防止数据从您的组织中泄露

数据从大部分组织中逃离。数据有时候是由内部人员泄露，但大部分时候是由外部行动者盗窃。数据以多种方式和通道离开。各种组织正在尝试阻止这种数据外流，原因各不相同，并且取得了不同程度的成功。McAfee 运用 *McAfee 2016 Data Protection Benchmark Study* (McAfee 2016 数据保护基准研究) 以更加深入地了解失窃背后的人员、被窃的数据类型以及数据从组织中外泄的方式。

在《McAfee Labs 威胁报告：2016 年 9 月》中，我们分析了调查数据并详细描述了我们的发现。首先我们发现：

- 数据丢失与发现泄露之间的时间差越来越大。
- 医疗保健提供商和制造商容易成为攻击目标。
- 典型的数据丢失预防方法对于新的盗窃目标越来越没有效果。
- 大部分企业不会看到第二大最常见数据丢失方法。
- 基于正确原因实施数据丢失预防措施。
- 监视很重要。

针对有效数据丢失防护的建议策略和规程

组织要创建数据丢失保护策略和规程来防止敏感数据无意间或故意传输到未经授权方。成功的数据丢失防护计划开始于在定义业务需求时规划阶段。例如，在规划阶段时应解决将组织的数据分类和数据丢失策略与隐私策略和数据分享标准保持一致的问题。建立良好的业务需求有助于专注数据丢失防护计划并且防止范围蔓延。

数据丢失防护计划的重要下一步骤是识别组织中的敏感数据。通过服务器和端点扫描技术，可以根据正则表达式、字典和非结构化数据类型来对文件进行分类。数据丢失防护产品通常提供对典型类别的敏感数据（比如支付卡数据或个人健康信息）的分类方式，从而加速发现过程。也可以创建自定义分类方式，以识别组织所特有的数据类型。

IT 部门认可和非认可的应用程序及其支持数据都存储在云中，这导致这一步骤变得很复杂。对于云中存储的 IT 部门认可数据，识别敏感数据可以也应该在订阅云服务时执行。如果是这种情况，则分类这种类型的数据相对简单。

但是，组织中的功能团队常常通过自行订阅云服务来绕过 IT 部，以满足其业务目标。如果 IT 部门没有意识到这些服务以及支持这些服务的数据，则数据丢失的可能性会增加。因此，在这一步骤中，重要的是与功能小组合作来识别云中数据的位置并使用前述过程来分类数据。

在完成敏感数据发现过程之后，在可信网络和所有端点中实施数据丢失防护产品可以对重要的静态和动态数据进行监视和控制。应实施策略来检测意外的敏感数据访问或移动。正常业务流程中可能会出现敏感数据传输到 USB 设备或通过网络传输到外部位置之类的事件，此类事件可能是有意或无意行为，但导致了数据丢失。

完善的安全意识培训可以减少数据泄漏的可能性。理由筛选可以帮助培训用户就敏感数据传输采取正确的操作，并且可以在正常工作日中对用户提供数据保护策略培训。例如，理由筛选可以通知用户，他们传输敏感数据违反了政策并提供完成传输的替代方法，比如首先编校敏感数据，然后再尝试传输。

数据所有者通常比组织中的其他团队更清楚如何更好地使用其数据。应为数据所有者分配数据丢失事故分类的任务和权力。将数据所有者与安全团队之间职责分离可降低单个团队绕过数据保护策略的可能性。

一旦确定了经过批准的数据移动并且管理这些数据移动的策略已整合到数据丢失防护产品，便可以开启用于阻止未经批准传输敏感数据的策略。在启用阻止时，将阻止用户执行违反策略的操作。可以根据业务的要求来调整策略来提供灵活性，以确保用户能够在安全的情况下履行职责。

随着数据丢失防护计划的进行，务必要根据计划的间隔来验证和调整策略。有时候，策略会过于严格或过于宽松，从而影响生产力或造成安全风险。

McAfee 可以如何帮助防御数据泄露

McAfee DLP Discover

正确保护数据的第一步是，了解信息所在位置以及该数据的确切内容。McAfee DLP Discover 通过以下功能简化此第一步来防御数据泄露：

- 通过使用内置分类（例如，HIPAA、PCI、SOX）或者创建自定义分类，确定要在可信环境中检测的分类。
- 使用确定的分类来执行库存扫描，以了解可信环境中存在的数据类型以及这些数据的位置。在 McAfee DLP Discover 界面中查看现有策略的违例。
- 执行补救扫描，以找出未授权位置中存储的数据，并将其移动到授权位置。
- 可以对本地资源（如网络共享内容）或者云资源（如Box）执行库存和补救扫描。
- 根据 McAfee DLP Discover 扫描的结果创建新的数据保护策略。

McAfee DLP Endpoint

McAfee DLP Endpoint 可以即时监控和阻止内部部署、外部部署和云中的数据泄露。快速监控实时事件，采用集中管理的安全策略，以及生成详细的取证和传播报告，而不妨碍日常运营。

- 在“发现”阶段完成后，创建数据保护策略以保护策略违例。这提供了必要的数据以更好地了解组织中的数据移动，并且支持强制实施阻止规则。McAfee DLP 包含内置分类（例如 HIPAA、SOX、PCI 和 ITAR），可用于识别组织中的数据。
- 创建辅导屏幕，以便用户在执行日常数据传输时更好地理解数据保护策略。这些可以自定义的教育弹窗帮助极大，并可减少员工进行的有风险数据传输。
- 查看事件管理器以识别正在传输到未经授权位置的数据的属性，比如执行传输的方式和执行传输的用户。
- 在创建了数据保护策略并且根据组织要求调整之后，启用对未经授权数据传输的阻止。
- 启用手动分类，以便用户能够对其已经创建的文档进行分类。在自动分类引擎无法检测任何结构化数据的情况下，数据所有者可能对文档的敏感性更了解。McAfee DLP Endpoint 中已经内置，无需任何其他第三方工具。
- 对于其他保护，创建和实施应用程序访问保护规则，该规则使用 McAfee Threat Intelligence Exchange 来防止未知应用程序访问敏感数据。这允许授权的应用程序传输敏感数据，但限制未经验证或恶意应用程序访问该数据。

McAfee DLP Monitor

McAfee DLP Monitor 可收集、跟踪和报告整个网络上传输中的数据。轻松发现针对数据的未知威胁并采取措施来保护数据。

- 启用相关的内置策略和规则以检测网络中的可能违例。
- 创建其他自定义策略和规则，比如监控敏感数据传输到云。
- 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。McAfee DLP Monitor 使安全专家能够快速了解威胁形势，以便制定应对威胁的规则和策略。
- 创建其他捕获过滤器以排除不相关数据并调整规则以降低误报。
- 配置警报以在发生策略违例时向发件人、收件人、数据所有者和系统管理员发送通知。

McAfee DLP Prevent

McAfee DLP Prevent 通过确保数据仅在必要时（无论通过电子邮件、网络邮件、即时消息程序、Wiki、博客、门户、HTTP/HTTPS 还是 FTP 传输）离开网络来防止数据丢失。保护重要数据的安全与成为下一个安全事件新闻头条主角之间的差距往往就在于快速识别和减少数据泄露尝试。

- 使用内置策略将 McAfee DLP Prevent 与 Web 代理或消息传输代理集成，以防止通过电子邮件网关或 Web 代理来传输未经授权的数据。
- 创建 McAfee DLP Prevent 规则以根据匹配百分比来允许或阻止敏感文档。
- 使用内置 DLP 模板来防止敏感数据传输到云。
- 查看安全事件的报告并调整策略以减少误报并最大限度保证业务连续性。
- 配置警报以在发生策略违例时向发件人、收件人、数据所有者和系统管理员发送通知。

进一步阅读

McAfee Expert Center 社区

- McAfee Data Loss Prevention

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