McAfee SaaS Email Protection and Continuity

通过电子邮件防护、可用性和合规性提高业务效率

利用 McAfee® SaaS Email Protection and Continuity 轻松部署电子邮件安全防护。除在垃圾邮件、网络钓鱼诈骗、恶意软件和不良电子邮件内容到达您的网络之前进行阻止，这种基于云的服务可执行出站邮件策略防止数据丢失。同时，您还可以依靠始终保持电子邮件连续性，确保您的组织能够全天候访问电子邮件。您无需购买硬件、无需安装软件和使用自动更新抵御最新威胁，从而集中保护您的企业安全而不是纯粹运行应用程序。

保护电子邮件和电子邮件访问安全 - 简便方法

McAfee SaaS Email Protection and Continuity 的主要电子邮件保护功能包括：

- 外围 IP 过滤功能，可在威胁到达您的网络之前预先阻止，防患于未然
- 高级垃圾邮件和欺诈防护
- 分层病毒和蠕虫扫描，可 100% 阻止所有已知病毒
- 电子邮件攻击防护
- 出站邮件和附件过滤和策略实施
- 全面的邮件连续性
- 组策略管理
- 邮件审核、邮件跟踪和处理工具
- 可选 McAfee SaaS Email Encryption

电子邮件是推动当今生产力发展的强劲引擎，平均每天有数以千计的邮件流经常规企业的电子邮件服务器。管理电子邮件确保安全和保持连接已成为一项艰巨的任务，必须不断从推动业务目标的战略性工作中转移 IT 资源。

易于管理的低成本电子邮件防护

部署工作成为举手之劳，McAfee SaaS Email Protection and Continuity 可有效防止入站和出站电子邮件威胁影响您的网络和最终用户，随时随地让您持续访问电子邮件。这种安全 Software-as-a-Service (SaaS) 软件始终开启、时刻保持最新，并且无需额外投入时间和资源进行维护。由于该服务可在垃圾邮件和基于电子邮件的威胁入侵网络之前提前进行阻止，因此大幅减少了电子邮件服务器的工作负荷，从而节省了您的宝贵带宽和服务器存储空间。与此同时，世界一流的全天候迈克菲客户支持服务可有效确保只需打个电话即可获得帮助。

基于 Web 的简化管理和报告

随着基于 Web 的单一直观管理控制台、各种最佳实践的植入，您便可以跨越自己的所有域和位置轻松管理电子邮件策略更新，释放各种 IT 资源并降低自身的总体拥有成本。管理员可以配置并实施策略，包括内容过滤和附件内容规则。策略可能会全面应用至用户组或个人用户以实现终极灵活性，同时范围广泛的报告、日志和隔离功能又可提供无与伦比的可见性。

您可以依赖的强劲基础设施

我们的 SaaS 数据中心策略可跨越四大洲维护多个数据中心。每个数据中心均经过 ISO 27001 认证，并且可在所有网络层使用 Active-Active 冗余硬件实现全冗余：防火墙、路由器和负载平衡程序交换机。我们还可以在每个数据中心内提供网络和应用程序自动监控功能，从而供远程操作人员查看可疑或故障警报和报警，同时还有全天候的安全专家对各系统进行严格监控。

有力的电子邮件安全防护

卓越的垃圾邮件防护

我们的 Stacked Classification Framework® 垃圾邮件检测系统由专利技术提供支持，运用多层分析确定电子邮件是垃圾邮件的概率，而无论邮件采用哪种语言。由于每种过滤技术在识别特定威胁（包括基于图像的垃圾邮件）方面均具有独特的优势，因而将各种技术有机融合将创造出业内最准确完善的过滤程序。

McAfee Global Threat Intelligence™ 邮件信誉功能可检查每一封邮件，以便检测基于邮件的已知威胁和新涌现的威胁（如垃圾邮件），即使这些邮件来源信誉良好也一样可以识别，如白名单公司内的受感染系统。所得出的分数不仅依赖于查询迈克菲云服务的各种传感器智能、McAfee Labs™ 研究人员和自动化工具执行的深入分析成果，而且还有效依据文件、Web 和网络威胁数据的交叉矢量智能关系，以便更加准确有效地阻止或隔离电子邮件，最大限度地提高性能。

经济实惠、方便管理的电子邮件安全和连续性

- 无需购买、维护、管理或更新硬件或软件
- 前期不需要投入资金
- 无安装或升级费用
- 自动实现连续性激活和同步，以实现无缝连续性
- 基于 Web 的简便管理
- 全天候客户支持，而且不需要额外付费
- ISO 27001 认证

无缝电子邮件连续性可保护您的企业信誉、运营和生产安全

- 在检测到中断后自动连接服务
- 通过安全的 Web 界面访问中断期间收到的电子邮件
- 全面的电子邮件功能，包括读取、编写、回复、转发和删除
- 中断后的智能电子邮件活动同步
- 中断通知和系统更新
- 入站和出站邮件过滤

了解更多

有关所有 SaaS 解决方案（包括 McAfee SaaS Email Protection and Continuity）的省时、工作效率和安全优势的详细信息，请访问 www.mcafee.com/cn/products/security-as-a-service/index.aspx。

依靠多层扫描有效阻止病毒和蠕虫

McAfee SaaS Email Protection and Continuity 包含我们的专有 WormTraq® 检测技术。还可以采用我们基于特征码的领先防病毒引擎（由 McAfee Global Threat Intelligence 提供支持）扫描邮件本身和所有附件中的恶意软件。出站电子邮件扫描与阻止入站攻击同等重要，必须过滤出站电子邮件以保护客户使其免受恶意软件的侵扰。

全面可扩展性确保有效抵御大规模的电子邮件攻击

全面的解决方案可以保护您的网络和关键邮件传输网关免受攻击，即时拦截拒绝服务攻击及其他基于 SMTP 的攻击，包括目录收集攻击、电子邮件炸弹和通道淹没攻击。

内置传输层安全性 (TLS, Transport Layer Security) 加密有效保护组织间的通信安全

对于需要更高级别入站和出站电子邮件安全防护的组织而言，我们的 TLS 协议还能接受和过滤经过加密的入站和出站邮件，并可通过安全隧道传输邮件。

随时随地始终保持电子邮件连续性

电子邮件网络中断时也不会停止工作。无论由于自然灾害还是电源故障，甚至是定期维护导致无法访问网络，McAfee SaaS Email Protection and Continuity 都能保证员工、客户、合作伙伴和供应商全天候保持联络。这种安全易用的 Web 界面还能够为客户提供持续防护，使他们像在普通的真实环境中一样收发邮件、搜索和检索所存储的邮件以及管理隔离区和邮件存储区。该服务可保留在运行中断期间正常收发所有邮件，并在电子邮件服务器恢复在线状态后通过智能方式同步中断期间所有邮件活动的准确记录。

预建规则和高级内容扫描

采用业内领先的迈克菲技术，高级数据丢失预防 (DLP) 及合规功能触手可及。McAfee SaaS Email Encryption 是 McAfee SaaS Email Protection and Continuity 的一项补充功能，您有权访问预建的 PCI DSS、医疗保健、财务数据、地区性隐私法规等内容规则，以便快速创建合规策略。扫描超过 300 种文件并保障它们的安全，从而持续保护您的组织以免发生出站数据丢失。

易于使用的推/拉加密

当您的企业需要与客户进行安全通信时，McAfee SaaS Email Encryption 能够协助您取得加密敏感信息的所有权，即使您的收件人并未部署加密解决方案也不例外。专为企业用户（甚至是移动设备企业用户）设计的易用性推/拉加密技术，可确保您的数据受到保护以防有人窥探。

利用 McAfee Security Connected 优化防护、管理及合规

功能组合能力可简化管理流程，确保您的安全解决方案相互之间紧密衔接，以最大限度地降低学习难度，并且可以从单一控制面板进行实时监控。McAfee SaaS 解决方案套件（包括 McAfee SaaS Email Protection、McAfee SaaS Email Encryption、McAfee SaaS Email Archiving、McAfee SaaS Web Protection、McAfee SaaS Endpoint Protection 和 McAfee SaaS 漏洞管理）可通过一站式控制台进行管理。

立即行动

我们将帮助您用更少的时间和资金轻松地获得更为有效的保护。购买后即可持续实现开支节省 - 了解如何最大限度地降低维护成本，解放过度忙碌的 IT 员工，使他们集中完成更具战略意义的项目。若要了解更多信息、注册获取免费试用版，请访问：www.mcafeesaas.com。

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 邮编：100020 电话：(8610) 85722000 传真：(8610) 85752299

上海市卢湾区湖滨路 222 号企业天地 1 号楼 1101 室 邮编：200021 电话：(8621) 23080699 传真：(8621) 63406606

广州市天河区体育东路 118 号财富广场西塔 15 楼 106 室 邮编：510620 电话：(8620) 38860668 传真：(8620) 38860638

销售热线：800-810-0369 www.mcafee.com/cn

26202ds_saas_protect-continuity_0411_fnl_ASD