McAfee Application and Change Control

全面防范对应用程序、端点、服务器和固定功能设备进行未经请求的更改和未经授权的控制

远程攻击或社会工程带来的高级持久性威胁 (APT) 导致为企业提供保护的难度日益增加，并且可能导致安全违规、数据丢失和服务中断。在当今不断发展的服务器和云环境中，尤其难以发现恶意更改。如果您的企业对抵御高级持久性威胁要求苛刻，不妨仔细了解一下 McAfee® Application and Change Control 软件。

McAfee® Application Control 可以帮助 IT 人员对付网络犯罪分子，为企业的安全和工作效率提供保障。利用动态可信模型、本地和全球信誉情报、实时行为分析和终端自动免疫功能，McAfee 的此解决方案可立即阻止高级持续性威胁 (APT)，无需进行耗工耗时的列表管理或签名更新。

McAfee® Change Control 软件可以阻止对关键系统文件、目录和配置进行未经授权的更改，同时简化新策略和合规措施的实施。凭借文件完整性监控和更改防护，McAfee Change Control 可实施更改策略，为关键系统提供持续监控。它还可以检测和阻止在分布式和远程位置执行不需要的更改。它的搜索界面非常直观，可以帮助用户快速找到更改事件信息的位置。

综合而言，McAfee Application and Change Control 仅允许对设备进行授权的访问，阻止未经授权的可执行文件，并采用系统方法监控和阻止对文件系统、注册表和用户帐户的更改，从而确保系统完整性。这有助于确保持续、高效的企业级检测和保护。

智能白名单

通过阻止未经授权的应用程序执行，而仅允许列入白名单的已知良好应用程序运行，从而防御零日威胁和高级持久性威胁 (APT) 攻击。McAfee Application and Change Control 根据应用程序和供应商对企业内部的二进制文件（.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。

主要优势

- 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和降低拥有成本。
- 在已连接或已断开的服务器、虚拟机、终端和固定设备（如销售点终端）以及传统系统上实行控制。
- 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。
- 为关键系统、配置和内容文件提供持续监控并实时管理更改。

联系我们

实施良好的安全计划

为了让应用程序在社交和云支持的业务世界有更大的灵活性，McAfee Application and Change Control 为组织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，如下所述：

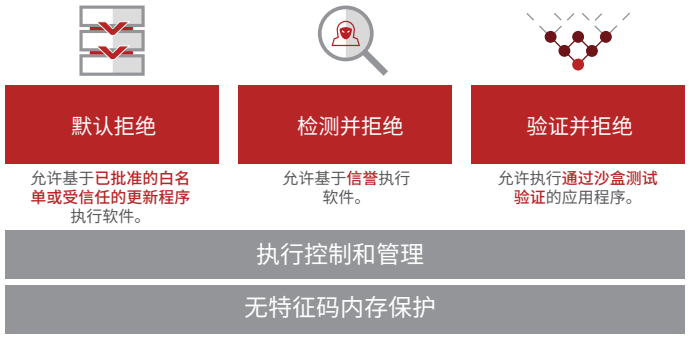

图 1. 充分发挥白名单策略作用的三种方式。

完成和快速响应

白名单利用 McAfee® Global Threat Intelligence 进行增强，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 使用这些知识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 and Change Control 会根据本地信誉情报更新白名单，从而即时抵御威胁。它还利用 McAfee Threat Intelligence Exchange 与 McAfee® Advanced Threat Defense 协作，从而在沙盒中动态分析未知应用程序的行为，并自动保护所有终端免受新检测到的恶意软件的攻击。

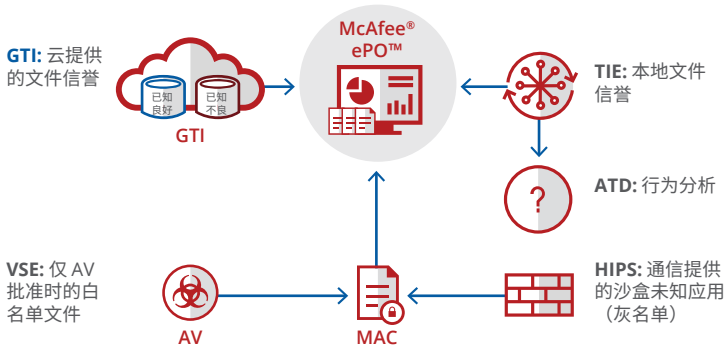

图 2. McAfee Global Threat Intelligence 和 McAfee Threat Intelligence Exchange 为 McAfee Application Control 提供全球和本地信誉。

主要优势（续）

- 防止未授权方篡改重要文件和注册表项。
- 通过前摄阻止进程外和不需要的更改支持紧凑的策略实施。

强有力的内置建议

清单搜索和预定义报告可帮助用户轻松管理与应用程序相关的文件和环境中的漏洞、合规性和安全问题。它还可以帮助您搜索有用的见解，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运行过期版本软件的系统。

清单模式是 McAfee Application and Change Control 8.3 中的新功能，可持续维护各系统/设备的最新清单。这样可以减少消耗的 CPU 和系统/设备资源，同时维护 SWAM/CPE 和 PCI-DSS 合规性。清单模式可以让用户长期跟踪端点上文件和二进制文件的更改。通用平台列举 (CPE) 可选择性地将 NIST CPE 数据与收集的清单相匹配，以便在创建白名单和报告合规性时使用。

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。

使用户成为解决方案的一部分

对于未知应用程序，McAfee Application and Change Control 向用户解释为何不允许访问未经授权的应用程序，并允许用户通过自我批准或批准请求，执行相应的步骤来批准应用程序。

保持系统的最新状态

利用最新补丁保持系统处于最新状态非常重要。McAfee Application and Change Control 的动态可信模型可自动更新系统，而不会影响业务持续性。利用可信用户、可信本地组、证书、流程和目录保持系统处于最新状态。McAfee Application Control 还可以防止通过 Microsoft Windows 系统上的内存缓冲区溢出攻击来利用白名单应用程序的漏洞。

更改防御和完整性监控

通常，“配置漂移”的可能性是存在的，而且并不清楚是谁执行了更改，这可能导致安全违规、数据丢失或服务中断。McAfee Application and Change Control 可以阻止或限制对系统/设备执行任何不符合策略的更改尝试。如果尝试执行更改，则会记录这种行为，并实时监控任何更改事件。系统控制器模块用于管理该系统控制器与各代理之间的通信。

支持的平台

McAfee Application and Change Control:

- 8.3.x、8.2.x、8.1.x、8.0.x、7.0.x（基于 Windows 的操作系统）
- 6.4.x、6.3.x（基于 Linux 的操作系统）6.2.x、6.1.x（基于 Windows 和基于 UNIX 的操作系统）
- Linux
- Microsoft Windows

下一层级文件完整性监控

McAfee Application and Change Control 支持以高效且经济的方式实时部署文件完整性监控 (FIM) 软件和执行 PCI-DSS 合规性验证。McAfee Application and Change Control FIM 可在同一位置集中为您实时提供执行更改的用户、时间、行为以及原因等基本信息，包括用户名、更改时间、程序名称和文件/注册表内容数据。此外，如果发生服务中断，它还可以在执行故障排除时帮助您找出根本原因。

跟踪内容更改

McAfee Change Control 可让 IT 人员跟踪文件内容和属性更改。您可以查看文件内容更改，您也可以进行并排对比，以查看添加、删除或修改的内容。您也可以配置包括/排除过滤器，从而只捕获相关的可操作更改。还可以按用户、本地用户组、应用程序、证书和/或 Web 服务限制系统和设备更改。您设置可以按特定时间和日期限制系统和设备更改（例如：仅允许星期二凌晨 2 点到 4 点之间应用 Windows 更新）。此外，专门的报警机制可立即针对重大更改向 IT 人员发出通知，从而防止与配置相关的服务中断，这是建议采用的信息技术基础架构库 (ITIL) 最佳实践。同时还会提供合格安全评估 (QSA) 表单，便于进行 PCI 报告。

防止计划外更改导致的服务中断

McAfee Change Control 使 IT 人员能轻松解决事件，自动执行监管合规控制，还能防止更改引起的服务中断。此外，它还可以消除往往与 Sarbanes-Oxley (SOX) 法规相关的容易出错的资源密集型手动合规策略需求。McAfee Application and Change Control 可让用户构建自动化 IT 控制框架，在单一报告系统中提供验证合规性所需的全部信息。针对授权的更改可以自动完成验证。紧急修复和其他进程外更改可自动归档并进行协调，以便审核。

集中的安全和合规管理

McAfee® ePolicy Orchestrator® (McAfee ePO™) 软件可合并和集中管理，从而提供企业安全的全局视图。这一备受赞誉的平台将 McAfee Application and Change Control 与 McAfee® Host Intrusion Prevention 和其他 McAfee 安全产品（包括黑名单的防恶意软件）相集成。McAfee Application and Change Control 部署的单步安装和更新也可以在 Microsoft System Center 中完成。您可以在任何位置及时激活新的配置文件来增强保护 — 从简单监控到采取应对措施。

后续步骤

自信地阻止或限制未经授权的应用程序，防止其以危及数据的方式执行，并采用系统方法来监控和阻止对文件系统、注册表和用户帐户的更改。McAfee Application and Change Control 仅允许对设备进行授权的访问，并且会阻止未经授权的可执行文件，从而确保系统完整性。

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）。

了解更多信息

有关详细信息，请参阅支持环境指南 — KB87944。

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