McAfee Web Gateway

安全、情报互联。高效。

与以前相比，如今各企业可通过 Web 完成更多的工作。如今的 Web 可提供动态、实时的用户体验。但是，Web 也变得更加危险，每天发布的复杂攻击数量不断增加。McAfee® Web Gateway 是企业防范新兴恶意软件威胁的一道关键防线。它能够让企业加强互联网访问安全性，同时将功能强大的本地意图分析与 McAfee Labs 支持的基于云的保护结合在一起，从而使用这种高级安全方法极大降低风险。

随着互联网的普及和技术复杂性的提高，市场对先进 Web 安全的需求越来越强烈。虽然看起来所谓“安全”的网站也可能成为恶意软件攻击的对象。如今，仅靠阻止已知病毒或限制对“已知不良”网站的访问是不够的。反应式技术（例如基于特征码的防病毒和仅根据类别的 URL 过滤）虽然也很有必要，但是并不足以保护对云应用程序的访问，也无法防范最新漏洞。

因为这些解决方案主要针对已知内容和恶意对象或可执行程序，所以它们无法防范当今看似值得信任的 HTTP 或 HTTPS 流量内隐藏有恶意代码的攻击，也无法抵御未知或新出现的威胁。支持对云应用程序进行安全、精细的访问控制，同时主动阻止未知及已知威胁的能力至关重要。

全面的入站和出站防护

McAfee Web Gateway 通过一个高性能设备软件建构对 Web 流量的各个方面提供全面的安全保护。对于用户发出的 Web 请求，McAfee Web Gateway 首先会实施企业的 Internet 使用策略。然后针对所有允许的通讯使用本地和全局技术，分析经由请求的网页进入网络的所有内容和活动代码的性质和意图，即时防范恶意软件和其他隐藏的威胁。与基本的数据包检查技术不同，McAfee Web Gateway 可以检查安全套接字层 (SSL) 流量来深入防范通过加密隐藏的恶意代码或控制应用程序。

入站保护还可以为允许从外部来源上载数据或文档的企业托管网站降低相关风险。在反向代理模式下，McAfee Web Gateway 对所有内容进行扫描之后再上传，确保服务器和内容安全。

McAfee Web Gateway

- 在多种硬件型号中可用，且可作为支持 VMware 和 Microsoft Hyper-V 的虚拟机。
- 与互补的 McAfee 解决方案集成，包括 McAfee Endpoint Security、McAfee Advanced Threat Defense 和 McAfee Threat Intelligence Exchange。
- 经 Common Criteria EAL2+ 及 FIPS 140-2 Level 2 认证。
- 支持多种加密密钥存储选项，包括 Gemalto SafeNet 硬件安全模块 (HSM)、Thales nShield HSM 和 Thales PCIe 卡。
- 安全 Web 网关中排名第一的反恶意软件 (AV-TEST)。

联系我们

为了保护出站流量的安全，McAfee Web Gateway 使用行业领先的 McAfee 数据丢失防护技术来扫描所有主要 Web 协议（包括 HTTP、HTTPS 和 FTP）中用户生成的内容。它还可以防范通过社交网络站点、博客、Wiki 或在线工作工具（例如基于 Web 的邮箱、企业程序和日历）丢失企业机密和敏感信息，或泄露受管制的信息。此外，McAfee Web Gateway 还可阻止“感染僵尸”的计算机将敏感数据传回原址或进行传播的企图，从而防止未经授权的数据外泄。

McAfee Web Gateway 提供行业内的最佳保护

作为业内评价最高的[1]恶意软件防护 Web 安全解决方案，McAfee Web Gateway 结合 McAfee Gateway Anti-Malware Engine 采用获得专利的无特征码意图分析方法。前瞻性意图分析功能会实时从 Web 流量中过滤出以前未知的或零日攻击恶意内容。通过扫描网页的活动内容，模拟和理解其行为以及预测其意图，McAfee Web Gateway 可防止零日恶意软件感染终端，从而显著降低与系统清理和补救相关的成本。

我们将这种分析技术与 McAfee 防病毒和 McAfee Labs 的全球信誉技术相结合，可快速阻止已知的恶意软件和恶意网站。McAfee Web Gateway 通过采用多项技术提供更佳的保护，同时部署多项不同辅助技术在单一平台上优化安全防护，许多企业都需要在其分层防护安全方法中使用这些技术。

- **McAfee 防病毒与实时的 McAfee Global Threat Intelligence（McAfee GTI）文件信誉相结合：**基于云的 McAfee GTI 文件信誉查找填补了从发现病毒到系统更新/保护这段时间的间隙。
- **McAfee GTI Web 信誉和 Web 分类** McAfee Web Gateway 通过综合采用基于信誉和分类的过滤技术的强大优势提供 Web 过滤功能和保护。McAfee GTI 基于通过 McAfee Labs 的大规模全球数据收集功能收集到的数百种不同的属性，创建所有 Internet 实体（网站、电子邮件和 IP 地址）的概要信息。它基于所造成的安全风险指定信誉分数，管理员藉此可对要允许或拒绝的内容应用非常精细的规则。
- **定位：**McAfee Web Gateway 具有定位功能，从而实现基于 Web 流量和用户来源国家/地区的地理可见性和策略管理。

对于 Web 分类和 Web 信誉，各企业可以在内部查找和云查找之间进行选择，或将两者组合使用。云查找消除了发现/更改和系统更新之间的防护缺口，并利用成千上万个独特恶意软件样本的数据提供广泛的覆盖面。

高级威胁分析集成

McAfee Web Gateway 与 McAfee Advanced Threat Defense 集成 — 我们的高级恶意软件检测技术将可定制的沙盒与深层静态码分析相结合。McAfee Advanced Threat Defense 与 McAfee Web Gateway 中 Gateway Anti-Malware Engine 的内嵌扫描功能可提供无比强大的防御解决方案来应对互联网催生的威胁。对于希望降低成本、简化高级威胁分析选项的组织，可以集成 McAfee Cloud Threat Detection，这是一种基于云的沙箱，包含多种额外的威胁分析层。

威胁情报共享

当今，许多安全工具孤立存在的，尽管重要的情报位于终端、网络、安全信息和事件管理 (SIEM) 解决方案、网关等等之中，但这些安全工具无法相互共享威胁情报。如果能够共享，利用这些情报可以改善威胁防御、现有漏洞检测，并有效地修复被入侵的系统，从而提升事件响应能力。通过 McAfee Threat Intelligence Exchange，McAfee 解决方案 (包括 McAfee Web Gateway) 可相互共享威胁情报，从而弥补这些差距。在此过程中，McAfee Web Gateway 可产生巨大的价值。它通过创建并共享 McAfee Gateway Anti-Malware Engine 发现的零日恶意软件的新文件信誉，可在发布新的 DAT 之前，为终端等设备提供保护。此外，McAfee Web Gateway 利用 McAfee Threat Intelligence Exchange 提供的丰富威胁情报，可以阻止更多的威胁。

对加密流量的洞察和保护

老练狡猾的网络犯罪分子已转向 SSL 通讯 (HTTPS 和 HTTP/2)，将其作为后门，穿越企业的安全屏障。具有讽刺意义的是，这是一个为了提供更高的安全性而设计的协议，其风险也一定经过了评估。McAfee Web Gateway 将恶意软件检测、SSL 检验和认证验证集成到一起，形成了针对加密流量检验的全面方法。

不需要在 SSL 扫描硬件方面额外投资，McAfee Web Gateway 可在单一硬件或虚拟设施架构中执行所有这些操作。McAfee Web Gateway 会直接扫描所有 SSL 流量，以确保加密事务获得完整的安全性、完整性和私密性。

如果组织希望积极地深入检验其 SSL 流量，则可以通过 McAfee Web Gateway 中的安全套接字层 (SSL) 分路器，通过策略卸载整个未加密流量或单独流。这种由软件支持的功能可以将完整或部分解密的 SSL 流量镜像发送到其他安全解决方案，比如入侵预防系统 (IPS) 或基于网络的数据丢失预防 (DLP) 解决方案。

数据丢失防护

McAfee Web Gateway 通过扫描所有主要 Web 协议 (包括 SSL) 的出站内容，保护企业免受出站威胁 (如机密信息泄露) 的侵扰。这使该产品成为预防知识产权丢失的强大工具，能够确保并记录法规合规性，并在发生违规行为时提供取证数据。利用 McAfee Data Loss Prevention (McAfee DLP) 解决方案提供的强大功能，McAfee Web Gateway 还支持内置的预定义 DLP 字典，并可通过关键字匹配和/或正则表达式创建自定义字典。

对于利用基于的存储服务的组织，内置的文件加密可以保护上传至文件共享/协作站点的数据，抵御未经授权的访问。用户不通过 McAfee Web Gateway 将无法检索和查看数据。

针对离网用户的保护

随着员工变得越来越分散、使用移动设备办公的情况越来越多，需要将 Web 过滤和保护功能从办公室无缝过渡到旅途中，这一点越来越重要。McAfee Client Proxy 作为防篡改客户端代理，可以使漫游用户无缝执行身份验证，并重定向至非军事区 (DMZ) 中的内置 McAfee Web Gateway 或 McAfee Web Gateway Cloud Service。这样即可对漫游用户或远程用户实施Internet访问策略并应用全面安全扫描，即使这些用户是通过公共门户（如咖啡厅、酒店或其他 Wi-Fi 热点）访问 Internet 也是一样。

利用 McAfee Web Gateway，企业还可以将 Web 流量定向到 McAfee Web Gateway，从而在移动设备上扩展和实施安全策略。借助我们与移动设备管理提供商 AirWatch 和 MobileIron 的合作关系，McAfee Web Gateway 可确保 Apple iOS 和 Google Android 移动设备受到高级反恶意软件防护和公司 Web 过滤策略的保护。

利用 McAfee Web Gateway 获得绝佳的灵活性

McAfee Web Gateway 具有强大的基于策略的引擎，可实现最佳的策略灵活性和控制力。为了简化策略创建，McAfee Web Gateway 提供了包含常见策略操作的预先构建的大型规则库。企业可以选择各种规则，轻松修改这些规则，并可以通过我们的在线社区共享他们自己的规则。为了实现先进的管理，一组基于环境的规则标准与共享名单打开了解决问题和网络安全优化无限可能的大门。交互性规则跟踪简化了规则调试过程。

McAfee Web Gateway 将控制力扩展到云应用程序，支持对 Web 应用程序的使用方式进行精细、基于代理的控制。组织可以对云应用程序施加数以千计的控制，具体包括：根据需要启用或禁用特定的功能，控制使用 Web 应用程序的人员和使用方式。您是否希望允许访问 Dropbox，但不允许上传文件？不必担心。

这一灵活性和控制力也扩展到了用户身份验证和访问权限。McAfee Web Gateway 支持多种身份验证方法，包括 NT LAN Manager (NTLM)、原生身份验证拨号用户服务 (RADIUS)、Active Directory (AD)/轻型目录访问协议 (LDAP)、eDirectory、Cookie 身份验证、Kerberos 或者本地用户数据库。McAfee Web Gateway 身份验证引擎允许管理员实施灵活的规则，包括多种身份验证方法的使用。例如，通过 McAfee Web Gateway，您可以尝试对某一用户进行透明地身份验证，并根据结果提示用户提供凭据，使用其他身份验证方法，应用限制性策略，或者直接拒绝访问。

McAfee Web Gateway Identity 作为一个可选插件，包含的单点登录 (SSO) 连接器适用于数百种流行的基于云的应用程序。McAfee Web Gateway Identity 为企业提供助力，帮助增强安全性，减少服务台收到的与密码相关的求助电话，用户通过它提供的 SSO 启动平台，只需单击鼠标即可访问授权的云应用程序。它同时支持 HTTP 开机自检 (POST) 和安全声明标记语言 (SAML) 连接器，因此可以覆盖各种应用程序。系统管理员可以通过配置的连接器在特定软件即服务 (SaaS) 应用程序上创建和终止用户帐户。

McAfee Web Gateway 还通过本机流式代理支持，将访问控制扩展到流式内容，从而节省带宽并降低延迟。更多带宽控制可以设置为强制实施最小值、最大值以及确定定义通信量类的优先级，允许组织优化使用其可用带宽。

凭借 McAfee Web Gateway 实现基础架构和性能的灵活性

McAfee Web Gateway 是一款高性能的企业级代理，有一系列可扩展的设备型号，这些设备全都具有集成高可用性、虚拟选项和 McAfee Web Gateway Cloud Service 的混合部署模式。McAfee Web Gateway 具有部署灵活性和性能以及可扩展性，可在单个环境中支持数十万名用户。

您也可以执行混合部署。例如，您可以为联网用户将所有 Web 流量转发到内置设备，而将离网用户转发到云服务，极大降低通过多协议标签交换 (MPLS) 线路或虚拟专用网 (VPN) 回送流量的成本。针对混合内部部署和云部署的自动化策略同步和报告功能，有助于简化管理，确保实施统一策略及简化报告，跟踪和调查过程。

McAfee Web Gateway 提供了大量的实施选项（从显式代理到透明网桥和路由器模式），可确保支持您的网络体系结构。

McAfee Web Gateway 支持大量的集成标准，旨在适合您的独特环境。无论是 Web 缓存通信协议 (WCCP)、Internet 内容适配协议 (ICAP/ICAPS)，还是 WebSocket 协议，亦或是安全套接层 (SOCKS) 协议，McAfee Web Gateway 均可以高效地与其他网络设备和安全设备进行通信。

此外，McAfee Web Gateway 还提供了 IPv6 支持，从而帮助大型企业和国家机构遵从法规。McAfee Web Gateway 在内部 IPv4 网络与外部 IPv6 网络之间架起了一座桥梁，并可将所有可用安全性以及基础设施特性和功能应用到通讯。

面向未来的统一平台

McAfee Web Gateway 将大量保护功能整合在一起，原本需要多个单独的产品才能提供这些保护功能。URL 过滤、防病毒、零日防恶意软件、安全套接字层 (SSL) 扫描、数据丢失防护和集中式管理 — 全部统一在一款设备软件架构中。所有规格中的部署管理都是统一的，因此可以从一个统一的管理控制台将一种策略扩展到所有内置设备、设备群集、虚拟设备和云服务。

安全风险管理和报告

McAfee ePolicy Orchestrator® (McAfee ePO™) 软件是最常用、备受推崇的安全管理技术，作为所有安全报告的单一来源受到 McAfee Web Gateway 支持。

McAfee ePO 软件通过 McAfee Content Security Reporter 扩提供详细的 Web 安全报告。McAfee Content Security Reporter 提供执行以下任务所需的信息和取证工具：了解企业的 Web 使用情况、遵从法规、确定趋势、隔离问题，以及定制过滤设置以实施您的 Web 安全策略。McAfee Content Security Reporter 提供一个独立的外置报告服务器，旨在减少现有 McAfee ePO 服务器上占用大量资源的数据处理操作以及存储，从而使其能够进行扩展以满足哪怕最大的跨国企业集团的报告需求。

许可

为了实现最大的部署灵活性并确保您投资的是不会过时的技术，McAfee 在一组套件中提供了 McAfee Web Gateway 和 McAfee Web Gateway Cloud Service 的所有功能，即：**McAfee Web Protection**。您可以自由选择在内部或在云中部署，或者实施混合部署以实现更强大的部署灵活性和高可用性。无论您选择哪种部署方式，都能享用备受赞誉的迈克菲防恶意软件保护和全面的 Web 过滤功能。

McAfee Web Gateway 硬件单独出售。

1. 在 AV-TEST 进行的测试中，McAfee Web Gateway 检测出了 94.5% 的零日恶意软件、99.8% 的恶意 Windows 32 可移植的可执行 (PE) 文件，以及 98.63% 的非 PE 文件。“McAfee Web Gateway Security Appliance Test”（McAfee Web Gateway 安全设备测试），AV-TEST GmbH。

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