs-finds-most-endpoint-security-products-lack-vulnerability-based-protection>

令人生厌的防病毒日子应该结束了。如今面临着严峻的威胁形势，蠕虫、间谍软件、特洛伊木马、僵尸程序 (Bot)、Rootkit、黑客、身份信息窃贼和具有针对性的攻击不断侵袭，而且攻击形式瞬息万变。用户希望能够随时随地工作和访问应用程序，但是在他们返回办公室后再使用笔记本电脑和移动设备（包括 Mac 系统）时，可能会危害企业网络和系统。再加上对数据保护与法规遵从验证和报告的严格要求，您所面临的风险已远远高于从前。然而，您的预算却并不充足。

您可以将一系列单个产品拼凑在一起，但却无法达到 McAfee Endpoint Security 套件的效率和有效性。这是因为我们通过集成相互协同的全面解决方案，针对当今的多方位威胁提供了最佳防御措施。我们的 Endpoint Security 套件能够防御所有五种威胁途径——系统、电子邮件、Web、数据和网络。

该集成安全解决方案不但可以提供可靠的保护，而且易于部署和管理。McAfee Endpoint Security 套件借助业界唯一的开放式安全与合规性管理平台提供了针对恶意软件和数据丢失的增强保护层。迈克菲公司的安全套件为帮助您保护用户、系统和数据提供了坚实的基础，而且运营效率很高，安全状况易于维护。

McAfee Total Protection for Endpoint—Enterprise Edition 套件

这是我们的旗舰解决方案产品，可为您的所有终端提供可靠的保护，包括 Windows、Mac、Unix 和 Linux 系统及移动设备。该无缝集成解决方案可保护系统和数据免遭复杂恶意软件攻击，例如僵尸程序 (Bot) 和零日攻击。并且还能抵御由于设备丢失或失窃所导致的威胁，阻止不合规系统和未经授权的设备访问关键业务系统和敏感数据的企图。

此控制组合是大型复杂企业的理想之选，可以满足其用户期待的自由，并且能够全面防护由于移动性和灵活性导致的风险。多平台支持、网络访问控制、策略审计、Web 过滤和终端加密等功能可帮助您满足用户的需要，并且能够确保满足管理层和审计人员对数据保护和相关责任的要求。



McAfee Endpoint Protection—Advanced 套件

该高级保护套件通过集成前瞻性安全解决方案保护当今分散在世界各地的员工，抵御针对 Windows 系统的复杂恶意软件和零日威胁。基于策略的集中管理、访问控制和审计可有助于保护贵公司资产的安全与合规性。

McAfee Endpoint Protection 套件

与 McAfee ePO 软件集成的最基本的防护功能可帮助您保护 Windows 系统免遭复杂恶意软件和未经授权的设备攻击。结合使用防恶意软件、设备控制、基本电子邮件和 Web 保护，这是一种保护传统桌面机和固定系统的好方法，因为这些系统已经限制了面临的 Internet 威胁。

运营管理成本得到降低

McAfee ePolicy Orchestrator® (ePO™) 软件是一个单一集中式平台，可管理安全、加强保护和降低安全运营成本。由于该平台基于 Web，可以随时轻松访问，提供了自动化和可操作的智能安全管理，使用户能够快速有效的作出决定和实现更好的控制。它还可以确保您遵从系统安全策略（无论您身在何处），并帮助您防范当今复杂攻击所引发的高代价业务中断。

该开放式管理框架充分利用了单一代理和单一控制台设计的优势。与旧式的单点解决方案相比，这一优化的方法可大大简化各种防护措施和相关规则及策略的安装和维护过程。它消除了多个代理对系统的影响以及多个控制台造成的决策效率低下问题。当由于威胁和法规的变更而需要更新策略时，可以快速、准确、一致地完成这些操作。

通过使用 McAfee ePO 平台将您的终端、网络与风险和合规流程联动起来，您可以了解整个安全和合规环境的全面状况，以便您的 IT 员工能够充分利用来自整个公司所有单点的安全数据，而不是依赖来自多个资源的孤立数据。您可以关联来自终端、网络和数据安全及合规审计方面的威胁、攻击和事件，从而提高安全工作和法规遵从报告的关联性和效率。没有其他供应商能够声称自己拥有此种能够跨所有上述安全领域的单一集成管

理平台。McAfee ePolicy Orchestrator 简化了安全管理，可以降低超过 60% 的 IT 安全和合规管理成本（资料来源：MSI International 对 488 家大中型企业的调查）。并且可帮助您找到更多节省运营成本的方法，我们的开放式体系结构使您能够与迈克菲安全创新联盟 (SIA) 中九十多家合作伙伴的产品建立连接。

永久性完整磁盘加密

为敏感数据提供前所未有的保护，帮助企业避免信息丢失，维持业务连续性。它为笔记本电脑和移动设备提供了永久性完整磁盘加密，可预防敏感数据丢失，特别是在设备丢失或被盗后防止数据丢失。终端加密使企业能够随时有效地加密和解密设备，不会影响用户使用或系统性能。加密的永久性有助于确保执行安全策略并满足合规要求。

全面的设备管理

防止关键数据通过可移动介质（例如 U 盘、iPod 设备、蓝牙设备、可刻录 CD 和 DVD）从公司内部泄露出去。我们提供了可监控来自所有桌面机和笔记本电脑的数据传输的工具，即使有移动设备连接到企业网络，也无需担心用户和保密数据的安全。

	McAfee Total Protection for Endpoint—Enterprise Edition 套件	McAfee Endpoint Protection—Advanced 套件	McAfee Endpoint Protection 套件
单一管理控制台	●	●	●
实时防病毒和防间谍软件	●	●	●
McAfee SiteAdvisor Enterprise Plus	●	●	●
设备控制	●	●	●
电子邮件服务器防病毒和反垃圾邮件	●	●	●
桌面防火墙	●	●	
Host Intrusion Prevention (Host IPS)	●	●	
应用程序阻止	●	●	
网络访问控制	●	●	
桌面策略审计	●	●	
Web 过滤 — 主机	●	●	
终端加密	●		
多平台和移动设备支持	●		

迈克菲树立了行业标准

- 连续四年被 Gartner 评为“终端安全和移动数据保护”领域的领先企业
- 首次提供用于终端安全的单一代理和单一控制台
- 首次通过单一控制台提供广泛的安全产品管理，包括终端、网络、数据、Web 和电子邮件安全等方面
- 囊括终端安全和法规遵从管理的第一款产品
- 用于管理迈克菲和第三方安全产品的第一款产品
- 首次在单一引擎中结合了策略审计和策略实施
- 首次在一个真正的集成式套件中结合了终端安全和数据保护

零日防护和漏洞防护

告别紧急安装修补程序的紧张状态。主机入侵防护通过巡视来保护终端免遭恶意软件的攻击，提供自动特征码更新，在按照计划实施和测试修补程序时保护桌面机和服务器免遭攻击。将其与迈克菲获得专利的行为保护技术（可防范缓冲区溢出攻击）相结合，您将获得市场上最先进的系统漏洞防护产品。McAfee Host IPS 已经针对几乎所有 (90%) 关键 Microsoft 漏洞提供了零日防护。

有效的策略法规遵从

McAfee ePO 软件提供了用于管理终端安全和合规审计的单一平台，实现了新的效率级别。企业可衡量其做法是否符合最佳做法策略 — ISO 27001 和 CoBIT — 和主要行业法规，包括支付卡行业数据安全标准 (PCI DSS)、格雷姆 - 里奇 - 比利雷法案 (GLBA)、1996 年美国健康保险可携性与责任性法案 (HIPAA)、2002 年萨班斯 - 奥克斯利法案 (SOX) 及其国际版本。策略审计功能已通过安全内容自动化协议 (SCAP) 的验证，使美国联邦机构能够轻松实现与联邦桌面机核心配置 (FDCC) 标准的遵从性。

高级电子邮件病毒和垃圾邮件防护

迈克菲的解决方案可以扫描进站和出站电子邮件，以确定其中是否含有垃圾邮件、不当内容和有害病毒。可疑的电子邮件将被隔离，以防止不断变化的电子邮件威胁影响您的网络 and 用户。防病毒层可保护电子邮件服务器，并在恶意软件到达用户收件箱前对其进行拦截。

前瞻性 Web 安全措施

许多 Web 威胁采用静默方式并且用户在浏览 Web 时无法发现。通过在用户访问恶意网站之前对他们发出警告，帮助确保合规性和降低 Web 浏览风险。您可以授权或阻止网络访问，控制用户在企业网络或外部网络上的 Web 浏览。精细化控制包括根据用户和组的内容过滤和网络访问监控，并且提供了全面的管理和报告功能。

灵活的网络访问控制

可以控制对企业网络的访问，实施终端安全政策以及与现有网络基础设施相集成。不管终端如何连接到网络，网络访问控制均会发现和评估终端合规状态，定义适当的网络访问策略以及提供自动修正功能。

对虚拟环境的保护

虚拟机承受着与物理系统相同或更大的安全压力，因此，应对其实施全面的保护。McAfee Endpoint Security 套件支持虚拟环境部署，以确保这些资产免受恶意软件或其他安全风险的侵扰。有关专门为虚拟环境构建迈克菲解决方案的详细信息，请访问 http://www.mcafee.com/cn/enterprise/solutions/system_protection/secure_virtualization.html。

McAfee Artemis Technology — 全天候实时恶意软件防护

随着高级持久性威胁的空前发展，企业已不能再依赖于仅使用特征码分析的解决方案来提供终端保护。从发现威胁到将其特征码应用到终端，中间总会有 24 到 72 小时的空窗期。在此期间，您的数据和系统将暴露于危险之中。McAfee Artemis Technology 可基于 McAfee Labs™ 收集的全球威胁情报提供不间断的实时保护，从而消除了这段空窗期。Artemis Technology 即使在威胁特征代码开发完成之前，也能随时随地隔离并阻止威胁。

McAfee Labs 提供的保护

McAfee Labs 借助全球研究团队，可提供市场上最全面的全球威胁情报。依靠 400 多项专利的组合、遍布 Internet 的数百万传感器和涵盖所有重要威胁途径的可见性，McAfee Labs 提供了无与伦比的保护功能，通过完整的组合方案抵御已知威胁和不断涌现的新威胁。

经实践验证的强大技术

迈克菲为全球约 1.2 亿终端提供保护，包括全球最大的企业和政府网络。迈克菲在总体威胁检测

率方面连续获得 AV-Comparatives 提供的最高检测级别，击败了 Symantec、Kaspersky、Sophos、Microsoft 和其他主要竞争对手。（资料来源：<http://www.av-comparatives.org/>）

迈克菲解决方案服务

迈克菲与其 McAfee SecurityAlliance™ 合作伙伴携手为您提供全面的服务，帮助您评估、规划、部署、调整和管理安全解决方案。要了解更多信息，请访问 http://www.mcafee.com/cn/enterprise/services/product_consulting/。

迈克菲技术支持

借助由迈克菲技术支持提供的灵活程序，确保在安装过程中和安装完成后，一切运行正常。迈克菲技术娴熟并经过认证的安全专家们拥有丰富的知识和资源，能够帮助您顺利启动并运行安全产品。有关更多信息，请访问 mysupport.mcafee.com。

了解更多

请访问 http://www.mcafee.com/cn/enterprise/products/system_security/index.html，或致电 800-810-0369（周一至周五上午 9 点至下午 6 点）。

迈克菲（上海）软件有限公司

北京朝阳门外大街 16 号中国人寿大厦 1709 室
上海市卢湾区湖滨路 222 号 1 号楼企业天地 1101 室
广州市天河区体育东路 118 号财富广场西塔 15 楼 106 室
销售热线：800-810-0369 www.mcafee.com/cn

邮编：100020

邮编：200021

邮编：510620

电话：(8610) 85722000 传真：(8610) 85752299

电话：(8621) 23080699 传真：(8621) 63406606

电话：(8620) 38860668 传真：(8620) 38860638

