

McAfee Network DLP Monitor

(原产品名为 Reconnex iGuard Monitor)

保护您最敏感的数据

确保客户和员工个人隐私数据的安全是每个企业必须做到的——无论是身份证号、信用卡号，还是其他个人信息都不例外。信息的无意泄露是导致数据丢失的“罪魁祸首”。对于企业来说，员工操作错误、笔记本电脑丢失、USB 盘放错地方都是重大的安全挑战。这些与 gmail、yahoo 电子邮件、即时消息、Facebook 等 Web 应用程序一起构成了信息丢失的主要渠道。企业现在需要高性能的数据丢失防护解决方案，它要能够分析所有的 Internet 通信流量并判断信息是否传播到了不合适的地方。而这些工作又不能增加工作负担本已很重的信息安全团队的工作量。同时，无论面临何种挑战，企业都必须确保对相关法规的遵从和知识产权的安全。



主要优势

识别和保护敏感信息

- 借助直观的搜索引擎快速识别敏感信息
- 执行取证分析，以便将当前和过去的风险事件关联起来、检测风险趋势和识别威胁
- 快速创建用于阻止后续行为的规则

采集网络流量，并将所有网络流量编入索引

- 过滤和控制敏感信息，以识别隐藏或未知风险
- 将所有类型的内容编入索引，然后对其进行查询和研究，从而判断哪些信息属于敏感信息以及这些信息已发送到了哪里
- 监控内部文件共享访问

创建成熟的规则并适时进行调整

- 识别所有端口和应用程序上的 300 多种不同内容类型
- 对不依赖端口的网络流量进行分类
- 通过扩展可支持数十万个并发连接

监控、跟踪和报告流通数据

无论您从事何种业务，您都需要通过强大的监控来准确识别通过所有应用程序、协议、端口传送的任何形式的敏感信息。

使用 McAfee Network Data Loss Prevention (DLP) Monitor，您可以实时收集、跟踪和报告整个网络上的流通数据，这样，您便可以知道您的用户和其他机构之间在传输哪些信息以及是通过什么方式传输的。McAfee Network DLP Monitor 是一款特制的高性能设备，它能以独特的方式检测通过所有端口或协议传输的 300 多种内容类型，因此，它可以帮助您轻松发现数据中的威胁，并采取措施保护企业免受数据丢失之苦。另外，借助终端用户通知功能，DLP Monitor 可以通知用户相关的违反数据保护策略的行为，从而及时纠正这种行为。

实时扫描和分析信息

McAfee Network DLP Monitor 借助 SPAN 或 TAP 端口集成到网络中，可以对网络流量进行实时扫描和分析。

它拥有 150 多个预建规则，从法规遵从到许可使用再到知识产权，无所不包，同时，它可以将文档的全文或部分（包括精心掩饰过的文档片段）与全面的规则集进行对照，这样，无论网络流量是大是小，您都可以检测出其中是否存在异常。

发现以前没有想到过的风险

借助 McAfee Network DLP Monitor 提供的针对所有网络流量（不单单是与实时规则匹配的信息）的细致分类、索引和存储功能，您可以利用历史信息快速判断出哪些数据属于敏感数据、这些数据的使用情况、谁在使用这些数据以及这些数据要传播到何处。另外，您还可以对信息执行深入而细致的调查和历史检查，以检测其中是否存在以前没有想到过的风险事件和数据漏洞。如果您将此产品与 McAfee Network DLP Discover 一起部署，您还可以识别数据的网络存储位置及其所有者。

规格

采集和索引能力

- McAfee Network DLP 1650 设备 (1U)
上高达 500 GB 的可用存储容量
- McAfee Network DLP 3650 设备 (3U)
上高达 6 TB 的可用存储容量

系统流量

高达 150Mbps 的完整内容分析、索引编制和存储流量

网络集成

通过 SPAN 端口或物理内联网 TAP 端口 (可选) 被动集成到网络。

内容类型

能够对 300 多种内容进行文件分类, 包括:

- 办公文档
- 多媒体文件
- P2P
- 源代码
- 设计文件
- 归档文件
- 加密文件

支持的协议 支持通过将 TCP 用作传输协议的各协议或端口进行的所有传输。包括适用于 HTTP、HTTPS、SMTP、IMAP、POP3、FTP、Telnet、Rlogin、SSH、webmail、Yahoo Chat、AOL Chat、MSN Chat、ICY、RTSP、SOCKS、PCAnywhere、RDP、VNC、SMB、Citrix、Skype、IRC、LDAP、DASL、NTLM、Kazaa、BitTorrent、eDonkey、Gnutella、DirectConnect、MP2P、WinMX、Sherlock、eMule 等的协议处理程序。

内建策略

提供了各种内建策略和规则, 以满足您的常规需求, 包括法规遵从、知识产权和许可使用。可以根据业务的具体需求, 利用迈克菲采集数据库对规则进行全面定制。

查看事件报告并发出相应操作通知

McAfee Network DLP Monitor 的分类引擎完成对网络流量的扫描、分析和分类之后, 它会将所有相关信息存储在专用的数据库中。通过一个直观的搜索界面, 您可以综合查看信息报告, 了解是谁发送了信息、信息发到了什么地方以及信息的发送方式等等, 这样, 您就可以判断哪些信息泄露、泄露到何处以及如何泄露的。根据这些信息, 您就可以采取措施应用各种操作来应对这些威胁, 确保对法规的遵从和对敏感数据的保护。

复杂数据分类

McAfee Network DLP Monitor 可以帮助您的企业保护各种类型的敏感数据 — 从常见的固定格式数据到多变而复杂的知识产权信息, 无所不包。综合以下目标分类机制提供的信息, McAfee Network DLP Monitor 能够构建精准而详细的分类引擎来过滤敏感信息, 并通过搜索识别隐藏或未知的风险。

目标分类机制包括:

- 多层分类 —— 涵盖采用层级格式的上下文信息和内容
- 文档注册 —— 包括信息出现变化时的生物识别签名
- 语法分析 —— 检测从文本文档到电子表格再到源代码等各种内容的语法
- 统计数据分析 —— 跟踪某个文档或文件中签名、语法或生物识别匹配出现的次数
- 文件分类 —— 识别内容类型 (无论文件或压缩文件采用的是何种扩展名)

平台规格

参数	1650 设备	3650 设备
3RU	1RU	机身外观
尺寸 (高 x 宽 x 深) /重量	1.7 x 17.2 x 27.75 (英寸) 43 x 437 x 705 (毫米) 39 磅/17.7 千克	5.2 x 17.2 x 25.5 (英寸) 132 x 437 x 648 (毫米) 72 磅/32.7 千克
可选扩展卡	外置存储互连卡	
数据存储容量	500GB	6TB
驱动器槽数量	4	16
磁盘容量	500GB	500GB
磁盘技术	SATA2	SATA2
RAID	RAID-1	RAID-1 和 RAID-5
系统内存	16GB	16GB
系统风扇	6 个冷却风扇	5 个冷却风扇、备用后置排风扇
工作温度	10-35 度 (C)、50-95 度 (F)	
湿度范围	8-90% (无冷凝)	
电源	备用热插拔 650W AC-DC 电源、100-240V AC、50-60 Hertz	
电源安全/EMC	USA-UL、Canada-CUL、Germany-TUV、EN 60950 Compliant、IEC 60950 Compliant、CB Report、CCC Certification	
网络接口	2 个 10/100/1000 铜缆网络接口	

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
 上海市卢湾区湖滨路 222 号 1 号楼企业天地 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

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

