

McAfee Change Control

持续防范未经授权的变更



在许多 IT 机构中，经授权并归档的变更和实际变更活动之间存在间隙。对于拥有众多合规法规的企业而言，如果能够监控文件和配置变更并集中执行变更授权策略，则会将可用性和可审计合规性提升至一个新的高度。借助 McAfee® Change Control，您可以轻松指定变更事件通知并确定通知优先级，以实现最有效的管理。对于文件或配置设置这样的关键系统组件，McAfee Change Control 可以通过阻止变更功能来全面防范未经授权的变更。

目前，大部分 IT 机构都投资部署了流程自动化工具，例如，变更管理系统或服务台。不过，实际变更活动与归档变更管理流程或书面策略之间始终存在着间隙。这一变更控制间隙致使 IT 部门要承担繁重的人工操作来支持审核和协调事件，因为必须通过人工方式验证根据所请求的变更工作或问题工单所进行的系统层实际变更。此外，通常还会在未验证和确认情况下执行临时变更，这可能会影响系统安全配置设置，导致系统背离企业策略或影响服务器的性能和可用性。通过对授权变更执行集中的或预定的信任模型（变更时间窗、变更源或批准用户），McAfee Change Control 软件可以将变更成本降至最低，同时还可提供持续的文件完整性监控。

借助 McAfee ePolicy Orchestrator® (McAfee ePO™) 管理控制台，企业可以灵活地调整要涵盖的系统类型或范围。另外，企业还可以确定变更警报应包括的文件、目录或配置以及警报优先级。可以利用我们为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来监控关键组件，而无需从头创建新的配置文件。

您可以随时激活新的配置文件，将保护从仅限于监控提升到策略执行，从而有效阻止对文件、目录或配置进行任何变更，除非是从可靠来源启动变更。可以调整变更防止功能，以允许本机应用程序继续在不中断的情况下更新其文件，同时禁止所有其他应用程序或用户进行任何变更，甚至通过 McAfee Change Control 软件的读/写保护功能禁止读取这些文件。

McAfee Change Control 软件为企业提供了持续检测对分布式和远程位置所做的变更，并提供变更防止功能来拦截不合规的变更。它还提供直观的搜索界面来帮助用户快速查找变更事件信息。例如，您可以通过搜索界面查询并找到包含对 c:\windows\system32 目录和服务器 xyz.acme.com 所做的全部变更的报告。通过为企业提供 IT 控制来进行变更管理，McAfee Change Control 软件可以有效地为企业弥合间隙。该解决方案使 IT 部门能够轻松实现 PCI 和 SOX 控制自动化，以确保合规，并通过防止变更导致的中断，显著提高服务可用性和加快信息技术基础设施库 (ITIL) 采用。McAfee Change Control 软件操作简便、占用资源少，而且几乎无需人工干涉，可以部署于各种服务器硬件平台。

持续变更控制

与基于扫描的获取系统状态“快照”并进行比较的解决方案不同，McAfee Change Control 软件可以实时根据定义的变更控制配置文件持续跟踪和验证服务器上的每个尝试变更。

McAfee Change Reconciliation 软件可与 McAfee Change Control 软件配合使用，能够将对服务器的变更与在现有工单系统中归档的变更工单相关联，并与常用的变更管理系统（例如，HP Service Manager 和 BMC Remedy）集成。另外，McAfee Change Reconciliation 还集成了常用的配置管理数据库 (CMDB)，例如，BMC Atrium 和 HP Universal CMDB。作为问题工单或工作单一部分的变更详细信息被封装并纳入工单系统，使企业不仅可以跟踪工作流程，而且还能跟踪已完成工作的系统级详细信息。

企业解决方案

符合并持续满足 PCI DSS 合规

确保遵从归档支付卡行业数据安全标准 (PCI DSS) 要求企业和服务提供商必须满足 12 大类中的约 180 项要求。不过，根据最新研究，要求使用文件完整性监控和审计轨迹的 PCI DSS 第 10 类和第 11 类被证明是最难履行和最难让人满意的规定。这些要求难以满足的原因是现有的工具仅提供“定期的”文件完整性监控功能，而这些功能是通过资源密集型系统扫描来检测变更。McAfee Change Control 软件可对 IT 基础设施提供绝对控制，使零售商和处理信用卡交易的机构能够履行苛刻的 PCI 要求，并可经济高效地验证 PCI 合规。

为帮助各种规模的企业轻松且经济高效地满足 PCI

DSS 第 1、10 和 11 类规定的文件完整性监控和审计轨迹要求，我们推出了 McAfee Change Control 和 McAfee Integrity Monitor 软件。作为全面的 PCI 合规策略的基本要素，许多世界领先的合格安全评估机构 (QSA) 正在对这些解决方案进行认证并推荐使用。

萨班斯-奥克斯利和用于其他合规法令的 IT 控制
萨班斯-奥克斯利 (SOX) 法案促进了公司治理的根本性转变。现在的企业平均必须满足四项合规标准。随着企业对满足多层次合规需求的重视，有一点是很明确的：合规不是一次性项目，而是持续地努力监控和保证业务流程和安全。为满足这些严格的法规遵从要求，许多企业已实施合规策略，但这些策略的缺点是人工操作、容易出错，并耗费大量资源。

通过利用 McAfee Change Reconciliation 软件构建自助式、自动化的 IT 控制框架，McAfee Change Control 软件已帮助众多客户解决了其所面临的复杂的合规挑战，在单一报告系统中即可获得验证合规所需的所有信息。迈克菲解决方案的持续变更检测功能以及自动化、高度准确的 Change Reconciliation 选项提供了一种自动化方法来验证变更是否获得授权。为便于审计，会自动归档和调整进程外变更（例如，紧急修复）。使用 McAfee Change Control 软件进行 SOX 审计的客户已在降低风险和成本方面获得了显著的优势。大多数情况下，第一阶段的优势是对现有人工控制实现自动化。第二阶段的优势是通过向审计人员证明控制功能已内置于环境中，从而合理地精简控制集。

优化安全与合规

大多数中型和大型企业正在寻找新的途径来提高安全和合规的运营效率。如果变更环境不受控制，在自动化和效率方面的所有投资都得不到应有回报，因为您投资的安全环境极不稳定。阻碍项目成功的主要文化壁垒是如何向企业证明能够收回投资，特别是在项目很大，需要多阶段实施的情况下。客户使用 McAfee Change Control 软件可以显著加快他们收回业务投资的步伐，并实现更高的 IT 可用性。部署 McAfee Change Control 软件后，它会维持一个支持自动化的持续受控环境。客户可以通过 McAfee ePO 管理平台监控变更，该平台是个中央控制台，您可以在具有直接影响的本地和分布式服务器上选择性地实施变更策略。

后续步骤

要了解详细信息，请访问 www.mcafee.com/Changecontrol，或联系您所在地的迈克菲代表或离您最近的经销商。

关于迈克菲风险和合规产品

使用迈克菲风险和合规产品，您可以最大限度地降低风险、自动实现合规和优化安全。我们的解决方案可以诊断您的环境，实时洞察您的漏洞和策略，以便您可以保护最重要的资产，将您的安全投资用在最重要的地方。要了解更多信息，请访问：www.mcafee.com/riskandcompliance。

本文档所提供的信息仅用于培训目的和为迈克菲用户提供便利。本文档包含的信息如有更改，恕不另行通知。这些信息“按现状”提供，对其准确性或这些信息对任何特定情况的适用性不做任何保证。

McAfee、McAfee 徽标和 McAfee ePolicy Orchestrator 是 McAfee, Inc. 或其分支机构在美国及其他国家/地区的注册商标或商标。其他商标和品牌可能是其各自所有者的财产。版权所有 © 2010 McAfee, Inc.



迈克菲（上海）软件有限公司