

★完全公开



奇安信网神网络数据泄露 防护系统 产品白皮书 V1.0

地址：北京市西城区西直门外南路26号院1号

邮编：100044

● 版权声明

奇安信集团，保留所有权利。

奇安信集团及其关联公司对其发行的或与合作伙伴共同发行的产品享有版权，本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程描述等内容，除另有特别注明外，所有版权均属奇安信集团及其关联公司所有；受各国版权法及国际版权公约的保护。

对于上述版权内容，任何个人、机构未经奇安信集团或其关联公司的书面授权许可，不得以任何方式复制或引用本文的任何片断；超越合理使用范畴、并未经上述公司书面许可的使用行为，奇安信集团或其关联公司均保留追究法律责任的权利。

由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

● 免责声明

本免责声明（“**本声明**”）适用于奇安信集团（包括但不限于奇安信科技集团股份有限公司、奇安信网神信息技术（北京）股份有限公司、北京网康科技有限公司，以及前述主体直接或者间接控制的法律实体）旗下推出的全部产品和/或服务（以下统称“**本产品**”）。如您使用前述产品，即表示您同意接受本声明的一切内容。如果您不同意接受，请立即停止使用相关产品。

奇安信集团有权随时自行决定修改、添加或删除本声明的全部或部分內容。您有责任定期**检查免责声明部分的内容**，以了解是否发生了变更。如您在我们发布变更后继续使用本产品，即表示您接受并同意这些变更。

1. 您明确理解并同意，**本产品按“现状”提供**，不存在任何形式的明示或暗示保证，并且在适用法律允许的最大范围内，奇安信集团不提供任何明示或暗示的陈述或保证，包括但不限于有关适销性、适用于特定目的以及不侵犯第三方权利的保证。奇安信集团不保证产品中所含的功能将满足您的全部要求，也不保证您对本产品的使用不会中断或出错。**选择本产品来达到预期结果，以及安装、使用本产品并获取结果所带来的所有责任和风险由您承担。**
2. 奇安信集团承诺致力于不断提升产品的质量，本产品是在现有技术水平基础上提供的，但奇安信集团无法保证您使用本产品将完全符合您的期望，包括但不限于不能保证您【通过本产品能够识别出所有的敏感数据以及监控和拦截到所有的泄露行为】，您理解并同意，出现前述不符合您对产品期望的情形不视为奇安信集团违约。
3. 您明确理解并同意，您在使用本产品过程中可能发生不可抗力或不可预见的情形，包括但不限于：1) 被某些未经许可的个人、团体或机构通过某种渠道获得或篡改；2) 因通信繁忙出现延迟，或因其他原因出现中断、停顿或数据不完全、数据错误等情况，从而使交易出现错误、延迟、中断或停顿；3) 因地震、火灾、台风及其他各种不可抗力因素引起的停电、网络系统故障、电脑故障等；4) 计算机系统可能因存在性能缺陷、质量问题、计算机病毒、硬件故障及其他原因；黑客攻击、计算机病毒侵入或发作等非可归责于奇安信集团的原因；5) 政府管制、网络故障、国家政策变化、法律法规之变化等。如发生不可抗力或不可预见的情形，奇安信集团将尽最大努力予以补救，但奇安信集团对于因不可抗力和不可预见的情形造成的各类直接或间接损失，均不承担任何责任。
4. 对于任何本产品的使用行为，包括但不限于您自身和/或任何第三方的行为，奇安信集团均不承担任何责任。
5. 对于从非奇安信集团指定途径以及从非奇安信集团发行的介质上获得的本产品，奇安信集团无法保证其是否感染计算机病毒、是否隐藏有伪装的特洛伊木马程序或者黑客软件。使用此类产品，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。
6. 上述免责声明适用于因任何性能故障、错误、遗漏、中断、删除、缺陷、操作或传输

延迟、电脑病毒、通信线路故障、失窃、毁坏、未经授权的访问、篡改或使用（无论是出于违约、侵权、疏忽或任何其他诉因）而导致的任何损害、责任或伤害。

7. 奇安信集团保留在**不发布通知**的情况下随时采取以下行动的权利：**在执行常规或非
常规维护、错误纠正或其他更改所必需时，中断或修改本产品的任何组成部分的运行或
功能。**
 8. 本声明受中华人民共和国法律的约束并依据其解释。
 9. 在法律允许的最大范围内，本声明最终解释权归奇安信集团享有。
-

修订记录

版本	状态	修订理由和内容摘要	修订人	批准人	修订日期
V1.0.0	C	新建	魏博		2023-5-5

状态：C-创建，A-增加，M-修改，D-删除

数据安全分级标注说明

■ 数据分级	公开数据 ()	内部数据 (Y)	普通商秘 ()	核心商秘 ()
<p>*数据分级标注及说明：</p> <ol style="list-style-type: none">1、文档编写前，应标注数据安全级别，默认为内部；2、请根据文档内容评估数据安全级别，在对应数据级别 () 中填写 (Y) ；3、分级 TIPS: <p>【核心商秘】：限于个别人、小范围共享和使用的信息，例如薪酬数据、未公开的产生严重危害的样本等。如泄露将导致法律风险或者影响到社会公众利益或者严重的恶意竞争等；</p> <p>【普通商秘】：限于特定人群、特定范围内共享和使用的信息，例如公司组织架构、产品样本集等。如泄露存在合规风险或者可能影响社会公众个人利益或者存在一般恶意竞争的风险等；</p> <p>【内部数据】：限于在公司范围内按需使用，除去公开数据、核心商秘、普通商秘，都为内部数据。如泄露不存在法律合规风险或不存在影响社会公众个人利益的风险，但会产生轻微的恶意竞争风险等；</p> <p>【公开数据】：对任何方面都无危害的、不会被任何方面进行利用的信息，例如官网上的产品简介等。如泄露对任何方面都无影响。</p> <p>更多分级 Tips 参考链接: https://sec.qianxin-inc.cn/data-security/data-classification-tips</p>				

目录

1 产品概述	1
1.1 产品简介	1
1.2 产品定位	1
1.3 产品形态及构架	2
2 产品功能	3
2.1 多文档格式内容识别	3
2.2 内容识别算法	4
2.3 流量管控	4
2.4 流转审计	4
2.5 敏感邮件管控	5
2.6 多协议识别和解析	6
2.7 过载保护	6
2.8 报表展示	6
2.9 自定义端口流量识别与审计	6
2.10 白名单功能	7
2.11 网络配置	7
2.12 自定义地址监控	7
3 特点与优势	7
3.1 策略的灵活部署	7
3.2 详尽的日志审计	7
3.3 便捷的系统运维	8
3.4 丰富的识别算法	8
3.5 图片识别功能	8
3.6 审计日志秒查	8
3.7 支持基于 IP 到人的反查	9
3.8 强大的组网能力	9
4 产品价值	9
4.1 完善的数据防泄露能力	9
4.2 运维轻、防护效果不减	10
4.3 对业务影响小	10
5 应用场景	10
5.1 合规应用场景	10
5.2 企业内部风险防护场景	11
5.3 数据出境监测场景	11
5.4 敏感数据泄露风险监测场景	11

6 安装部署 11

1 产品概述

1.1 产品简介

网络数据防泄露产品（以下简称 NDLP）是一种保护企业组织敏感数据，防止敏感信息通过网络链路泄露的安全设备。通常，针对电子邮件、Web 应用程序和 FTP 等数据传输通道，网络数据防泄露产品解析网络流量，识别网络中传输的数据，检测数据泄露行为（有意的或无意的），并根据企业组织的安全策略对数据泄露行为进行审计或拦截，以监控其网络上的数据流，满足合规要求，目前 NDLP 产品已经适配当前主流国产化系统，并且存储容量也达到 16T，增加了数据存储能力。支持通过 Syslog、Kafka 等方式向第三方平台发送日志及告警信息。吞吐量 3Gbps。网络数据防泄漏系统满足等保三级要求。

产品面向的市场包含：

- 企业通用数据防护市场。针对企业自身数据安全防护诉求，企业希望能够通过技术手段减少数据泄露的风险，通过 NDLP 能够提高企业自身的数据安全防护的能力，减少数据泄露的风险；
- 企业合规自查市场。一些企业或组织会对互联网用户进行应用开放，用户上传一些内容可能包含敏感信息，这些敏感信息不适合对外展示，企业运营者需要对这些敏感信息进行过滤展示，减少企业的法律风险。
- 运营监管市场。运营商针对互联网用户的敏感信息发送进行审计或者阻断。或者数据跨境流转场景，监管单位需要利用技术手段对企业涉及到的流转数据是否有敏感内容。

1.2 产品定位

NDLP 产品定位为一款数据安全领域的的数据泄露防护产品，旨在提供全面的敏感数据保护和安全防御解决方案，确保敏感数据在网络中不被泄露，它满足组织对数据保护、合规性和威胁防御的需求，能够提供包括数据保护、满足合规性等能力。

NDLP 产品旁路部署，收取镜像流量，对常见的 HTTP、SMTP 等协议外发的所

有数据进行解析还原，数据安全分析人员通过设置相应的规则，对敏感数据、敏感数据流向等进行有效的监控、分析，监测敏感数据泄露、外发情况，实现对敏感数据的有效监控、分析。

1.3 产品形态及构架

NDLP 产品形态为硬件产品，为 2U 的物理服务器，可根据市场场景选择不同的型号款型，适用不同带宽吞吐，如：1G、3G、5G、10G 等不同环境的应用。产品的整体构架及工作原理如下：

产品的整体构分为两部分，采用 C/S 架构，Server 部分是 WEB 管理平台组件（以下简称管理平台），Client 部分是网络数据防泄露业务处理模块（以下简称 NDLP 业务组件）。将管理和业务解耦，提高系统整体的可靠性。

管理平台部署在服务器侧，负责整个系统的配置管理工作，包括网络 DLP 设备管理、系统管理、防护策略配置、外发行为处理、业务配置，以及系统安全审计等相关工作。

网络防泄露产品是一款对网络流量进行管控的设备，其工作原理与防火墙等网络产品非常类似。当流量经过网络防泄露产品时，会被报文接收组件获取，基于网络协议解析等技术，拆掉层层封装的协议头后，提取出应用层的数据内容，这可能是在论坛上发表的一段文字，也可能是通过 FTP 上传的文档。

根据特征库中所定义的正则表达式、关键字和文档指纹等信息，从提取出的文字或文档中找出符合特征库中定义的敏感信息。同时，基于匹配规则中定义的数据分类分级规则，可以对识别出的敏感数据赋予密级标签，反映数据的安全级别。

响应规则定义了敏感数据泄露发生时应采取的一系列措施，包括网络流量阻断、审计、证据留存、发送电子邮件通知等响应动作。根据数据泄露事件的严重程度，可以设置不同的响应动作，一般的数据传输，可以只进行审计，对于特别严重的数据泄露，可以选择流量阻断的管控方式，同时将证据进行留存，方便追溯定位。

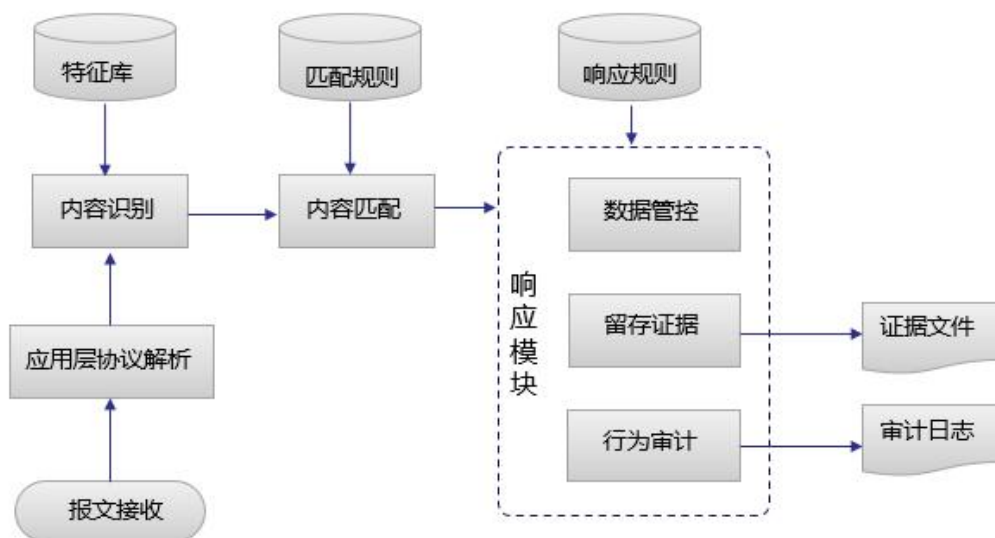


图 1-1 产品工作原理逻辑图



图 1-2 产品架构图

2 产品功能

2.1 多文档格式内容识别

对常见的文档格式能够进行内容识别，例如识别 png、jpg、jpeg、bmp 等图片中的文字；识别 html、xml、pdf、rar、tar、zip、7z、txt、xls、xlsx、msg、ppt、pptx、vsd、doc、docx 等文档的内容。

2.2 内容识别算法

支持正则表达式，用来检索和识别匹配符合某个模式(规则)的文本。支持关键字和关键字对的设定，通过对关键字的识别匹配，实现对外发敏感数据的过滤。支持权重字典识别匹配，可以通过权重值衡量词句的敏感度，并以外发数据的权重值来判断是否存在泄露风险。支持自定义文档指纹，通过检测外发文档内容与敏感数据的指纹近似程度，来识别匹配外发文档的敏感百分比。支持机器学习算法的内容识别，用户可将企业数据样本上传，系统自动识别、聚类，结合样本校验功能调整阈值从而提高匹配精准度，解决传统方案中数据分类分级难、效率低下等问题。支持自定义脚本方式内容识别功能，可根据企业规范灵活编写，方便易用。

支持解析常见文件格式并提取内容，至少包含文本、PDF、Office 文档、图片、压缩文件、代码；支持使用关键字、词典和正则表达式规则匹配内容；支持自定义数据分类分级的灵活配置；支持重要敏感数据数量、明细的统计。支持全流量以及单向上行或下行流量的解析还原，能保存原始网络流量包、URL 和五元组信息以及包含有重要敏感数据的文件，并提供多种形式的查询方式；

2.3 流量管控

支持常见网络协议的分析与还原,能够对电子邮件、web 邮件、web 应用程序 HTTP、FTP、SMTP、IMAP、SMB 和 TCP/IP 上的流量进行检查和控制。支持对网盘、文库、贴吧、微博、论坛、FTP 和 QQ 等上传文件进行自定义敏感内容识别。系统识别匹配后的外发敏感事件，支持审计、附件上传、通知、阻断、证据留存等响应动作。

2.4 流转审计

系统支持详细记录事件触发的事件 ID、策略名称、检测规则名称、应用类、应用名称、用户名、严重性、源 IP/目标 IP、附件列表及敏感内容摘要等重要信息。可记录管理员对管理平台各项操作的详细日志；并对用户进行敏感数据外

发的识别匹配记录详细的外泄事件等功能，确保事件的可追溯性。支持动态识别应用接口，自动发现并记录 URI、敏感数据、用户信息、请求方法和参数、业务系统。

2.5 敏感邮件管控

系统采用分级管控思想，可以根据数据敏感度、人员权限的不同进行分级防护，从而可以最大程度降低对组织业务、人员行为的影响和改变。能够对邮件的发件人、收件人进行检查，对于不同发件人、收件人赋予不同等级数据的外发权限，同时支持自定义黑白名单机制，对指定人员外发的邮件进行控制，如：

邮件拦截能力：能够对包含敏感数据邮件进行实时拦截，并可以对审批通过的邮件再次转发；

流程审批能力：能够根据人员、部门定义不同的审批流程、审批模式和审批人员，通过审批机制确保外发的敏感数据可控、可审；

修改邮件内容：能够对邮件收件人、附件、正文、邮件头进行修改，从而满足邮件外发要求同时不影响邮件发送过程；

证据提取能力：能够对敏感邮件提取快照信息，甚至保存原始邮件，帮助安全人员快速完成风险行为审核；

自动告警能力：系统可以根据邮件内容不同定义不同的告警对象，及时告知对应人员进行相关事件处理。

发件人检测能力：能够识别发件人邮箱，并根据邮箱账号定位到具体人员、所在部门，能够根据人员、部门、账号等信息配置白名单；

收件人检测能力：能够识别出敏感邮件接收人员邮箱账号信息，可以通过收件人账号、目标域等信息设置收件人白名单；

抄送人员识别能力：能够识别邮件的抄送人员；

密送人员识别能力：能够识别邮件的密送人员。

邮件采集留存：系统能够对邮件服务器所有外发的邮件进行采集，详细记录邮件外发过程和备份原始邮件，通过对采集的外发记录和备份的邮件进行反查实现泄露行为的溯源与反查。

组织架构同步：系统支持 AD、LDAP 等协议自动从组织账号管理体系中同步

人员部门等信息，支持在线认证登录检测，完成用户权限认证，同时也支持通过 excel 或手动创建方式设置组织架构和人员信息。通过组织架构、人员信息可以实现按部门、业务需要进行定向防护。支持发现 API 请求和应答中的用户认证和鉴权信息。

2.6 多协议识别和解析

NDLP 支持丰富的网络协议的识别和解析，包括 HTTP、FTP、NFS、SMTP、POP、IMAP 等协议，也包括对应的加密协议，比如 HTTPS、FTPS、SMTPS、POPS、IMAPS 等。同时也支持这些协议自定义端口的识别，比如当 HTTPS 的端口更改为 8443 时，NDLP 也可以识别和解析，并且进一步识别是否携带敏感内容。

2.7 过载保护

NDLP 支持各种场景下的过载保护，比如可以灵活的设置针对超大文件的处置结果及定义超大文件的大小。也可以根据 NDLP 的服务能力设置扫描逃生能力，也可以根据硬件的处理性能，比如 CPU 的使用率，内存的使用率，磁盘的使用率阈值设置逃生能力，当 CPU、内存、磁盘的使用率触发了阈值时，系统启动过载保护，当恢复到某个阈值时，自动启动业务处理能力。

2.8 报表展示

NDLP 系统内置多种报表模板，可以根据外泄事件、系统策略、告警日志等类别新增报表展示项，每个类别又支持多种数据源，可以根据数据源进行详细展示。整体用户可以根据实际需要定制报表看板，并且报表可以下载，支持下载为图片及 PDF 格式。

2.9 自定义端口流量识别与审计

NDLP 支持对自定义端口的流量进行识别与审计。通常网络的协议端口都是固定，都是存在端口自定义的情况，NDLP 协议识别引擎能够解析自定义的端口

的流量并准确识别出其协议，同时针对协议引擎的补充，NDLP 还支持协议和端口的自助绑定匹配，通多自助绑定，也可以快速实现对自定义端口的流量识别和审计。

2.10 白名单功能

NDLP 默认所有的 TCP 流量都要进行敏感检测，但是有些情况需要对某些特定的流量直接放行，NDLP 支持以白名单的形式进行免检测。白名单支持常见的形式，包括 IP，邮件，URL 等形式。

2.11 网络配置

NDLP 支持通过以 WEB 图形化的形式进行网络相关的配置，包括接口 IP，掩码，网关，接口聚合，桥接口，DNS，静态路由等常见的网络功能配置。

2.12 自定义地址监控

NDLP 旁路镜像时，不需要对应用系统进行改造、不需要应用系统调用特定接口，可以根据需要自定义地址监控，当配置自定义地址监控时，NDLP 只监控审计匹配的流量，对于非监控地址断的流量丢弃不进行审计。特点与优势

2.13 策略的灵活部署

系统支持策略的灵活部署，与、或、非的多种逻辑结合，针对性强，有效减少审计事件的误报率。

2.14 详尽的日志审计

可记录管理员对管理平台各项操作的详细日志；并对用户进行敏感数据外发的识别匹配记录详细的外泄事件等功能，确保事件的可追溯性。

支持自动生成风险统计和趋势分析报告，支持从访问数量、访问时间、访问地点等维度展示异常行为，智能分析异常账户，评估其风险分数并按风险高低排

序，可查阅、导出用户的操作行为记录。

2.15 便捷的系统运维

采用了 B/S 模式的系统架构，通过浏览器即可登录系统管理平台，可远程管理登录用户等操作。

2.16 丰富的识别算法

系统支持：文档属性识别、关键字技术的内容识别、正则表达式技术的内容识别、权重字典技术的内容识别、数据标识符技术的内容识别、文档内容指纹技术的内容识别、表格内容指纹技术的内容识别、神经网络和机器学习算法的内容识别、自定义脚本方式实现的特定内容识别，充分满足单位各种业务场景，确保数据资产安全。支持源 IP、目的 IP、HOST、URL 等单个条件或组合条件的过滤能力。可通过识别接口设计弱点，至少包含：敏感数据伪脱敏、认证方式不合理。支持对被监测的应用系统用户行为分析建模，生成行为基线，允许安全管理人员手工调整部分机器学习算法的参数。

2.17 图片识别功能

基于深度内容识别技术与领先的 OCR 引擎，支持截图、拍照、扫描等多种方式的多种格式的图片文件识别。

2.18 审计日志秒查

随着企业敏感事件的不断积累，数据库中存储的事件信息会越来越多，在如此庞大数据中查询和调用响应迅速尤为重要，系统支持千万数据秒查，且不影响其他功能使用。并具备多种组合条件高级查询方式。

支持通过 Syslog、Kafka 等方式向第三方平台发送日志及告警信息。

2.19 支持基于 IP 到人的反查

通过与 AD 域对接，实现 IP 地址到域用户的反查。最终实现基于人的溯源发查。

2.20 强大的组网能力

作为一款基于网络协议交互的网络设备，组网能力的强弱直接影响到实际部署使用。NDLP 能够支持适应各种组网，部署模式也多样，能够旁路部署，也能够单臂旁挂，也可以透明串接，也可以旁挂路由。丰富的组网能力，让 NDLP 可以灵活适应各种网络部署。

3 产品价值

3.1 完善的数据防泄露能力

1、超强的网络支持能力：支持丰富的网络协议，支持丰富的网络应用，能够对网关通道的数据防泄露分析。

2、丰富的组网适应能力：支持各种组网模型，能够完美的兼容各种网络组网，并对现网网络实现最小化的改造，支持各种云化环境。

3、超强的规则检测能力：丰富的内容识别能力，除常规的关键字匹配、数据字典匹配、数据标识符等内容识别能力外，还支持各种人工智能算法识别，包括使用人工智能实现样本数据的聚类、分类。自动按照内容进行主题梳理，进行训练学习，帮助进行分类识别策略的生成。同时支持各种文件属性识别，文件类型识别。

4、完善的泄露审计能力：完善的泄密事件溯源分析系统，内置各种类型的泄密分析报表，可根据泄露途径、泄露文件类型、泄露原始文件等进行泄密分析，并且追踪到原始泄密个体。强大的文件识别引擎，可帮助安全管理人员掌握所有外发数据的概况，包含文件或消息总数，数据类型（客户信息、财务数据、设计图纸等），外发通路等，并支持留存以满足网安法的要求。

3.2 运维轻、防护效果不减

网络 DLP 基于网络模式进行防泄露防御，和终端类 DLP 相比，免去了复杂的环境适配、安装、维护，传统的终端 DLP 终端都将越做越重，要求能搜集足够多的数据，最终难以落地，对 IT 部门来讲难以管理，并且价格高昂。而网络 DLP 只需在网络出口处部署一台网络 DLP。同时网络 DLP 上线简单，只需配置 IP 注册到统一管理平台，后续便可在平台进行统一的配置下发和设备监控。

3.3 对业务影响小

基于网络 DLP 的产品解决方案属于轻模式方案，整体对用户影响较小，整体包括如下：

- 1、网络改造小，不改变用户的访问习惯；
- 2、业务影响小，不影响用户的访问体验；

4 应用场景

4.1 合规应用场景

网络数据防泄露产品也常用于满足合规要求。例如 2019 年正式发布的《信息安全技术网络安全等级保护基本要求》版本，其中第三级安全要求，安全区域边界的访问控制应对进出网络的数据流实现基于应用协议和应用内容的访问控制。另外，支付卡行业数据安全标准（PCI-DSS）要求，机构要限制不相关人员对支付卡持卡人信息的访问，并监测对持卡人信息的所有访问行为。除了等级保护建设 2.0、PCI-DSS、HIPAA 和塞班斯法案等。许多法律法规对数据防泄露技术有明确的要求，包括监测和控制受监管数据，管控数据的访问或传输的能力。由于其易于部署和广泛的合规要求，网络数据防泄露产品是最常用于合规性建设的产品之一。

4.2 企业内部风险防护场景

为了履行其业务职责，许多员工、合作伙伴和承包商需要访问敏感的公司数据。这些用户正在以前所未有的速度创建、操纵和共享数据，这意味着数据在企业网络、企业和个人设备以及云上移动。如果你的公司雇佣了独立的承包商和自由职业者，他们在公司网络之外工作，这会使你的数据面临更大的损失或意外暴露风险。网络数据防泄露仍然是网络数据丢失预防解决方案的主要用例。这些解决方案提供的数据可见性和控制使基于策略的保护能够确保敏感数据仅被传输给授权接收方或由授权接收方访问。保护知识产权免受公司网络的渗透。

4.3 数据出境监测场景

企业在开展数据出境业务之前，需要向监管部门进行申报，就出境数据的规模、范围、种类、敏感程度进行说明。实际出境的数据如果与申报内容不符，不但对国家造成损失，企业也将面临着处罚。因此，无论监管部门还是企业，都需要持续监测网络流量中的出境数据，识别违规行为。网络防泄露产品对网络流量进行解析，能够采用正则表达式、关键字和指纹匹配等技术识别出个人信息等敏感数据，帮助用户实时掌握出境数据的信息，识别数据出境风险。

4.4 敏感数据泄露风险监测场景

敏感数据的可见性，能够增强员工的安全意识。无意中违反策略会触发用户通知，向用户提示违规行为，并提供解释以帮助改进到正确的行为。

5 安装部署

NDLP 支持各种组网模型，可以根据实际网络选择对应的模式进行部署。

(1) 网桥模式

设备串联在网络中，上游设备直接将流量发送到网络防泄露系统，再由网络防泄露系统进行转发。网桥模式部署简单，用户不需要为此变更应用服务的访问地址。

(2)代理模式

类似 Web 代理服务器的部署方式。需要将被监控终端的代理服务器地址配置为网络防泄露系统的地址。未配置代理服务器的终端不受网络防泄露的监控。

(3)路由模式

通过配置路由策略，将网络流量转发到网络防泄露系统，经过检测之后，再根据路由策略转发。该模式的特点是可以指定监控范围，且不需要更改之前访问的服务地址。

(4)ICAP 模式

ICAP 模式是网络防泄露产品比较特殊的部署方式，用于对接网络中的上游设备。如果用户现场已经部署了 Web 代理服务器或者上网行为管理服务器，那么这些服务器可以作为上游设备，将流量通过 ICAP 协议传到网络防泄露系统，网络防泄露系统处理完成后，将下一步操作指令返回给上游设备。该模式需要上游设备支持 ICAP 协议。

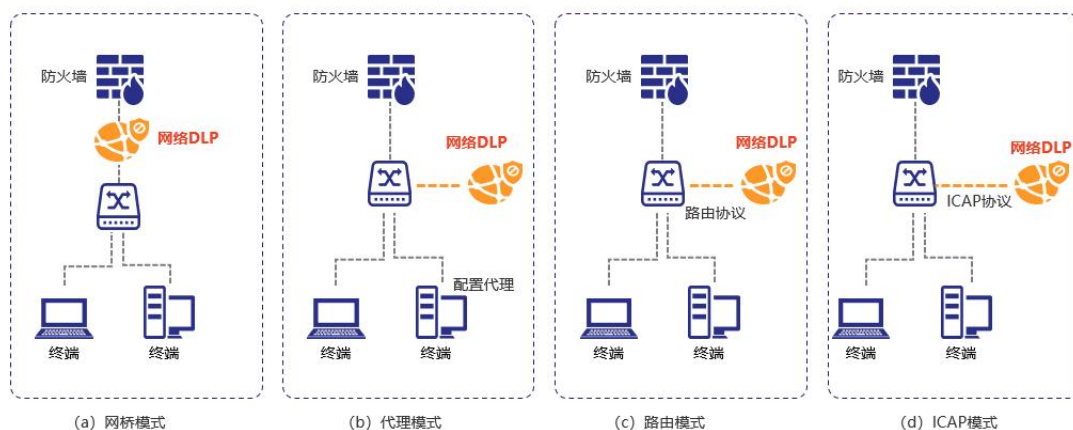


图 6-1 产品部署模式