McAfee Change Control

防止未经授权的更改。自动执行监管合规控制。

目前在许多企业中服务器环境的更改时刻都在发生，但我们未能察觉。这种情况无论从安全方面还是合规性方面考虑，都是十分危险的。McAfee® Change Control（McAfee 产品的一部分）可以持续不断地对整个企业内发生的授权更改执行检测。可以阻止对关键系统文件、目录和配置的未授权更改，同时简化新策略和合规措施的实施。

McAfee Change Control 软件消除了当今企业环境中过于频繁的更改活动。更改活动可能会导致安全违规、数据丢失和服务中断。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。它还会检测各分散位置和远程位置的更改，并组织不必要的更改。

凭借直观的搜索界面，McAfee Change Control 可帮助用户快速找到更改事件信息。例如，您可以在该界面上查询 xyz.acme.com 服务器上对 c:\windows\system32 目录中内容所做的所有更改的相关数据。

下一层级文件完整性监控

支付卡行业数据安全标准 (PCI DSS) 第 10 条和第 11.5 条要求对网络资源和持卡人数据的访问进行追踪和监控，并部署文件完整性监控 (FIM) 工具，让相关人员警惕对关键系统、配置和内容文件的未授权修改。McAfee Change Control 让您能够运用实时 FIM 软件以经济高效的方式验证 PCI 合规性。McAfee Change Control FIM 可以提供当事人、时间、事件以及原因等必要信息。它可以在同一位置集中为您实时提供用户名、更改时间、程序名称及文件/注册表内容数据。此外，如果发生服务中断，它还能在故障排除时帮您找出根本原因。

主要功能

- **文件完整性监控：**持续跟踪文件和注册表项更改并确定哪些人员对哪些文件进行了更改。
- **更改防护：**可以保护您的关键文件和注册表项，使其免遭未授权篡改，从而只允许根据更新策略执行的更改。

内存需求量小且运行开销低

- 设置简便，初始和后续运行开销均很低
- 内存使用量可忽略不计
- 不执行可能影响系统性能的文件扫描

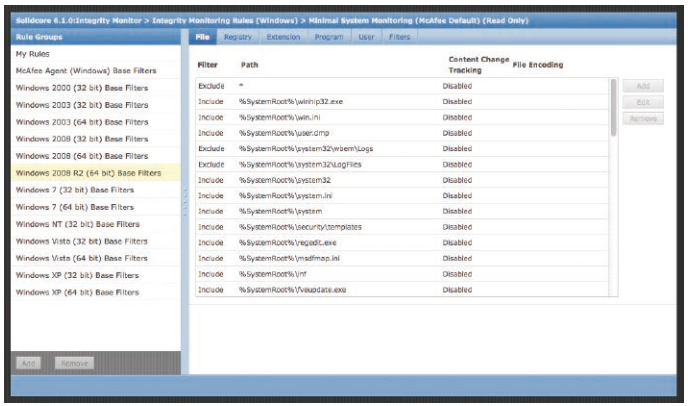

图 1. McAfee Change Control 的特色在于具有现成的 FIM 规则和精细的过滤器，只会监控相关文件。

跟踪内容更改

McAfee Change Control 可让您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。这非常便于解决与配置相关的服务中断问题。

可配置包括/排除过滤器，从而只捕获相关的可操作更改。此外，专门的报警机制可立即针对重大更改向您发出通知，便于您防止与配置相关的中断，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，McAfee Change Control 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 Change Control 可让您构建自动化 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 ePO 软件可合并和集中管理，提供企业安全状况的全局视图。该软件能让您灵活调整覆盖的系统类型或范围，并让您决定更改警报中应包含哪些文件、目录和配置，同时确定警报的优先级。针对最常见的服务器操作系统和企业应用程序开发的默认配置文件可用于监控关键组件，而无需从头开始创建新的配置文件。借助 McAfee Change Control 和 McAfee ePO 软件，可以在任何位置及时激活新的配置文件以增强保护 - 简单监控到采取应对措施均可。

McAfee ePO 软件可伸缩且易于扩展。它可以将 McAfee Change Control 软件和我们的其他安全管理产品与我们合作伙伴的产品集成到一起。

主要优势

- 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
- 防止未授权方篡改重要文件和注册表项
- 支持文件完整性监控系统实现 PCI DSS 监管要求
- 简化入门操作的现成 FIM 规则
- QSA 友好报告，便于进行 PCI 报告
- 单击排除项功能可避免追踪无关信息
- 通过提前阻止进程外和有害的更改实现紧凑的策略实施
- 与 McAfee ePolicy Orchestrator® (McAfee ePO™) 控制台集成以便实施集中 IT 管理

实施改变一切

McAfee Change Control 软件会对您的服务器上的所有尝试更改进行实时追踪和验证。该软件可以规定必须在某一时间段内由受信任来源或借助已批准的工作票证来执行更改，从而实施更改策略。可以对 McAfee Change Control 软件的更改防护组件进行微调，从而允许本机应用程序不间断持续更新其文件，而同时禁止任何其他应用程序或用户执行更改或读取特定的文件。

最大限度地降低风险并加强多方面的合规性

我们可提供大量风险与合规解决方案，帮助您降低风险，自动执行合规工作并进行安全优化。尤其值得一提的是，McAfee Change Control 与 McAfee Application Control 结合使用能形成消除漏洞并确保整个企业合规性的强大产品组合。

后续步骤

McAfee Change Control 软件消除了服务器环境中可能会导致安全违规、数据丢失和服务中断的更改活动，让您能够轻松地满足监管合规要求。现在可以利用 McAfee Change Control 防止未经授权的更改，同时自动执行监管合规控制。

支持的平台

Microsoft Windows（32 位和 64 位）

- 内嵌：Windows XPE、7E、WEPOS、Pos Ready 2009、WES 2009
- 服务器：Windows NT、2000、2003、2003 R2、2008、2008 R2、2012
- 桌面机：Windows XP、Vista、7

Linux

- RHEL 5、6
- Suse 10、11
- CentOS 5、6
- OEL 5、6
- SLED 11
- OpenSUSE 10/11

AIX

- AIX 6.1、7.1

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