McAfee Complete Data Protection

全方位终端加密解决方案

敏感数据始终面临丢失、被盗或曝光的风险。很多时候，数据仅仅通过笔记本电脑或 USB 设备就能堂而皇之地泄露出去。遭受这种数据丢失的公司可能面临严重后果，包括监管处罚、公开披露、品牌形象受损、失去客户信任和经济损失。根据 Ponemon Institute 的一份报告，所有公司笔记本电脑中有 7% 会在使用寿命期间丢失或被盗。[1] 具有大存储容量的移动设备快速增加，并且 Internet 访问往往为数据丢失或被盗开放了更多渠道，因此保护敏感、专属和个人可识别的信息刻不容缓。McAfee® Complete Data Protection 套件可解决所有这些以及其他更多顾虑。

主要功能

- Drive Encryption
- File and Removable Media Protection
- Management of Native Encryption

企业级驱动器加密

通过企业级安全解决方案保障您的机密数据安全，该解决方案已经过 FIPS 140-2 和 Common Criteria EAL2+ 认证，并通过 Intel® Advanced Encryption Standard-New Instructions (Intel AES-NI) 集得到加速。McAfee Complete Data Protection 使用驱动器加密结合强大的访问控制功能，通过开机前双重身份验证阻止对终端上机密数据的未授权访问，这些终端包括台式机、VDI 工作站、笔记本电脑、Microsoft Windows 平板电脑、USB 驱动器等等。

可移动介质、文件和文件夹以及云存储加密

确保特定文件和文件夹始终加密，无论是在哪里编辑、复制或保存数据。McAfee Complete Data Protection 以内容加密功能为主要特色，可自动、透明地对即时选择的文件和文件夹进行加密 - 在这些文件和文件夹在您的组织中移动之前。您可以根据用户和用户组，为特定的文件和文件夹创建并实施集中式策略，而无需用户交互。

Management of Native Encryption

Management of Native Encryption 可让客户直接从 McAfee® ePolicy Orchestrator® (McAfee ePO™) 软件管理 OS X 平台上的 Apple FileVault 和 Windows 平台上的 Microsoft BitLocker 提供的本机加密功能。因此，Management of Native Encryption 可以与 Apple OS X 和 Microsoft Windows 补丁、升级和固件更新实现无缝兼容，并可为 Apple 推出的新硬件提供即时支持。Management of Native Encryption 允许管理员在用户已经启用 FileVault 和 BitLocker 的地方手动导入恢复密钥。

集中式安全管理和高级报告

使用集中式 McAfee ePO 软件控制台贯彻执行强制性企业安全策略，严格控制数据的加密、监控和保护方式，避免其丢失。集中定义、部署、管理和更新安全策略，以便加密、过滤和监控敏感数据，并阻止未经授权的访问。

McAfee Complete Data Protection 功能

企业级驱动器加密

- 自动加密所有设备，无需用户操作或培训或对系统资源造成影响。
- 使用强大的多重身份验证，识别和验证授权用户。
- 支持 Intel Software Guard Extensions (Intel SGX)。
- 与第三方凭据提供程序兼容。
- 针对 Windows 10 周年更新的就地升级支持。

可移动介质加密

- 可针对几乎任何移动存储设备（无论是否由公司发放）实施自动、即时的加密。
- 加密或锁定对 VDI 工作站上可移动介质的写入权限。
- 无需在设备主机上安装任何其他软件，也无需具备本地管理员权限，随时随地访问加密数据。

文件、文件夹和云存储加密

- 无论文件和文件夹保存在何处（包括本地硬盘驱动器、文件服务器、可移动介质，以及云存储中，如 Box、Dropbox、Google Drive 和 Microsoft OneDrive），均可确保其安全。

管理 Mac 和 Windows 上的本机加密

- 直接从 McAfee ePO 软件管理任何可以运行 Mac OS X Mountain Lion、Mavericks、Yosemite 和 El Capitan 的 Mac 硬件上的 FileVault。
- 直接从 McAfee ePO 软件管理 Windows 7、Windows 8 和 Windows 10 系统上的 BitLocker，无需单独的 Microsoft BitLocker Management and Administration (MBAM) 服务器。
- 通过 McAfee ePO 软件中的各种报告和信息显示板报告合规性。

主要优势

- 遏止复杂恶意软件引起的数据丢失，这些恶意软件会劫持敏感的个人信息。
- 当数据存储在台式机、笔记本电脑和云中时提供保护。
- 直接从 McAfee ePO 管理终端上的 Apple FileVault 和 Microsoft BitLocker 本机加密。
- 在硬件级别与您的终端通信并进行控制，无论这些终端是否已关机、禁用或加密，以便停止由于安全事故、病毒爆发或忘记加密密码，而到现场咨询或无休止地拨打技术支持电话。
- 使用高级报告和审核功能证明合规性；监控事件并生成详细报告，以向审核者和其他利益相关者证明您的组织符合内部和监管隐私要求。

集中式管理控制台

- 使用 McAfee ePO 软件基础设施管理来管理全盘加密、文件和文件夹加密，及可移动介质加密；控制策略和补丁管理；恢复丢失的密码；以及证明监管合规性。
- 使用 Microsoft Active Directory、Novell NDS、PKI 等同步安全策略。
- 使用大量审计功能证明已对设备进行了加密。
- 日志数据事务用于记录如下信息：发件人、收件人、时间戳、数据证据、上次成功登录的日期和时间、上次接收更新的日期和时间，以及加密成功与否。

了解更多信息

有关迈克菲数据保护的更多信息，请访问 **www.mcafee.com/cn**.

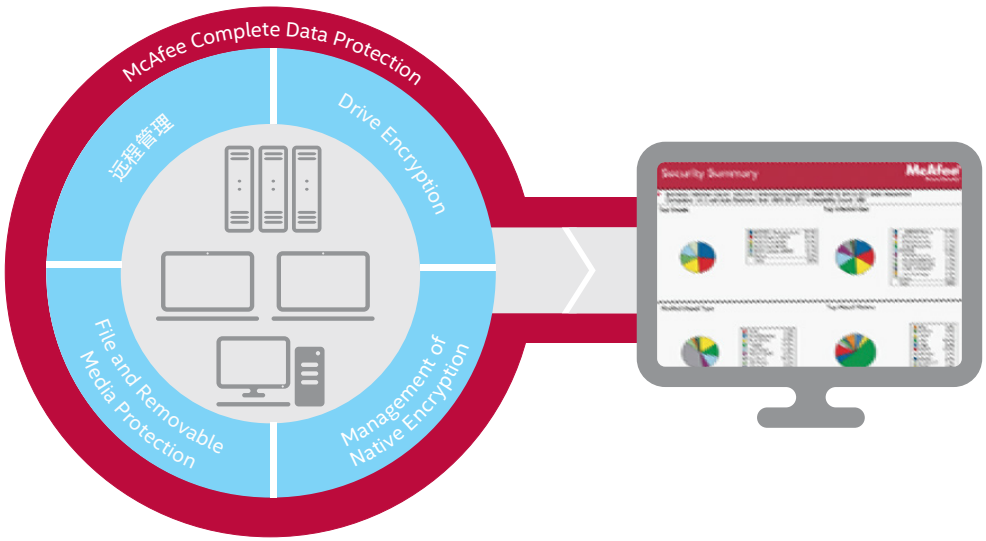

图 1. McAfee Complete Data Protection

McAfee Complete Data Protection 规格

Microsoft Windows 操作系统

- Microsoft Windows 7、8 和 10（32/64 位版本）
- Microsoft Windows Vista（32/64 位版本）
- Microsoft Windows XP（仅限 32 位版本）
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003（仅限 32 位版本）
- 硬件要求
  - CPU：Pentium III 1GHz 或更高版本的笔记本电脑和桌面机
  - RAM：最少 512 MB（推荐使用 1 GB）
  - 硬盘：最少 200 MB 可用磁盘空间

Apple Mac 操作系统

- Mac OS X El Capitan、Yosemite、Mountain Lion 和 Mavericks
- 硬件要求
  - CPU：基于 Intel 的带 64 位 EFI 的 Mac 笔记本电脑
  - RAM：最少 1 GB
  - 硬盘：最少 200 MB 可用磁盘空间
- 集中式管理

1. *The Billion Dollar Lost Laptop Problem Study*（十亿美元的损失：笔记本电脑问题研究），Ponemon Institute，2010 年 9 月。

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