McAfee Endpoint Security 套件

增强的安全、更低的运营成本、简化的合规流程

为您的企业提供一个可靠的安全环境绝非易事。复杂的恶意软件以及变化多端的移动工作环境使网络犯罪分子能够轻松窃取敏感数据。相关法规的陆续出台也要求您必须增强数据保护并验证合规性。然而，不断增加的单点安全产品则增加了管理成本和响应复杂性。McAfee® Endpoint Security 套件将行业领先的终端安全和数据保护与集中式管理相结合，实现了可靠的安全保护，同时显著简化了运营与合规。

主要优势

- 为所有终端提供统一保护
- 通过集中管理降低运营成本
- 通过标准模板简化合规和审计

“NSS Labs 创造了极光行动 (Operation Aurora) 攻击的各种变体，并测试了七款恶意软件防护产品，以了解其中哪些产品能够有效拦截攻击和恶意代码负载。基于攻击的可视性水平以及发现攻击到开始测试的时间，原以为多数产品（即便不是全部）都能应对该漏洞。然而，这七款产品中仅有一款正确拦截了多个攻击和负载，展现了基于漏洞的防护优势 [迈克菲]。”

— NSS Labs 发现多数终端安全产品缺乏“基于漏洞的防护”

简单地部署防病毒扫描程序即可解决问题的日子已经一去不复返了。如今，蠕虫、木马、僵尸、rootkit、黑客以及身份信息窃取等威胁持续性强且不断变化。用户想随时随地访问应用程序来进行工作，但是他们的移动设备和笔记本电脑（包括 Mac）则可能会危害到您的网络和系统。由于保护数据以及验证并报告合规性的要求极为严格，因此风险比过去高得多。同时，企业的预算也越来越紧张。

您可以拼凑一组单点产品来提供保护，但是其效率和效果绝对无法与 McAfee Endpoint Security 套件相媲美。原因在于我们将各种技术整合在一起，为您提供协调、全面的解决方案来帮助您防范当今的各类威胁。我们的终端安全套件能够针对全部五种威胁媒介提供有效防护 — 系统、电子邮件、Web、数据和网络。

这种集成安全套件可以提供统一保护，而且易于部署和管理。借助业界唯一的开放式安全和合规管理平台，这些套件将各层保护整合在一起，帮助您有效防范恶意软件和数据丢失。我们的套件不仅可帮您为用户、系统和数据的保护奠定坚实基础，而其高效的运营效率也可确保安全的有效实施和维护。

McAfee Total Protection™ for Endpoint—Enterprise Edition Suite

我们的旗舰解决方案可为您的终端提供强大保护，包括 Microsoft Windows、Mac、Unix 和 Linux 系统以及移动设备。无缝集成可防止系统和数据遭受复杂恶意软件的攻击，例如，僵尸 (bot) 和零日 (zero-day) 攻击。如果您的设备丢失或被盗，它会为您提供保护并阻止可能尝试访问您关键业务系统和敏感数据的不合规系统或未经授权的设备。

对于有注重自由的用户的大型企业而言，这种控制整合是理想模式 — 能够有效防范因移动性和灵活性所导致的风险。多平台支持、网络准入控制、策略审计、Web 过滤和终端加密有助于您满足用户的需求，同时确保达到管理层和审计人员的数据保护和责任要求。

McAfee Endpoint Protection— Advanced Suite

鉴于目前日益增多的移动工作人员，我们的解决方案可为其提供集成的前瞻性安全保护，以有效防范针对 Windows 系统的复杂恶意软件和零日威胁。基于策略的集中管理、准入控制、设备控制以及审计可确保资产安全、合规。

McAfee Endpoint Protection Suite

我们将最基本的保护功能与 McAfee ePO 软件进行整合，可确保您的 Windows 系统能够有效防范复杂的恶意软件和未经授权的设备。凭借恶意软件防护、设备控制以及电子邮件和 Web 保护，可为面临 Internet 威胁的传统桌面和固定系统提供出色保护。

能够降低运营成本的管理

McAfee ePolicy Orchestrator® (McAfee ePO™) 软件是一个单一的集中平台，能够管理安全、强化保护并降低安全运营成本。它基于 Web，便于您随时随地轻松访问，可提供自动化智能安全保护，有助于您快速做出高效决策，实施更强控制。此外，它还可以保证对系统安全策略的遵从（无论处于什么位置），有助于抵御当今的复杂攻击，从而避免代价高昂的业务中断。

这一开放式管理框架充分发挥了单一代理和单一控制台的优势。与单点解决方案相比，我们的方法能够显著简化防护功能以及相关规则与策略的安装与维护。有效消除了多代理的影响，以及多控制台的低效性。因威胁和法规变更需要修改策略时，可快速、准确、一致地进行更新。

通过使用 McAfee ePO 平台来统一您的终端、网络、风险和合规流程，您可以全面掌握整个安全与合规环境，以便您的 IT 人员能够充分利用来自公司各处的安全数据，而不是依赖于来自多个源的孤立数据。您能够将来自终端、网络的威胁、攻击和事件与数据安全以及合规审计相关联，以提高安全工作与合规报告的相关性和有效性。

McAfee ePO 软件能够简化安全管理并使 IT 安全管理与合规管理成本降低 60% 以上（来源：MSI International 针对 488 家大中型企业进行的调查）。此外，为了帮助您节省更多成本，我们的开放式架构可让您使用 100 多家迈克菲安全创新联盟 (Security Innovation Alliance) 合作伙伴的产品。

一致而完整的磁盘加密

为敏感数据提供前所未有的保护有助于企业防止信息丢失并维护业务持续性。适用于笔记本电脑和移动设备的一致性全盘加密可以有效避免敏感数据的丢失，尤其是由于设备丢失或遭窃导致的数据丢失。终端加密可让企业随时对设备进行高效加密和解密，而不会影响用户使用或系统性能。其一致性有助于确保您实施安全策略并实现合规。

全面的设备管理

防止通过可移动介质（例如，U 盘、iPod、蓝牙设备、可刻录 CD 和 DVD）将重要数据带出公司。我们为您提供工具以监控数据传输 — 从桌面机到笔记本电脑，无论用户和机密数据身处何处（甚至在没有与企业网络连接的情况下），都能获得全面的保护。

	McAfee Total Protection for Endpoint—Enterprise Edition	McAfee Endpoint Protection—Advanced Suite	McAfee Endpoint Protection Suite
单一管理控制台	●	●	●
实时防病毒和反间谍软件	●	●	●
Web 安全（主机）	●	●	●
设备控制	●	●	●
电子邮件服务器防病毒和垃圾邮件防护	●	●	●
桌面机防火墙	●	●	●
主机入侵防护	●	●	
应用程序拦截	●	●	
网络访问控制	●	●	
桌面机策略审计	●	●	
Web 过滤（主机）	●	●	
终端加密	●		
多平台和移动设备支持	●		

迈克菲的领先之举

- 自 2006 年以来连续被 Gartner 评为终端安全与移动数据保护领域的领导者
- 率先提供单一代理和单一控制台来管理终端安全
- 率先采用一个控制台管理各种安全产品，包括终端、数据、Web 和电子邮件安全
- 首款采用统一管理平台管理终端安全与合规的产品
- 首款可同时管理迈克菲及第三方安全产品的产品；超过 100 家安全创新联盟合作伙伴
- 率先在单一引擎中整合策略审计与策略实施
- 率先在真正的“集成”套件中整合终端安全与数据保护

零日攻击和漏洞防护

告别紧急补丁安装。主机入侵防护可以“巡视”您的终端以防范恶意软件，并提供自动更新的签名，以便在您按计划实施和测试补丁程序时防止桌面机和服务器遭受攻击。由于结合了迈克菲获得专利的行为防护技术（可以阻止缓冲区溢出攻击），此款产品拥有当今市场上最先进的系统漏洞防护。McAfee Host Intrusion Prevention 提供了针对大多数（超过 90%）Microsoft 严重漏洞的零日防护。

迈克菲全球威胁智能感知系统（McAfee Global Threat Intelligence™）

迈克菲 GTI 是一个基于云的威胁智能感知系统，它借助遍及 120 个国家/地区的 1 亿多个传感器来持续扫描以查找新出现的威胁。然后将防护信息传递给全球部署的迈克菲终端和网络产品。基于云的迈克菲 GTI 会将传入数据流与已知或可疑的威胁进行对比，将有关各接触点发生情况的独特智能信息返回给所支持的产品。与其他基于云的威胁智能感知系统不同，迈克菲的系统使用了诸如文件、Web、邮件、网络连接信誉和 Web 类别等智能感知技术。

不间断的实时恶意软件防护

随着高级持续性威胁前所未有的增长，企业无法仅依靠使用签名分析的解决方案来实施终端保护。对于其他的安全产品供应商，从识别威胁到将其签名应用到终端存在 72 小时以上的防护间隙。在此期间，您的数据和系统存在遭受威胁攻击的风险。McAfee VirusScan® Enterprise 能够有效缩短这一防护间隙，基于迈克菲 GTI 技术采集的全球威胁信息，可提供实时的、不间断的安全保护。它可以随时随地隔离或拦截威胁，即使签名尚未开发出来，依然能够实施有效防护。

高效的策略遵从

McAfee ePO 软件可通过一个平台管理终端安全与合规审计，极大地提高了效率。企业可以衡量对最佳实践标准（ISO 27001 和 CoBIT）以及相关行业法规（包括 CI DSS、GLBA、HIPAA 和 SOX 等）的遵从情况。策略审计功能通过了 SCAP 验证，该协议旨在使美国联邦机构能够轻松遵循 FDCC 标准。

高级电子邮件病毒和垃圾邮件防护

我们的解决方案可以对企业进出的电子邮件进行扫描，以隔离垃圾邮件、不当内容和有害病毒。一旦发现可疑电子邮件，会对其进行隔离，从而防止不断演变的电子邮件威胁干扰您的网络和用户。防病毒层能够为您的电子邮件服务器提供保护，并在恶意软件进入用户邮箱前进行有效拦截。

前瞻性 Web 安全

很多 Web 威胁对上网者来说是静默且不可见的。通过在用户访问恶意网站前及时向其发出警告，有助于确保合规，降低上网风险。您可以授权和阻止网站访问，对用户使用企业网络的行为加以控制，无论他们是联机还是脱机。细化控制包括通过全面的管理和报告功能进行内容过滤并按用户和组执行网站访问。

灵活的网络准入控制

控制对企业网络的访问、实施终端安全策略，以及将终端控制与现有网络基础设施相集成。无论终端与网络连接方式如何，网络准入控制都能够监控并评估终端合规状态，定义适当的网络准入策略，并提供自动补救功能。

虚拟环境保护

虚拟机面临着与物理环境相同甚至更大的安全压力，因此，应当为虚拟机提供全面保护。McAfee Endpoint Security 套件支持虚拟化环境部署，从而可确保这些资产免遭恶意软件或其他安全风险的威胁。要了解有关迈克菲专为虚拟环境设计的解决方案的详细信息，请访问 http://www.mcafee.com/cn/solutions/virtualization/virtualization.aspx。

成熟且强大的技术

迈克菲为全球近 1.2 亿个终端提供保护，其中包括全球最大的企业和政府网络。迈克菲在 AV-Comparatives 的检测率测评中保持领先，在总检测率（百分比）方面胜过赛门铁克、卡巴斯基、Sophos、微软以及各主要竞争对手。AV-Test 测评显示，除检测率出色外，迈克菲还提供具备最高性能的商用恶意软件防护解决方案。（信息来源：www.av-comparatives.org 和 www.av-test.org）

迈克菲解决方案服务

我们与迈克菲安全同盟的合作伙伴一起，共同为您提供多种服务帮助您评估、规划、部署、调整和管理您的安全。有关详细信息，请访问 www.mcafee.com/cn/ services/sol ution-services/index.aspx。

迈克菲技术支持

借助由迈克菲技术支持提供的灵活计划，可确保在安装期间和之后，一切运行正常。我们技术娴熟且经过认证的安全专家拥有丰富的知识和资源，可保证您的安全产品持续稳健运行。要了解更多信息，请访问 mysupport.mcafee.com

了解更多信息

可访问 www.mcafee.com/endpoint，或随时拨打 800–810–0369（周一至周五 9am–6pm）与我们联系。

McAfee
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

28902ds_tops-e_security-suite_0511_fnl_ASD