终端数据防泄漏（EndPoint DLP）

北京天空卫士网络安全技术有限公司

2021 年 1 月

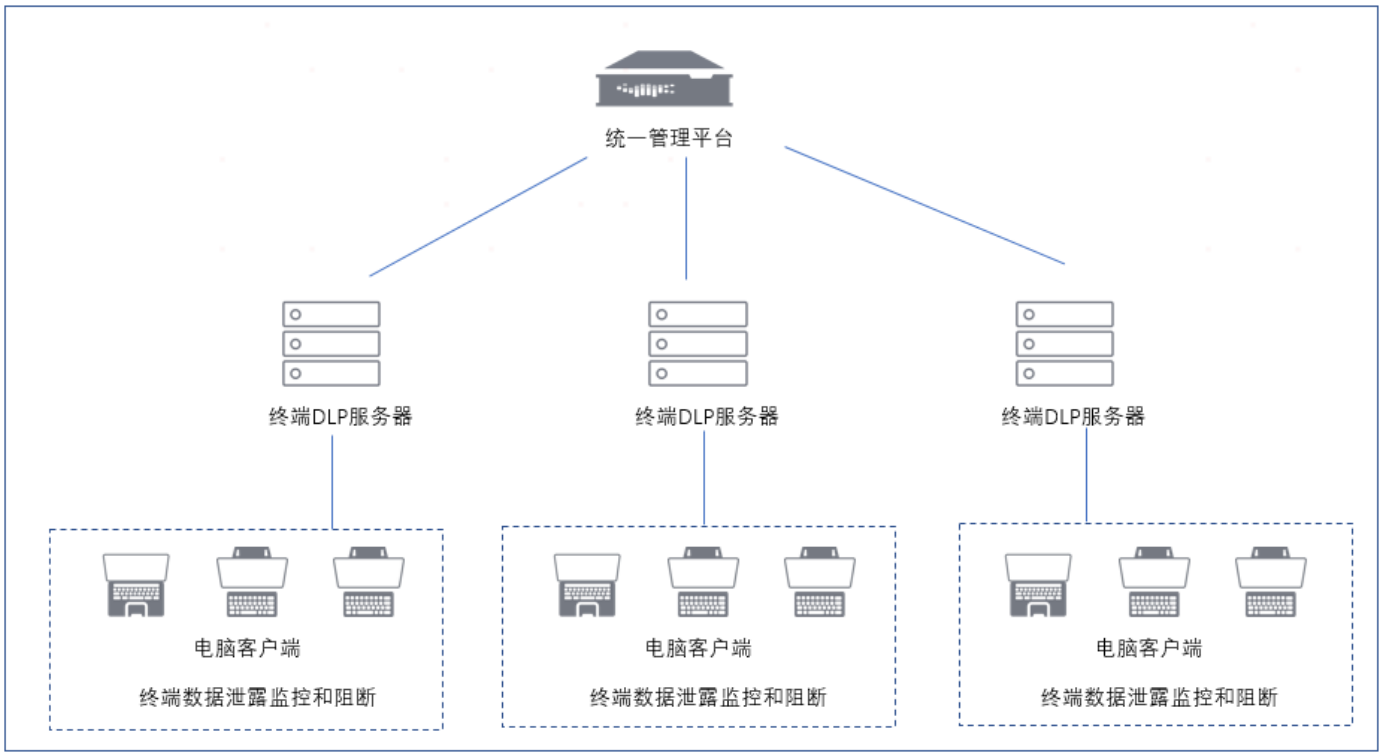
1. 产品概述

终端数据防泄漏（EndPoint DLP，简称终端 DLP）安装在员工的 PC 机上，可监控下载到内置硬盘的数据，并且监控及阻止复制到 USB 设备、CD/DVD 和其他可移动介质的数据，终端 DLP 还可监控及阻止网络数据以及复制/粘贴和打印/传真操作。终端 DLP 通过扫描 PC 上的存储介质保存的机数据，识别敏感信息的分布，按照预定的策略对数据执行分级分类管理，对于违规存储的数据，将其记录或移动至安全位置，防止企业的核心数据资产以违反安全策略规定的形式流出企业，当数据以违规的方式发送时，并以弹窗的方式警告用户的违规情况。即便当客户端不在公司网络内部时，终端 DLP 仍然执行离线数据防泄漏检测，提供随时随地的安全防范。

终端 DLP 覆盖的协议和应用程序包括 Web 和安全 Web (HTTP/HTTPS)、即时消息传送(IM)、文件传输 (FTP) 以及通过 Outlook 等客户端收送的电子邮件。

2. 体系架构图

终端 DLP 产品包含服务器端（Server）和客户端（Client）。



客户端安装在 Windows XP、Windows Vista、Windows 7（32 位、64 位）上， 终端 Server 向下推送的数据泄露防护策略和过滤器/配置。无论客户端是在执行数据发现、监控还是保护功能，其工作方式都类似于本地检测，

即通过“破解”打开文件并检查其中的数据查看其是否违反策略。如果数据违反策略，客户端将启动实时本地响应规则（例如 USB/CD/DVD、电子邮件、Web、打印或传真阻止）， 然后通过终端 Server 将事件数据收送到管理平台。管理平台随后将启用其他任何适用的自动响应规则（例如收送电子邮件通知给最终用户和/或其管理员），并且系统将存储管事件信息以用于报告和补救操作，同时使企业可全面了解其电脑终端上的数据泄漏风险。

3. 关键技术

为防止数据泄漏，需要对终端存储和使用的所有数据进行检测。检测的准确性，是终端 DLP 产品的精髓，如果检测不够精准测，数据安全系统会生成大量误报和漏报。误报会使进一步的调查和解决貌似有问题的事件花费高昂的时间和资源成本。漏报会隐藏安全漏洞，造成数据泄漏、可能的财务损失、法律风险以及对组织声誉的损坏。

3.1 关键字

关键字检测能够匹配任何字词或短语，包括那些使用任何常见字词分隔符（例如空格、逗号、短横线或斜杠）的字词或短语。用户可为每个条件的关键字匹配进行区分大小写的配置。也可以单独为每个条件配置可定义管事件的匹配关键字或关键短语的数量。

3.1 标识符

标识符技术可以准确标识基于模式的敏感数据，例如信用卡号、社会安全号或驾驶执照号码。数据标识符使用的检测算法结合了模式匹配和其他准确性检查和验证，例如对信用卡号的检查。与其他仅使用正则表达式识别模式的解决方案不同，数据标识符还包括有关不同数据类型的有战数字范围的内置信息。通过此额外信息，客户可以筛选出测试数据和其他常见误报，并识别特定于广泛的行业、国家/地区和区域的数据类型，包括信用卡号、支付卡行业 (PCI) 数据安全标准的磁条数据、银行标识号码 (BIN)、国家保险号码。

3.2 文件识别技术

在开始分析内容之前，首要的一个工作就是对文件进行正确的识别和处理，把文件中的文字提取出来进行后续的处理。还能对文字进行自然语义分析和处理，留出其中的关键字来进行处理。文件识别的最大难度在于支持文件类型的广泛性和正确性，而天空卫士 DLP 以其高性能的处理引擎都能最大化的正确识别并进行分析和处理。

3.3 数字指纹技术

数字指纹技术分为结构化指纹技术（EDM）和非结构化指纹技术（IDM）。EDM 用于保护通常为结构化格式的数据，例如客户或员工的数据库记录。IDM 用于保护非结构化数据，例如 Microsoft Word 或PowerPoint 文档，或 CAD 绘图。对于 EDM 和IDM，都是首先由组织标识机密数据，然后由策略管理平台 对这些数据进行指纹加密以进行持续的精确检测。指纹加密过程包管理平台访问和提取文本和数据，对其进行规范化，然后使用不可逆哈希为其提供保护。可以将策略管理平台 配置为定期自动为 EDM 或IDM 文件编制索引，仍而使这些数据配置文件始终保持最新状态。这种检测方法的基础是使用常见特征查找数据，这些特征有关键字、正则表达式、已验证数据类型、文件类型、文件大小、文件名和收件人/收件人/用户组合等。终端 DLP 检测基于实际的敏感内容，而非文件本身。因此，终端 DLP 不仅可以检测敏感数据的提取信息或衍生信息，而且还可以识别采用指纹加密信息之外的其他文件格式的敏感数据。例如，如果一份佯 Microsoft Word 机密文档经过指纹纹加密，即使该内容作为 PDF 附件通过电子邮件收送，终端 DLP 依然可以可准确检测到它。

无论是具有结构化格式的数据，如客户或员工数据库记录；还是非结构化格式的数据，如 Office 或 PDF 文档，SkyGuard 可对其进行扫描和提取，并可以配置为定期自动更新，保证指纹数据永远和机密数据同步，不管信息泄露者采用何种数据变形手段都无处遁形

- ✓ 结构化数据(数据库)，如客户信息，数据库管理员无需分配特殊权限或干预数据库服务，DLP 仅需以只读权限对数据库表抓取指纹并录入指纹数据库，并可指定安全策略引擎进行整行数据记录匹配，减少误拦截。
- ✓ 非结构化数据(文件)，如红头文件，将文本文件分段后选择性地计算各片段的哈希值，并将哈希值存入指纹数据库中供安全策略引擎进行相似度对比，既可以非常精确的辨认出原始文件内容，也能够识别在一定范围内修改后的文件内容。

3.4 机器学习

机器学习可以对大量的无特定格式文件样本进行快速学习和分类，分类产生的模（Model）可用来对数据进行分析并计算该数据是否属于某一个分类。机器学习的优势在于其生成的模的大小基本恒定，所以很适合处理大量的样本，另外机器学习技术可以对新的、并未出现在样本中的数据进行较为准确的预测。

- ✓ 基于人工智能的预测机制，通过分类样本中共同的”特征”进行预测和分析
- ✓ 无格式文本文件样本进行快速的分类
- ✓ 适合处理大量的样本
- ✓ 对新的、并未出现在样本中的数据进行较为准确的预测

3.5 静态对比分析技术

在这种技术中，通常会采用关键词、正则表达式，数据字典或者内容识别器（比如信用卡号识别器可以快速判断一串数字是否是信用卡号）的方式对被处理数据进行对比分析，在被处理对象中快速的查找出匹配的字符串，从而判断被处理对象是否违背安全策略，需要进行日志记录、审计或者进行阻止。天空卫士 DLP 包含多达 1700 种预定义的不同行业、不同类型的组合模板。

3.6 图像识别(OCR)

DLP 安全策略分析引擎对图片、打印文件等提取文字并执行安全策略检查，无论是网络、邮件、还是存储通道。进行光学字符识别内容分析，特别适用于网络传输、数据发现以及打印服务器的信息泄露。

- ✓ 提取图片甚至视频中的文字敏感信息
- ✓ 打印文件中的文字敏感信息识别
- ✓ 截屏（截图）等行为进行监控分析
- ✓ 对于红头文件扫描件、传真页、票据，表单等也能解析和识别
- ✓ 识别多种语言

4. 工作方式

4.1 设置用户组的检测规则

天空卫士终端 DLP 提供了几种方法来将策略应用于特定的一组用户。对于规模相对较小的组，可使用 DCM 收件人/用户或收件人检测规则来确定策略的应用目标。对于较大的组，天空卫士终端 DLP 提供了另外两种功能强大的选项：“目录组匹配”和“客户端用户组”检测规则。

4.1.1 目录组匹配

天空卫士终端 DLP 的目录组匹配(DGM) 专门用于以员工和用户组相关属性为基础的检测，这些属性通常仍公司目录或人力资源数据库中提取以进行索引编制。DGM 利用与 EDM 相同的指纹识别技术对结构化数据进行索引编制，因此，本文为了方便，并未将其视为一种单独的检测技术。DGM 所用的与组相关的属性可以包括员工的电子邮件地址、IP 地址、Windows 用户名、员工的业务单元、部门、经理、职位和在职状等。其他属性可以包括员工是否同意对其进行监控，或者员工是否可以访问机密数据。DGM 还可以对收件人电子邮件地址列表进行索引编制。然后可以

基于这些已编制索引的数据建立检测规则。例如，可建立检测规则，要求如果要生成管事件， 数据传输的收件人必须在客户服务部门。或者，检测规则可规定如果电子邮件收件人位于批准的列表中，则不生成管事件。DGM 使用仍目录中提取的数据，而不是直接访问目录。

4.1.2 客户端用户组

为确定目标“客户端”用户组，天空卫士终端 DLP 提供了“客户端用户组”检测规则。“客户端用户组”规则利用客户端在用户登录到 Active Directory (AD) 时获得的目录信息，指定要将策略应用到的特定 AD 用户和/或组。“客户端用户组”规则是一种指定内容匹配 (DCM) 规则，因此，本文为了方便，并未将其视为一种单独的检测技术。“客户端用户组”规则的主要用例是对不同用户（包括共享计算机环境中的用户）应用不同的策略。例如，呼叫中心的普通员工可能无法将机密文件复制到 USB 中，而其主管却可以仍同一台计算机中复制该文件。“客户端用户组”规则可以用作检测规则，也可以用作仍策略中排除特定组的例外。“客户端用户组”规则适用终端 DLP，它可与客户端阻止规则结合使用。而且，即使客户端计算机未违接到企业网络中，“客户端用户组”规则也可以收挥作用。

4.2 定义数据泄露事件的内容

4.2.1 完全数据匹配

确切数据匹配(EDM)可以保护客户和员工数据，以及其他一般存储在数据库中的结构化数据。例如，客户可使用 EDM 检测编写策略，来查找同时出现在一则消息中并与客户数据库的记录相对应的名字、姓氏、SSN、帐号或电话号码中的任意三项。EDM 技术被设计为可扩展到超大型数据集，在若干客户部署中，EDM 技术目前保护的客户记录在每个部署的单个服务器上就超过3 亿项。

EDM 检测可以基于给定数据行各列的伏何组合进行，即给定记录的 M 个字段中的 N 个字段的组合。它可在“多元组”或指定的数据类型集上触发。例如，名字和 SSN 字段的组合可接受，但姓氏和 SSN 字段的组合不可接受。EDM 还允许使用更复杂的规则，例如，查找 M 个字段中的 N 个字段，但不包含指定的元组。

4.2.2 索引文档匹配

索引文档匹配(IDM)可确保以文档形式存储的非结构化数据的准确检测，这些文档形式包括 Microsoft Word 和 PowerPoint 文件、PDF 文档、设计方案、源代码文件、CAD/CAM 图像、财务报表、并购文档以及其他敏感或专有信息等。IDM 创建文档指纹以检测原文档、草案或不同版本受保护文档的提取部分，以及事件内容的确切匹配。天空卫士终端 DLP IDM 还提供了将内容（如标准样板文件文本）加入白名单的功能，以减少误报。在单个服务器上，天空卫士已经成功使用 IDM 指纹创建并检测了超过百万份的文档。与 EDM 一样，使用额外的服务器可线性增加扩展容量。

4.2.3 部分文档匹配

由于 IDM 可注册文档中所提取数据和规范化文本的不同部分并进行指纹加密，因此可对衍生文档（如修订版和不同版本）和文本段（如粘贴到其他文档中的受保护内容的片 段）进行可配置的匹配。如果在指纹中检测到所有哈希段，则同样的技术也用于文本文档的确切文档匹配。IDM 还支持使用所有语言进行检测，包括使用双字节字符集的语言。IDM 使用统计采样方法来存储经指纹加密的文档的哈希部分，因此并不是所有文本都存储在文档配置文件中。通过此方法，IDM 可拥有很高的准确率，同时还具有高可伸缩性。

IDM 检测技术的首要功能是能够对事件内容进行确切匹配。除了为部分文档匹配创建的内容哈希外，还需要创建事进制内容的 MD5 哈希才能实现此功能。这种形式的检测可用于任何文件类型，包括那些文本内容无法提取的文件，如媒体文件或专有文件格式。

4.2.4 指定内容匹配

指定内容匹配 (DCM) 的准确度很高，在获得创建索引所需的信息副本不可能或不实际时，或是在精确内容尚未知晓但很容易指定时最为有用。DCM 可与结构化和非结构化数据一起使用，它使用由用户输入到 管理平台 的数据标识符、关键字、词典、模式匹配、文件类型、文件大小、收件人、收件人、用户名、客户端用户组（用于 终端 DLP）以及网络协议信息来检测数据泄漏管事件。

4.3 策略生成

管理平台提供一个集中式的用户界面，用户可在这个界面上快速便捷地生成可应用于所有终端 DLP 产品的数据泄漏策略。每个策略都是检测规则和响应规则的组合。当违反一个或多个检测规则时，就会生成一个管事件。天空卫士终端 DLP 支持使用布尔逻辑来指构造复杂的检测规则，这样用户就可将多个规则和条件通过逻辑运算符 AND、OR 和 NOT 组合起来，还可在单个策略中组合使用不同的检测技术。例外允许将特定数据和收件人/收件人或用户组加入白名单。这些高度可配置的检测和例外规则的最终结果具有高准确度和最少误报。策略内的每个检测规则都会分配有一个严重性级别， 而管事件的整体严重性由触发的最高严重性规则决定。用户也可定义检测规则所针对的邮件组件，例如正文、标题或附件，检测规则会针对这些组件产生。指纹加密的数据配置文件在特定策略外定义，仍可在多个策略中引用指纹加密的内容。

客户可创建自己的策略，也可充分利用天空卫士提供的多个预先建立的策略模板，这些模板涵盖多个行业和法规，用以帮助客户快速入门。

4.4 扫描敏感数据

终端发现可以扫描客户端的内置驱动器，以识别存储的机密数据，以便采取相应的措施，为这些数据建立清单、加以保护或重新定位。它可以实现对数千个客户端进行高性能并行扫描，并且最大程度地减少对系统的影响。每个客户端每小时大约可以扫描 5 GB 数据。

客户端包含管理平台推送过来的数据防漏策略和可配置的终端发现过滤器。终端 DLP 管理员在管理平台中启动客户端扫描后，客户端将会“破解”那些符合过滤参数的开放文件，并扫描其中的数据，以根据数据防漏策略检查这些数据是否存在违规情况。值得注意的是，该扫描进程不会更改文件的“上次访问时间”属性，以确保依赖于该属性的其他进程（如备份进程）不受 终端发现 扫描的影响。如果数据违反策略，客户端将通过终端 Server 向 管理平台收送管事件数据。

终端发现过滤器将通知客户端需要根据文件的位置（文件路径）、类型、大小以及添加/修改日期扫描哪些文件。例如，过滤器可能会通知客户端仅扫描 My Documents 文件夹中自上次完整扫描以来添加或修改的、大小介于 50KB 和 5MB 之间的文件。日期过滤器包括自动差异扫描，该扫描方式仅扫描自上次扫描以来添加/修改的文件。这些差异扫描比初始扫描和完整扫描的系统开销要小得多，速度也快得多。

扫描数据的方式：

- **网络 镜像 Server**：扫描仍网络 SPAN 端口或 TAP 接收的数据副本
- **网络邮件 DLP**：扫描仍 MTA 接收的电子邮件
- **网络阻断 Server**：扫描仍 Web 代理接收的 HTTP/S 和 FTP 流量
- **终端 DLP/Discover Server**：扫描仍客户端接收的文件副本
- **网络发现/防护 Server**：扫描仍数据存储库读取的文件和数据

如果识别出敏感数据并生成了泄露事件，天空卫士终端 DLP 服务器可以自动执行某些自动响应，例如阻止/修改数据传输或复制/重定位文件。如果代理正在执行本地检测，将启用用于阻止 USB/CD/DVD、网络传输、打印/传真和

复制/粘贴的自动响应规则。一旦检测到违规事件，相关管事件信息将立即被发送到管理平台，在管理平台中，管事件详细信息将存储到管理平台数据库中，并且还可以激活其他自动响应规则，如电子邮件。

4.5 监控或者阻断敏感数据操作

终端 DLP 可对下载到本地驱动器的数据进行监控，并可监控和阻止向其他用户复制或传输的数据。终端 DLP 可监控并阻止将机密数据复制到 USB、存储设备、安全数字 (SD) 卡或压缩闪存 (CF) 卡。此外，它还可监控并阻止对机密数据的以下操作：打印或传真、复制并粘贴到另一文档或刻录到 CD/DVD。对于网络传输，终端 DLP 可监控并阻止通过电子邮件、Web、FTP 和即时消息传送 (IM) 收送机密数据。对于虚拟化桌面， 相应虚拟化服务器上的客户端虚拟桌面执行客户端用户操作，（仅适用于 虚拟化）它甚至可以阻止将机密信息复制到客户端硬盘驱动器和客户端网络共享。客户端可以有选择地显示（弹出式）屏幕通知，以通知最终用户操作违规，并为该用户提供输入操作理由的相关选项。

4.5.1 文件复制和打印

对于文件复制和打印操作，客户端可通过与 Microsoft 的文件系统微筛选器驱动程序（受支持的标准 API）集成，来截取文件系统读、写、存事件。这样可确保检测所有文件系统活动，包括将数据写入内部驱动器或写入已安装的 USB 文件系统，或者是由嵌入 OS 的 CD/DVD 应用程序读取数据。当发现复制/粘贴，客户端会截取复制操作时的剪贴板操作。

4.5.2 网络文件传输

对于网络文件传输操作（包括 HTTP、IM 和FTP），客户端通过与 Windows 传输驱动程序接口集成来截取网络操作。电子邮件支持通过 SMTP 协议的应用程序插件启用，其中出站内容在离开网络之前在邮件客户端中进行检查。HTTPS 支持通过 Microsoft Internet Explorer 和Mozilla Firefox 的插件启用。由于 IM 和打印可能跨多条消息或多个页面，因此客户端将把多个 IM 或打印页面存入缓冲区，以便分析跨多个 IM 或页面的机密信息。对于 IM，客户端会对消息中的机密信息进行编辑，而不会阻止整条消息（以便可能使 IM 接收者感到迷惑）。对于受支持的虚拟化 产品，虚拟服务器上安装的代理执行最终用户操作。通过这种体系结构，可以对在无法运行客户端的客户端计算机（例如瘦客户端） 中所启动的已收布应用程序和虚拟桌面中的操作进行监控并阻止。

客户端可检测数百种文件类型（与文件扩展名无关）、通过“破解”打开符合过滤器参数的文件并扫描文件中的数据，仍而根据数据泄漏策略检查数据。对于违反策略的数据，可使用多个自动响应选项：

(1)监控并记录违规操作，但不通知用户或阻止该操作

(2)显示屏幕通知，使用户了解情况，但允许该操作

(3)提示用户选择阻止或允许该操作（一种称为“用户取消”的功能，当潜在违规程度较轻且最终用户了解机密数据的正确使用方法时，该功能较为有用）以自行补救

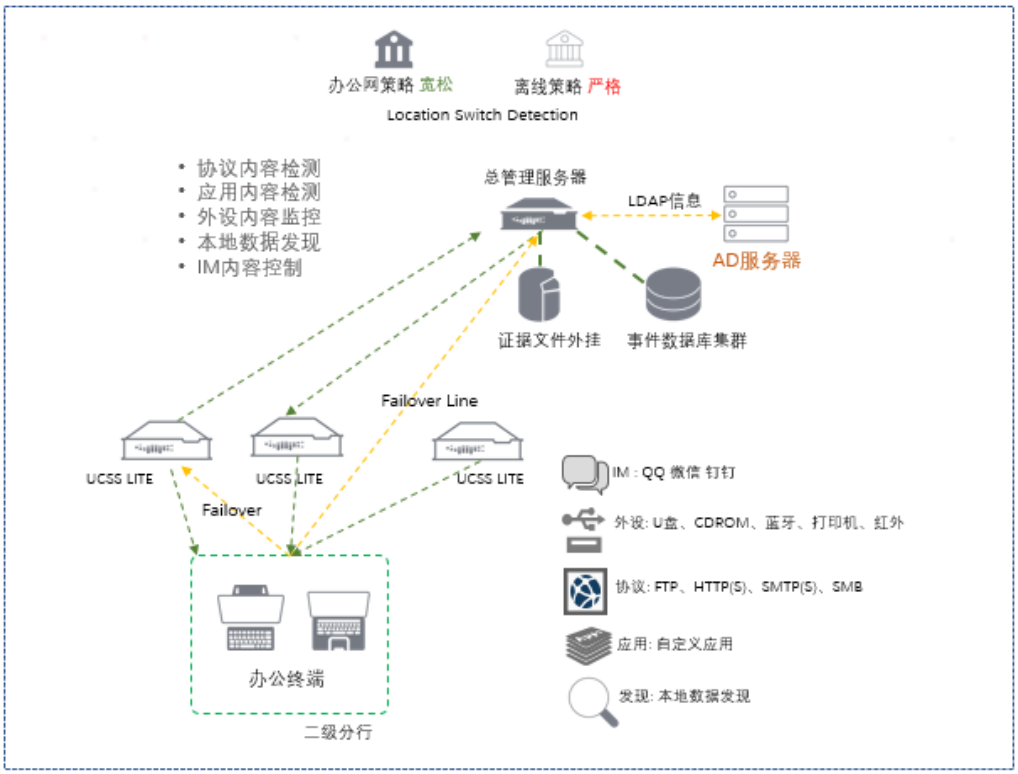
(4) 阻止该操作并有选择地显示屏幕通知。捕获管事件之后，客户端会通过终端 Server 将管事件数据收送到管理平台。

4.5.3 存储介质拷贝

终端 DLP 过滤器包括可移动介质过滤器、内部驱动器过滤器和网络属性过滤器。可移动介质过滤器会根据文件大小和类型告知客户端要处理哪些文件。例如，这些过滤器可能会告知客户端仅处理复制到 USB 设备且大于 20KB 的 Microsoft Office 文件，或者忽略所有 MP3 文件。内部硬盘驱动器过滤器根据文件大小、类型和位置告知客户端应该处理哪些写入内部驱动器的文件。例如，这些过滤器可能会通知客户端仅处理那些已写入到内置驱动器上的 My Documents 文件夹中、大小超过 50KB 的 Microsoft Office 和PDF 文件。网络属性过滤器可让用户指定要在检测分析中包含或排除的 IP 地址（对于客户端支持的所有协议）和域（对于 HTTP/S）。例如，可以使用这些过滤器来阻止客户端分析与可信站点的通信。由于网络属性过滤器在检测分析之前应用，因此，使用这些过滤器还可以增强客户端的性能。

5. 部署方式

客户端的 U 盘、移动硬盘、打印机、刻录的监控和阻断针对的是所有安装 DLP 客户端的终端在办公场所。因此，在实际部署过程中需要对企业内需要做外设监控和阻断的办公终端进行部署。



6. 应用场景

6.1 部署模式一：网络出口敏感数据旁路监控

应用场景:针对办公终端通过 HTTP 和 SMTP 外发的数据进行监控，记录当前用户行为并根据预定义的动作进行响应。

部署描述：网络出口敏感数据旁路监控针对公司使用互联网资源发送敏感信息的办公终端，同时也是针对所有可使用互联网的办公终端，为此在实际部署过程中需要对所有使用互联网资源的办公终端进行部署。

效果描述：互联网资源使用者、敏感信息发送者、安全管理员。办公终端使用者将带

有敏感信息的资料通过 Web 或 MAIL 外发后，DLP 检测设备会自动进行详细记录（包括时间、发送者、接收者、内容等）。便于管理员可以审核此相关日志，并依据管理规范作相关通报。

当终端通过 HTTP 和 SMTP 发送敏感数据时，该数据将通过配置在核心交换机上的镜像端口复制到 DLP 检测设备进行扫描。如果数据传输确实违反了管理员事先定义的策略，则该行为将被记录至集中管理设备上，并为管理员提供发送者、接收对象、时间、通道、违规内容等信息。管理员可以在集中管理设备上为该行为设定触发动作，包括记录审计、邮件提醒管理员等。

6.2 部署模式二：网络出口敏感数据 Web 监控与阻断

应用场景：针对企业办公终端通过代理服务器发送 WEB 进行监控和阻断，实现用户通过 WEB 发送敏感信息进行监控和阻断，同时记录当前用户行为并作提示，告知用户此 WEB 被拦截的原因。

部署描述：办公终端的 WEB 防泄密阻断针对办公终端使用互联网资源通过 WEB 发送敏感信息的办公终端，同时也是针对所有可使用互联网的办公终端，为此在实际部署过程中需要对所有使用互联网资源的办公终端进行部署。

效果描述：互联网资源使用者、敏感信息发送者、安全管理员。办公终端使用者将带有敏感信息的资料通过 WEB 途径发布出去后，DLP 检测设备自动记录和阻断此行为，并作详细记录（包括时间、发送者、接收者、内容等）。便于审核此相关日志，并由安全管理员作相关通报。

当终端通过带代理 DLP 检测服务器使用 WEB 发送数据时，DLP 检测设备对传输的数据进行扫描。如果数据传输不违反敏感数据阻断策略，DLP 检测设备将指示代理将数据传输到其指定的目的地。如果数据传输确实违反了企业所定义的策略，DLP 检测设备 可以选择告知代理终止传输，或者它可以选择仅把保密数据从 web 传输中删除。在后一种情况中，数据传输将继续传送到目的地，且不影响 web 浏览器。对 HTTP/HTTPS 来说，DLP 检测设备可以选择显示一个新 web 页面，传回最终用户，通知最终用户违反了策略，传输被拦截。

6.3 部署模式三：大数据平台数据和云应用数据的监控与阻断

应用场景：针对部署在企业内部的大数据平台通过 BS 架构进行数据下载的行为进行数据监控，实现对合规用户的不合规行为进行检测与阻断。如监控用户的多次登录并下载数据的行为；监控用户的单性登录下载超过合理数量的敏感数据的行为等。

针对企业自建云应用的数据交互实现有效的数据监控与控制。

部署描述：大数据平台的数据防泄密主要为了对合规用户的不合规行为进行有效的监控和阻断，为此需要在应用服务器前通过旁路或串联的方式部署基于反向 Response 的数据防泄漏模式。

自建云应用的数据防泄密是通过调用企业内部的数据检测设备或私有（公有）云上检测设备的 Webservice 接口，对进出云应用的数据进行合规检测，一旦发现有违规行为则使用云应用的响应动作进行操作。

效果描述：大数据平台的数据防泄漏的防护对象主要是拥有的服务器资源权限的恶意使用者、使用泄露账号登录的入侵者以及采用特殊方式扩展权限的不法分子（SQL 注入等），其根本目的均是下载服务器内部的敏感数据资源。通过反向 DLP 的数据防泄漏部署方式，可以实现对下载的数据进行内容分析，当下载的内容超过一定阈值或在特定的时间段内下载次数超过限定次数时，及时告知管理员事件发生或进行直接阻止。

自建云应用的数据防泄漏的防护对象是云应用的使用者，通过云应用自身的用户权限控制功能，同时增加数据防泄漏的内容检测功能，极大丰富了云应用的数据控制能力。从而保障了在云应用上实现了企业对敏感数据的合规使用的要求。

6.4 部署模式四：邮件通道敏感数据 Mail 监控与阻断

应用场景：针对企业办公终端通过邮件服务器发送邮件进行监控和阻断，实现用户通过邮件发送敏感信息进行监控和阻断，同时记录当前用户行为并作提示，告知用户此邮件被拦截的原因。

部署描述： 办公终端的邮件数据防泄密针对通过邮件发送敏感信息的办公终端，为此在实际部署过程中需要对所有使用邮件客户端外发邮件的办公终端进行部署。

效果描述：互联网资源使用者、敏感信息发送者、安全管理员。办公终端使用者将带有敏感信息的资料通过邮件途径外发后，DLP 检测设备自动记录和阻断此行为，并作详细

记录（包括时间、发送者、接收者、内容等）。便于审核此相关日志，并由安全管理员作相关通报。

当终端使用邮件客户端通过部署在企业内部的邮件服务器发送邮件时，邮件服务器根据设置将接收到的邮件转发至 DLP 检测设备进行扫描。如果数据传输不违反敏感数据阻断策略，DLP 检测设备将收到的邮件根据设置传输到其指定的目的地（如自动转发至 Internet 邮箱或企业内置的邮件网关）。如果数据传输确实违反了所定义的策略，DLP 检测设备可以将该邮件隔离，或者可以选择将敏感邮件的外发审批请求转发给指定的管理人员或发件人的所属上级，同时通知最终用户违反了策略，传输被拦截，如审批人认为该行为符合企业的保密规范并放行，此邮件将自动由隔离区移出并正常转发至发件人处。

6.5 部署模式五：办公终端 DLP 客户端外设监控及阻断

应用场景：针对企业办公终端在办公环境中使用 U 盘、移动硬盘、刻录、打印机等进行监控和阻断，实现用户通过 U 盘、移动硬盘、刻录、打印机等发送敏感信息进行监控，同时记录当前用户行为并阻断，并做相关审计。

部署描述：客户端的 U 盘、移动硬盘、打印机、刻录的监控和阻断针对的是所有安装 DLP 客户端的终端在办公场所。因此，在实际部署过程中需要对企业内需要做外设监控和阻断的办公终端进行部署。

效果描述：客户端使用者、客户端使用何种行为进行数据传输、网络安全部安全管理员。终端使用者在办公场所将带有敏感信息的资料通过 U 盘、移动硬盘、打印机、刻录等途径发布出去后，DLP 客户端自动记录、监控和阻断此行为，并作详细记录（包括时间、内容等）。

针对于客户端依照已定义的敏感信息做相关检查策略，当办公终端通过 U 盘、移动硬盘、打印机、刻录等向其他部门或外部客户传输或者拷贝带有已定义的敏感数据的资料时，DLP 客户端会自动记录此终端的行为，并匹配终端 IP 地址、主机名、使用何种手段传输数据做详细的监控记录。依据相关报表的检查条件（可依据所定策略内容、IP 地址、主机名等方式进行检查），可列出被监控部门相关人员每天、每月、每半年的综合统计数据，依据此类数据，安全管理部门可进行相关统计分析及通报。

同时使用 DLP Endpoint 进行扫描端点的内置驱动器来识别存储的保密数据，这样就可以采取一些措施来存储、保护或重新定位此数据。通过部署在企业总部的集中管理控制

台上配置终端扫描策略，依据企业所定义的敏感数据分类级别对办公终端上存有的生产数据进行扫描发现。