NSFOCUS

绿盟数据泄漏防护系统

产品白皮书

© 2019 绿盟科技

目录

一. 前言

1.1 简介

本白皮书的目的在于帮助技术评估小组复查绿盟科技所提供的 Nsfocus Data Loss Prevention Solution。内容包括 NSFOCUS DLP 软件包的技术特色，涵盖 SIP 检测技术和控制技术的“工作方式”说明、构成整个 NSFOCUS DLP 软件包的多项产品，以及基本的系统基础配置、架构及安全性。

本白皮书还讨论 NSFOCUS DLP 与客户已有的基础配置与网络进行交互和集成的典型方式。

1.2 适用范围

本文档适用于需要对绿盟数据泄漏防护系统（以下简称“NSFOCUS DLP”）进行全面了解或以前接触过 DLP 概念并想做进一步了解的用户。如需要了解产品的其他相关信息，请联系绿盟科技的销售工程师，由他们对您提出的问题和疑问集中进行解答。

1.3 术语和缩略语

术语、缩略语	解 释
SIP	Security Intelligence Platform（智能安全管理平台）
DLP	Data Leakage(Loss) Prevention（数据泄露防护）

表 1-1 常用术语及缩略语

二. 产品介绍

2.1 产品概述

DLP 是一款内容识别安全技术，可解决敏感企业信息的三大关键问题：

1、敏感企业信息存储在何处？

2、敏感企业信息使用情况如何？

3、如何保护敏感企业信息，以防丢失和被窃？

无论处于下列哪种状况，NSFOCUS DLP 均可让组织保护客户数据、公司信息、知识财产及敏感或机密信息：通过电子邮件、Web 邮件或其他 Internet 协议离开网络 (网络 DLP)；通过 USB/CD/DVD 离开终端或存储在终端 (终端 DLP)；存储在共享服务器及数据存储库中 (存储设备 DLP)。

NSFOCUS DLP 软件包由 SIP 智能安全平台管理应用程序及八项组件组成：

SIP Network Monitor （网络监控 DLP）

SIP Network Prevent for E-mail （邮件防护 DLP）

SIP Network Prevent for WEB （网络防护 DLP）

SIP Endpoint Prevent （终端防护 DLP）

SIP File Storage Insight （文件存储洞察 DLP）

SIP Database Insight （数据库洞察 DLP）

SIP Business Interface System （商用接口服务器）

SIP Workflow Management System （工作流管理系统）

虽然这八项组件都可以单独部署或组合部署，但它们始终需要与 SIP(Security Intelligence Platform) 智能安全平台管理应用程序一起实现。

SIP （Security Intelligence Platform）

SIP 是所有产品模块的中央管理应用程序，用于自动运行组织的数据安全策略。在 SIP 平台 WEB 中，可创建用于自动检测和保护敏感数据的数据丢失策略、控制策略、工作流程及审计信息、生成报告，并配置以角色为基础的访问权限和系统管理。

SIP Network Monitor

SIP Network Monitor 常驻于网络出口点，可监控网络数据。所涵盖的协议包括电子邮件 (SMTP)、Web (HTTP)、即时消息 (IM)、文件传输 (FTP)，以及通过任何端口进行的所有其他 TCP 会话。

SIP Network Prevent for E-mail

SIP Network Prevent for E-mail 常驻于企业邮件服务器后，可监控和禁止/修改企业邮件中的敏感信息。包含邮件的发件人、标题、内容和附件。

SIP Network Prevent for WEB

SIP Network Prevent for WEB 常驻于网络出口点，可监控和禁止/修改网络数据。所涵盖的协议包括电子邮件 (SMTP)、Web 和安全 Web (HTTP/HTTPs) 以及文件传输 (FTP)。

SIP Endpoint Prevent

SIP Endpoint Prevent 常驻于员工的笔记本电脑及台式机计算机，可监控下载到内部硬盘的数据，并监控和禁止复制到 USB 设备、智能移动设备及 CD/DVD 的数据。

Endpoint DLP 可在终端进行网络层面的安全控制，比如禁止敏感信息邮件外发，禁止 QQ 发送敏感信息内容等。

对于文档，Endpoint DLP 可以进行权限授权、加密控制、标定密级等安全控制，保证数据更高的安全等级。

Endpoint DLP 可以对终端计算机进行端口、磁盘和外设设备（如 U 盘）的安全管控，如全磁盘加密、可信介质管理等功能。

对于敏感文件的发现，Endpoint DLP 可以提供终端数据快速扫描的功能，可供管理员对于每个员工存储的敏感信息数据数量和位置进行查询，以便采取相关步骤。

SIP File Storage Insight

SIP File Storage Insight 可对文件共享服务器上的文件进行扫描，且不需要在服务器上安装 agent 程序，对于扫描出的机密数据文档进行事件通知和告警管理员，以便采取相关步骤。

SIP Database Insight

SIP Database Insight 可对数据库表或字段进行扫描，且不需要在服务器上安装 agent 程序，对于扫描出的非法数据表存储敏感数据的情况进行事件通知和告警管理员，以便采取相关步骤。

SIP Business Interface System

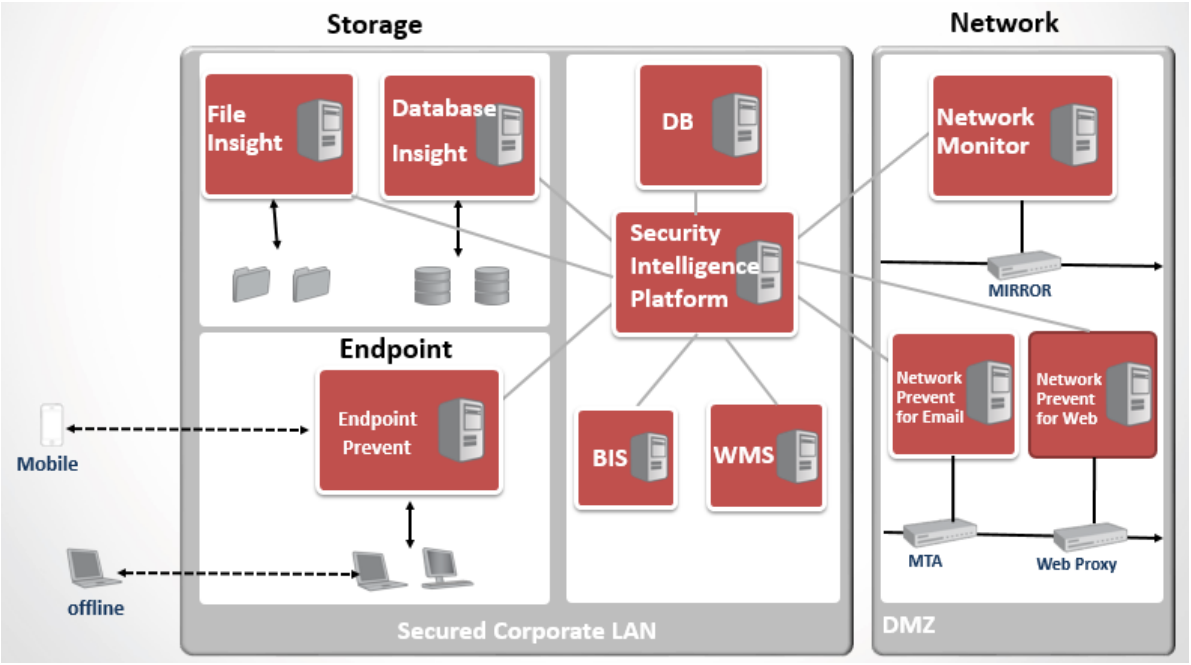
SIP Business Interface System 商用接口服务器通过 Web Service 方式向第三方系统提供一系列的服务能力，比如加密、解密、授权、外发文件制作、数据敏感信息检测、审批工作流托管等功能，以便和用户侧的 OA、ERP、PDM、SAP 等系统进行对接，更深入的和客户业务系统结合，提供一体化的服务。

SIP Workflow Management System

SIP Workflow Management System 工作流管理系统，当客户需要将敏感文档进行脱敏、解密、外发、权限变更时，工作流管理系统提供了流程审批的功能，其中提供会签、多级审批等场景设置，并且可分别设置不同部门的审批管理员，所有提交的审批和相关文件都将被存储备份保存可被审计，同时提供多种查询方式。

2.2 产品组成

下图说明 NSFOCUS DLP 的实体配置，以及不同产品在组织内的常驻位置。“网络 DLP”产品常驻于 DMZ 中，而其他产品则常驻于企业 LAN 或数据中心。 除了“终端 DLP”产品以外，所有其他产品都是以服务器为基础；您可以在附录中找到各种 NSFOCUS DLP 产品的硬件要求。



2.3 检测与准确性

为了预防数据丢失，无论数据的存储、复制或传输位置在哪里，都必须准确地检测所有类型的机密数据。如果没有准确的检测，数据安全系统就会生成许多误报（将并未违规的消息或文件标识为违规）以及漏报（未将违反策略的消息或文件标识为违规）。误报会大量耗费进行进一步调查和解决明显事故所需的时间和资源。漏报会掩盖安全漏洞，导致数据丢失、潜在财务损失、法律风险并有损组织声誉。

检测技术概述:

为了确保最高的准确性，NSFOCUS DLP 采用了三种基础检测技术和三种高级检测技术：

基础检测技术：

正则表达式检测（标示符）

关键字和关键字对检测

文档属性检测

基础检测方法采用常规的检测技术进行内容搜索和匹配，比较常见的都是正则表达式和关键字，此两种方法可以对明确的敏感信息内容进行检测；文档属性检测主要是针对文档的类型、文档的大小、文档的名称进行检测，其中文档的类型的检测是基于文件格式化进行检测，不是简单的基于后缀名检测，对于修改后缀名的场景，文件类型检测可以准确的检测出被检测文件的类型，目前支持 100 多种标准的文件类型，并且可以通过自定义特征，去识别特殊的文件类型格式的文档。

高级检测技术：

精确数据比对 (EDM)

指纹文档比对 (IDM)

向量分类比对 (SVM)

EDM 用于保护通常为结构化格式的数据，例如客户或员工数据库记录。IDM 和 SVM 用于保护非结构化的数据，例如 Microsoft Word 或 PowerPoint 文档。对于 EDM、IDM、SVM 而言，敏感数据会先由企业标识出来，然后再由 NSFOCUS DLP 判别其特征，以进行精准的持续检测。判别特征的流程包括 NSFOCUS DLP 访问和检索文本及数据、予以正规化，并使用不可逆的打乱方式进行保护。

NSFOCUS DLP 检测是以实际的机密内容为基础，而非根据文件本身。因此，NSFOCUS DLP 不只能检测敏感数据的检索项或衍生项，而且能够标识文件格式与特征信息格式不同的敏感数据。例如，如果已经判别出机密 Microsoft Word 文档的特征，NSFOCUS DLP 就能够在相同的内容以 PDF 附件的方式通过电子邮件进行提交时，将其准确检测出来。

精确数据比对：

精确数据比对（EDM）可保护客户与员工的数据，以及其他通常存储在数据库中的结构化数据。例如，客户可能会撰写有关使用 EDM 检测的策略，以在消息中查找“名字”、“身份证号”、“银行帐号”或“电话号码”其中任意三项同时出现的情况，并将其映射至客户数据库中的记录。

EDM 允许根据特定数据列中的任何数据栏组合进行检测；也就是在特定记录中检测 M 个字段中的 N 个字段。它能够在“值组”或指定的数据类型集上触发；例如，可接受名字与身份证号这两个字段的组合，但不接受名字与手机号这两个字段的组合。

由于会针对每个数据存储格存储一个单独的打乱号码，因此只有来自单个列的映射数据才能触发正在查找不同数据组合的检测策略。例如，有个 EDM 策略请求“名字 + 身份证号 + 手机号”的组合，则“张三”+“13333333333”“110001198107011533” 可触发此策略，但是即使 “李四”也位于同一数据库中，“李四”+“13333333333”“110001198107011533”也不能触发此策略。EDM 也支持相近逻辑以减少可能的误报情形。对于检测期间所处理的自由格式文本而言，单个特征列中所有数据各自的字数均必须在可配置的范围内，方可视为匹配项。例如，依默认，在检测到的电子邮件正文的文本中，“张三”+“13333333333”“110001198107011533”各自的字数必须在选定的范围内，才会出现匹配项。对于含有表式数据（例如 Excel 电子表格）的文本而言，单个特征列中所有数据都必须位于表式文本的同一行上，方可视为匹配项，以减少整体误报情形。

指纹文档比对：

“指纹文档比对”（IDM）可确保准确检测以文档形式存储的非结构化数据，例如 Microsoft Word 与 PowerPoint 文件、PDF 文档、财务、并购文档，以及其他敏感或专有信息。IDM 会创建文档指纹特征，以检测原始文档的已检索部分、草稿或不同版本的受保护文档。

SIP IDM 首先要进行敏感文件的学习和训练，拿到敏感内容的文档时， IDM 采用语义分析的技术进行分词，然后进行语义分析，提出来需要学习和训练的敏感信息文档的指纹模型，然后利用同样的方法对被测的文档或内容进行指纹抓取，将得到的指纹与训练的指纹进行比对，根据预设的相似度去确认被检测文档是否为敏感信息文档。这种方法可让 IDM 具备极高的准确率与较大的扩展性。

向量机分类比对：

支持向量机（Support Vector Machines）是由 Vapnik 等人于 1995 年提出来的。之后随着统计理论的发展，支持向量机也逐渐受到了各领域研究者的关注，在很短的时间就得到很广泛的应用。支持向量机是建立在统计学习理论的 VC 维理论和结构风险最小化原理基础上的，利用有限的样本所提供的信息对模型的复杂性和学习能力两者进行了寻求最佳的折衷，以获得最好的泛化能力。SVM 的基本思想是把训练数据非线性的映射到一个更高维的特征空间（Hilbert 空间）中，在这个高维的特征空间中寻找到一个超平面使得正例和反例两者间的隔离边缘被最大化。SVM 的出现有效的解决了传统的神经网络结果选择问题、局部极小值、过拟合等问题。并且在小样本、非线性、数据高维等机器学习问题中表现出很多令人注目的性质，被广泛地应用在模式识别，数据挖掘等领域。

SVM 比对算法适合那些具有微妙的特征或很难描述的数据，如财务报告和源代码等。

使用过程中，先将文档按照内容细分化分类，每一类文档集合有属于本类的意义，经过 SVM 比对，确定被检测的文档属于哪一类，并取得此类文档的权限和策略。

同时，针对 SVM 的特点，可以进行终端或服务器上的文档按照分类含义进行分类数据发现。

IDM 和 SVM 的比对区别是，IDM 将待检测文件的指纹和训练模型中的每一个文件进行指纹比对；而 SVM 是将待检测文件向量化，并归属到某一类训练集所建立的向量空间。

2.4 多语言和语义的检测支持

NSFOCUS DLP 提供多种语言的检测支持，简体中文、繁体中文、日文、韩文、英文。

同时也提供多种语言的语义识别。

2.5 策略建置程序

NSFOCUS DLP 提供集中化的用户界面，用户可通过 UI 快速而轻松地建置可应用到所有模块产品的数据丢失防护策略。每项策略都是由检测规则与响应规则组合。若违反一条或多条检测规则，则会生成事故。系统支持布尔逻辑以建构复杂的检测规则，让用户得以利用 AND、OR 及 NOT 逻辑运算符来组合多个规则及条件，以及将不同的检测技术结合到单个策略中。对于特定程序及发件人/接收人的“白名单”，则允许异常错误状况。这些可高度配置之检测及异常错误状况规则的最终结果，就是准确性很高并使误报情形减至最少。策略中会指定一个严重性等级，而事故的整体严重性则是由触发的最高等级严重性规则来决定。用户也可以定义要应用任何检测规则的消息组件，例如正文、标题或附件。此外，特征数据配置文件是定义于特定策略之外，这可让多项策略参照特征内容。

客户可以创建自己的规则，也可以利用系统提供的内置检测规则，可帮助客户快速开始使用。

违反数据丢失策略时，会针对该策略自动触发响应规则。自动响应规则可由不同的条件触发，包括事故严重性、事故匹配项计数、消息的协议、非法的应用程序等。系统提供的自动响应规则，包括发送电子邮件通知（提交给最终用户及/或其管理者等等）、设置事故的状态、禁止文件使其不能复制到 USB 设备，不能上传到网盘，不能通过 web mail 发送，不能通过 IM 聊天工具发送，不能通过 outlook 等终端进行邮件发送，并在员工的屏幕上显示弹出式消息、禁止数据传送(SMTP/HTTP/HTTPS/FTP)、修改 SMTP 电子邮件，阻断违规程序。这些自动响应规则提供多种方法来自动处理违规事件，以着重于补救措施，并确保适当的响应级别。

三. 组件描述

3.1 网络 DLP（Network DLP）

3.1.1 概述

SIP Network DLP 产品常驻于 DMZ 中的网络出口点，由 SIP Network Monitor、SIP WP DLP、 SIP MAIL DLP 组成。 SIP Network Monitor 会扫描所有离开组织的数据，以查看是否含有敏感信息。SIP MAIL DLP 会保护所有对外发送的邮件，对于涉及敏感信息的邮件会被审计、重定向、阻断、加密、审批后发送等方式进行处理。 SIP WP DLP 将会对于通过 http 或 https 加密协议向外发送的数据进行敏感信息检测，并根据配置的策略进行审计、脱密或阻断等方式进行处理。

大多数 DLP 客户会将 Network DLP 产品用于多个协议，以确保防止各种数据丢失威胁。此外，客户也会了解到交替使用这三个组件的价值，因为 SIP 网络防护 DLP 添加了额外的自动禁止功能，而 SIP Network Monitor 则可涵盖其他两个组件所未涵盖的协议。SIP 的 Network DLP 解决方案可让组织监控离开组织的数据，以便保护知识财产、证明法规遵循，以及保护其品牌及声誉。

3.1.2 网络监控 DLP 的工作方式

SIP 网络监控(SIP Network Monitor) 会以被动的方式检查网络通信，并针对所有网络协议及内容类型，在信息离开网络之前检测其是否包括机密信息，从而让组织界定和量化数据丢失的风险。例如，SIP Network Monitor 可以检测到员工正在使用实时通信或公共 Web 邮件给竞争对手发送产品计划或机密文件。它也可以找出不完善的企业流程，这种流程会导致社会安全号码未经加密就通过电子邮件发送给可信的伙伴。SIP Network Monitor 的基本操作相当简单明了。它位于网络出口点，可分析网络数据包副本并检查数据是否违反策略，详见“检测与准确性”一节。

SIP Network Monitor 设置中包含网络协议配置，可以包括常用数据传输及交互式协议，例如：SMTP、HTTP、FTP 通信（包括主动及被动模式的传输数据及控制会话）、IM 通信、IRC 及 Internet News(NNTP)。通过常用 TCP 协议定义，可以自定义对非标准及专有协议的监控。

SIP Network Monitor 不会认识端口，但会根据协议特征来标识应用程序级别的网络通信，即使通信是从非原生端口离开，也可执行策略。例如，只要 TCP 连接的格式与 SIP 系统中配置的 HTTP 协议特征相匹配，则仍会对不使用标准 TCP 端口 80 的通信进行分析并分类为 HTTP。同样，由于 SIP 可以基于协议特征比对通信并识别通道协议，以 HTTP 做为通道的实时消息传送也会被适当地标识为 IM 协议。

SIP Network Monitor 通常是由客户配置，以检查最有可能丢失机密数据的通信。典型的数据中心会有相当多的低威胁通信（例如 UDP 或安全 VPN 通信），以及与高威胁通信（例如 SMTP、HTTP、FTP 及 IM）交错的入站通信。在标准部署中，SIP Network Monitor 的配置会过滤掉低威胁通信，以确保 CPU 不会耗费于低风险数据的处理。可从分析中去除的数据包括加密的通信、流媒体或低风险的自动管理服务（例如 IM Keep-Alive）。如果针对 IP 网络及地址、应用程序级别发件人和接收人，以及标题中的任意名称值配对来配置过滤器，即可将检查的网络通信范围缩小为风险最高的通信。

3.1.3 网络监控 DLP 部署

SIP Network Monitor 端口镜像配置。如果在网络切换器上使用端口镜像方法，则所有网络数据包（无论入站或出端口）都会复制到另一个连接至 SIP Network Monitor 的专用切换端口。通过这种方式，SIP Network Monitor 可获取所有通信的副本。这种方式不会影响客户原有组网拓扑和安全防护结构。

SIP Network Monitor 会实时处理通信，因此它必须能够处理尖峰负载。对于持续通信负载较高的网络，SIP 建议使用分流负载。镜像一份万兆流量引入分流设备，分流设备根据逐流进行 HASH，将流量分散到多个 Monitor 设备上，从而支持速度高达 10Gb/s 的持续传送量，而不会丢失数据包。为了支持高负载环境，SIP Network Monitor 可进行水平扩展，能够在多个 SIP Network Monitor 之间平衡通信负载。多个 Monitor 可连接到网络端口映射或接点，其中个别的 Monitor 可配置成搜索特定协议或某个范围的 IP 地址。另一种选择就是使用负载平衡设备，在网络接点与 Monitor 之间疏导通信。SIP Network Monitor 的扩展性极

佳，单个服务器能够分析多达 1Gb/s 的通信，而不会丢失数据包。在大型客户部署中，多个 SIP Network Monitor 可涵盖多于 100,000 多个用户，而一个客户在 24 小时内可处理多于十亿则消息。有关产品硬件要求，请参见“附录”。

3.1.4 网络防护 DLP 的工作及部署方式

网络防护 DLP 可用于 SMTP(网络防护 DLP for Email)或 HTTP/HTTPS/FTP (网络防护 DLP for Web)，并且可通过重定向、隔离或禁止含有机密数据的传送，主动防止丢失机密数据。HTTP 的涵盖范围包括 Web 邮件传送 (例如 163 或 QQ)、网站 POST、博客或 BBS 文章等通信。网络防护 DLP 会依“检测与准确性”一节所述来检查数据，以判定数据是否违反数据丢失策略。

3.1.5 邮件防护 DLP

邮件防护 DLP 服务器可通过以下两种集成模式之一，集成到现有的企业通信基础配置中：反射模式或转发模式。在反射模式中，来自 MTA 的电子邮件会转发到邮件防护 DLP 进行检查，然后再反射回同一 MTA。在转发模式中，邮件防护 DLP 会接收来自上游 MTA 的消息、分析消息，然后将消息反射到下游 MTA(而非反射回到原始 MTA)。邮件防护 DLP 使用的 API 能与各种的企业级 MTA 兼容，而这些 MTA 都支持标准 SMTP 及扩展 SMTP(eSMTP)消息与转发功能。这可让公司使用其现有的基础配置，无需在出端口 SMTP 消息流程中添加额外步骤。

邮件防护 DLP 已经成功执行来自以下公司之 MTA 的集成测试：IronPort、Postfix、CipherTrust、Sendmail、Proofpoint、SonicWall 及 Clearswift。在加密方面，邮件防护 DLP 可与绿盟科技全资子公司--亿赛通①加密网关产品搭配使用。

在邮件防护 DLP 服务器上部署的策略会指示与邮件防护 DLP 集成的 MTS，根据特定内容或其他消息属性来禁止、重新路由或修改电子邮件。例如，电子邮件若匹配策略，则会返回至 MTA 以便与电子邮件链一起提交，而不会做任何修改。如果电子邮件违反数据丢失策略，邮件防护 DLP 可以修改电子邮件标题，然后将该邮件返回至 MTA。例如，禁止 SMTP 消息可能会返回 SMTP 5xx 失败响应码，内含策略响应规则所指定的文本。MTA 也可以丢弃邮件、将邮件重

① （亿赛通为绿盟科技全资子公司，拥有密码局和保密局资质认证）

定向到隔离文件夹，或是将邮件转发到电子邮件加密网关。重定向邮件的方法如下：在主题行中添加关键字，或者修改 Prevent 服务器所创建的 RFC 2822 消息标题，例如“X-Cfilter：加密”。根据这些经过修改的主题行或标题，MTA 可做出邮件转发决定，并包括从加密网关或其他下游邮件系统进行处理时所需的任何其他邮件格式。

由于邮件防护 DLP 服务器会让入站邮件流保持开放，直到关闭出端口邮件流为止，因此除非接收 MTA 保有邮件的第二份副本，否则绝不会从发送 MTA 中删除该邮件。请注意，邮件防护 DLP 服务器不是 MTA。它不会存储邮件，也不会以任何方式重新路由邮件--它只会将电子邮件“反射”或转发到 MTA 而已。

3.1.6 WEB 防护 DLP

对于 HTTP、HTTPS 及 FTP 而言，网络防护 DLP 可与 Blue Coat、Cisco 及 Network Appliance 等 ICAP 兼容 Web 代理集成。Web 代理会配置为将出站数据排入队列，并将副本发送到 WEB 防护 DLP 进行扫描。如果数据传送并未违反数据丢失策略，则 WEB 防护 DLP 会指示代理开始数据传送，让其前往预定目标。如果数据传送的确违反策略，则 WEB 防护 DLP 可以告知代理终止原始传送，或者可以选择性地只删除 Web 传送中的机密数据。在第二种情况下，传送会继续前往目标，Web 浏览器也不受影响；这在处理复杂的 Web 2.0 应用程序时特别有用，因为如果在这种情况下禁止整个传送，则此类应用程序可能会使浏览器崩溃。对于 HTTP/HTTPS 而言，网络防护 DLP 可以选择性地呈现全新网页以返回给最终用户，而将违反策略及禁止传送的情况通知最终用户。

WEB 防护 DLP 使用标准的 Internet Content Adaption Protocol (ICAP) 接口，该接口检查请求修改 (REQMOD) 及响应修改 (RESPMOD) 是否有内容违规情形（根据配置的策略）。REQMOD 允许扫描出站的 HTTP、HTTPS 及 FTP 请求，包括网站 GETS、Web 邮件 POSTS 及 FTP PUTS。RESPMOD 允许扫描映射的入站 HTTP/HTTPS 响应，而这类响应会基于原始请求返回内容。这项检查可监控企业 Web 邮件访问及 Intranet 应用程序，而机密数据可通过这两种方式下载到不可信的计算机、个人用户计算机或远程位置。

虽然 WEB 防护 DLP 可扫描所有的出站及入站 Web 传送，但客户通常会选择扫描特定的请求。例如，网络防护 DLP 可配置为只扫描 Web 邮件 POSTS 并忽略所有 CONNECTS 及 OPTIONS。客户可以进一步限制对纯文本或 HTML 文本等特定 MIME 类型的响应。选择这种请求类型及内

容级别过滤限制是为了删除大量不应扫描的无害图表及映像。这种过滤级别可以使用 WEB 防护 DLP 过滤器设置的组合来进行配置。

3.1.7 网络防护 DLP 扩展性

网络防护 DLP 可以扩展，以满足大型全球性组织的要求，且通常能够针对每台服务器的标准提供支持：

每秒处理 20 封电子邮件或 20 篇 Post

WEB 防护 DLP 增加小于 100 毫秒的延迟

邮件防护 DLP 增加小于 1 秒的延迟

请务必注意，根据邮件大小及通信量整体分布，标准会有相当大的差异。因此，在预先部署的流程中，会提供更精确的大小改变指导原则。

对于大容量网络环境，可以部署多台网络防护 DLP 服务器来分担数据扫描负载。通过使用所有 MTA 都支持的 MX 记录负载平衡功能，即可完成 SMTP 的负载平衡。或者通过在 MTA 代理与网络防护 DLP 服务器之间安排第三方负载平衡解决方案，也可以达成负载平衡。

对于单个服务器部署，网络防护 DLP 支持旁路配置，在这种情况下，即使 SIP 发生故障(虽然不太可能)，数据仍会继续流向预定目标。对于电子邮件，可以配置 MTA 中的 MX 记录，这样如果 MTA 不能将电子邮件副本传递给 SIP，则 MTA 会将原始电子邮件自动路由至其预定目标。对于 Web 及 FTP 传送，可以配置 Web 代理，这样如果在传递数据传送副本给 SIP 之后，代理没有立即收到来自 SIP 的响应，则代理会发放数据传送，让它前往预定目标。

3.2 终端 DLP（Endpoint DLP）

3.2.1 概述

SIP Endpoint DLP 为数据安全小组提供了保护终端（尤其是笔记本电脑及台式机计算机）上的机密数据所需的洞察力及掌控力。SIP Endpoint DLP 由几项产品模块组成。

终端敏感数据发现 Endpoint Data Discover

终端敏感数据防护 Endpoint Data Prevent

终端文档密级管控 Endpoint Document Classification Management

终端文档权限管控 Endpoint Document Right Management

终端文档凭证管理 Endpoint Document Evidence Management

终端文档外带管控 Endpoint Document Outward Management

终端外设端口管控 Endpoint Exterior Ports Security Management

终端磁盘加密管控 Endpoint Harddisk Security Management

终端敏感数据发现模块可扫描终端是否有存储的机密数据。

终端敏感数据防护模块可监控和禁止离开终端的机密数据，它可以在屏幕上显示弹出式通知，告知最终用户违反策略的情况。终端文档密级管理模块可以进行文档的密级自动或手动标密。

终端文档权限管控模块可以针对文档的访问权限进行授权管理。

终端文档凭证管理模块可以针对文档的溯源、防篡改、完整性、唯一性等文档凭证属性进行管理。

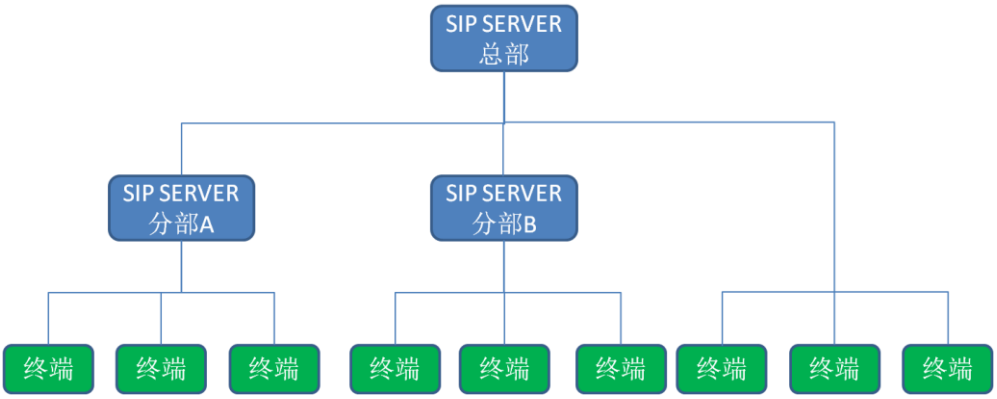
终端文档外带管控模块可以对离开终端安全环境的涉密文档进行管控。

终端外设端口管控模块可以对终端物理端口和外设设备进行管控。

终端磁盘加密管控模块可以对整个物理磁盘进行加密防护，保证意外丢失的情况下，数据不会被泄漏。

这些产品均由一个安装在终端上的一个代理(SIP Endpoint Agent)提供支持，由 SIP 策略服务器进行策略下发，统一进行终端防护管控。收到策略后，即使终端未连接至企业网络，该代理也能让这些产品模块工作，从而提供“随时随地”的持续保护。激活这些产品时，需要有适当的授权 license。

SIP 是 C/S 二层架构,Server 端通过分级来支持含有成千上万个终端的可扩展企业部署。下图说明了使用多个 SIP Endpoint Server 的大型企业部署。



SIP Endpoint Agent 可安装在 Windows XP、Windows 7、8、10 上，最多占用 100MB 的磁盘空间以及 80MB 的内存。它包括由 SIP Endpoint Server 推送的数据丢失策略及过滤规则和配置。这些数据丢失策略包括检测规则及响应规则。无论 SIP Endpoint Agent 执行的是发现、监控或防护，它均以类似的方式处理本地检测，即解读打开的文件的内容，然后检查其中的数据是否违反策略。如果数据违反策略，则 SIP Endpoint Agent 会启动实时的本地响应规则(例如 USB/CD/DVD 禁止、网络发送禁止、强制加密、标定对应密级)，然后通过日志上传将事故数据发送至 SIP SERVER。同时，SIP Endpoint Agent 会根据预置的规则而启动适用的通知(例如向最终用户和/或其管理者提交电子邮件通知)，并存储事故信息以供报告及补救之用，以让企业完全了解其终端上存在的数据丢失风险和事件。

如“检测与准确性”一节所述，如果推送到 SIP Endpoint Agent 的检测规则是关键字、“数据标识符”、正则表达式、IDM、SVM、文件属性等，则 SIP Endpoint Agent 会执行本地检测。如果策略包括任何以 EDM 检测规则，则 Endpoint Agent 不能执行本地检测，因为特征索引的大小可能非常大，而且可能需要服务器等级的硬件，才能存储这些索引并运行检测。在此情况下，数据会从 SIP Endpoint Agent 传递到内容服务器进行检索，供服务器检查其是否违反策略，而所采用的检查方式与所有其他 SIP 服务器产品类似。

3.2.2 终端敏感数据发现 Endpoint Data Discover

SIP Endpoint Discover 会扫描终端的内部驱动器以标识存储的机密数据，进而采取相关步骤来清点、保护或重新安置此数据。它可对数千个终端进行高性能的并行扫描，并尽量减少对系统的影响，而且每个 SIP Endpoint Agent 每小时大约可以扫描 6GB。

SIP Endpoint Agent 包括由 SIP Server 推送的数据丢失策略及可配置的 SIP Endpoint Prevent 过滤器。当 SIP 管理员在 SIP Server 中启动终端扫描后，Endpoint Agent 会“解读”那些匹配过滤器参数的已打开文件，并扫描文件内的数据，然后将数据与 Endpoint Agent 中存储的数据丢失策略进行比较，以查看是否违反策略。请务必注意，此扫描进程不会更改文件的“上次访问日期”属性，以确保依赖该属性的其他进程（例如备份进程）不会受到 Endpoint Discover 扫描的影响。如果数据违反策略，则 SIP Endpoint Agent 通过 SIP Endpoint Server 将事故数据发送至 SIP Server。

3.2.3 终端敏感数据防护 Endpoint Data Prevent

SIP Endpoint Prevent 会监控要下载至或写入本地磁盘的数据，并监控和禁止要复制到 USB、Firewire 或 SCSI 存储设备或刻录到 CD/DVD 的机密数据。也可以选择性地在屏幕上显示弹出式通知，将违规的情况告知最终用户，其中还包括可供用户说明原因的字段。

SIP Endpoint Agent 包括由 SIP Server 推送的数据丢失策略及可配置的 SIP Endpoint Prevent 过滤器。通过与 Microsoft 文件系统过滤器驱动程序(受支持的标准 API)集成，SIP Endpoint Agent 可拦阻文件系统写入及读取事件。这可确保所有文件系统活动的可见性，包括写入内部磁盘或外接 USB 文件系统的数据，或者由操作系统嵌入的 CD/DVD 应用程序读取的数据。使用此 API 还可确保与终端上其他代理之间的互通性。SIP Endpoint Agent 会“解读”那些匹配过滤器参数的已打开文件，并扫描文件内的数据，然后将数据与 SIP Endpoint Agent 中存储的数据丢失策略进行比较，以查看是否违反策略。如果数据违反策略，则会启动适当的实时响应规则，例如禁止和/或呈现弹出式通知。SIP Endpoint Prevent 过滤器包括移动介质过滤器及内部驱动器过滤器。

针对云的普及，终端防护 DLP 可以对云文件同步和共享功能进行监控和阻止，控制用户将敏感信息从桌面同步至云存储站点，如百度云盘、华为云盘、DropBox、Google Drive、Hightail、iCloud 和 Microsoft OneDrive 等。

3.2.4 终端文档密级管控 Endpoint Document Classification Management

文档密级管控模块为企业提供自定义的密级管理业务，企业可根据内部的规定，制定企业全部的内部文档密级范围，并准确标识密级的优先级。SIP 会提供两种密级标定方式，自动标定和手动标定。

自动标定密级：根据配置敏感信息识别规则策略，在响应动作指定明确的密级等级，并将策略绑定到终端用户，终端 DLP Agent 会讲符合检测规则的文件自动标定为策略中所对应的密级。密级的变更只能由低向高进行自动标识，无密级情况为最低优先级。

手动标定密级：在 Server 端初始化密级级别和优先级后，如果单独将文档密级策略绑定给制定的用户，则终端用户可以在客户端手动进行密级标定，但是标定的规则也是只能由低向高进行自动标识，无密级情况为最低优先级。

自动标定密级和手动标定密级可以同时配置，如果同一个文档同时分别被两种方式标记为不同登记时，均按照选取高优先级密级优选的原则，举例说明：根据敏感内容识别定义的密级为机密密级，但是当前用户欲手动标级为秘密，则此文件最终标级为机密（机密优先级高于秘密）；如果当前文档已经被用户手动标记为秘密等级，但是修改后，涉密内容检测后符合机密识别策略，则当前此文档按照自动标级的结果，标记为机密。

密级降级：密级降级需要客户通过 server 端提交密级降级审批流程方可进行密级降级。

3.2.5 终端文档权限管控 Endpoint Document Right Management

终端文档权限管理模块用于说明获准访问数据的用户，以及他们可以或不可以对文档运行的确切操作。DRM 可决定文档的访问及使用方式，相当于随文档一起移动的贴身保镖。权限包括读取、更改、剪切/粘贴、提交电子邮件、复制、移动、保存到便携式保存设备及打印等操作。

当前，DRM 最适合在最需要全面控制的工作组级别中保护极为敏感的数据。这些情况包括工程团队信息、非结构化的客户数据、未来的产品计划，以及特定的工程、产品或其他技术

内容等。组织通常会使用 DRM 来保护数据，使数据免于遭受外部人员窃取或获得授权的内部用户滥用。

因此，SIP 的文档权限管理模块提供自动授权和手动授权两种模式，工作方式类似文档密级标定，由服务器制定企业所需要的各种权限模块，针对不同的检测规则关联不同的授权模板，同一个检测规则可以被引用到不同策略中关联不同的授权模板，但是一个文档按照最高优先级的策略中的授权模板进行授权。

手动授权则是根据管理员配置的模板，对文档进行模版授权，模板根据公司相关要求由管理员统一定制和管理，并根据用户的属性控制可使用模板的范围。

对于被授权过的加密文档，敏感信息识别引擎将不再对其内容进行检测，即便是删除所有文档内容后，此文档的权限也不会变化。

下表为权限详细分类：

打印控制	1）拥有打印权限用户，允许打开权限文档，弹出权限提示信息，并将电子权限文档打印成纸质文件，可根据策略设置内容，加载打印水印内容 2）无打印权限用户，禁止将权限文档打印成纸质文件
复制控制	1）拥有复制权限用户，允许打开权限文档，弹出权限提示信息，并对文件内容进行编辑、保存、复制到任意明文或密文中 2）无复制权限用户，禁止将授权文档内容复制到任意明文或密文中
分发控制	1）拥有分发权限用户，允许将自身权限二次授权至其他用户，控制分发权限小于或等于自身拥有的最大权限，并且仅允许分发一次 2）具有分发权限的用户，用户可以自主分发及变更文档权限
完全控制	1）拥有“完全控制”权限的用户可以将该文档通过鼠标右键方式还原为明文文档 2）拥有“完全控制”权限的文档，用户可以自主分发及变更文档权限，并修改其他非作者的任意使用权限
阅读次数控制	1）可以设置文档的阅读次数、阅读有效期限 2）客户端在线时，文档打开会与服务器进行实时权限认证，当文档超出阅读次数控制后弹出提示，禁止用户打开权限文档（支持离线下的阅读次数控制）
阅读时限控制	1）客户端在线时，文档打开需与服务器进行实时权限认证，当文档超出阅读时限控制后将禁止用户打开权限文档 2）授权人给其他用户授权时，可以指定权限的有效期，有效期包括开始和截止时间，超出这个时间范围后权限失效，最小控制单元为“小时”
打印次数控制	1）控制加密文档打印次数，授权人可以限制授权对象（支持对若干单个用户，不支持对部门或组）设置文档打印次数，控制次数用完后将不允许再打印； 2）授权人可以限制用户打印文档的次数，当文档超出打印次数后也将禁止用户再次打印权限文档；

水印控制列表：

阅读浮水印	支持加密与授权文档合法阅读时添加当前使用者及文档版权归属水印信息，防止非法用户进行屏幕拍照或录屏窃密

打印浮水印	支持具有打印权限的加密与授权文档打印时自动添加打印浮水印： 1）水印内容自定义包含自定格式化内容和自主字符串内容，格式化内容包含：打印人账号、打印人姓名、打印日期、打印时间、打印人机器 IP、打印人机器 MAC、打印人机器计算机名、打印部门、文档授权人姓名 2）支持自主字符串内容定义及打印显示 3）支持对水印内容显示的字号大小、水印深浅度进行设置，水印内容采用倾斜方式显示

3.2.6 终端文档凭证管理 Endpoint Document Evidence Management

终端文档凭证管理模块可以针对文档的溯源、防篡改、完整性、唯一性等文档凭证属性进行管理。

SIP 溯源由系统创建的四维模型，此模型将溯源看成一系列离散的活动集，这些活动发生在整个工作流生命周期中，并由四个维度(时间、空间、层和数据流分布)组成，四维溯源模型通过时间维区分标注链中处于不同活动层中的多个活动，进而通过追踪发生在不同工作流组件中的活动，捕获工作流溯源和支持工作流执行的数据溯源。

数据溯源方法主要采用标注法，通过记录处理相关的信息来追溯数据的历史状态，即用标注的方式来记录原始数据的一些重要信息，如背景、作者、时间、出处等，并让标注和数据一起传播，通过查看目标数据的标注来获得数据的溯源。

溯源的使用方式支持两种，一种为识别信息后对目标文件进行溯源处理，一种为整个终端上所有的文件都进行溯源处理。

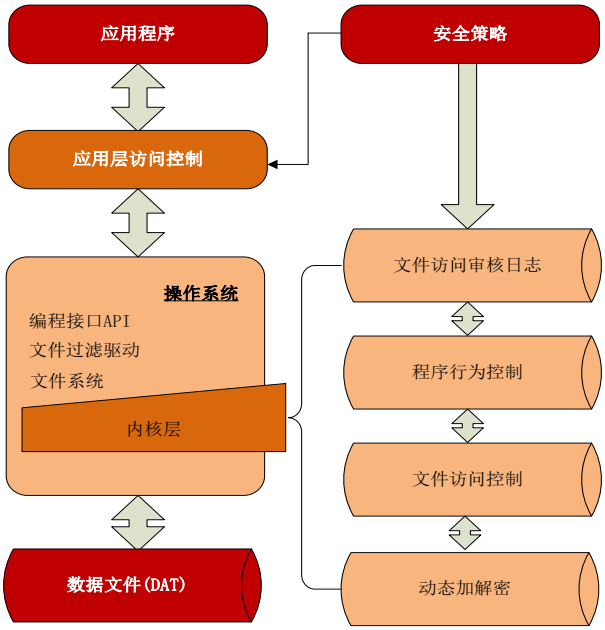
目标文件的检测需要专有设备进行查询。涉及商业秘密，细节需向公司产品经理询问。

3.2.7 终端文档外带管控 Endpoint Document Outward Management

终端文档外带管控模块主要针对回家办公的业务场景，将终端内的文档拷贝进入专有移动存储过程中自动进行加密，只有专有移动存储连接外部电脑后才可以打开企业内部文档，并进行文档的相关编辑工作，并保护企业内部文档的内容不会泄漏，比如禁止复制和打印等控制功能，同时对于外部使用电脑上的非企业内部文档不会进行误加密。当企业内部文档返回企业时，进入终端电脑后，会自动进行解密处理，从而完成回家办公的场景。

绿盟全资子公司--亿赛通①核心自主知识产权“智能动态加解密” 技术，应用于操作系统文件级过滤驱动层，实时拦截加密文件的读/写请求，对文件进行动态跟踪和透明加解密处理，采用目前国际上通用的 SM4 加密算法，结合内容防拷贝、防拖拽、防打印、防拷屏等访问控制技术，实现文档加密保护功能。

该技术安全、稳定、高效，且具有较强的兼容性和延展性，无论应用层为何种格式文件类型，只需通过简单的策略配置，即可对各类格式文件进行加密，加解密过程透明、不改变使用者的操作习惯和原始文件格式，使用户在无感知情况下保护文件安全。



文件级动态加解密技术实现图

3.2.8 终端外设端口管控 Endpoint Exterior Ports Security Management

终端外设端口管控模块为终端安全提供端口管控的能力，企业管理者可以根据需要将员工的终端外设端口进行管控，防止涉密数据在未经许可的情况下，通过计算机外设将涉密数据拷贝出去，该模块能够提供对计算机各种常用外设的访问控制，如光驱、软驱、打印

① （亿赛通为绿盟科技全资子公司，拥有密码局和保密局认证资质）

机、网卡、无线网卡 WIFI、串口、并口、 红外设备、蓝牙设备、调制解调器、Pcmica 卡、1394、USB 存储设备等。

特别对移动设备，比如 iphone、android 等智能设备，也可以对其进行管控。

3.2.9 终端磁盘加密管控 Endpoint Harddisk Security Management

终端磁盘防护模块在 Endpoint Agent 也可以叫做 DiskSec 模块，主要用于防止在计算机丢失或失窃后硬盘数据的泄密，它不改变用户使用计算机的习惯，除在每次启动计算机时需输入加解密硬盘数据的密码外，用户在正常使用计算机的情况下，根本感觉不到它的存在。DiskSec 采用基于物理扇区级的加密方法，它可将保存在硬盘上的所有数据进行加密，与文件加密方式不同，DiskSec 能够加密硬盘上的任何数据，当然也能够加密操作系统，非授权用户不仅看不到硬盘上的文件内容，而且也看不到保存在磁盘上的任何文件的名称。

DiskSec 通过拦截操作系统或应用软件等对硬盘数据的读写请求，实现对磁盘数据的实时加密和解密操作，当系统向硬盘写入数据时，DiskSec 首先获得控制权，用户输入的密码对要写的数据进行加密操作，然后将数据写入硬盘的指定位置，反之，当程序读取硬盘数据时，DiskSec 同样能够获得优先控制权，到磁盘的指定位置读取数据并根据用户输入的密码进行解密操作，然后将解密后的数据提交给相应的程序，这样，在操作系统或应用软件看来，磁盘上存储的数据和未加密时的数据完全一样，能够以正常的方式直接使用磁盘数据，如同磁盘上的数据未加密一样。同样，用户也感觉不到 DiskSec 的存在，可以不改变任何习惯而直接使用计算机。

在计算机上安装 DiskSec 后，计算机的启动过程会被改变，图 1 给出了在安装 DiskSec 的情况下，计算机的实际启动过程。

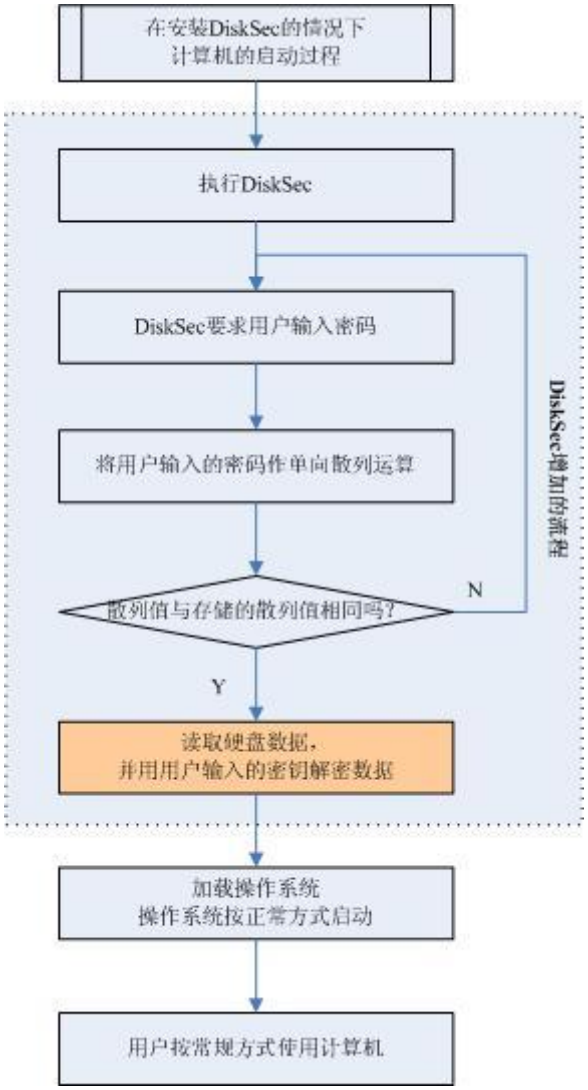


图 1. DiskSec 对计算机启动流程的影响

由于磁盘数据被加密，要想使用磁盘数据，必须对其进行解密操作，为方便用户操作和不改变用户的计算机使用习惯，DiskSec 采用的是动态加密和解密的方法，她在操作系统和磁盘之间安装了一个数据加密和解密程序，该程序不需要用户的干预，自动对存储到磁盘的数据作加密运算，对从磁盘读取的数据做解密操作，用户在正常使用计算机的时候，根本感觉不到 DiskSec 的存在。图 2 给出了 DiskSec 采用的动态加密和解密的原理。

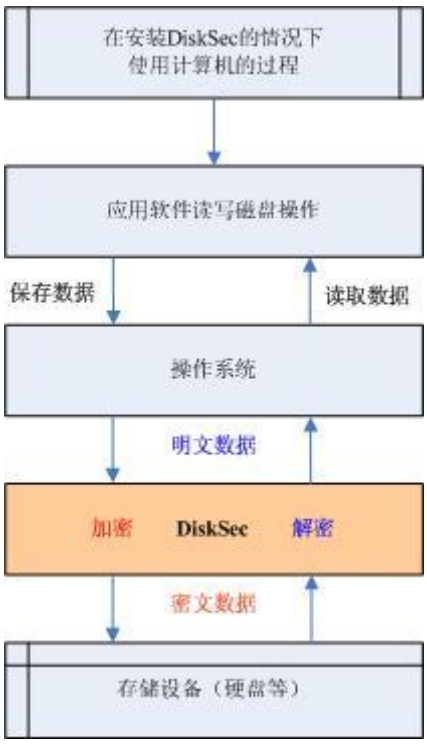


图 2. DiskSec 采用的动态加密和解密的方法

DiskSec 可以对系统盘进行加密，且支持最新的 UEFI 启动方式。

对于忘记个人密码，且被 DiskSec 加密过的终端电脑，企业管理者可以通过策略中配置的超级用户进行登陆或解密操作，保证安全的回收能力。

3.2.10 对网络及终端的影响

SIP 的终端解决方案对最终用户计算机及企业网络的影响很小。大部分影响均可通过前几节所提的可配置检测策略，以及下面所讨论的其他过滤器来加以管理。所有过滤器都是根据每台服务器来设置，并会推送到所有 SIP Endpoint Agent。

终端影响：

与其他应用程序相比，SIP Endpoint Agent 会做为优先级较低的进程自动运行，如此一来，若最终用户运行其他需要较多资源的应用程序，SIP Endpoint Agent 就会只能调节检测所需的资源或和暂停，基本控制在用户使用过程中无感知。

网络影响：

如果 SIP Endpoint Agent 不含有使用 EDM 的策略，则所有检测都会在本地发生，这样网络影响也就微不足道了。只有事故数据才会提交至 SIP Server，而不会提交所有已扫描文件中的所有数据。

即使因为策略使用 EDM 而将数据提交到 Server 进行检测，由于 Endpoint Agent 是在本地破译内容，因此提交到服务器的数据也远远少于原始文件中的数据（约 2%）。

3.2.11 防篡改与安全性

有数种方法可以确保员工不能禁用或篡改 SIP Endpoint Agent：

驱动层面控制 Agent 需要运行的文件不被修改或删除，因为有磁盘加密的防护，即使采取 U 盘启动的方式独立删除程序软件的方式，也没有办法读取到磁盘上的文件信息。

SIP Endpoint Agent（包括数据丢失策略、过滤器/配置及阴影高速缓存)都会经过完整加密。此外，SIP Endpoint Agent 会使用“高级加密标准”(Advanced Encryption Standards，AES）将任何提交到 SIP Endpoint Server 的数据加密。SIP Endpoint Agent 会在每次连接时，使用共享私钥来身份验证 SIP Server，以确保访问的安全性。

3.2.12 终端 DLP 部署

SIP 会使用集群部署来支持含有成千上万个终端的可扩展企业部署。一台 SIP SERVER 可以支持 100000 个 Endpoint Agent 终端。为了让管理优化，建议用户按照实际企业部门进行分级部署。有关 SIP SEVER 的产品硬件要求，请参见“附录”。

SIP Endpoint Agent 是 Microsoft 安装程序（MSI）软件包的一部分，可通过桌面管理工具（例如 Altiris、Microsoft SMS、CA Unicenter 及 IBM Tivoli）推送到终端，或是手动安装在每台计算机上。在安装期间，必须提供某些参数，包括 SIP Endpoint Agent 应该连接之 SIP Server 的主机名称或 IP 地址、SIP Endpoint Agent 的安装目录。至于系统管理工具部署选项，由于 SIP Endpoint Agent 已软件包于 MSI 文件中，所以基本上可通过任何主要的系统管理工具进行部署，并确保安装和运行都正确无误。此外，还可以将安装设置为静默模式，并且上述配置字段均已键入完成，所以最终用户并不会觉察到他们的计算机正在

安装 SIP Endpoint Agent。完成安装后，SIP Endpoint Agent 会自行向适当的 SIP Server 进行注册，然后下载之前所讨论的检测规则和安全策略。

SIP Endpoint Agent 可通过 SIP Server 升级，将相关补丁上传到 Server 服务，选择用户后对其进行补丁推送，实现客户端统一或局部进行升级。

3.3 存储 DLP（Storage DLP）

3.3.1 概述

SIP Storage DLP 产品包括 SIP Database Discover 和 SIP Fileserver Discover。SIP Storage DLP 可标识文件服务器、数据存储库中暴露或常驻的敏感数据。

SIP Storage DLP 产品可解决现今企业在存储数据方面所面临的一些最重大的挑战，包括法规遵循（例如 PCI 及 GLBA）、降低风险、数据分类、数据保留，以及电子化发现收集。

3.3.2 存储 DLP 的工作方式

存储 DLP（SIP Storage DLP）基本上可以扫描任何数据存储库，包括：

文件服务器：Windows、Linux、Unix、Novell、Solaris、NAS 编档程序等

数据库：Oracle、Microsoft SQL Server、IBM DB2 等

如“检测与准确性”一节所述，SIP Storage DLP 会检查数据是否违反策略。但是 SIP Network Monitor 扫描数据的方式是常驻于网络出口点并分析离开网络的数据通信副本，而 SIP Storage DLP 扫描数据的方式则是通过网络连接到数据存储库，然后读取文件及其内含的其他存储数据。与所有其他 SIP 产品类似，如果 SIP Storage DLP 发现违反预先创建检测策略的敏感数据，则会激活适用的自动响应规则，并将事故信息提交到 Server 进行事故补救和报告。SIP Server 中的 Storage DLP 事故快照包括文件拥有者，以及有关文件或数据的访问控制列表(ACL)信息。如果是文件系统扫描，这项信息将从 NTFS 文件系统读取；如果是存储库扫描，这项信息将从存储库(例如 SharePoint)读取。ACL 信息可提供有关具备敏感文件读取/写权限之用户的详细数据，且可帮助安全小组判定目标共享是否有访问控制问题。

SIP Storage DLP 对目标进行原始扫描，而且扫描只能从 SIP Server 进行配置和下发-不需要安装代理，也不需要配置其他软件，即可扫描目标。SIP Storage DLP 能够以无代理的方式扫描的文件存储库类型包括可从 Windows 或 Linux 访问的任何文件系统（包括 CIFS/SMB、NTFS、NFS、DFS、Novell、ext2、HFS 及其他）。这包括 Windows 及 UNIX 文件服务器、台式机计算机及笔记本电脑。SIP Storage DLP 也能够对可通过 JDBC 或 ODBC 访问的任何 SQL 数据库进行原始扫描。这包括 Oracle、Microsoft SQL Server 及 IBM DB2 数据库。

如果是文件系统扫描，SIP Storage DLP 会使 SIP Storage DLP 服务器上的基本操作系统，来挂载并扫描远程文件系统。

使用 SIP Storage DLP 的第一个步骤就是在 SIP Server 中设置扫描任务。这包括标识扫描目标以及要扫描的文件共享，然后在 SIP Server 中键入目标共享的适当登录证书（用户名及密码）。接着，SIP Storage DLP 可以使用这些证书来挂载远程目标共享，以便采用无代理的方式进行扫描。这种可使用不同证书的功能非常实用，因为它可以让 SIP Storage DLP 具有不同的使用实例。例如，SIP 用户可能想扫描一个由多个部门共享的文件系统，以了解其中包括哪种敏感数据可能会暴露在拥有标准证书的“常规”员工面前。在这种情况下，用户可以为 SIP Server 提供包括文件服务器标准访问权限的登录信息，这样 SIP Storage DLP 就可以扫描暴露在常规员工面前的文件。但是，如果 SIP 用户是为了法规遵循或分类目的而希望查看服务器上的所有数据，则可以对 SIP Storage DLP 提供该服务器的指定管理员级证书，使其能够扫描整个服务器及其所有文件夹。可以指定默认扫描证书，也可以在共享级别加以覆盖。这种以证书为基础的扫描的优点在于，通过使用不同的访问级别来运行扫描，各公司即可迅速找出暴露最严重的数据，并执行情况访问控制与数据分类策略。此外，当 SIP Storage DLP 运行扫描时，文件内容或数据仅在需要扫描时才会保留在内存中。最后 SIP Storage DLP 文件系统扫描不会更改文件的“上次访问日期”属性，以确保依赖该属性的其他进程（例如备份进程）不会受到扫描的影响。

3.3.3 对网络的影响

扫描对企业网络的影响是由服务器安置、扫描过滤器、调度窗口和通信管制进行管理。

做为总体扫描控制流程的一部分，用户可以开始、暂停、停止扫描以及对扫描进行通信管制，并可应用过滤以便仅扫描特定文件。可过滤的参数包括文件名称、文件类型、文件大小和最后修改日期。通信管制设置可限制每分钟处理的文件数或每分钟处理的字节数，这对低带宽环境很重要。此外，不只能将扫描调度在特定的日期和时间自动开始和/或暂停，以便组织能够持续监控其存储的数据，而且也可以将扫描安排在用户网络通信最小的非尖峰时间段运行。不仅如此，SIP Storage DLP 还可配置为仅对自上次完整扫描后添加或修改的数据执行差异扫描。这种对目标进行连续性扫描的方法比初始化的完整扫描速度更快。如先前所述，扫描程序和代理会执行本地文件“解读”，使得经由网络返回 SIP Storage DLP 进行检测的数据远远少于原始文件中的数据。

3.3.4 存储 DLP 部署

为了使扫描速率和网络使用情形达到优化，建议将 SIP Storage DLP 服务器放在扫描的内容附近。使用扫描程序时，单个 SIP Storage DLP 服务器能够以多于 500GB/天的速率扫描内容，通过添加其他处理器或 SIP 服务器，可以让扫描速率呈直线提高。有关产品硬件要求，请参见“附录”。

3.4 商用接口服务器 BIS（Business Interface System）

3.4.1 概述

为了更好的客户的业务系统进行对接，给企业提供更便利的安全防护能力，SIP 提供强大的接口能力，企业可以通过 WebService 方式调用 BIS 进行安全业务控制，提供相应的安全服务能力，如果需要了解更详细的信息，如接口文档等，请向公司产品部门咨询。

3.4.2 DLP 接口服务

通过接口方式提高敏感数据的检测能力，在 server 上配置相应的检测规则后，其他业务系统通过接口将文件或内容发送给接口服务器，接口服务器检测后，同样通过 WS 返回结果，提供敏感数据检测能力的服务。

3.4.3 加解密接口服务

通过接口方式提供文档加解密的能力，通过 WS 将文件传送给接口服务器，接口服务器自动对文件进行加密或解密，然后同样方式将处理过的文件返回给第三方业务系统。

3.4.4 权限接口服务

通过接口方式提供文档加密权限赋权或修改的能力，通过 WS 将文件和此文件的 ACL 传送给接口服务器，接口服务器自动对文件进行权限赋权或修改后，然后同样方式将处理过的文档返回给第三方业务系统。

3.4.5 审批流程接口服务

SIP Server 自身拥有工作流和审批流，对于信息化建设比较高的企业，所有业务都审批都会被要求由一个系统进行管理，比如 OA 系统，因此 SIP 也提供 WS 方式的审批流接口服务能力，与第三方业务系统进行完美对接。

3.5 安全智能平台 SIP（Security Intelligence Platform）

3.5.1 概述

安全智能平台 SIP（Security Intelligence Platform）是支持所有 SIP 产品的基本基础配置。无论数据位于网络、终端还是存储设备中，它所提供的技术平台均可防护数据所面临的威胁。

3.5.2 系统管理

SIP 采用 linux 系统和 mysql 数据库，为了客户安全性，操作系统和数据库均进行安全加固，并关闭业务外的所以服务和端口从而进一步提高安全性。用户可以购买软件安装，也可以直接购买与安装好的硬件服务器，详细配置见附录。SIP 软件是为了与现有系统管理、网络监控和备份基础配置完全兼容所设计。所有 SIP 产品的软件和策略更新都是从集中式 SIP

Server 自动传播到 SIP 服务器产品。软件升级的目的在于维护与现有硬件平台的兼容性，客户毋需 SIP 的帮助即可自行部署。

系统监控、警报和诊断：SIP Server 所提供的网络通信详细数据报含捕获的数据量、检查的文件数、创建的事故数和尚未处理的文件数。此类信息是针对可配置的时间段以图表格式提供，让客户可以为各种 SIP 服务器产品执行疑难解答分析和容量管理。此外，SIP Server 可捕获有关所有服务器状态（运行中、已停止、失去连接等）以及近期警告事件(没有响应的服务器或服务器的磁盘空间不足等）的摘要数据，以便管理员采取适当的移动。也可以设置电子邮件警报，将某些系统级别的事件状况立即通知管理员。SIP Server 还会记录所有用户启动的事件以供审核。这些事件包括在 SIP Server 中创建敏感数据的索引、创建或删除策略，或将用户新建到 SIP Server 等例行事件，包含安全业务管理员的操作日志供日志管理员审计。

3.5.3 分布式配置

SIP 可让各组织在其全球企业中部署产品，并使用单个 SIP Server 服务器来集中管理软件。多层分布式配置：SIP 的多层分布式设计使其能够满足世界上最大型全球组织的要求。通过将 SIP 软件放在地理位置上接近最终用户的位置，各组织可以在支持分公司或境外营运机构等远程地点的同时，仍旧可以利用单个的 Server 中央服务器。此外，通过在所有 SIP 服务器（而非一部中央服务器）上启用检测技术和数据扫描功能，整体系统可以更有效率地进行扩展，因为这样可以分散处理负载并且尽量减少通过 WAN 进行的数据传输。这种多层方法让组织得以灵活性部署子组件，使最终用户系统资源、服务器要求和网络带宽考虑事项达到优化。一级服务器还可以将配置的策略下发到下属服务器，保证策略的统一性和可监控性。

3.5.4 适用于用户和身份管理的 LDAP 集成

SIP 可与企业目录系统集成，以提供两种主要优势：第一种优势是可以访问 SIP 系统并提供有关事故补救的其他信息。通过企业目录，可以将用户同步到 SIP 或将其从 SIP 用户体系中删除，且用户可使用常驻于企业目录中且在整个企业皆可使用的相同密码来向 SIP 身份验证。第二种优势是，企业目录集成可以用来提供与涉及数据丢失事故之用户的身份有关的其

他属性。可以自动查询与用户身份有关的用户名和其他相关属性，以帮助补救事故并激活特定的响应规则。例如，SIP Endpoint 事故一开始可能仅显示引发事故者的 Windows 登录信息，而至于是 SMTP 事故的话，该事故可能仅显示发件人的企业电子邮件地址。通过使用企业目录集成，可启用对员工的其他相关属性（如其全名、电话号码、ID 号码、事业单位、其主管的名字和电子邮件）的自动查询，且这些属性可以包括在事故快照中，以帮助进行事故的调查和补救。属性值完全可以自定义，且包括两个部分：(1)查询 API；(2)适用于不同数据来源的自定义插件。此 API 提供接口给一个或多个可以从各种数据来源（例如 LDAP 目录或其他企业系统和数据库)检索所需值的自定义插件。此 API 会决定应该装载哪些插件以及这些插件的执行顺序。可通过将一个插件的结果做为下一个属性查询之参数的方式，将查询串在一起形成查询链。例如，在 WEB 防护 DLP 部署中，客户可以有个插件能在代理日志档或系统数据库中查询发件人的 IP 地址，以返回用户名。下一个插件可能使用由第一个插件所找到的用户名，在企业 LDAP 目录中查找用户的电子邮件地址和事业单位。

3.5.5 系统安全性

SIP 提供领先业界的安全性和审核功能，以确保在 SIP 系统内所收集和存储的组织机密数据受到保护。

SIP 可提供所有系统组件的加密，且机密信息绝不会以纯文本方式存储在系统中的任何位置。此种加密等级支持 PCI 数据处理标准。SIP 可提供完全的事故生命周期加密，如下所述：

由 SIP 检测服务器捕获的所有敏感数据皆使用 256 位 AES 对称密钥进行加密。此种加密发生于捕获时，会安全地传输到 SIP Server 数据库，并以相同的加密格式进行存储。

所有上传至 SIP Server 用以创建 EDM/IDM/SVM 配置文件的索引数据，都是以加密方式进行保护。SIP 检测服务器和 SIP Server 间的所有双向通信通道皆以 SSL（RSA 1024 位密钥）进行加密。SIP 检测服务器和 SIP Server 之间的这些 SSL 通信会使用服务器端和客户端证书来执行相互身份验证。加密密钥可以按照可配置的时间周期（默认为 30 天）进行轮替，并通过 SSL 连接安全地从 SIP Server 更新至 SIP 检测服务器。

当前的加密密钥常驻于检测服务器的内存中，且绝不会以永久方式存储在磁盘中。所有

“旧的”加密密钥都存储在常驻于数据库内的安全密钥库中，并且受到数据库安全性措施的额外保护。此密钥库会以从 SIP“管理员”帐户密码衍生的“主要”密钥进行加密。

密钥管理体系能够实现按照每个用户一个密钥，每个策略一个密钥，每个文件一个密钥的高强度密钥管理体系，保证系统的安全性。