

McAfee Total Protection for Server

极大地改善安全状况，同时保持系统的可用性和正常运行时间

对于 IT 部门来说，一方面要保证正常运行时间和服务器可用性，另一方面要确保服务器及其数据得到妥善保护，如何实现两者之间的平衡，是必须面临的巨大挑战。这种情况往往会导致 IT 部门为确保正常运行时间不得不在安全上做出让步，但此举很容易使服务器遭受恶意软件威胁、内部攻击和数据泄露的风险。

借助一款统一的安全与合规解决方案 McAfee® Total Protection™ for Server（包括单一管理平台和多项用于维护系统可用性并确保最优安全的轻型组件），迈克菲重新诠释了企业服务器安全的概念。这款解决方案可以有效减少流程管理时间，降低硬件要求，从而使效率水平得到显著提升。

主要优势

极大地改善安全状况，维持正常运行时间和可用性

显著提升效率，减少流程管理时间并节省开支

灵活的交付模式，可以适应各种部署方案

有效减轻数据泄露和内部攻击风险

充分利用您在 McAfee ePolicy Orchestrator® (McAfee ePO™) 软件方面的安全投资

非常适合应用程序、文件服务器和数据中心使用

McAfee Total Protection for Servers 整合了：

- McAfee VirusScan® Enterprise 软件
- McAfee VirusScan Enterprise for Linux 软件
- McAfee Application Control for Servers 软件
- McAfee Change Control for Servers 软件
- McAfee Policy Auditor 软件
- McAfee ePolicy Orchestrator 软件

为了维持服务器的可用性，许多企业不得不以牺牲安全为代价（选择性地使用防病毒软件）。传统的安全解决方案会产生延迟、影响服务器运行，而且会导致关键流程和应用程序中断。随着威胁形势的不断变化，服务器将成为头号攻击目标。据 SANS 统计，2009 年针对 Web 服务器的攻击占到了全部攻击的 60%。黑客伺机潜入企业网络窃取有价值的敏感信息。企业当务之急就是找到一种有效的方法，在确保最佳安全的同时，不对可用性和正常运行时间产生负面影响。

McAfee Total Protection for Server 强势出击

McAfee Total Protection for Server 经过独特的架构设计，旨在保护您的关键任务服务器及其中的数据，同时维持关键应用程序和流程的处理能力。借助 McAfee Total Protection for Server，企业可以全面监控并控制敏感数据和系统的访问，从而高效管理风险及详细合规报告。而且，它对初始安装和后续运行开销的要求都非常低。

通过优化的安全保证可用性和正常运行时间

组合使用黑名单（防病毒）、动态白名单以及强大的变更管理控制（可进一步减轻针对性攻击和数据泄露风险），可以实现全面的威胁拦截。同时，通过确保只有经过授权的程序和代码可以运行，集成的轻型安全组件还能够保持关键应用程序的处理能力。

提高运营效率

在单一解决方案中组合安全与合规两方面的功能，有助于减少流程管理时间和所需的硬件数，从而大大节省开支。而通过单一解决方案同时满足应用服务器和文件服务器的安全需求，则有助于整合许可，进一步提高成本效益。

企业可以根据自己的部署方案灵活选择配置选项和要运行的组件。集中的管理为添加和删除组件以及更改配置选项提供了便利。

规格

支持的操作系统

Microsoft

- Microsoft Windows 2000/2003/2008/ 2008 R2, 7
- Microsoft Windows XP

Linux

- RedHat
- Centos 4/5

其他

- Oracle EL 5
- Solaris 8/9/10

McAfee VirusScan Enterprise 软件、McAfee Application Control 软件、McAfee Change Control 软件和 McAfee Policy Auditor 软件分别支持其他操作系统。

实现持续合规性

强大的变更策略管理和持续的文件完整性监控提供了长期有效的合规模式。对于 PCI-DSS 这类需要测试和验证安全控制的合规标准，它能够针对服务器级别的变更提供警报和丰富的可审核数据。同时，内置的主要法规和行业安全策略模板，可使企业轻松评估并证明其遵从了主要策略和标准。

主要特性

- 通过组合使用黑名单和白名单，能够最大程度地防范当今各种威胁
- 阻止执行未经授权的代码、脚本和 DLL，并通过内存保护和内存扫描进一步防范内存漏洞
- 应用程序控制和变更策略管理所需的开销极低，可以最大限度地降低对 CPU 周期的影响
- 安装简便，初始安装及后续运营开销较低
- 可以轻松适应连接或断开的服务器和终端中的现有变更流程
- 具有设备的物理访问或远程访问权限的管理员无法改写保护
- 集中管理有助于进一步降低 IT 开销。

运营流程

McAfee Total Protection for Server 经过独特的架构设计，可以与 IT 运营流程无缝整合。通过组合使用策略审核、黑名单和白名单，企业不仅可以定义并切换到良好状态，而且可以锁定系统配置。策略审核提供了用于报告的最佳模板。

McAfee ePO 平台可以整合并集中执行所有迈克菲产品的管理

通过使用单一的集成管理平台，企业可以大大减少通过多个控制台管理终端安全所需的 IT 管理人员。借助 McAfee ePO 平台，企业能够：

- 通过基于 Web 的单一管理平台访问集中的事件监控、报告、信息显示板和工作流程
- 通过单一管理平台部署、管理和升级代理及策略
- 提供丰富的取证分析和审核报告功能，降低总合规成本

可与其他迈克菲解决方案集成和兼容

McAfee Total Protection for Server 可采用不同的网络拓扑和防火墙配置工作。它能够与多款迈克菲解决方案无缝集成，包括：

- McAfee Vulnerability Manager, 可让企业利用无代理策略合规扫描以及网络级漏洞扫描
- McAfee Endpoint Encryption, 可让企业按照主要法规的要求，对重要文件进行加密
- McAfee Total Protection for Endpoint, 使客户从增强的终端和服务器控制中受益

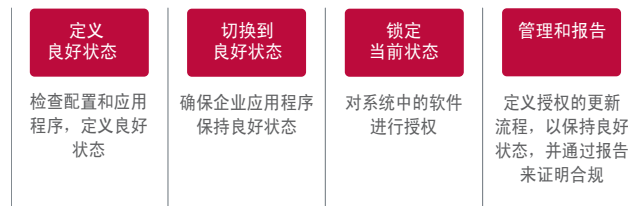


图 1. McAfee Total Protection for Server: 运营流程。

McAfee、迈克菲、McAfee 徽标、McAfee Total Protection、McAfee ePolicy Orchestrator 和 McAfee ePO 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。其他标记和品牌可能是其各自所有者的财产。此处提及的产品计划、规格和说明仅供参考，如有更改，恕不另行通知，迈克菲对此不作任何明示或暗示保证。Copyright © 2010 McAfee, Inc. 9276ds_tops_server_0410_fnl_ASD



迈克菲（上海）软件有限公司