McAfee®

Protect what you value.

McAfee Host Data Loss Prevention

不要成为下一个重大数据丢失事件新闻的主角

当您的数据被泄漏出去的时候，您是否都毫无察觉？您的客户信息、知识产权信息、财务数据以及个人文件可能正在面临被泄漏出去的危险。而这类事件的罪魁祸首不一定全是黑客，还可能是您自己的员工。不管是无意还是恶意，电子邮件、网上信息发布、U 盘和打印等都可能成为数据丢失的途径。数据丢失可能会给您造成巨额损失。

主要优势

无与伦比的全面防护

- 无论在任何情况下（工作中、家里或途中），都能有效防止数据丢失

全面的设备管理

- 指定详细的基于内容的过滤、监控和拦截规则，确保移动存储设备中的机密数据的安全

多层防护

- 无论终端设备使用的是哪种操作系统，也无论设备类型如何，均能保护其中数据的安全

ePO 集中管理

- 利用您的 McAfee 安全风险管理架构防止数据丢失

全面监控

- 向审计人员、高级管理人员和其他利益相关者证明自己遵从了内部安全策略和相关法规

防止数据丢失应做到防患于未然

每天都会有与您企业类似的公司因信息被无意或恶意泄露而成为恶性数据丢失事件的牺牲品。最新调查表明，75% 以上的《财富》1000 强企业都曾因为信息被无意或恶意泄露而蒙受损失。另有一项新的调查显示，每周有超过 55% 的员工会使用便携设备将机密信息带出工作场所。[1] 数据泄露以及后续的补救使企业付出沉重的代价。2007 年，平均损失高达 630 万美元。[2]

如果能够轻松有效地防止数据丢失，您是否会感到如释重负呢？如果同时还能让您确保始终遵从行业和政府法规，是否更加令您高枕无忧？现在，您可以借助我们的解决方案来监控、审核和控制那些涉及机密数据的用户行为。

安全防护与法规遵从

借助 McAfee® Host Data Loss Prevention (Host DLP) 解决方案，您可以全面监控最重要数据的传输。无论在任何情况下（工作中、家里或途中），都能对数据进行即时监控，有效防范机密数据丢失。Host DLP 可使您的企业避免诸多风险：经济损失、品牌受损、客户流失、竞争受挫以及违规等。

借助于 Host DLP，您可以：简单快捷地监控实时活动；采用集中管理的安全策略来规范和限制员工使用和传输机密数据的方式；生成详细的取证报告。而这一切都不会影响您的日常业务活动。使您的企业避免发生因内部原因而导致的数据丢失，例如，电子邮件、即时消息、CD 刻录、网上信息发布、USB 复制和打印等都可能成为数据外泄的途径。同时，该解决方案还能帮助您预防木马、蠕虫和文件共享应用程序等导致的机密数据丢失，这类威胁会在员工不知情的情况下窃取员工的数据。

全面的保护，业务不受任何影响

借助该解决方案，即使数据被修改、复制、粘贴、压缩或加密，也能够有效防止数据丢失或泄露，而且不会影响合法的业务活动。可保护 390 多种类型的数据文件。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）有助于更全面、更深入地实施数据保护，从而始终确保企业信息的安全。

法规遵从管理更加简便

McAfee ePolicy Orchestrator® (ePO™ 简化了您的管理工作，使您能够有效监控事件，并生成详细的事件报告，以便向审计人员、董事会成员以及其他利益相关者证明自己遵从了内部安全策略和相关法规。Host DLP 与 ePO 的集成使您能够轻松收集各类重要的数据（例如，发件人、收件人、时间戳以及数据证据等）。只需点击一下按钮，ePO 就能轻松监控事件并生成详细的报告，以便您向审计人员、高管人员和其他利益相关者证明自己遵从了内部安全策略和相关法规。

得偿所愿：无与伦比的数据保护

借助这款解决方案，您可以对数据实施全面监控，做到防患于未然，从而有效防范数据丢失，避免成为负面新闻报道的主角。

Host DLP 只是全面数据保护解决方案的一部分。McAfee Total Protection™ for Data 与 Host DLP 和 McAfee Endpoint Encryption 相结合，能够形成一套更加全面的数据保护解决方案。

1 Illuminas 2007, Threats Within Volume II Data Loss Disaster
2 Ponemon Institute' s 2007 Cost of Data Breach Study

系统要求

ePO 服务器

操作系统

- Microsoft　Server 2003 SP1、Microsoft　Server 2003 R2

桌面机和便携式计算机终端

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 或更高频率
- RAM：512 MB（推荐使用）
- 磁盘空间：200 MB（最低要求）
- 网络连接：符合 TCP/IP 协议，以进行远程访问

特点

无与伦比的强大保护

- 控制用户通过网络、应用程序和存储设备发送、访问和打印机密数据的方式。保护电子邮件、Webmail、P2P 应用程序、即时消息 (IM)、Skype、HTTP、HTTPS、FTP、Wi-Fi、USB、CD、DVD、打印机、传真机和移动存储设备的使用安全
- DLP 实施选项包括：
  - 监控—允许数据传输
  - 预防—阻止数据传输
  - 警报—向管理员和最终用户发出通知
  - 加密—确保在数据传输前对其进行加密*
  - 隔离—等待验证*

*包含在 McAfee Data Loss Prevention 设备中

全面的设备管理

- 控制和阻止将机密数据复制到 USB 设备、闪存设备、iPod 和其他移动存储设备中
- 根据基于 Windows 的设备参数（包括产品 ID、供应商 ID、序列号、设备类别、设备名称等）来指定和划分可使用的设备

为终端设备提供多层防护

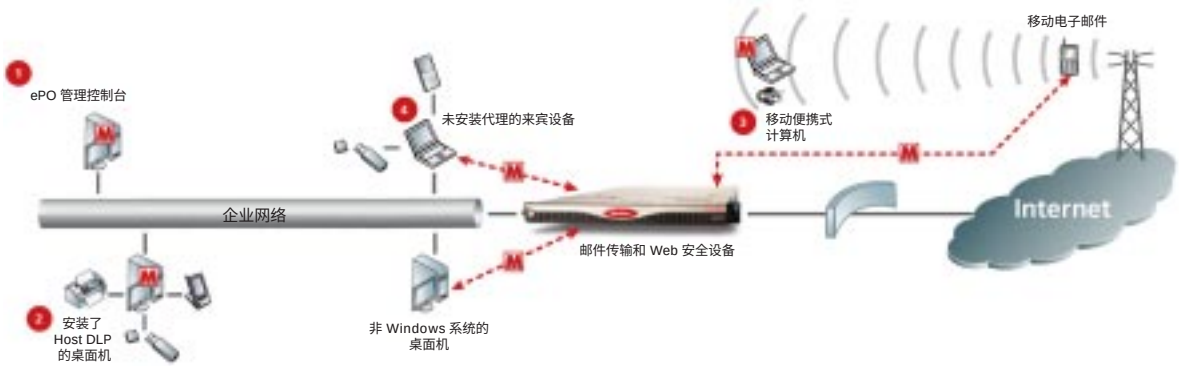
- 通过监控并防范针对企业最机密数据的高风险用户行为，基于主机的防护可以防止数据通过企业的终端设备泄漏出去
- 通过与 McAfee Endpoint Encryption 结合使用，Host DLP 可以为数据提供全面且多层的防护，防范数据丢失

ePO 集中管理

- 通过 ePO 管理控制台使用 Host DLP 集中策略和事件监控功能
- 借助 ePO 集中管理策略和监控事件
- 通过 ePO 部署和更新代理
- 通过与 ePO 4.0 集成，可提供基于 Web 的高级管理功能以及更多的报告/审核功能

轻松进行全面监控

- Host DLP 全面的事件报告和监控功能可以收集您所需要的各种数据，例如，发件人、收件人、时间戳以及数据证据等，以便进行适当分析、调查和审核、损失控制以及风险评估



1 ePO 管理控制台 — 可集中管理策略、审核、报告以及分配软件。确保您的安全策略能够与您的业务流程和运营相吻合。

2 Host DLP 和 McAfee Endpoint Encryption — 监控、报告、控制和防止可能会给数据带来风险的用户行为。通过 FIPS 认证的强大加密功能可对整个磁盘或个人文件及文件夹进行加密，即使在设备丢失或被盗的情况下，也能确保其中数据的完整性。

3 适用于移动设备的 McAfee Endpoint Encryption — 在移动设备上创建加密的、受保护的空间以保存机密数据。即使在设备丢失或被盗的情况下，也能确保其中的数据的完整性和机密性。

4 McAfee Device Control 和 McAfee Endpoint Encryption — 控制用户对外部介质设备（例如 iPod 和 U 盘等）的使用，以防止机密数据丢失。强大的全盘加密功能可以确保便携式设备在丢失和被盗时不会遭到非法使用。

有关数据保护的更多信息，请访问 *www.mcafee.com/data_protection*。

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

迈克菲（上海）软件有限公司

北京市朝阳门外大街18号丰联广场B座1215B室	邮编: 100020	Tel : (8610) 65383399	Fax: (8610) 65885601
上海市徐汇区虹桥路3号港汇2座4005-4006室	邮编: 200030	Tel : (8621) 61458878	Fax: (8621) 61132278
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	Tel : (8620) 38860668	Fax: (8620) 38860638

McAfee销售热线：800-819-8879