

McAfee Application Control

减少来自未经授权应用程序的风险，实现更强大的终端控制

主要优势

- 防范零日威胁且无需特征码更新
- 增强固定功能系统（此类系统包括零售环境中的销售点终端、银行 ATM 设备以及早期的固定功能 Microsoft Windows NT 和 2000 系统）的商业生命力
- 采用动态白名单，无需人工操作，大幅降低拥有成本
- 充分利用您对 McAfee ePO 软件的安全投资
- 在终端透明运行的低投入软件解决方案

主要功能

- 自动接受通过经授权流程添加的新软件
- 阻止所有未经授权的软件、脚本和动态链接库 (DLL) 的执行，进一步防范内存漏洞
- 在多个已连接或已断开的服务器和终端上轻松提供现有更改流程
- 具有计算机物理或远程访问权限的管理员不能更改保护设置
- 集中管理进一步减少 IT 投入

用户无意中引入的一些软件可能会安装恶意软件、引发支持问题并违反软件许可，从而损害系统和您的整体业务。McAfee® Application Control 软件能够有效阻止未经授权的应用程序。另外，与简单白名单不同，该软件使用一种动态信任模型来避免极为耗工耗时的名单。面对来自 Internet 的众多未知软件，这种集中管理的解决方案为您的系统安全策略增加了及时控制，并且十分适合企业的运营需要。

确保终端和服务器遵从安全策略、操作流程和法规，对于当今资源匮乏的 IT 部门来讲是一个巨大的压力。最终用户可能无意中引入对业务构成风险的不良软件。各种规模的企业都需要一种高效方式来实现终端和服务器的标准化，以确保它们运行经过许可的软件，同时不影响最终用户的生产力。

在受控环境中实现业务效率

McAfee Application Control 软件增强了黑名单功能、实时信誉认知和行为方法，能够帮助 IT 部门一致地启用已知良好软件，阻止已知不良软件，并正确处理新的和未知软件。

我们的动态白名单信任模型无需其他白名单技术成本高昂的人工支持，从而大幅降低成本。

完全防范有害应用程序和代码

恶意代码充分利用当今业务环境中使用的灵活软件和模块化代码。McAfee Application Control 软件将保护范围扩大到 Java、ActiveX 控件、脚本、批处理文件和专业代码，并且能够阻止高级威胁而无需更新特征码。

可扩展的集中管理

McAfee Application Control 软件充分利用您对 McAfee ePolicy Orchestrator® (McAfee ePO™) 管理平台的安全投资。McAfee ePO 软件所具备的远程部署功能可使您通过一个中心位置轻松管理和报告软件在整个企业部署的情况。

灵活安全、成本低微且易于管理

动态白名单管理能够轻松支持不同业务需要的多种配置：销售点终端、后台服务器以及不同用户配置文件的多个桌面映像。它在终端上透明运行，初始和持续运行成本都很低。

增强对固定功能系统的控制

在法规要求比较严格的行业，例如银行、零售、制造和关键基础设施，销售点 (POS) 终端、客户服务终端等设备以及早期的 Microsoft Windows NT 和 2000 系统执行关键功能并且通常存储敏感数据。

McAfee Application Control 软件非常适合用于为固定功能系统扩充一个保护层，在 CPU 或内存资源占用方面表现出色。该软件占用系统资源少，不影响系统性能。只需很低的初始和持续运行投入，而且在没有网络连接的独立模式下同样高效。

规格

操作系统 (OS)

- Microsoft Windows NT*
- Microsoft Windows 2000/2003/2008
- Microsoft Windows XP/Vista
- Microsoft Windows XPE
- Microsoft Windows XP/Vista (64 位)
- Microsoft Windows 2003/2008 (64 位)
- Microsoft Windows CE 6,0*
- Microsoft Windows 7
- Microsoft 2008 R2
- Linux RHEL 3/4/5
- CentOS 4/5
- SuSE EL 9/10
- Oracle EL 5
- Solaris 8/9/10

* 这些平台不受 McAfee ePolicy Orchestrator 和管理平台的支持, 或者以独立模式工作。

利用信任模型的动态白名单

利用信任来源模型, McAfee Application Control 软件使 IT 管理员无需人工维护获得批准的应用程序列表。只允许获得授权的软件运行, 而且不能篡改它们。



图 2: 安全更新流

低投入软件解决方案

McAfee Application Control 软件是一种低投入软件解决方案。

- 设置简便, 初始和持续运行投入均很低
- 对 CPU 周期的影响极小, 只占用不到10 MB 的 RAM
- 不执行可能影响系统性能的文件系统扫描
- 特别设计, 可在断开或“脱机”模式下工作
- 无需特征码更新

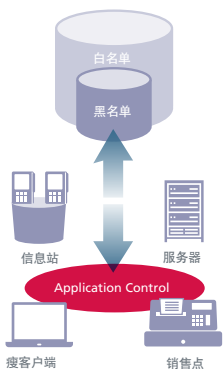


图 1: McAfee Application Control 软件为固定功能设备 (如信息站、POS 终端) 和早期平台扩充了一个保护层, 从而极大地降低了客户风险。

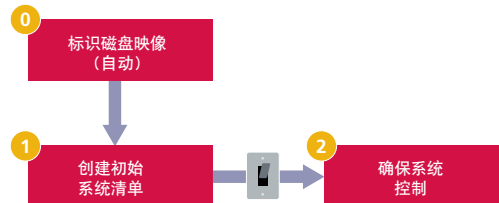


图 3: 动态白名单的工作原理:
0. 完全自动发现系统上的所有执行软件
1. 预先计算极轻型的运行时系统
2. 系统维护期间实施完全自动的代码进入控制

McAfee ePO 软件整合并集中管理所有迈克菲产品通过使用单个集成式管理平台, 公司可大大减少使用多个控制台来管理终端安全的 IT 管理人员的数量。借助 McAfee ePO 平台, IT 部门可以:

- 通过基于 Web 的单一管理平台, 获得集中的事件监控、报告、信息显示板和工作流等信息
- 从一个管理系统部署、管理和更新代理和策略

与迈克菲解决方案的集成和兼容性

McAfee Integrity Control 软件将应用控制和更改控制相结合以确保完全的系统完整性。更改控制增加了持续文件完整性监控和更改策略管理。McAfee Integrity Control 软件可用于固定功能系统, 例如销售点 (POS) 设备和自动柜员机 (ATM)。

McAfee Endpoint Protection 客户还可以从终端和服务端控制增强中获益。McAfee Application Control 软件通过消除未经授权代码在桌面机上执行而补充了基于特征码和行为的组件, 从而进一步保护企业环境。

McAfee Application Control 软件可在多种网络拓扑和防火墙配置中工作, 并且在虚拟化环境中提供了一个理想的控制层。

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 1 号楼企业天地 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

