McAfee DLP Manager

集中管理 McAfee DLP 设备

主要优势

集中系统管理
- 统一策略和规则
- 简化事件工作流程
- 提供全面而灵活的报告
- 配置和管理设备

整合案例管理和工作流程
- 集成常见事件
- 转移所有权和补救措施
- 使用基于角色的访问权限和许可对用户进行限制

搜索、发现和分析数据
- 快速搜索历史数据
- 查找敏感数据并了解其使用情况
- 快速调整规则并实时进行验证
- 执行用户调查

使用不同方式对事件进行过滤和分组
- 列出事件并对其进行分组和汇总
- 自动分配事件
- 对事件进行动态过滤和分组
- 显示误报工作流程

如今，很多企业习惯将数量巨大的电子信息存储在自己的网络中。无论是通过电子邮件或即时消息 (IM) 发送这类信息，还是将它们存储到数据库或文件共享系统，亦或是下载到 USB 设备后转移到其他位置，它们始终都摆脱不了业务关键性或者敏感性这一特质。了解网络中存在哪些信息、是不是敏感信息、哪些人在访问这些信息以及访问信息的方式，对于每个企业的安全策略来说至关重要。这类敏感信息绝对不容丢失或受到安全威胁。为了降低数据丢失风险，企业必须知道哪些信息属于敏感信息、哪些不是，并要能够借助单一且直观的管理控制台管理对其的访问、存储、传输和使用。

端到端数据丢失防护管理

McAfee® Data Loss Prevention (DLP) Manager 专为在网络中部署了多个 McAfee DLP 设备的大中型环境而设计。McAfee DLP Manager 可以通过直观的集中管理界面提供对这些设备的完整控制。

借助 McAfee DLP Manager，您可以通过单一视图集中查看分布在网络中的所有 McAfee DLP 设备和主机代理。这能使 McAfee DLP 学习应用程序充分减少确认和保护敏感数据相关的时间和成本。

McAfee DLP Manager 通过使您从中央控制台掌控这些功能，为您节省管理和维护信息安全基础设施的总运营成本：

- 管理所有策略和规则
- 访问事件和案例管理工作流程
- 针对一个或多个 McAfee DLP 设备进行搜索
- 配置和监控多个 McAfee DLP 设备

协同性事件工作流程和案例管理

McAfee DLP Manager 提供了覆盖整个企业环境的许可和工作流程框架，以及基于角色的访问控制功能。同一企业的多个用户可就事件工作流程和案例管理进行协作。

McAfee DLP Manager 支持跨部门参与，因此，您无需增添所需的支持人员即可实现信息防护的扩展。它还可以在事件检查、分析和补救过程中借助主题专家（例如法律人员、人力资源人员和内容或业务所有者）的力量。同时，这些专家还能帮助您确定应该保护的数据。

基于角色的事件视图控制

借助基于角色的全面访问控制，您可以获得宏观的风险报告和统计数据以及可能直接影响到企业责任的微观事件信息和行为。您可以通过角色权限控制这些视图，确保用户只能看到与其职务相关的事件。例如，基于角色的访问控制功能可以确保从事法规遵从工作的用户无法执行特定的管理任务。它还可以确保这一用户看不到知识产权事件，或者防止某内容所有者查看与隐私或法规遵从性数据相关的事件。

集中的策略和规则

- 自动为特定或全部 McAfee DLP 设备分发策略和规则
- 配置和分发操作规则，包括电子邮件通知、加密、拦截、隔离、重定向和退回

事件工作流程

- 将事件关联集中到统一的事件信息显示板
- 借助嵌入式案例管理工具逐步上报事件
- 将特定案例的责任分派给关键用户
- 使用误报工作流程消除误报现象
- 自动更新受工作流程变动影响的规则

案例管理

- 整合并解决需要补救且涉及相同利益相关者的组相关事件
- 实施灵活的事件和案例逻辑 — 多个事件可以属于同一案例，或者单个事件可以属于多个案例
- 将事件逐步上报给不同的团队
- 访问附有说明的案例历史记录审计线索
- 导出案例以供脱机查看
- 如果对案例进行了更改，则通过电子邮件给案例拥有者发送通知

报告和事件

- 访问集中视图，查看任何 McAfee DLP 设备或网络中 McAfee DLP Endpoint 代理所生成的所有事件
- 生成涉及一个或多个甚至所有 McAfee DLP 设备的报告
- 借助 50 个打包报告自动生成报告，这 50 个报告均可以配置，通过预定时间，这些报告能以 PDF 和 CSV 格式通过电子邮件自动发送

动态过滤

- 快速过滤信息，以便查看特定数据
- 通过点击表格视图中单元格的内容可以自动填写过滤
- 动态添加、删除和合成过滤

预配置角色

- 使用企业内各团队主要成员的预配置角色（包括管理员、法律人员、人力资源人员、合规人员、运营人员和信息安全人员）加快设置的速度
- 只需点击几下鼠标便可定义其他角色
- 详细为角色分配权限
- 与 LDAP 或 Microsoft Active Directory 集成，实现集中的身份验证服务

集中的设备管理

- 从单一界面配置和管理 McAfee DLP 设备
- 检查受管理 McAfee DLP 设备的状态，包括 CPU 利用率、硬盘利用率和网络流量
- 查看受管理 McAfee DLP 设备生成的所有修补警报和警告

规格：McAfee DLP 4400 设备

组件	说明
主板	Intel TimberCreek 系统 (S5520URR)
CPU	2 X Intel X5660 12M 缓存，2.8GHz（六核）
内存	24 GB P1333 DDR3 内存
RAID 控制器	Intel RS2MB044 RAID 控制器
电源	2 X 760 W 热插拔电源模块
硬盘	12 X Seagate Constellation ES 1T 7200 rpm 3 1/2" SATA 硬盘
NIC 卡	Intel Dual Copper 1Gbps 以太网 I/O 模块
DVD 光驱	SATA DVD ROM
IPMI	Intel 远程管理模块 3 (AXXRMM3)
产品大小	2 机架单位 (2U)

规格：虚拟机

McAfee DLP Discover 可以作为虚拟机运行于 VMware ESX 或 VMware ESXI 4.1 服务器上。以下是运行虚拟机的一些最低硬件要求。

组件	要求
CPU	Intel 四核
内存	8 GB RAM
硬盘	硬盘 1：最小容量，128 GB - VM 软件 硬盘 2：最小容量，640 GB - DLP 虚拟镜像
网络端口	1 个用于 McAfee DLP Discover 应用程序的端口
BIOS	启用 VT 线程

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

39705ds_dlp-manager_1111