McAfee Enterprise Security Manager

确定顺序。深入调查。迅速响应。

要实现最有效的安全性，必须从监控系统、网络、数据库及应用程序上的所有活动入手。安全信息和事件管理 (SIEM) 是建立有效安全框架的基础。McAfee® Enterprise Security Manager 是 McAfee SIEM 解决方案的核心组件，可提供性能优越且切实可行的情报，并根据安全组织所要求的速度和规模集成解决方案。它还可以让您快速确定事件优先顺序，深入调查并响应隐藏的威胁，从而遵从合规性要求。

McAfee Enterprise Security Manager 可让用户实时了解外部形势（威胁数据和信誉源）以及企业内部的系统、数据、风险和活动情况。它可以为您的安全团队提供对内容和环境的完整且相关联访问权限，以便根据风险的实际情况作出快速决策，进而投入资源来应对动态威胁和运营形势，实现最佳效果。这对于调查底层慢速攻击、搜索攻陷指标或补救审核中发现的问题至关重要。为了将威胁和合规性管理纳入安全运营之中，McAfee Enterprise Security Manager 还提供了配置和变更管理、案例管理以及集中策略管理的集成工具 — 即改善工作流程和提高安全运营团队效率所需要的一切。此外，McAfee Enterprise Security Manager 的内容包还可以提供针对高级安全用例的预建配置，可帮助您简化安全运营。

企业级解决方案

由于当今企业往往采用动态变化和分布式的架构，安全运营团队需要收集和快速分析不断增长的大量原始数据和经过分析的数据，所以他们对效率的要求日益苛刻。为了应对这一挑战，McAfee Enterprise Security Manager 使用了开放性的可扩展数据总线，专为大容量数据处理而构建。此外，高度可扩展的数据架构支持吸收、管理和分析数据，从而防止数据收集、搜索和保留受影响。如果不能及时提供关键数据，查询响应延缓分析，或者是由于性能问题导致搜索不完整，则会产生这种影响，使调查受阻。

主要优势

- **高度智能：**先进的分析功能和丰富的上下文信息可以帮助您检测威胁和确定威胁优先级。
- **切实可行：**您需要的数据可动态显示，并且提供了执行调查、包含、补救等各种操作的选项，同时可根据重要的通知和模式采取相应的措施。
- **广泛集成：**解决方案监视和分析来自广泛异构安全基础设施的数据，并通过开放接口提供双向集成。同时还可以实现许多自动化第一响应操作。

联系我们

在几分钟(而非数小时)内了解关键事实

快速访问长期存储的事件数据对于调查事件、搜索高级攻击的证据或尝试补救未能通过的合规审核都是至关重要的,这些操作都要求能够查看历史数据,还要对每个特定事件的完整详细信息具有完全访问权限。

经过高度优化的设备能够按照要求的速度收集和处理多年累积的日志事件,并将这些事件与其他数据流(包括基于 STIX 的威胁情报源)相关联。McAfee Enterprise Security Manager 可以存储数十亿个事件和流,从而确保所有信息可立即用于临时查询,同时长期保留数据,以供取证、规则验证及合规。此外,数据可以立即复制到多个存储位置,维护业务连续性。

环境和内容感知

如果存在可用的环境信息(包括威胁数据和信誉源、身份和访问管理系统、隐私解决方案或其他支持的系统),那么每个事件都可以包含环境信息。这样丰富的信息可以让您根据网络和安全事件与资产属性、实际业务流程以及政策之间的关联来深入理解和准确判断。

McAfee Enterprise Security Manager 的可扩展性和卓越性能可让您从更多来源(包括文档、事务和通信等应用程序内容)收集更多信息,以提供深入的取证价值。这种信息均编制了大量索引,经过了规范化处理且相互关联,可帮助您在更大范围内检测风险和威胁。

高级威胁鉴定

无论是网络流量、用户活动,还是应用程序使用,只要与正常活动存在任何偏差都可能表明威胁迫在眉睫,而您的数据或基础设施也会因此面临风险。McAfee Enterprise Security Manager 会对收集到的所有信息进行基准活动计算,并在潜在威胁发生前按优先级发出警报以期发现威胁,同时分析这些数据中是否存在可能潜藏着更大威胁的模式。此外,McAfee Enterprise Security Manager 还利用上下文信息,并使用对应的上下文丰富各个事件,以便更有效地了解安全事件可能会对实际业务流程造成的影响。

McAfee Enterprise Security Manager 的 Cyber Threat Manager 信息显示板可提供增强的实时监控功能和对新兴威胁的理解。对于通过 STIX/TAXII、McAfee Advanced Threat Defense 和/或第三方 Web URL 报告的可疑或已确认威胁信息,可采用接近实时地或追本溯源地方式(利用回溯功能)对事件数据进行汇总和关联,从而为安全团队提供环境中威胁传播情况的深入理解。这种智能化功能支持组织为适当的人员提供适当的数据,以便接近实时地采取措施,并做出更明智的决策。

优化安全运营

McAfee Enterprise Security Manager 以分析员为中心的用户体验，不仅能够提供更大的灵活性和定制便捷性，而且能够更快地对调查作出响应。简化的工作流程可实现更及时有效的事件管理。通过快速智能访问威胁信息，任何专业水平的分析人员（从入门级到专家）都能够轻松地对瞬息万变的威胁进行优先级划分，执行调查并做出响应。

McAfee Enterprise Security Manager 的易用性与生俱来，其中自带的数百种报告、视图、规则和警报可供立即使用，所有内容均可轻松地进行自定义。无论是为了解典型网络使用情况设置基线，还是简单自定义警报，McAfee Enterprise Security Manager 的信息显示板均可轻松地监控、调查和报告相关度最高的安全信息。而今，组织可以全面关联访问做出快速明智决策所需的数据和上下文。

此外，McAfee Enterprise Security Manager 还提供了内容包，可通过预先配置的“现有”安全用例简化安全运营，并提供对高级威胁或合规管理功能的快捷访问。内容包是针对通用安全用例的预建配置，提供了多套规则集、警报、师徒、报告、变量和关注列表。许多内容包针对可能需要额外审核或自动补救的行为提供了预设的触发条件。

简化遵从性

通过集中自动执行合规监控和报告，McAfee Enterprise Security Manager 消除了耗时的手动流程。此外，与统一合规框架 (UCF) 集成，还可采用“收集一次，实现多项合规”这一方法来满足合规要求，并最大程度地减少审核工作和开支。UCF 支持通过实现法规细节标准化（支持将收集的一组事件轻松地映射到各项法规）提高合规效率。

McAfee Enterprise Security Manager 通过以下方法简化和加速合规管理：数百种预置信息显示板、全方位审计跟踪及超过 240 种全球法规和控制框架报告，包括 PCI-DSS、HIPAA、NERC-CIP、FISMA、GLBA、GPG13、JSOX 和 SOX。除范围广阔的开箱即用支持以外，所有 McAfee Enterprise Security Manager 合规报告、规则和信息显示板均完全可自定义。

连接 IT 基础设施

通过与您的安全基础设施集成，可提供对组织安全态势史无前例的实时可见性。McAfee Enterprise Security Manager 可从数百种第三方安全供应商设备以及威胁情报源收集有价值的数据。通过与 McAfee Global Threat Intelligence (McAfee GTI) 集成，可从 1 亿余个 McAfee Labs 全球威胁传感器收集数据，从而提供不断更新的已知恶意 IP 地址源。McAfee Enterprise Security Manager 还可以吸收通过 STIX/TAXII 和/或第三方 Web URL 报告的威胁信息，并根据分析采取相应的措施。

同时，McAfee Enterprise Security Manager 能够与许多互补事件管理和分析解决方案有效集成，包括 McAfee 解决方案和 McAfee Security Innovation Alliance 合作伙伴解决方案。

例如，McAfee Threat Intelligence Exchange 根据终端监控，汇总流行程度较低的攻击，充分利用全球、第三方和本地威胁情报。McAfee Threat Intelligence Exchange 还可以利用其他集成式产品（如 McAfee Advanced Threat Defense）进一步分析和论证文件。

分析师也可以从与 McAfee Behavioral Analytics 的集成中受益，这是专用的用户和实体行为分析解决方案，从数十亿个安全事件中提出数百个异常现象，以获得一些经过优先排序的威胁线索，并允许分析师发现异常和高风险的安全威胁，这些威胁通常无法通过其他解决方案来识别。同样，McAfee Enterprise Security Manager 与 McAfee Investigator 集成，有助于让分析师变成调查专家，增强他们的信心，帮助他们更快速地终结更多确定了根本原因的案例。

事件响应团队和管理员可以利用 McAfee Active Response 查找系统上潜伏的恶意零日文件以及内存中的活动进程。McAfee Active Response 也可以利用持久性收集器不断监控终端上的特定攻陷指标 (IoC)，如果在您的环境中发现了这样的攻陷指标，则会自动发出警告。此组合不同于标准安全方法，将为组织提供从发现到控制和补救的详细闭环工作流。

McAfee 提供了一款集成式安全系统，可让您阻止和响应新兴威胁。我们可以帮助提高效率，减少资源，同时解决更多威胁。我们的互联架构和集中式管理机制可有效降低您的整个安全基础设施的复杂性并提高运营效率。McAfee 致力于成为您的首选安全合作伙伴，竭力为您提供全套集成式安全功能。

了解更多信息

有关 McAfee Enterprise Security Manager 的详细信息，请访问 **http://www.mcafee.com/cn/products/siem/index.aspx**。

有关集成解决方案的详细信息，请访问 **https://www.mcafee.com/cn/solutions/intelligent-security-operations.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：8610 8572 2000
www.mcafee.com/cn