

McAfee Device Control

防止未经授权在企业网络中使用可移动介质设备

U 盘、MP3 播放器、CD、DVD 以及其他可移动介质虽然很实用，但也会给您的企业带来安全隐患。这些设备体积小巧，但存储容量巨大，这些特点使它们非常容易被带出工作场所，而一旦丢失或被盗，其中存储的机密客户数据和知识产权就很容易流出公司，从而落入别有用心的人手中。

迈克菲公司进行的一项调查显示，超过半数（大约 55%）的被调查者承认，他们每周都会使用便携式设备将一些机密文档带出企业。¹ 您如何知道哪些人将哪些信息存储到哪类设备上了？即使他们有权使用某些数据，您又如何确定他们是否能够确保这些数据的安全？

主要优势

无与伦比的全面保护

- 防止未经授权使用可移动存储设备而造成数据丢失

全面的设备管理

- 指定基于硬件和内容的详细策略，过滤、监控和拦截可移动存储设备上的机密数据
- 可以安全地使用可移动介质设备 — 无需“全部阻止”，因而不会影响您的正常工作

ePO 集中式管理

- 利用迈克菲安全风险管理平台防止数据通过可移动存储设备外泄
- 集中部署和管理安全策略，防止机密数据通过移动介质外泄

全面的可见性

- 向审核人员、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

遏制由于机密信息泄露而导致的成本上升

数据丢失是当今各类企业面临的最广泛、最严重、也是代价最高的安全问题之一。事实上，75% 以上的财富 1000 强企业都曾因为数据被无意或恶意泄露而蒙受损失。这类事件造成的损失令人咋舌。2008 年，数据丢失事件使企业蒙受的平均损失高达 665 万美元。²

监控和管理复制到便携式设备和介质中的数据

McAfee® Device Control 可以防止企业的重要数据通过 U 盘、iPod、蓝牙设备、可刻录 CD 和 DVD 等可移动介质泄露出去。借助该解决方案，您可以监控和管理各类桌面机和笔记本电脑上的数据传输，不论用户和机密数据在什么地方，即使没有连接到企业网络，也可以提供保护。

Device Control 可以非常精确地管理您的敏感数据。指定哪些设备可以使用，哪些不可以使用。规定哪些数据可以复制到允许使用的设备中，以及哪些不可以。还可以限制用户从特定设备（例如存有专属信息的文件服务器）和个别应用程序（例如可生成机密报告的会计程序）复制数据。

自动实施详细的设备和数据策略

可以轻松集中控制您的信息资产。使用 McAfee ePolicy Orchestrator® (ePO™) 为托管的桌面机和笔记本电脑分配 McAfee Device Control 代理。然后，具体指定哪些数据可以或不可以复制到哪些可移动存储设备上。其余工作则由 Device Control 为您完成，该解决方案可以自动监控设备的使用情况，阻止任何违反既定策略的设备使用和数据传输行为，即使数据在修改、复制、粘贴、压缩或加密时，也能提供全面保护。而且，Device Control 不会阻止合法业务活动的顺利进行。

随时证明法规遵从情况

借助 McAfee Device Control，您可以全面掌握和管理向可移动存储设备和介质传输机密信息的行为。通过与 ePO 集成，可以轻松收集各类重要的使用数据（例如设备、时间戳和数据证据）。只需点击一下鼠标，即可实时监控活动并生成详细的取证报告，以便您向审核人员、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。

1 McAfee. 《The Threats Within Volume II: Data Loss Disaster》。2007 年 2 月。

2 Ponemon Institute 的《2008 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

硬件要求

- 磁盘空间：250 MB
- 内存：512 MB
1 GB 内存（推荐使用）
- CPU：Intel Pentium II 或更快的处理器，450 MHz（最低要求）

Device Control 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 或更快的处理器
- 内存：512 MB（推荐使用）
- 磁盘空间：200 MB（最低要求）
- 网络连接：TCP/IP，用于进行远程访问

功能

无与伦比的数据保护

- 规范用户将数据复制到 U 盘、iPod、可刻录 CD 和 DVD、软盘、蓝牙和 IrDA 设备、成像设备、COM 和 LPT 端口等可移动设备或介质的行为
- 保护所有数据、格式和衍生品，即使数据在修改、复制、粘贴、压缩或加密时，也依然能够提供全面保护
- 无论用户身在何处，都可以有效防止数据丢失，而且不会干扰合法的业务活动

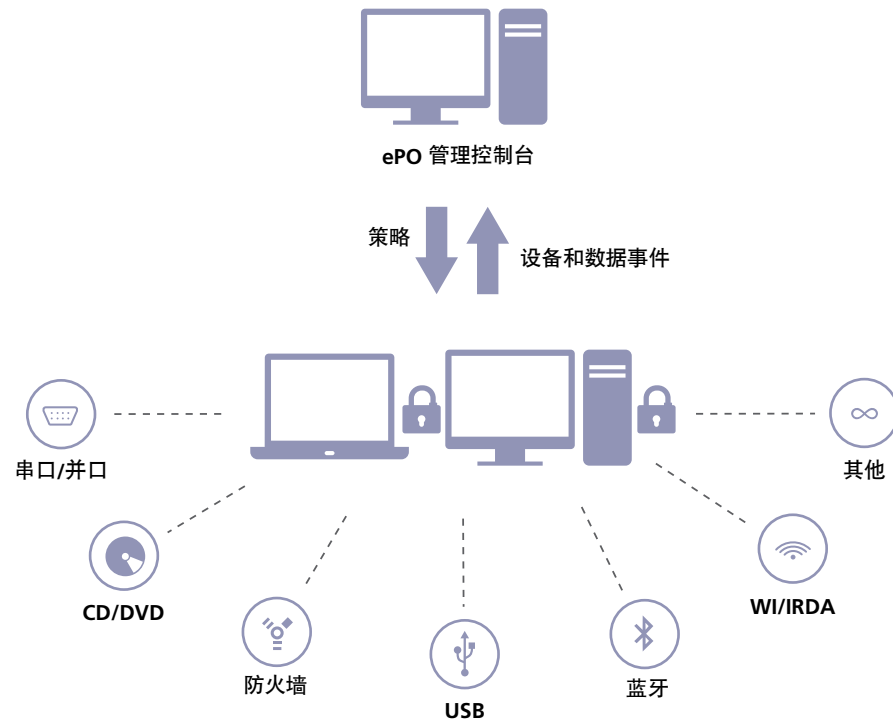
通过 McAfee ePO 进行集中式管理

- 借助这款集成式的管理控制台，可以快速、便捷地在整个环境中配置、部署和更新策略及代理

- 按用户、组或部门设置设备和数据策略
- 根据 Windows 设备参数（包括产品 ID、供应商 ID、序列号、设备类型和设备名称等）来指定哪些设备可以使用，哪些不可以使用
- 指定哪些内容可以或不可以复制到允许访问的设备中

轻松进行全面监控

- 借助详细的用户级和设备级日志来满足审核和法规遵从要求
- 收集事件详细信息（例如设备、时间戳和数据证据等），以便可以迅速地采取适当的响应、调查和审核措施



McAfee Device Control 可以指定哪些设备允许使用，哪些数据允许复制。

要了解有关数据保护的详细信息，请访问 www.mcafee.com/data_protection。

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

