McAfee Application Control

降低未授权应用程序控制终端、服务器和固定设备的风险。

远程攻击或社会工程带来的高级持久性威胁 (APT) 使得为企业提供保护的难度日益增加。McAfee® Application Control 可以帮助您对付网络犯罪分子，为企业的安全和工作效率提供保障。使用动态可信模型和创新性安全功能，如本地和全球信誉智能、实时行为分析技术和终端自动免疫，这种 McAfee 解决方案可立即阻止持久性威胁，无需进行耗工耗时的列表管理或签名更新。如果您的企业对抵御零日威胁有着苛刻要求，您不妨仔细了解一下 McAfee Application Control。

智能白名单

McAfee Application Control 通过阻止未经授权的应用程序执行来防御零日威胁和高级持久性威胁。利用清单功能，您可以轻松地查找和管理与应用程序相关的文件。该功能根据应用程序和供应商对您企业中的二进制文件（.EXE、.DLL、驱动程序和脚本）进行分组，以一种直观的层级格式显示，并将应用程序智能地分为已知良好、未知和已知不良三类。利用白名单，您可以只允许已知良好的列入白名单的应用程序运行，从而抵御未知的恶意软件的攻击。

实施良好的安全计划

由于用户需要在他们的社交和启用云的商业环境中更加灵活地使用应用程序，所以 McAfee Application Control 为企业提供了三个选项来充分发挥白名单策略的功能，从而抵御威胁，如下所示：

图 1. 充分发挥白名单策略作用的三种方式。

主要优势

- 抵御零日威胁和高级持久性威胁 (APT)，且无需特征码更新。
- 利用 McAfee Global Threat Intelligence 和 McAfee Threat Intelligence Exchange 来提供文件和应用程序的全球和本地信誉。
- 利用自动接受通过可信渠道添加的新软件的动态白名单来增强安全的同时降低拥有成本。
- 利用 McAfee® ePolicy Orchestrator® (McAfee ePO™) 软件（用于管理 McAfee 安全解决方案的集中平台）集中管理平台有效控制应用程序访问。
- 通过安全性高的白名单和高级内存保护缩短修补周期。
- 借助受信任的更新程序保持系统安装最新的补丁。
- 在已连接或已断开的服务器、虚拟机、终端、固定设备（如销售点终端）和旧版系统（如 Microsoft Windows XP）上强制实行控制。

强有力的内置建议

使用清单搜索和预定义的报告，可以快速查找和修复您所在环境中的漏洞、合规性和安全问题。您也可以搜索有用的信息，如近期添加的应用程序、未经验证的二进制文件、信誉未知的文件以及软件版本已过期的系统等，从而快速查明漏洞并验证软件许可证的合规性。

完成和快速响应

白名单利用 McAfee Global Threat Intelligence (McAfee GTI) 的全球威胁智能感知技术而得以增强，这是一种独有的 McAfee 技术，通过全球范围内数百万个传感器实时追踪文件、消息和发件人的信誉。McAfee Application Control 使用这些信息来确定位于您的计算环境中的文件的信誉，将其分为良好、不良和未知三类。

通过 McAfee Threat Intelligence Exchange（单独销售的可选模块）进行部署时，McAfee Application Control 会根据本地信誉智能更新白名单，从而即时抵御威胁。利用 McAfee Threat Intelligence Exchange，McAfee Application Control 会与 McAfee Advanced Threat Defense 相互协调，在沙盒环境中对未知应用程序的行为进行动态分析，以及让终端自动免受新检测到的恶意软件的威胁。

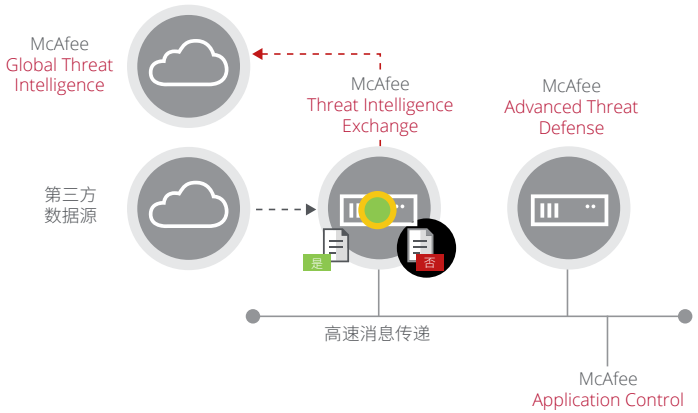

图 2. McAfee GTI 持续监控文件和发件人的信誉。通过 McAfee Threat Intelligence Exchange 进行部署时，McAfee Application Control 会根据本地信誉智能自动更新白名单，如果需要文件相关的更多信息，则可以与 McAfee Advanced Threat Defense 相互配合。

对业务连续性无影响

为了避免影响业务连续性，会根据应用程序信誉自动允许新应用程序。对于未知应用程序，建议界面会根据终端的执行模式为用户推荐新的更新策略。这是一个用来管理已阻止的应用程序生成的例外的良好方法。检查已阻止的应用程序的例外和详细信息之后，只需批准和将文件列入白名单，或忽略以阻止应用程序。

主要优势（续）

- 根据应用程序评级或自我审批允许新的应用程序，从而改善业务连续性。
- 采用低开销的解决方案来维护用户工作效率和服务器性能。
- 轻松保护旧版系统和现代技术投资。

支持的平台

Microsoft Windows（32 位和 64 位）

- 内嵌：Windows XPE、7 Embedded、WEPOS、POSReady 2009、WES 2009、Embedded 8、8.1 Industry、10
- 服务器：Windows Server 2008、2008 R2、2012、2012 R2
- 桌面机：Windows NT、2000、XP、Vista、7、8、8.1 和 10

Linux

- Red Hat/CentOS 5、6、7
- SUSE/openSUSE 10、11
- Oracle Enterprise Linux 5、6、7
- Ubuntu 12.04

使用户成为解决方案的一部分

对于未知应用程序，McAfee Application Control 为 IT 部门提供了多种方式来让用户安装新应用程序。

- **用户通知** - 用户可收到提示性弹出消息，解释禁止访问未授权应用程序的原因。这些消息会提示用户通过电子邮件或服务台请求批准。
- **用户自我批准** - 具有此权限的用户不需要等待 IT 部门批准，就可安装新软件。IT 部门会检查这些自我批准的软件，并创建企业范围的策略，以禁止或允许该应用程序在所有系统中运行。

保持系统的最新状态

我们知道，保持您的系统安装最新的补丁很重要。这就是我们提供动态可信模型来自动更新您的系统却不影响业务连续性的原因。利用可信用户、证书、流程和目录来保持系统的最新状态。McAfee Application Control 还可以防止通过 Microsoft Windows 32 位系统和 64 位系统上的内存缓冲器溢出攻击来利用白名单应用程序的漏洞。

实现高级执行控制

为了加强保护，McAfee Application Control 可让您根据文件名、进程名、父进程名、命令行参数和用户名合并规则。您可以使用高级执行控制来阻止攻击，防止其绕过文件输入/输出 (I/O) 机制，为系统解释程序阻止交互模式，并防止对系统工具的利用。此外，您还可以获得更强大稳健的 SHA-256 算法来创建策略。

McAfee ePolicy Orchestrator 软件：单一控制面板

McAfee ePO 软件可合并和集中管理，提供企业安全状况的全局视图（无盲点）。这一备受赞誉的平台将 McAfee Application Control 与 McAfee Host Intrusion Prevention 及其他 McAfee 安全产品（包括黑名单的防恶意软件）相集成。McAfee Application Control 部署的一站式安装和更新也可以在 Microsoft System Center 中完成。

在观察模式下观看和学习

观察模式可以帮助您发现适用于动态桌面机环境的策略，而无需执行白名单锁定。同时还能让您在不断开应用程序的情况下，在预生产或早期生产环境中逐步部署 McAfee Application Control。通过 McAfee Application Control，管理员可以使用单个策略发现页面，为观察和自我批准请求定义策略。

保护旧版系统和最近技术投资

是否需要保护较旧的操作系统（如 Microsoft Windows NT、2000 和 XP）？尽管 Microsoft 和其他安全供应商不支持这些旧系统，但 McAfee Application Control 可以为这些系统提供保护。而且，McAfee Application Control 支持最新的操作系统，如 Microsoft Windows 10。

后续步骤

有关详细信息，请访问 **http://www.mcafee.com/cn/products/application-control.aspx**。请致电 400-610-0369 或 800-810-0369（周一至周五上午9 点至下午 6 点）。

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