McAfee Data Loss Prevention Monitor

保护重要数据

保护客户和员工的个人隐私数据(身份证号和信用卡号或其他个人信息)在今天是每个人都关心的问题。由于员工失误、笔记本电脑丢失和 USB 设备放错地方而造成的数据意外泄露,是几乎每个组织都会面临的安全挑战。更糟糕的是,当通过 Web 应用程序(如 Google Gmail、Yahoo! Mail、即时消息和 Facebook)传输和共享数据时,可能造成数据泄露或落入不法分子手中。McAfee® Data Loss Prevention Monitor (McAfee DLP Monitor) 是一款高性能的数据丢失防护解决方案,可分析所有 Internet 通信并确定信息的流向是否不当。它可以帮助您最大限度地降低安全团队的工作负荷、满足合规性要求、保护财产和知识产权以及其他重要资产。

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 DLP Monitor,您可以实时收集、跟踪和报告整个网络上传输中的数据,以便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 端口集成到网络中,可以对网络流量执行实时扫描和分析。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,McAfee DLP Monitor 可以将文档的全文或部分(包括精心掩饰过的文档片断)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。

发现以前没有意识到的风险

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

主要优势

- **完全与 McAfee® ePolicy Orchestrator® (McAfee ePO™) 软件一致:**利用 McAfee DLP Endpoint 共享一般政策、事件和案例管理。
- **高性能和可扩展性:**多达 8 个设备的群集,具有 6 Gbps 扫描带宽。
- **全面分析:**检测所有端口和应用程序上的 300 多种不同内容类型。
- **便于使用的内置策略:**提供了各种内置策略和规则,以满足您的常规需求,包括法规遵从、知识产权和许可使用。

联系我们

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考虑到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。

分类所有类型的数据

McAfee DLP Monitor 可以帮助您的企业扫描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 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：**涵盖语境信息和层级格式中的内容。
- **文档注册：**在信息发生变化时包括信息签名。
- **语法分析：**检测从文本文档、电子表格到源代码中的任何内容的语法或句法。
- **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：**无论文件或压缩包采用何种扩展名，都能识别内容类型。

取证和规则调整功能

独特的 捕获 技术使您能够利用自己的历史数据大大提升实施部署的速度和效率，而无需进行猜测或数月的试错，也无需中断业务。这样，您便可以根据不断变化的业务需求轻松调整 DLP 规则（包括分类调整），进而确保规则的准确性。此外，捕获 技术可以充当数字记录仪，允许在事后重放 DLP 事件以进行全面的调查，从而有助于进行取证调查。捕获技术既可以用作一个虚拟环境，也可以用作通过 SAS 线缆连接到 NDLP 6600 设备的一个 2U 16TB 存储阵列。

外形规格和设备选择

McAfee DLP Monitor 作为硬件设备提供，并且具有虚拟设备选项。有关其他详细信息，请参阅 **McAfee DLP 6600 硬件设备产品简介**。

规格

- **系统吞吐量：**能以高达 800 Mbps 的速度对内容分类（无需采样）。
- **网络集成：**通过 SPAN 端口或物理串联网络分路器（可选）被动集成到网络。
- **群集功能：**多达 8 个设备的群集，具有 6 Gbps 的性能。
- **可支持 300 多种内容类型的文件分类，包括：**
  - Microsoft Office 文档
  - 多媒体文件
  - P2P
  - 源代码
  - 设计文件
  - 存档
  - 已加密的文件
- **包括以下协议的处理程序：**
  - FTP
  - HTTP
  - IMAP
  - IRC
  - LDAP
  - POP3
  - SMB
  - SMTP
  - Telnet

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