McAfee Complete Endpoint Protection — Enterprise

针对整个威胁生命周期提供智能、关联的防御

终端安全产品应当为您的业务提供支持，而不是影响业务的发展。捍卫企业安全并使员工保持较高的工作效率。McAfee® Complete Endpoint Protection — Enterprise 套件具有强大、简单、快捷的特点，既能够提供实时的安全和风险监控，也能够提供统一的管理。此套件能够利用本地和全局威胁情报提供高级威胁防护，并且能够利用应用程序控制、遏制和行为入侵防御，保护您的系统和数据免受复杂、隐蔽的威胁侵扰 - 所有这些都是以一套易于管理的集成式解决方案的形式来实现。

主要优势

- 通过跟踪和遏制“Patient Zero”（第一感染源）威胁并击败沙盒感知恶意软件，为您提供完善的防御机制，并且无需降低安全性和中断业务。
- 通过智能的协作性终端防御、入侵防御以及适用于桌面机和笔记本电脑的防火墙、设备控制等等，获得顶级、全面的分层保护。
- 统一管理所有终端：PC、Mac、Linux 系统和虚拟机。
- 通过动态白名单缩小应用程序攻击面，节省时间和精力。
- 用易于理解的语言提供可操作的威胁取证，从而更好地了解高级威胁，并迅速采取行动。
- 通过集中精力解决最迫切的安全问题来控制风险。

McAfee Complete Endpoint Protection — Enterprise 套件拥有诸多优势，从即开即用的安装方式到快速的响应速度，都能够确保用户轻松地获得安全保护。通过一套统一的解决方案，您可以将企业中的所有设备覆盖进来 - PC、Mac、Linux 系统、虚拟机等等。此套件既能够降低管理工作的复杂度并缩减成本，同时能够保护终端免受 Rootkit、针对性 Web 和电子邮件攻击以及持久性威胁的侵扰。此套件提供强大、高效的保护和管理，如此强大、高效的保护和管理只有终端安全市场领军企业 Intel Security 才能够实现。

高级威胁防护

至于威胁防护方面，恐怕没有哪款产品比 McAfee Complete Endpoint Protection — Enterprise 做得更加出色。我们的动态应用程序遏制可保护系统免遭最新的灰色软件、勒索软件、“Patient-Zero”（第一个传染源）和其他高级威胁的入侵 — 在它们访问您的系统之前。它会检查可疑威胁的行为，而无需降低您的系统的安全性。您甚至可以创建自己的自定义访问控制规则。此外，由于这是一个轻型程序，无需连接到云，所以不管您的用户是否连接到了网络，您都可以为其提供保护。

Intel Security 能够借助多层保护来防御、检测并快速修复恶意软件，多层保护包括智能的协作型终端防御、入侵防御、适用于桌面机和笔记本电脑的防火墙、设备控制等等。通过应用程序控制实现的智能白名单功能能够保护用户免受有害应用程序的威胁，并且免受来源于零日威胁或高级持久性威胁 (APT) 的代码侵扰。

基于云的 McAfee Global Threat Intelligence (GTI) 能够全方位地实时监控所有载体（文件、Web 和网络）上的新涌现的威胁，让您可以看到更多、了解更多、更好地防护您的组织。您可以利用来自于 McAfee GTI 的本地威胁情报来增强您的全局情报，从而在威胁出现时能够及时应对。Intel Security 在全球 120 多个国家/地区拥有 1 亿多台全球威胁传感器，每天处理 450 多亿次查询，每天分析 150 多万个文件和 100 万条 URL，能够提供目前市场上最强大的全局威胁情报。

快速的智能扫描

通过集中扫描和集中行动提供安全防护，保障您的业务实现全天候流畅运转并尽量缩短停机时间。在所有平台上的卓越性能得益于高级智能扫描和内存管理技术，能够优化 CPU 和内存使用。借助

intel Security

McAfee Application Control 及其无特征码更新，您可以体验到超低的 CPU 和内存使用率，同时可以避免过度扫描和 .DAT 更新周期。

McAfee Application Control 使用动态信任模型，无需耗工耗时的名单管理工作，即可动态地补充白名单。

Intel Security：行业领袖

- 连续 13 年获得终端保护平台 Magic Quadrant 领导者荣誉。(Gartner)[1]

简单部署，集中管理

只需四次单击和 20 分钟的时间，您的安全产品即可整装待发。通过 McAfee® ePolicy Orchestrator® (McAfee ePO™) 软件实施实时统一管理，简化所有设备的策略管理工作流程，并通过单一界面实施监控。

查看、管理和响应威胁防御生命周期

McAfee Complete Endpoint Protection — Enterprise 汇集了一系列强大的前瞻性防御措施，从而在各个阶段对您实施保护，帮助您抵御当今的各种复杂威胁。

我们的高级威胁防御如何运作

技术	功能	执行机制
McAfee Endpoint Security 10	能够在多个威胁防御之间建立通信，以便检测到看似互不关联、实则作为针对性攻击组成部分的事件。	• 动态应用程序遏制可在勒索软件、灰色软件、“Patient-Zero”（第一感染源）威胁等获得系统访问权限之前将其阻止。 • 威胁防御之间会相互交流并且告知对方有哪些新出现的威胁。 • 自适应智能扫描会利用来自于多个来源的观察结果，检测并实时地相互告知新出现的攻击形式。 • 防御会通过本地和全局威胁情报获取信息。 • 套件会针对可疑的应用程序和流程采取自动行动并快速升级，同时通知其他防御和全球社区。
McAfee Threat Intelligence Exchange	能够提供从全球数据来源和第三方获取的全面的威胁情报，同时能够从实时事件和历史事件中获取本地威胁情报。	• 安全组件能够通过终端、网关和其他安全组件，在全局网络中发现针对组织发起的攻击，并针对此类攻击获取额外的深入分析。 • 从恶意软件中收集的威胁详细信息能够在数毫秒的时间内在数据交流层进行传播，从而覆盖到所有的终端并为终端提供信息，帮助它们主动地防御威胁。 • 能够提供自定义威胁情报，根据组织偏好列出发行者证书、文件哈希值和风险容忍度决定。
McAfee Active Response	能够凭借详细的实时、交互式持续调查分析，增强事件响应能力。	• 能够自动捕捉并监控可能属于攻击指标 (IoA) 的上下文和系统状态变化，以及处于休眠状态的攻击组件，并且会将情报发送给分析、运营和法律团队。 • 允许根据攻击方式、自动数据收集、警报和对兴趣目标的响应等方面的变化进行调整，并且提供自定义工作流。 • 持续不断的收集器能够触发对攻击事件的侦测，同时能够为管理员和系统发出攻击活动警报。
McAfee Application Control	能够在公司桌面机和固定功能设备上阻止未经授权的可执行文件。	• 采用动态信任模型及创新安全功能遏制高级持久性威胁，同时无需进行特征码更新和极为耗工耗时的名单管理。 • 与 McAfee Global Threat Intelligence 相集成，这样用户就可以始终启用“已知合法”的应用程序和代码，拦截“已知恶意”和“未知恶意”的应用程序和代码。 • 如果与 McAfee Threat Intelligence Exchange 一起部署，就能够用本地威胁情报增强白名单功能，即时抵御未知的和针对性恶意软件。McAfee Threat Intelligence Exchange 与 McAfee Advanced Threat Defense 相互协作，能够动态地在沙盘中分析未知应用程序的行动，并且自动保护所有终端免受新检测到的恶意软件的攻击。

注意：McAfee Threat Intelligence Exchange、McAfee Active Response 和 McAfee Advanced Threat Defense 是为 McAfee Endpoint Protection 客户提供的选购型号，可单独销售。

Intel Security 集成架构

McAfee Complete Endpoint Protection — Enterprise 套件能够帮助您优化安全和风险状态，同时帮助您降低成本、提高灵活性。采用集成式安全架构 - 以及协作式、可扩展的终端架构 - 您可以去繁求简，从而简化管理并提高事件响应效率。您还可以实现集中化管理、降低安全成本，并且构建一种适用于现在和未来的框架。您可以实现安全保护和事件管理流程的简单化和自动化，从而降低安全成本、提高效率。凭借实时安全管理和无与伦比的全球威胁情报，Intel Security 能够帮助您针对企业遇到的风险，敏捷地进行识别、优先级排序并予以解决。有关详细信息，请访问：**www.mcafee.com/cn/products/complete-endpoint-protection-enterprise.aspx**。

McAfee Complete Endpoint Protection — Enterprise 套件亮点

防恶意软件（PC、Mac、Linux、虚拟机）

McAfee Endpoint Security

- 能够实时地与多种终端防御技术进行通信，从而分析并携手对抗新的高级威胁：在此类威胁对您的系统或用户造成影响之前予以拦截并快速中断。
- 业界领先的企业级防恶意软件保护和集成的零日威胁防护。
- 准备获取集成式高级威胁防御工具，如 McAfee Active Response。

动态应用程序遏制

- 安全检查行为并遏制如灰色软件、勒索软件、Patient-Zero（第一感染源）威胁等，无需连接到云。

应用程序控制

- 阻止安装和执行有害应用程序和恶意软件，并尽量减少对系统性能、用户和管理员的影响。

入侵防御以及适用于桌面机和笔记本电脑的防火墙

- 抵御未知零日威胁和新漏洞。
- 缓解修补紧迫性。
- 创建自定义控件来阻止对内存的利用和攻击，以及尝试以更高权限运行的威胁。

Global Threat Intelligence

- 通过遍布世界各地的数百万传感器收集实时情报，抵御各种威胁媒介中新涌现出的威胁。
- 我们在 120 多个国家/地区拥有 1 亿多台全球威胁传感器，让我们能够看到更多、保护更多、提供目前市场上最强大的全球威胁情报。

Web 和邮件传输安全

带有 URL 筛选和安全搜索功能的 Web 控制

- 在用户访问恶意网站之前发出警告，以降低风险并保持合规性。
- 通过授权或拦截网站访问来强制执行 Web 流程策略。

电子邮件防恶意软件和反垃圾邮件

- 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。
- 通过 McAfee GroupShield 检测、清除恶意软件，阻止其进入 Microsoft Exchange 和 Lotus Domino 服务器。

数据保护

设备控制

- 通过限制使用可移动介质防止敏感数据丢失。

管理

McAfee ePO 软件

- 从一个单一的集中式控制台管理策略、合规性和报告。
- 利用跨平台策略简化混合式操作系统环境中的管理。

1. 首份报告发布于 2002 年。之前的标题包括“企业防病毒 Magic Quadrant”。

McAfee. Part of Intel Security.

北京市东城区北三环东路 36 号环球贸易中心 D 座 18 层	邮编：100022	电话：(8610) 85722000	传真：(8610) 85752299
上海市延安西路 2299 号上海世贸商城 22 层	邮编：200336	电话：(8621) 23080699	传真：(8621) 63406606
深圳市南山区高新南九道 9 号威新软件园 3 号楼 3 楼	邮编：518057	电话：(86755) 82825003	传真：(86755) 82825001

销售热线：400 610 0369 或 800 810 0369 www.intelsecurity.com www.mcafee.com/cn