McAfee DLP Prevent

实施敏感信息保护策略

借助电子手段共享信息的人越多，敏感数据被人无意或故意发送给未经授权的个人的可能性就越大，这就会导致企业的机密数据面临风险。信息可以通过许多不同渠道流出公司，包括电子邮件、Web、即时消息（IM）或 FTP。有些消息或交易记录是允许使用的，但应当对其进行加密以确保数据的隐私性。其他类型的通信在任何时候都是不可接受的，并且必须被阻止。适时实施正确的策略对于确保数据安全、监管合规和知识产权保护来说至关重要。

针对传输中的数据实施安全策略

各个企业的员工都会使用各种应用程序和协议在部门间共享数据。通过前瞻性地保护敏感信息，防止这些信息通过网络泄露出去，并实施正确的业务流程，可防止这些数据被无意或故意泄露。

McAfee® DLP Prevent 集成了使用简单邮件传输协议 (SMTP) 的消息传输代理网关或兼容 ICAP 的 Web 代理，可帮助您对通过电子邮件、Web 邮件、即时消息、Wiki、博客、门户网站、HTTP/HTTPS 和 FTP 传输等途径离开网络的信息强制实施有效的策略。一旦遇到违反策略的内容，McAfee DLP Prevent 就可以让您采取多种操作，包括加密、阻止、重新定向、隔离等，这样便可确保您对有关敏感信息隐私性保护的法规遵从性，同时还能降低安全威胁风险。

完全与 McAfee ePolicy Orchestrator 软件一致

McAfee DLP Prevent 利用共同的策略、事件和案例管理，完全与 McAfee® ePolicy Orchestrator® (McAfee ePO™) 软件和 McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint) 一致。管理员可以在 McAfee ePO 软件中创建单一的电子邮件和 Web 保护策略，并将其部署到终端和网络。此外，McAfee DLP Endpoint 和 McAfee DLP Prevent 共用同一分类引擎，允许使用单一的电子邮件和 Web 策略。

主要优势

充分利用现有基础设施。

- **通过与消息传输代理 (MTA) 网关的集成来保护企业电子邮件的安全，MTA 网关使用了带有 X-Header 的 SMTP，它具有阻止、退信、加密、隔离和重定向功能。**
- **通过与兼容 Internet Content Adaptation Protocol (ICAP) 的 Web 代理的集成来实现流量传输控制，阻止 HTTP、HTTPS、即时消息、FTP 和 Web 邮件中违反策略的内容。**

针对所有类型的信息前瞻性地实施策略。

- **可以保护 300 多种不同的内容类型。**
- **针对已知敏感的信息以及可能未知的信息强制实施策略。**
- **通过扩展可支持数十万个并发连接。**

联系我们

通用字典和正则表达式 (regex) 语法可提供创建通用 Web 和电子邮件保护策略的连续性。凭借集中式管理，McAfee DLP 解决方案可通过单一管理平台进行安全监控，有助于提高业务效率和减少管理开销。

监控移动电子邮件

利用具有 DLP 功能的 ActiveSync 代理，适用于移动电子邮件的 McAfee® DLP Prevent 可拦截下载到移动设备的电子邮件，为移动电子邮件提供内容感知保护。此外，它还可以在内部 Microsoft Exchange 和 Microsoft Office 365 Hosted Exchange 上拦截 ActiveSync 数据。此工具完全通过 McAfee ePO 软件进行管理，并且 McAfee DLP Prevent 许可证包含了其授权。它不要求在移动设备上安装任何代理。利用适用于移动电子邮件的 McAfee DLP Prevent，企业可以监控电子邮件的合规性并收集证据，从而保护受管和非受管移动设备。

与 Web 代理和 MTA 集成，提供更有力的保护

McAfee DLP Prevent 与 Web 代理（使用 ICAP）和 MTA（使用 X-Header）集成，以便在需要时执行相应的操作。它可以在应用程序层终止未经授权的事务，而不是简单地停止 TCP 会话（仅仅停止 TCP 会话无法更改应用程序行为），因此当出现违反策略的行为而导致传输遭拒时，McAfee DLP Prevent 就会向导致信息泄露的应用程序发出警告。这可以使您的企业获得更有力的数据保护，因为 McAfee DLP Prevent 的记忆功能可以避免应用程序再次尝试同一行为。

保护已知和未知的敏感信息

McAfee DLP Prevent 能够对 300 多种不同的内容类型进行分类，因此，它不但可以帮助您确保已知要绝对保密的信息的安全（如身份证号、信用卡号和财务数据），同时还能帮助您判断哪些信息或文档需要保护，例如非常复杂的知识产权。McAfee DLP Prevent 内置了大量策略，从法规遵从到许可使用再到知识产权，无所不包。借助这些策略，您可以将所有和部分文档与全面的规则集进行对照，这样您便可以对所有敏感信息（包括已知和未知敏感信息）提供保护。

可自定义的视图和事件报告

利用 McAfee ePO 软件，您可以根据任何两个语境轴心点自定义安全事件汇总视图和后续操作。您随时可以查看列表视图和详细信息视图，以及包含趋势信息的汇总视图。McAfee DLP Prevent 还提供了大量的预建报告，您可以查看各个报告，也可以保存供以后使用，还可以将这些报告设置为定期发送。

对数据泄露进行分类、分析和补救。

- **过滤和控制敏感信息，以防御已知和未知风险。**
- **将所有内容类型编入索引，并对它们实施细致周密的安全策略。**
- **应用与内部文件共享访问相关的策略，防止用户通过未授权的方式访问信息或存储库。**

规格

系统吞吐量

高达 150Mbps 的完整内容分析、索引编制和存储吞吐量。

网络集成

可以使用 MTA 和兼容 ICAP 的 Web 代理作为在数据路径中活动的路径外设备集成到网络中。

内容类型

支持 300 多种内容类型的文件分类：

- **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**

复杂数据分类

McAfee DLP Prevent 可以帮助您的企业保护各种敏感数据 - 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 Prevent 能够利用精准而详细的分类引擎阻止敏感信息泄露，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所有内容的语法或句法。
- **统计数据分析**：跟踪特定文档或文件中签名、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 Prevent 有硬件设备或虚拟设备两种形式。有关其他详细信息，请参阅 **McAfee DLP 6600 硬件设备产品简介**。

支持的协议

通过针对兼容 ICAP 的代理的 ICAP 协议支持 HTTP、HTTPS、FTP 和即时消息协议。有关您的代理支持的协议，请咨询您的代理供应商。借助集成的 MTA 支持 SMTP。

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。**
- **可以根据业务的具体需求，利用 McAfee 采集数据库对规则进行全面定制。**

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

2018 年 12 月