McAfee DLP Monitor

保护您最敏感的数据

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发送到了哪里
- 监控内部文件共享访问

创建完善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

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。信息的无意泄漏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 设备放错地方都是重大的安全隐患。这些与 Google Gmail、Yahoo! Mail、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。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。

监控、跟踪和报告传输的数据

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 Data Loss Prevention (DLP) Monitor，您可以实时收集、跟踪和报告整个网络上的传输数据，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 DLP Monitor 是一款专用型高性能设备，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，McAfee 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 DLP Monitor 借助 SPAN 或 TAP 设备可以集成到网络中，进而对网络流量进行实时扫描和分析。它拥有 150 多个预置规则，从法规遵从到许可使用再到知识产权，无所不包，同时，它可以将所有和部分文档（包括“可以乱真”的抄袭文档）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。

发现未知的风险

借助 McAfee 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 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。

查看事件报告并发出相应操作通知

McAfee 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、泄露到何处以及是如何泄漏的。根据这些信息，您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。

规格

采集和索引功能

- 在 McAfee DLP 4400 设备上最高能为 80TB 的信息和 5000 万的文档创建索引

系统吞吐量

- 以高达 500Mbps 的速率采集内容（不采样）
- 以高达 200Mbps 的速率对内容进行分类（不采样）

网络集成

- 通过 SPAN 端口或物理内联网络 tap 设备（可选）被动集成到网络

内容类型

支持 300 多种内容的文件分类，包括：

- Office 文档
- 多媒体文件
- P2P
- 源代码
- 设计文件
- 存档
- 加密文件

支持的协议

- 支持通过任何协议或将 TCP 用作传输协议的端口进行各种传输。
- 包括适用于 HTTP、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。

内置策略

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。

对复杂数据进行分类

McAfee DLP Monitor 可以帮助您扫描企业的各种类型的敏感数据 — 从普通数据到固定格式数据再到复杂且极易变化的知识产权，无一不能。借助以下这些目标分类机制，McAfee DLP Monitor 可以创建高度准确且细致的分类引擎，用于过滤敏感信息和执行能够识别隐藏或未知风险的搜索。

对象分类机制包括：

- *多层分类* — 以层级格式覆盖上下文信息和内容
- *文档注册* — 随着信息的变更，提供其生物特征签名
- *语法分析* — 检测文本文档、电子表格、源代码等各种内容的语法
- *统计数据分析* — 跟踪某个特定文档或文件的签名、语法或生物识别匹配出现的次数
- *文件分类* — 识别内容类型，无论文件或压缩包使用何种扩展名

规格：McAfee DLP 4400 设备

组件	说明
主板	Intel TimberCreek 系统 (S5520URR)
CPU	2 X Intel X5660 12M 缓存，2.8GHz（六核）
内存	24 GB P1333 DDR3 内存
RAID 控制器	Intel RS2MB044 RAID 控制器
电源	2 X 760 W 热插拔电源模块
硬盘	12 X Seagate Constellation ES 1T 7200 rpm 3 1/2" SATA 硬盘
NIC 卡	Intel Dual Copper 1Gbps 以太网 I/O 模块
DVD 光驱	SATA DVD ROM
IPMI	Intel 远程管理模块 3 (AXXRMM3)
产品大小	2 机架单位 (2U)

规格：虚拟机

McAfee DLP Discover 可以作为虚拟机运行于 VMware ESX 或 VMware ESXI 4.1 服务器上。以下是运行虚拟机的一些最低硬件要求。

组件	要求
CPU	Intel 四核
内存	8 GB RAM
硬盘	硬盘 1：最小容量，128 GB - VM 软件 硬盘 2：最小容量，640 GB - DLP 虚拟镜像
网络端口	1 个用于 McAfee DLP Discover 应用程序的端口
BIOS	启用 VT 线程

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

39706ds_dlp_monitor_1111