McAfee Security for Email Servers

为 Microsoft Exchange 服务器提供的强大内容安全保护产品

McAfee® Security for Email Servers 用于检测和过滤病毒、蠕虫、特洛伊木马程序及其他潜在有害程序。它与 Microsoft Exchange 服务器兼容，可以拦截垃圾邮件和过滤邮件，防止不当或敏感信息进入或离开网络，从而帮助您满足策略与合规性要求。

作为 McAfee 产品的一部分，McAfee Security for Email Servers 通过提供从按需恶意软件扫描到策略实施等多种功能，为入站和出站电子邮件提供多层保护，从而防止敏感数据丢失或滥用。

- **业界领先的安全防护** - 运用我们屡获殊荣的内存和增量式按需扫描，清除入站和出站电子邮件中的病毒、蠕虫、特洛伊木马程序及其他威胁。
- **高级威胁检测** - 通过 McAfee Threat Intelligence Exchange 与 McAfee Advanced Threat Defense 紧密集成，实现电子邮件附件中潜在零日威胁的深入分析和确定。
- **强大的内部保护** - 检测可能会逃脱外围防御或通过受感染的笔记本电脑和内部电子邮件进入网络的威胁。此外，它还可以借助垃圾邮件防护模块阻止垃圾邮件。
- **功能强大的内容过滤** - 实施企业电子邮件使用策略，过滤禁止文件类型、不良内容并阻止敏感数据泄露。
- **单一控制台管理** - 运用 McAfee ePolicy Orchestrator® (McAfee ePO™) 平台部署、管理安全产品并显示详细的图形报告

多层电子邮件保护

全方位恶意软件防护

McAfee Security for Email Servers 利用依靠实时文件信誉信息的防恶意软件，大大降低了面临新兴威胁的风险。通过我们基于云的 Global Threat Intelligence (GTI) 向 McAfee Labs 发送所有可疑文件的指纹以进行即时信誉分析。如果该指纹被识别为已知的恶意软件，将在几毫秒内发送相应的

McAfee 将内容检查、信誉分析和恶意软件防护等功能相结合，为您的电子邮件提供安全保护。我们为确保电子邮件安全，针对位于网络外围的边缘传输服务器、集线器传输服务器和邮箱服务器提供了多层安全防御功能和多个部署选项。

联系我们

响应以阻止或隔离该文件。仍然可疑的文件会自动发送到 McAfee Advanced Threat Defense 以进行深入沙盒分析。通过 McAfee Threat Intelligence Exchange 实现的集成增强了保护，具体方式是在整个生态系统启用 McAfee Security for Email Servers 和所有连接的解决方案，对恶意附件采取措施。

邮件信誉

McAfee GTI 邮件信誉服务是一项基于云的全方位实时邮件和发件人信誉服务，通过发送相关信誉数据使我们的产品能够及时保护客户免受已知威胁及垃圾邮件等基于邮件的新兴威胁的侵扰。邮件信誉将垃圾邮件发送模式和 IP 行为等因素相结合，以确定可疑邮件是恶意邮件的可能性。这项技术的优势不仅在于查询 McAfee 云服务的各种传感器具备智能，以及 McAfee Labs 提供的分析结果，而且还在于对 Web、电子邮件和网络威胁数据的交叉引用和关联。

IP 信誉

根据发送服务器的 IP 地址检测电子邮件中的威胁。IP 信誉技术通过在网关阻止电子邮件来防范数据破坏和窃取。

URL 信誉

根据电子邮件中嵌入的 URL 的信誉，防范已知和新兴的基于 Web 的威胁。

全天候保护您的服务器

检查入站和出站电子邮件中是否有病毒、蠕虫、特洛伊木马程序和其他恶意软件。此外，您还可以扫描所有内部电子邮件，以阻止蠕虫在内部肆意传播。McAfee Security for Email Servers 通过 HTTP、FTP、网络文件共享或 McAfee ePO 集中管理控制台自动下载最新的病毒定义（DAT 文件）。

实施合规性

根据邮件大小、邮件内容或附件内容，对邮件进行过滤。阻止或隔离邮件主题、正文或附件中包含受控内容的邮件。

节省时间和资源

预建的内容过滤器可简化策略创建和实施过程。以整个企业为基础，并结合个人或部门的例外需要创建规则。通过内置 HTML 界面或 McAfee ePO 平台进行管理。

内容过滤

扫描电子邮件的主题行或正文，以及电子邮件附件。根据正则表达式 (Regex) 创建自己的内容过滤规则。

数据丢失防护与合规

数据丢失防护 (DLP) 可确保已发送（动态）或未发送的电子邮件符合组织的机密性与合规性要求。可以快速安装预建的企业字典和国家/地区特定的合规规则。内置工作流程会自动将隔离的电子邮件发送给审核人进行审查。

主要优势

- **保持您的系统不中断且正常运行:**防止病毒、蠕虫和高级威胁通过电子邮件侵入网络或通过 Microsoft Exchange 在内部传播。
- **保证员工持续高效工作:**阻止垃圾邮件和网络钓鱼攻击。
- **单一控制台管理:**McAfee ePO 软件提供了一个功能强大的管理控制台，用于控制、管理及查看报告。
- **保护关键数据:**利用 DLP 和信誉技术（IP、邮件和文件信誉）过滤入站和出站电子邮件，从而保障信息安全及减轻企业违规风险。
- **直观的图形用户界面:**易于使用的界面，可提供丰富的报告、图表和实时电子邮件通讯统计信息。

过滤垃圾邮件，提高效率

通过反垃圾邮件模块捕获垃圾邮件和网络钓鱼电子邮件，确保员工能够高效工作，并减少这些邮件占用的电子邮件服务器存储空间。用户可以创建自己的白名单和黑名单。我们的多个网关电子邮件解决方案共用一种隔离解决方案，使用户能够轻松访问隔离区。

产品运行状况警报

McAfee Security for Email Servers 会向指定的管理员发送有关产品状况的通知。它监控扫描每个文件所用的时间。如果发现任何问题，会采取修正措施来避免对 Exchange 服务器性能产生不良影响。

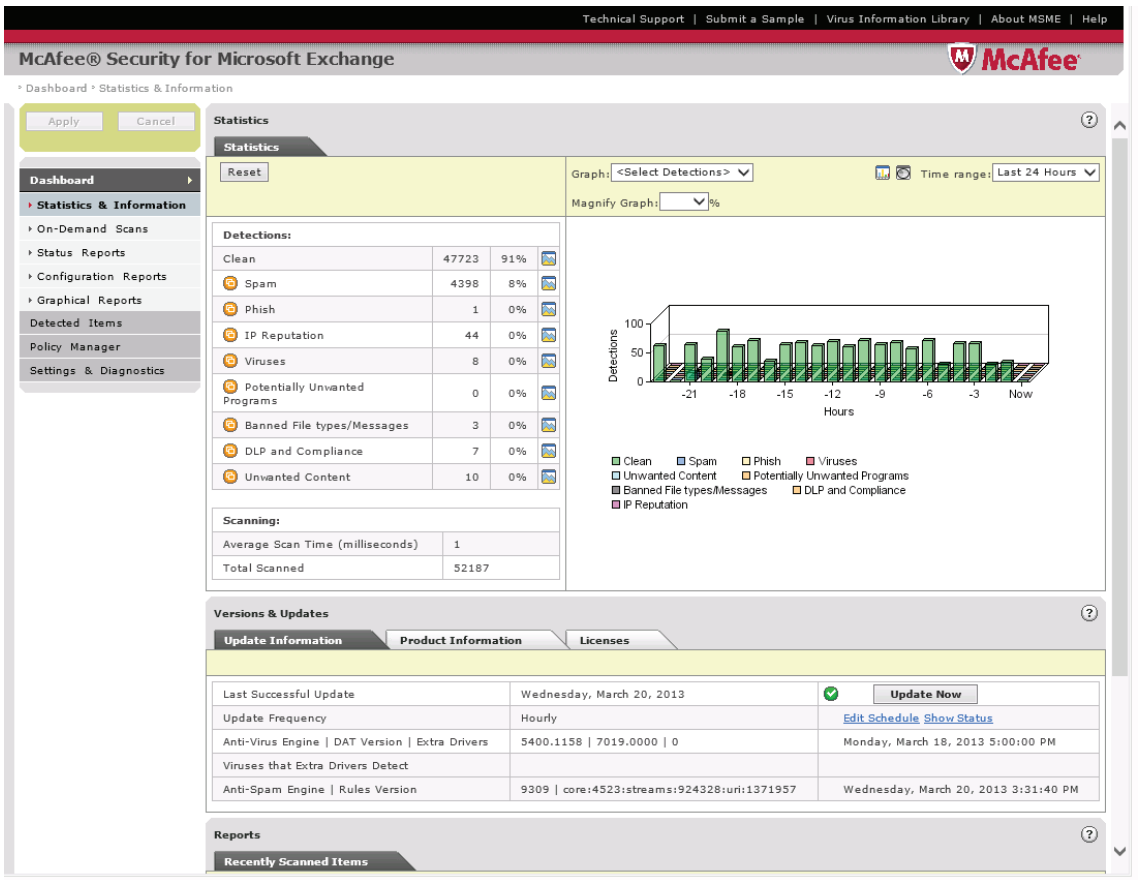

图 1. 易于使用的界面，可提供丰富的报告、图表和实时电子邮件通讯统计信息。

规格

随着电子邮件服务器上的电子邮件和共享数据量不断激增，McAfee Security for Email Servers 支持 Microsoft Exchange 环境，从而保证员工持续高效工作并使企业全天候正常运营。

McAfee Security for Microsoft Exchange 要求

操作系统要求

- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Microsoft Exchange Server 要求

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013
- 支持带有群集的 Microsoft Exchange Server

便于更新

通过自动更新功能确保及时了解来自 McAfee Labs（全球顶级威胁研究中心）的最新安全信息。

集中管理您的电子邮件隔离区

McAfee Quarantine Manager 已包含在解决方案中，通过这个解决方案可以对电子邮件隔离区和反垃圾邮件进行集中管理。McAfee Quarantine Manager 易于管理，可以通过 McAfee ePO 平台向 McAfee Labs 提交样本，提供精确的管理控制，实现与 LDAP 服务器的自动用户同步，管理用户或全局黑名单和白名单，以及生成详细报告。

扫描并保护电子邮件存储

McAfee Security for Email Servers 支持通过精细配置选项进行计划式按需扫描，比传统的全面扫描更迅速。其中包含一个选项，可以选择只扫描带附件的电子邮件、未读电子邮件、主题、发件人、收件人、抄送、邮件 ID、特定期限内收到的电子邮件或特定大小的电子邮件。

有关详细信息，请访问 **McAfee Security for Email Servers**。

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

2020 年 4 月