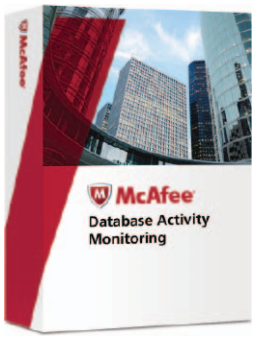
McAfee 迈克菲

McAfee Database Activity Monitoring

经济高效地为数据库提供保护，满足您的合规要求



各组织都将最重要的、敏感的数据存储在数据库中，但是外围环境的保护措施和数据库自身的基本安全保护措施不能抵御来自当今顽固的黑客或恶意内部人员的潜在威胁。研究[1]表明，超过 92% 的违规都与数据库有关，其中，超过 87% 是通过高技能的漏洞攻击。McAfee® Database Activity Monitoring 能够自动发现网络上的数据库，并采用一套预设的防御措施保护它们，还能帮助您量身定制适合您环境的安全策略，以便您能够更轻松地向审核人员证明合规性，提高重要资产数据的保护水平。

主要优势

- 实现最大的可视性并抵御各种攻击
- 监视外部威胁、内部特权人员和数据库内部的复杂威胁
- 在攻击造成危害之前加以阻止，将风险和责任降到最低
- 通过加快部署速度、提高体系结构效率来节省时间和资金
- 使您可以灵活地在所选的 IT 基础架构上轻松部署
- 与迈克菲的核心产品集成，如 McAfee ePolicy Orchestrator® (McAfee ePO™) 管理平台和 McAfee Vulnerability Manager for Databases

使用 McAfee Database Activity Monitoring，组织可以看到所有数据库活动，包括本地特权用户的访问和来自数据库内部的复杂攻击。McAfee Database Activity Monitoring 可帮助他们保护最重要、敏感的数据不受外部威胁和恶意内部人员的侵害。除了提供可靠的审核跟踪外，McAfee Database Activity Monitoring 还可以通过终止违反安全策略的会话防止入侵。使用 McAfee Database Activity Monitoring，组织可以：

- 快速构建自定义安全策略，满足行业法规或内部 IT 管理标准
- 记录对敏感数据的访问以供审核之用，其中包括完整的交易明细
- 终止违反策略的会话并隔离可疑用户，防止数据泄露
- 根据许多管理法规的要求明确责任

McAfee Database Activity Monitoring 通过监视每个数据库服务器上的本地活动并实时警报或终止恶意行为，能够经济高效地保护您的数据免受所有威胁，甚至在虚拟或云计算环境中运行时也可以做到这一点。

防御所有数据库威胁媒介的攻击

网络上、登录到服务器的本地用户，甚至是数据库内部（通过存储的程序或触发器），都可能形成以数据库中所存储的重要数据为目标的攻击。McAfee Database Activity Monitoring 可以使用基于内存的传感器通过单一的无中断解决方案捕获所有这三种威胁。然后可以使用此信息证明合规性，以供审核使用，并提高组织最有价值数据的总体安全性。

在威胁发生之时即将其确定下来，以降低风险和责任

通过基本审核或日志分析，只能在事件发生之后了解发生了什么，但实时监视和侵入防护功能却可以在违规行为造成危害之前将其阻止。然后，直接在监视信息显示板上显示警报，其中包括违反策略的完整详情，以便采取解决措施。您可以配置高风险违规行为，以便自动终止可疑的会话和隔离恶意用户，使安全团队能够有时间对入侵展开调查。

1 2010 年 Verizon Business 研究

虚拟修补可以防御已知的漏洞攻击和许多零日威胁

用户并不是始终都能即时安装供应商的补丁程序，因为它们通常需要进行应用程序测试以及停机来应用更新。而且有些应用程序仍在使用较旧版本的数据库，供应商已经不再为这些数据库提供补丁程序。McAfee Database Activity Monitoring 可以检测尝试利用已知漏洞的攻击和常见的威胁媒介，而且经过配置后，可以实时发出警报或者终止会话。该软件可以针对新发现的漏洞定期提供虚拟修补更新，而且这些更新可以在数据库不停机的情况下实施，从而保护敏感数据，直到数据库供应商发布补丁程序，而且用户可以应用这些补丁程序为止。

以最少的资源快速无中断地部署

McAfee Database Activity Monitoring 是一种纯软件解决方案，在一个小时的时间内即可实施完毕并对数据库提供保护，无需特殊的硬件或其他服务器。McAfee Database Activity Monitoring 可自动扫描网络中的数据库，并针对各种监管环境使用向导驱动的模板，指导用户快速创建自定义安全策略来满足审核要求，从而进一步加快部署。通过将实施安全策略的责任分配给在每个数据库服务器上运行的独立传感器，McAfee Database Activity Monitoring 可以经济高效地进行扩展，以支持最大规模的企业。

支持当今的现代化 IT 基础架构，包括虚拟化和云

其他的数据库监控系统都是通过分析网络流量来确定违反策略的行为，不过在用于数据中心虚拟化和云计算的高度动态的分布式体系结构中，这种方式无法实现或者效率低下。但迈克菲传感器却不同，它们可以配置为根据每个新数据库自动调配，可以基于所托管的数据请求安全策略，然后开始向管理服务器发送警报。即使网络连接中断，数据仍可以得到保护，因为传感器在本地实施安全策略，在管理服务器重新连接之后，警报将排入队列，等待发送。

后续步骤

有关更多信息，请访问 www.mcafee.com/dbactivitymonitoring，或者与您当地的迈克菲代表联系以了解详情。

关于迈克菲风险与合规产品

迈克菲风险与合规产品能够帮助您降低风险、自动实施合规工作并进行安全优化。我们的解决方案可以让您实时了解漏洞和策略，以便您能够将安全投资集中在最关键的地方，更好地保护最重要的资产。要了解更多信息，请访问：www.mcafee.com/riskandcompliance 。

迈克菲（上海）软件有限公司

北京朝阳门外大街 16 号中国人寿大厦 1709 室	邮编：100020	电话：(8610) 85722000	传真：(8610) 85752299
上海市卢湾区湖滨路 222 号企业天地 1 号楼 1101 室	邮编：200021	电话：(8621) 23080699	传真：(8621) 63406606
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

销售热线：800-810-0369 www.mcafee.com/cn

16001ds_vm-db_1010_fnl_ASD