McAfee Embedded Control

为您依赖的设备提供简单安全防御功能

在当今不断扩大的攻击面中，非传统终端占据主导地位，这些终端包括可穿戴健身设备，以及控制发电和配电的关键联网传感器。随着联网设备数量的增多，遭受恶意软件和攻击侵害的风险也就越来越大。McAfee® Embedded 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。

McAfee Embedded Control 主要解决因在嵌入式系统中采用商业操作系统而引发的越来越多的安全风险问题。McAfee Embedded Control 是一种小型解决方案，它独立于应用程序、投入低，可提供“部署和忽略”安全防护。McAfee Embedded Control 可将构建于商业操作系统之上的系统转换为“黑盒子”，因而看起来像是一个封闭的专有操作系统。防止执行磁盘上的任何未授权程序或注入内存的任何未授权程序，同时阻止对授权基准进行未经授权的更改。此解决方案可帮助制造商畅享采用商业操作系统的各种优势，而不必承担额外的风险，也不会导致现场使用的系统失控。

保障系统完整性

执行控制

采用 McAfee Embedded Control 后，仅会执行 McAfee 动态白名单中所包含的项目。其他程序（exe 文件、dll 文件和脚本）均视为未经授权项目。默认情况下，系统将会阻止执行这些项目，并且会对这一失败进行记录。这样便可有效防止自行安装的蠕虫、病毒、间谍软件及其他恶意软件的非法执行。

内存控制

内存控制可确保运行的进程得到保护，有效防止恶意劫持。抑制、终止并记录注入运行进程的未授权代码。这样，便可以消除妄图通过缓冲区溢出、堆溢出、堆栈执行及类似的漏洞控制系统的操作影响，并会对此加以记录。[1]

主要优势

- 通过控制您的嵌入式设备上运行的程序及保护这些设备的内存安全，最大限度地降低安全风险。
- 让您轻松访问、持续控制、降低支持成本。
- 选择性实施。
- 部署和忽略。
- 让您妥善完成设备合规和审核工作。
- 实时监控。
- 全面审核。
- 更改存档可供搜索。
- 闭环协调。

McAfee GTI 集成：为分离环境处理全球威胁的智能方式

McAfee® Global Threat Intelligence (McAfee GTI) 是 McAfee 专用技术，可通过全球范围内数百万个传感器实时追踪文件、邮件和发件人的信誉。此功能使用基于云的信息来确定位于您的计算环境中的所有文件的信誉，将其分为良好、不良和未知三类。利用 McAfee GTI 集成，您可以确切地了解到何时有恶意软件不经意地列入了白名单。在连接 Internet 或独立的 McAfee® ePolicy Orchestrator® (McAfee ePO™) 软件环境中均可以获取 GTI 信誉。

更改控制

McAfee Embedded Control 会实时监测更改。它能够监控更改来源，并验证更改已部署到正确的目标系统。它还能够提供更改的审核跟踪报告，仅允许更改以授权方式进行。

McAfee Embedded Control 允许您通过指定更改的授权方式，实施更改控制过程。您可以控制哪些人能够应用更改、需要具备哪些证书才能允许做出更改、能够更改哪些项目（例如，您可以将更改限定至特定的文件或目录范围），以及何时能够应用更改（例如，只能在一周的几个特定时间才能更新 Microsoft Windows）。

主动式更改会在将每项更改应用至目标系统前对其进行验证。启用此模块后，只能以受控方式进行软件系统更新。

跟踪模块的实时更改可记录对系统状态（包括代码、配置和注册表）做出的所有更改。在发生更改事件时对其进行实时记录，并发送到系统控制器进行汇总和存档。

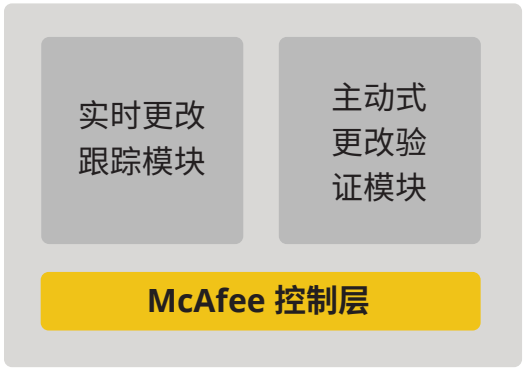

图 1. McAfee 控制层。

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。它会在独立记录系统中汇总和存储来自代理的更改事件信息。

图 2. 报告、搜索和分析模块。

审核与策略合规

McAfee®IntegrityControl将提供仪表板和报告协助您满足合规要求。这些仪表板和报告均从 McAfee ePO 控制台生成，从而为用户和管理员提供基于 Web 的 UI。

McAfee Embedded Control 可提供集成式的闭环实时合规与审核功能，辅以防篡改记录系统用于记录授权活动和未授权尝试。

关于 McAfee 嵌入式安全

McAfee 嵌入式安全解决方案可帮助制造商确保其产品和设备得到保护，防止遭受网络威胁和攻击。McAfee 解决方案跨越范围广泛的各种技术，包括应用程序白名单、防病毒和防恶意软件保护、设备管理、加密以及风险和合规技术，所有一切均采用业内领先的 McAfee Global Threat Intelligence。我们的解决方案可以量身定制，以满足制造商设备及其体系结构的特定设计要求。

产品简介

功能	描述	优点
保障系统完整性		
外部威胁防御	确保只能运行授权代码。非授权代码无法注入内存。无法篡改授权代码。	▪ 取消紧急修补功能，减少修补周期的数量和频率，从而在修补之前完成更多测试，降低难以修补的系统的安全风险。 ▪ 降低通过蠕虫、病毒、特洛伊木马程序及代码注入（如缓冲区溢出、堆溢出和堆栈溢出）开展的零日攻击和变形攻击所带来的安全风险。 ▪ 维护授权文件的完整性，确保生产系统处于已知的验证状态。 ▪ 通过限制计划内修补和恢复停机时间降低运营成本，并提高系统可用性。
内部威胁防御	本地管理员锁定技术能灵活地禁止用户（甚至管理员）更改受保护系统上运行的授权内容，除非提供真实可信的密钥。	▪ 抵御内部威胁。 ▪ 锁定嵌入式生产系统上运行的内容，防止用户（甚至管理员）进行更改。
高级更改控制		
保护制造商授权更新的安全	确保现场采用的嵌入式系统上只能执行授权更新。	▪ 确保现场采用的系统上不能部署带外更改。在未授权系统更改造成业务中断及发出支持呼叫前预先做好防护工作。 ▪ 制造商可以选择继续自行控制所有更改，也可以仅授权受信任的客户代理控制更改。
确认更改发生在经过批准的窗口内	确保并未在授权更改窗口以外部署任何更改。	▪ 防止在财务敏感期或业务高峰期进行未授权更改，以防止运营中断和/或违规。
已授权更新	确保只有已授权更新（人员或程序）才能在生产系统上执行更改。	▪ 确保无法在生产系统上部署任何带外更改。
闭环实时审核与合规		
实时更改跟踪	于发生更改时立即在整个企业内进行跟踪。	▪ 确保无法在生产系统上部署任何带外更改。
全面审核	为每一次系统更改捕获完整的变更信息：是谁于什么时间在哪个位置通过何种方式做出了哪些更改。	▪ 保留所有系统更改的准确、完整和明确的记录。
确定更改来源	将每一次更改都与其来源关联起来：做出更改的人员、完成更改的事件顺序，以及对其产生影响的进程/程序。	▪ 验证经过批准的更改，快速识别未经批准的更改，提高更改成功率。

功能	描述	优点
运营费用低		
部署和忽略	在数分钟内完成安装，无需初始配置或设置，也无需后续配置。	▪ 开箱即用。安装后立即生效。不会产生任何持续维护费用，因此是低运营成本安全解决方案配置的理想选择。
无规则、无签名、无学习周期，且独立于应用程序	不依赖规则或签名数据库，无需经过学习周期立即在所有应用程序中生效。	▪ 在服务器生命周期中，管理员极少需要加以关注。 ▪ 以较低的持续运营成本保护服务器直至修补或分离服务器。 ▪ 其有效性不依赖于任何规则或策略的质量。
内存需求量小、运行时费用低	占用的磁盘空间小于 20 MB。不会对应用程序的运行时性能产生任何干扰。	▪ 随时可在任何任务关键生产系统上进行部署，而不会影响其运行时性能或存储要求。
保证不存在任何误报或漏报情况	仅记录未经授权的活动。	▪ 相较于其他主机入侵防护解决方案，通过大幅降低每日/周分析日志所需的时间，其分析结果准确性便可减少运营成本。 ▪ 提高管理员工作效率，降低运营成本。

后续步骤

有关更多信息，请访问 **www.mcafee.com/cn/partners/oem-alliances/index.aspx**，或者与您当地的 McAfee 代表联系。

1. 仅适用于 Microsoft Windows 平台。

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