

McAfee DLP Endpoint

不要让重大数据丢失事件再次见诸媒体报端

主要优势

- **无与伦比的防护** — 无论您是在办公室、家中还是在旅途使用数据，都可防止数据丢失
- **全面的设备管理** — 对任何移动存储设备中的保密数据，指定详细的基于内容的过滤、监控和拦截
- **多层防护** — 确保所有终端上的数据都得到妥善保护，不论设备使用何种操作系统和类型
- **McAfee ePO 集中式管理** — 充分利用迈克菲安全风险管理架构来防止数据丢失
- **全面的监控** — 向审核人员、高级管理人员和其他利益相关方证明执行了企业内部及监管机构的合规性措施

您是否在不知不觉中遭受着数据丢失的困扰？您的财务数据、客户信息、知识产权以及员工个人记录在此时此刻可能就面临着丢失的危险。而造成这种情况的罪魁祸首不仅是黑客，还有您自己的员工。多种常见渠道（如电子邮件、Web 发布、U 盘和打印等）都可能导致数据的偶然丢失以及恶意窃取，给您造成潜在的巨大损失。

未雨绸缪，避免数据丢失

每天都有众多像您这样的企业由于恶意和无意地泄露信息而遭受严重的数据丢失。最近一项研究发现，超过 75% 的《财富》1000 强企业曾惨遭意外或恶意的数据泄露。一项最新调查表明，超过 55% 的员工每周使用便携式设备将保密数据带出工作场所。¹数据泄露及后续补救措施使企业付出巨额代价。2008 年，平均损失为 665 万美元。²

如果您能够轻松有效地阻止数据丢失，同时又可以遵从行业法规和政府法律，是否会让您如释重负？现在，借助一款可监控、审核和控制用户使用敏感数据行为的解决方案，您将如愿以偿。

防护与合规

利用 McAfee® DLP Endpoint，您可以全面监控最关键数据的传输。无论是在办公室、家中还是路上，都能即时监控和防止保密数据丢失。利用 McAfee DLP Endpoint，可保护您的企业远离经济损失、品牌受损、客户流失、处于竞争劣势以及违规等风险。

借助 McAfee DLP Endpoint，您不仅可以快速、轻松地监控实时事件，应用集中管理的安全策略来规范并限制员工使用和传输敏感数据的方式，而且能够在不影响日常业务活动的情况下生成详细的取证报告。保护您的企业免遭源自内部渠道（如电子邮件、即时消息、CD 刻录、Web 发布、USB 复制和打印等）的数据丢失威胁。另外，您还可以

阻止由木马、蠕虫和文件共享应用程序（在员工不知情时劫持其凭据）造成的保密数据丢失。

出色的防护，无任何负面影响

即使在数据被修改、复制、粘贴、压缩或加密时，也能有效防止数据丢失和泄露，而且丝毫不影响合法的业务活动。为 390 多种数据文件的内容提供全面保护。独特的指纹算法和内容标记选项（基于位置、应用程序、文件类型、正则表达式、关键字等）拓展了数据保护的广度和深度，从而确保贵公司的信息自始至终安全无忧。

简化的合规管理

利用易于管理的 McAfee ePolicy Orchestrator® (McAfee ePO™) 软件，您能够监控事件并报告事件详情，以向审核人员、董事会成员和其他利益相关方证明执行了企业内部和监管机构的合规性措施。McAfee DLP Endpoint 与 McAfee ePO 软件相集成让您能够轻松收集重要的数据，例如，发件人、收件人、时间戳和数据证明等。只需点击一下按钮，McAfee ePO 软件就能监控事件并生成详细的报告，以向审核人员、高级管理人员和其他利益相关方证明企业内部和监管机构的合规性措施已执行到位。

投资回报：无与伦比的数据保护

全面监控离开您终端的数据，这样，您可以前瞻性地阻止数据丢失和负面的头条新闻，防范于未然。

系统要求

McAfee ePO 服务器操作系统

- Microsoft Server 2003 SP1/2003 R2

台式机和笔记本电脑终端操作系统

- Microsoft Windows XP
- Professional SP1 或更高版本
- Microsoft Windows 2000 SP4 或更高版本

硬件要求

- CPU: Pentium III 1 GHz 或更高
- RAM: 512 MB (建议)
- 磁盘空间: 200 MB (最低)
- 网络连接: 采用 TCP/IP, 支持远程访问

McAfee DLP Endpoint 是整个数据保护解决方案的一部分。McAfee Total Protection™ for Data 整合了 McAfee DLP Endpoint 和 McAfee Endpoint Encryption, 能够提供更加完善的数据保护解决方案。

特性

无与伦比的防护

- 控制用户通过网络、应用程序与存储设备发送、访问和打印敏感数据的方式。全面保护电子邮件、网络邮件、P2P应用程序、即时消息、Skype、HTTP、HTTPS、FTP、Wi-Fi、USB、CD、DVD、打印机、传真机以及移动存储设备。
- McAfee DLP Endpoint 功能选项包括:
 - 监控 — 允许数据传输
 - 防护 — 阻止数据传输
 - 警报 — 通知管理员和最终用户
 - 加密 — 确保先加密数据后再进行传输³
 - 隔离 — 等待授权³

全面的设备管理

- 控制和阻止复制到 USB 设备、闪存、iPod 和其他移动存储设备的保密数据
- 根据任何基于 Windows 设备的参数 (包括产品 ID、厂商 ID、序列号、设备类别、设备名称等) 指定哪些设备可以使用并进行分类

为终端提供多层防护措施

- 通过监控和预防有关最敏感数据行为的风险, 基于主机的防护可有效阻止终端数据丢失
- 融合了 McAfee Endpoint Encryption 的 McAfee DLP Endpoint 可提供全面的、分层的方法来防止数据丢失

McAfee ePO 集中式管理

- 通过 McAfee ePO 管理控制台访问 McAfee DLP Endpoint 集中策略和事件监控
- 使用 McAfee ePO 软件集中管理策略和监控事件
- 通过 McAfee ePO 软件部署和更新代理
- 与 McAfee ePO 软件相集成可提供高级的基于 Web 的管理以及更多的报告/审核功能

轻松实现全面监控

- 使用 McAfee DLP Endpoint 的完整事件报告和监控来收集您需要的所有数据 (例如, 发件人、收件人、时间戳和数据证明等), 以执行适当的分析、调查和审核、损失控制及风险评估



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

¹ Illuminas 2007, Threats Within, Volume II Data Loss Disaster

² Ponemon Institute's 2008 Cost of Data Breach Study

³ 内置在 McAfee Data Loss Prevention 设备中