McAfee Network Threat Behavior Analysis

全方位监控网络行为和威胁

产品简介

McAfee® Network Threat Behavior Analysis 增强功能可以帮助企业加大网络基础设施的实时监控力度。它通过网络流数据分析，识别入侵防护系统 (IPS) 外围的威胁并确认其特征。

通过分析供应商（如：Cisco、Juniper 和 Extreme Networks）交换机/路由器的流量，McAfee Network Threat Behavior Analysis 能够查明网络中存在风险行为的特定点并有效拦截内外部威胁。这款产品能够迅速深入分析复杂的多重攻击和混合威胁，从整体上评估网络级威胁，识别每个网络组件的总体行为并且支持即时提取潜在的异常或攻击类型 —— 包括分布式拒绝服务 (DDoS)、僵尸网络 (botnet) 或蠕虫。

McAfee Network Threat Behavior Analysis 分析器设备拥有强大配置 —— 四核处理器、RAID 磁盘阵列和千兆以太网连接。此外，它还提供了脱机存储局域网 (SAN) 连接。利用特有的流量容量，它能够处理高网络流量，从而提高流量分析速度。

McAfee Network Threat Behavior Analysis 可以与 McAfee Network Security Platform IPS 无缝集成，通过 McAfee Network Security Manager 实现 McAfee Network Threat Behavior Analysis、McAfee Network Access Control (McAfee NAC) 以及 IPS 传感器的统一管理。

通过监控网络事件（如：未经许可的应用程序使用和用户行为），McAfee Network Threat Behavior Analysis 可以执行更为严格的法规遵循策略。这不但有助于满足重要的 PCI DSS 要求，而且能显著增强“审计信心”。

同时，它还能在 McAfee NSM 和 McAfee® ePolicy Orchestrator® (McAfee ePO™) 软件的统一管理下实现网络威胁信息的关联。McAfee Network Threat Behavior Analysis 不仅有助于确保全面、高效的网络安全基础设施，而且能显著节省相关成本和人力。

主要优势

最大限度地降低 IT 及业务风险

- 基于行为的主动式威胁检测
- 有效检测未知威胁
- 通过网络流量分析监控和报告异常网络行为
- 通过检测攻击防止网络渗透
- 快速识别未经许可的应用程序使用，并及时采取措施

实现覆盖范围和价值最大化

- 经济高效的网络监控
- 轻松地对网络流量进行分类和分析
- 无需再手动诊断网络相关的流量问题
- 准确查明问题所在
- 异常检测，包括：零日攻击、垃圾邮件攻击、botnet 攻击和侦测攻击

提高竞争优势

- 提供额外的安全防护层
- 防止网络威胁和漏洞攻击影响业务运营
- 快速、有效地执行分析
- 提供企业级性能并确保稳定可靠
- 简化威胁及签名管理相关操作
- 提高网络性能、扩展能力以及灵活性
- 有助于制定实时安全决策

有效的集成有助于确保法规遵从

- 与 McAfee Network Security Platform IPS 集成，将与网络入侵相关的异常网络行为进行关联
- 与 McAfee ePO 软件和 McAfee Vulnerability Manager 软件集成，加快安全风险管理

重要特性

强大配置实现卓越性能

- 每台 McAfee Network Threat Behavior Analysis 分析器设备都配有：
  - ≫四核处理器
  - ≫RAID 磁盘阵列
  - ≫千兆以太网连接
  - ≫脱机 SAN 存储
  - ≫特有的流量容量
- 满足当前不断增长的安全及网络需求
- 以合理的价格提供稳定可靠的网络级性能

无与伦比的网络监控与分析

通过单一 McAfee Network Threat Behavior Analysis 传感器收集来自整个网络的流量，提供经济高效的网络监控

- 通过网络流量分析监控和报告异常网络行为
- 通过基于行为的算法识别威胁
- 分析主机和应用程序行为
- 检查网络中是否存在蠕虫、僵尸网络或垃圾邮件相关行为
- 检测零日威胁和侦测攻击

轻松的集成和策略实施

- 与 McAfee Network Security Platform IPS 集成，将网络入侵导致的异常网络行为进行关联
- 与 McAfee ePO 软件和 McAfee Vulnerability Manager 软件无缝集成
- 兼容 Cisco、Juniper、Extreme Networks 等供应商的交换机/路由器
- 通过 McAfee Network Security Manager 实现 McAfee Network Threat Behavior Analysis、McAfee NAC 和 IPS 传感器的统一管理
- 促进内部策略和法规策略的实施

系统规格

基础单元	PowerEdge R710（拥有可容纳 6 个 3.5 英寸硬盘的机箱）、无 TPM、OEM (224-4864)
处理器	PowerEdge R710、OEM (330-4285)
内存	12 GB 内存(6x2 GB)、1333 MHz 双通道 UDIMM — 针对双处理器进行了优化 (317-0361)
显示器	Embedded Broadcom GB Ethernet 网卡，带 TOE (430-1764))
硬盘	146 GB 15 K RPM 串行连接 SCSI 3.5 英寸热拔插硬盘 (341-8718)
硬盘控制器	PERC 6/i SAS RAID 控制器 2x4 接头、内置、PCIe 256 MB 缓存、X6 机箱 (341-9152)
软驱	性能 BIOS 设置 (330-3492)
操作系统	未安装操作系统 (420-6320)
网卡	Intel Gigabit ET NIC、双端口、铜线、PCIe-4 (430-0651)
调制解调器	iDRAC6 Enterprise (467-8648)
CD-ROM 或 DVD-ROM 驱动器	DVD ROM、SATA、内置 (313-9092)
声卡	Brand/no-bezel、MCAFEE2、China、R710、OEM (313-8627)
扬声器	Riser，带 2 个 PCIe x8 和 2 个 PCIe x4 插槽 (320-7886)
其他存储产品	600 GB 15 K RPM SA SCSI 3 Gbps 3.5 英寸热拔插硬盘 (341-9624)
特性	适用于 PERC 6/i 或 SAS 6/iR 控制器的 RAID 0/RAID 0 (341-8702)
	可滑动导轨，带缆线收纳臂 (330-3477)
其他	高输出功率电源冗余，870 W (330-3475)
	146 GB 15 K RPM 串行连接 SCSI 3.5 英寸热拔插硬盘 (341-8718)
电源线	250 V、中国 (310-5098)——数量 2

关于迈克菲（McAfee）

迈克菲公司（McAfee, Inc.）总部位于美国加利福尼亚州的圣克拉拉市，是全球最大的专注于安全技术的公司，致力于解决安全领域最艰巨的挑战。迈克菲所提供的具有前瞻性且经实践验证的解决方案和服务，为全球范围内的系统和网络提供安全保护，同时使用户能够安全地在网上冲浪和购物。依靠屡获殊荣的研究团队，迈克菲为家庭用户、企业、公共机构和服务提供商开发了创新的产品，让他们能够实现法规遵从，保护数据、预防网络中断、识别安全漏洞，并持续监测和改善他们的安全状况。http://www.mcafee.com/cn

迈克菲(上海)软件有限公司

北京市朝阳门外大街 16 号中国人寿大厦 1709 室 邮编: 100020 电话: (8610) 85722000 传真: (8610) 85752299
上海市徐汇区虹桥路 3 号港汇 2 座 4005-4006 室 邮编: 200030 电话: (8621) 61458878 传真: (8621) 61132278
广州市天河区体育东路 118 号财富广场西塔 15 楼 106 室 邮编: 510620 电话: (8620) 38860668 传真: (8620) 38860638

迈克菲销售热线: 800-810-0369 www.mcafee.com/cn

7856ds_nts_threat-behavior_0110_ETMG