McAfee 迈克菲

McAfee Network DLP Discover

（原产品名为 Reconnex iGuard Discover）

识别和保护敏感数据

保留在笔记本电脑、共享文件服务器、门户或文档管理系统中的信息可能会给企业带来风险。 企业必须对大量（数 TB 甚至数 PB）的数据提供保护。做到这点非常困难，因为企业无法百分之百地准确识别出哪些信息属于敏感信息。此外，对于大多数企业来说，他们根本无法确定或查证敏感信息是否面临着风险，或者这些敏感信息传播到了何处 —— 即使采用了有效的访问控制也无济于事。更为糟糕的是，敏感数据通常都包含知识产权（IP）资产，界定这些资产比信用卡或身份证号等固定数据更加困难。

主要优势

识别数据泄露风险

- 扫描所有可访问资源上存储的信息
- 识别敏感数据的存储位置及内容所有者
- 借助一个直观的界面即可搜索和查看所有扫描数据

创建策略和自定义报告

- 执行查询，然后将结果转化为防护规则
- 使用预建的法规遵从、企业管理和知识产权策略
- 将敏感信息登记到相关信息安全系统对数据泄漏进行分类、分析和补救
- 使用多方位分类方法对敏感信息进行过滤和管理
- 将所有内容编入索引，然后在对其进行查询和研究，以了解哪些属于敏感数据
- 注册并生成签名，以保护其中包含的文档和信息，即使是借用或调换的文档和信息也不例外
- 一旦有内容违反了防护策略，即发送警报通知

防止敏感数据丢失

从源代码到商业机密再到商业战略计划，知识产权（IP） 和其他信息资产对于您的企业形象、公共信誉和竞争优势都有至关重要的作用。保护传输数据的安全固然重要，而保护敏感数据免受不安全的访问或转移并了解这些数据存放在何处才应当是数据防护的重中之重。

McAfee Network DLP (Data Loss Prevention) Discover 可以帮助您的企业免受数据丢失之苦。与旨在让您详细了解要保护内容的传统解决方案不同，McAfee Network DLP Discover 不但可以全面保护明显的敏感信息，还能帮助您查找不明显的敏感信息。

确定需要保护的信息

为了识别信息和传播风险，您可以对 McAfee Network DLP Discover 进行配置，以扫描特定存储库并识别数据，从而明确防护目标。同时，McAfee Network DLP Discover 爬网所获得的数据都将编入索引，通过直观的界面即可访问，这样，您就可以快速搜索可能的敏感数据，以便了解这些内容的所有者以及存储位置。

定义防护策略

明确了要保护的信息后，McAfee Network DLP Discover 就会帮助您确保这些信息万无一失。这款产品提供了直观统一的策略创建、报告和管理功能，能够让您更有力地控制针对存储数据的信息保护策略。McAfee Network DLP Discover 策略、规则和分类的关键优势包括：

- 大量的内建策略 —— 便于您现成可用
- 功能强大的规则构建引擎 —— 从简单的结构化数据（信用卡、身份证号）到复杂信息（知识产权），无所不包
- 简化的规则创建和验证 —— 将搜索结果分析转化为防护规则
- 集成相关信息安全媒介 —— 确保防护的一致性
- 排除公共文档和共享文本—— 防止这类重要信息带来意外

规格

采集和索引能力

- McAfee Network DLP 1650 设备 (1U) 上可以支持对最高 5TB 的信息和最多 200 万个文档编入索引
- McAfee Network DLP 3650 设备 (3U) 上可以支持对最高 50TB 的信息和最多 2500 万个文档编入索引

系统流量

- 内容读取流量最高达 500Mbps
- 内容索引流量最高达 150Mbps

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
- 源代码
- 设计文件
- 归档文件
- 加密文件
- 内建策略
- 知识产权

支持的存储库

- 常规 Internet 文件系统/服务器消息块 (CIFS)
- 网络文件系统 (NFS)
- HTTP/HTTPS
- FTP
- Microsoft Sharepoint
- EMC Documentum

文档可以从任何存储库注册。注册文档的签名可以在本地用来检测敏感信息的扩散情况，也可以用于其他 McAfee Network DLP 设备。

报告

用于事件和搜索结果视图的分析引擎功能强大，它可以让您根据任意两个上下文基点对摘要视图进行定制。同时，您还可以使用列表和详细视图以及带有趋势分析的摘要视图。该系统提供了 20 多种可定制的预建报告和可定制报告。

扫描网络，查找是否存在违反策略的行为

策略定义完成后，可以设置 McAfee Network DLP Discover 定期扫描网络资源，查找其中是否存在违反策略的行为。灵活的时间安排选项可以帮助您执行持续扫描、按日扫描、按周扫描或按月扫描。

McAfee Network DLP Discover 可以自动扫描所有可访问资源，包括笔记本电脑、台式机、服务器、文档存储库、门户和文件传输位置，以查找是否存在违反策略的行为。您可以根据 IP 地址、子网、范围或网络路径定义扫描分组。同时，您还可以按照特定的参数进行集中扫描，例如只扫描所有用户的“我的文档”而不扫描系统文件夹，或者查找特定用户的文件或特定类别或大小的文件。

检查和补救违反策略的行为

McAfee Network DLP Discover 借助集成的事件工作流和案例管理可以避免或最大程度地减少敏感资料的传播。如果 McAfee Network DLP Discover 发现有内容违反了防护策略，便会生成事件并发出通知。McAfee Network DLP Discover 生成的事件可以添加到案例管理框架，这样，您就可以召集企业各部门的专业人员来共同处理违反策略的内容。另外，安全人员借助风险信息显示板可以轻松查看违反策略内容的概况，并根据任何需要的存储数据参数来生成报告。

采集和分析存储数据

除了扫描网络资源以检查其中是否存在违反策略的内容之外，McAfee Network DLP Discover 还可以将所有网络上的存储内容编入索引，方便您对这些信息进行查询和研究，以了解哪些信息属于敏感信息。McAfee Network DLP Discover 能够帮助您快速了解您的敏感数据及其使用情况、所有人、存储位置以及传播到了哪里。

复杂数据分类

McAfee Network DLP Discover 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 Discover 能够创建高度准确的多向量分类，进而用于过滤和控制敏感信息，执行可以识别隐藏或未知风险的搜索。 这些目标分类机制包括：

- 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）

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

5585ds_network-dlp-discover_0109