McAfee Enterprise Log Manager

借助自动化日志收集、存储和管理来削减合规成本。

通过正确地收集和存储日志，您可以借助具有不可否认性且清晰的活动审核记录来降低合规成本。McAfee® Enterprise Log Manager 可有效收集、压缩和存储所有日志文件。与 McAfee Enterprise Security Manager 的集成可提供高级搜索、分析、关联、警报及报告功能。所有事件和警报均提供对原始来源日志记录的轻松一键访问，从而使您的取证工作也能从中受益。

主要优势

- 可满足合规要求的通用日志收集和保留功能
- 适用于每个日志来源的灵活存储和保留功能
- 支持监管链和取证
- 日志分析和搜索
- 在本地或通过托管的存储区域网络来存储日志
- 与 McAfee® Enterprise Security Manager 完全集成
- 灵活的混合交付选项包括物理设备和虚拟设备

只要是日志文件，McAfee Enterprise Log Manager 都可以对其进行收集、签署和存储。McAfee 可针对所有日志类型自动执行日志管理和分析，包括 Microsoft Windows 事件日志、数据库日志、应用程序日志和系统日志。日志经过签名和验证，从而确保真实性和完整性，这是法规合规性的一项必然要求。现成可用的合规规则集和报告可轻松证明您公司的合规状态及策略实施情况。

采用这一紧密集成的日志收集、管理和分析环境既能增强您的安全状况，又能显著提升遵循 PCI DSS、HIPAA、NERC-CIP、FISMA、GLBA 及 SOX 等标准的能力。

智能日志管理

McAfee Enterprise Log Manager 可以智能地收集日志、存储正确的合规日志，并解析和分析这些日志以确定其安全性。您可以根据需要以原始格式将日志保留任意时长，以满足特定的合规需求。由于我们不会更改原始日志文件，因此 McAfee 可支持监管链和不可否认性。

信息保留需求千差万别，具体取决于日志来源以及您必须满足的不同合规要求。McAfee Enterprise Log Manager 使用易于定制的存储池来确保您的日志能够正确地存储适当的时间长度。选择能够满足您需要的最佳存储选项：设备上的硬盘存储，以及可选的适合高速存储区域网络 (SAN) 的光纤通道卡。

仅凭日志文件无法向我们提供所需的全部信息。这些文件包含重要的证据，是建立监管链的关键环节，但也会引发重要的安全问题。例如，我们可能会在访问日志中看到某个用户名，但找不到任何有关该用户的角色或权限的信息。我们还可能知道哪个系统被访问了，但也许对该系统使用的信息类型或有权访问的人员一无所知。

与 McAfee Enterprise Security Manager 集成

McAfee Enterprise Log Manager 是 McAfee Enterprise Security Manager 中一个可选的集成组件。在 McAfee Enterprise Log Manager 存储日志时，McAfee Enterprise Security Manager 可以深入解析、规范化和分析日志信息，从而使其可立即用于实时安全调查和事件响应。

在生成安全事件时，经过解析的事件文件被直接链接到源日志文件和特定的日志记录，以便在事件管理和取证流程期间实现一键访问。没有多余的步骤，不需要启动额外的应用程序，也不会浪费更多时间手动搜索日志。

便于分析的丰富的上下文信息

McAfee Enterprise Security Manager 和 McAfee Enterprise Log Manager 共同为每一份日志提供上下文信息，使得每条经过解析的日志记录更有价值。这些信息可能包括：

- 源 IP 地址或目标 IP 地址
- 身份信息上下文
- 正在使用的主机名或服务
- 漏洞评估扫描程序中的漏洞信息
- 网络拓扑信息
- 策略和隐私信息

灵活的存储池

McAfee Enterprise Log Manager 存储池可以更灵活地长期保存日志。存储池是可用存储的虚拟组，可分布在各种物理存储设备组（本地存储、NFS、SAN 和 CIF 等）中，以满足不同的日志管理需求。

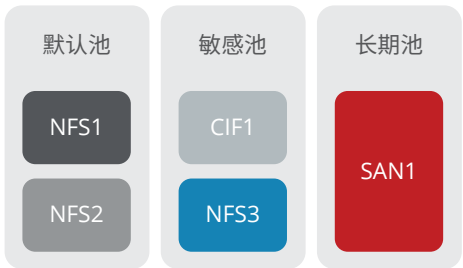

图 1. 灵活的存储池可支持自定义日志保留。

一个存储池可以由多个设备组成，而且可以根据来源设备将数据分配到特定的池，因此可以根据日志与安全性、合规性、机密性或其他标准的相关性将其存储到不同的位置。例如，对于合规性至关重要的日志可能会存储到包含多个冗余网络存储设备的池中。而重要性较低的日志可能被存储到冗余度较低的系统中，而对取证而言最有用的日志则可能存储在本地，以便更快速地进行分析。

快速部署

McAfee Enterprise Log Manager 和 McAfee Enterprise Security Manager 可以通过单个集成设备同时部署，也可以广泛分发，为最大型企业网络提供支持。灵活的混合交付选项包括物理设备和虚拟设备。

与您的基础设施集成

大多数日志管理解决方案都是单独运作的，而 McAfee Enterprise Log Manager 可与其他信息安全系统协同工作。借助 McAfee Enterprise Security Manager，它可以与安全基础设施的其他组件建立连接，以简化安全操作、提高整体效率并降低成本。您可以将智能日志管理与强大的分析、网络检测及数据库事件监控等功能集成在一起。

了解更多信息

有关详细信息，请访问 **www.mcafee.com/cn/products/siem/index.aspx**。

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：861085722000
www.mcafee.com/cn