世平信息
SPINFO

SIMP-NDLP V1.5

网络数据泄露防护系统
产品技术白皮书

商标声明

免责声明

由于产品版本升级、调整或其他原因，本文档内容可能有变更，杭州世平信息科技有限公司保留在没有任何通知或提示的情况下对本文档进行修改的权利。此举并不代表本公司属违约行为，您应当实时关注文档的版本变更并通过杭州世平信息科技有限公司获取最新版的文档。如因文档使用不当而造成的直接或间接损失，本公司不承担任何责任。

引　　言

编写目的

本文档主要阐述了世平网络数据泄露防护系统的设计背景、功能、特点、应用价值及其典型应用场景等内容，帮助您快速和全面的了解世平网络数据泄露防护系统。

读者对象

- 销售人员
- 售前人员
- 目标客户
- 其他想要全面了解本产品的相关人员

约　　定

说明需要注意的信息，突出重要/关键信息、最佳实践和小窍门等。

1 术语及缩略语

表格 1 术语及缩略语表

缩写、术语	说明
数据泄露防护	数据泄露防护指通过一定的技术或管理手段，防止企业组织中指定的数据或信息资产以违反安全策略规定的形式被有意/无意流出。
DLP	Data Leakage Prevention，即数据泄露防护。
EDLP	Endpoint Data Leakage Prevention，终端数据泄露防护。
NDLP	Network Data Leakage Prevention 网络数据泄露防护。
ANDLP	Advanced Network Data Leakage Prevention，增强版网络数据泄露防护。
HTTP	HyperText Transfer Protocol，超文本传送方式。
HTTPS	Hyper Text Transfer Protocol over SecureSocket Layer，超文本传输安全协议。
SMTP	Simple Mail Transfer Protocol，简易电子传输协议。
IM	Instant Messaging 即时通讯（类似 QQ、微信等即时聊天工具的统称）。
SMB	Server Messages Block Samba 是一种对于 SMB 协议的开放源码实现，提供绝大多数 Windows 系统的 SMB 文件打印和共享服务，可与 Windows 系统网络无缝结合。

修订记录

版本	日期	修订人	修订说明
V1.0	2021-02-01	周亚飞	初始发布版本
V1.1	2021-12-15	黎伊帆	内容及排版修改
V1.2	2024-07-05	李艾功	更新场景等

目　　录

2 产品概述

随着信息技术的快速发展，世界经济形态发生了巨大的变迁，知识资产逐渐取代了实体资产作为经济价值表现的主要载体，企业的价值越来越多地体现在无形资产中，包括不限于专利技术、版权、企业敏感运营数据等，据统计分析，世界 500 强企业的无形资产价值高达总资产价值的 70%，其中大部分内容均以数据文档的形态存储于信息系统中。同时，在经济发展从传统形态向知识经济形态的转化过程中，企业的数据也从单纯的数据本身向着数据资产转化。因此数据一方面其内涵急剧丰富，体现出越来越多的经济价值；另一方面不再仅仅局限于应用系统范围内的单纯使用，而是成为对整个企业业务发展起到支撑甚至驱动作用的资产。

数据资产的这种转化逐步引起了受利益驱动犯罪分子的注意，加剧了数据资产安全管理，尤其是敏感信息安全管理的迫切性。企业借网络安全建设之势，投入建设以纵深式防护为指导之路的安全体系建设。

传统网络安全建设从边界防火墙、入侵检测、漏洞管理，到身份和访问控制，再到从上网行为管理到数据内容的审计，可谓铜墙铁壁。但从近年来频发的安全事件来看，敏感信息泄露已经成为了造成企业经济利益、公民隐私权益甚至国家安全隐患的最大元凶，并有愈演愈烈之势。说明传统的防护体系和思路已不足以保护企业的数据资产安全。

纠其缘由，还是由于数据重要性、信息技术的高迭代性以及网络环境的复杂性在短期内的激增，而安全防护体系作为被动响应动作天然存在滞后性导致，可以说是必然结果。为避免刻舟求剑、缘木求鱼的防护思路，弥补传统信息安全技术的不足，杭州世平信息科技有限公司（以下简称“世平信息”）基于多年的信息安全从业经验，自主研发出基于内容识别技术的新一代**数据泄露防护系统（DataLeakagePreventionSystem，以下简称 DLP）**系列产品，以协助用户快速、精准地感知和阻止潜在的涉敏数据泄露威胁，实现遵从行业标准、法规以及降低数据安全风险的目标，确保企业核心数据资产全生存周期的安全。

3 产品介绍

网络数据泄露防护系统（NetworkDataLeakagePrevention，以下简称 NDLP）可以针对网络传输中的动态敏感信息进行监控，防止人员有意或无意将敏感信息文件外发（通过邮件、WEB、FTP 以及 IM 即时通信等渠道），有效提高涉敏数据的安全性。

NDLP 可对网络中的数据进行深度内容分析，集成多种内容检测技术，针对不同安全级别的数据可采用不同的技术，兼顾准确与效率。可对网络传输层各类应用流量所承载的涉敏数据进行识别、监控、审计与溯源，并支持可视化展示涉敏数据动态分布地图。支持多种响应规则，可实现敏感数据保护与业务畅通之间的平衡，做到适度安全，同时为确保设备的可实施性，提供灵活的策略框架，简化策略配置过程。

NDLP 产品形态为机架式硬件产品，采用专有硬件平台和专用安全操作系统，支持多核 CPU 与并行计算，实现高性能的网络处理和敏感数据检测。NDLP 并联部署于交换机镜像或专用流量分离设备（NetworkTAP）设备上。

4 产品主要功能

4.1 全面的网络协议支持

NDLP 支持对 HTTP、HTTPS、SMTP、SMTPS、POP3、POP3S、FTP、IM、SMB2、DNS、MSN、TELNET 以及自定义协议等的网络通道进行识别和解析，再通过内容识别技术发现涉敏数据传输情况，进而辅助数据泄露防护体系建设。

针对加密场景，系统支持 SSL 协议隧道的解密功能，能够通过简单对接配置实现通过 HTTPS 协议方式加密数据的识别，以发现加密状态下的违规内容传输行为，降低数据泄露隐患。

4.2 先进的图像识别技术

NDLP 内部集成光学字符识别技术（OCR），可对各类图型、图片中的敏感信息进行准确抽取与识别。DLP 还具备独特的图像相似度匹配技术，可对图像进行识别与管控。

4.3 广泛的文档类型支持

NDLP 支持识别的文档类型覆盖各行业日常使用文档类型的 98%以上，例如 OFFICE 办公文档（(DOC/DOCX、XLS/XLSX、PPT/PPTX…）、WPS、iWORK、PDF、OFD、纯文本、标记文本、源代码、图片内容、设计文档等，总计达千余类。

4.4 强大的内容识别引擎

NDLP 内置强大的内容识别引擎，支持丰富的内容识别方式，包括：关键字词、正则表达式、表单格式识别、红头文件识别、各类报告识别等，满足多种识别需求，同时系统搭载基于人工智能的数据识别引擎，支持包括中文自然语言识别、机器学习训练、数据精确指纹、相似度指纹等识别技术，满足用户深度定制需求。

基于多年领域深耕，系统预置了近百类内容识别模板，方便各行业用户灵活、快速使用。

4.5 数据异常行为检测

NDLP 通过对网络流量进行分析，实时获取涉敏数据的查询、下载、网络外发（邮件、FTP、HTTP）等各类行为特征，依据行业用户数据安全政策，对高敏感度的涉敏数据获取行为，大批量、非工作时间以及点滴式持续异常获取涉敏数据等行为进行关联检测与预警，及时发现数据泄露风险。

针对应用服务器，基于用户访问内容进行用户行为审计（HTTP/HTTPS 协议），包括用户数据过量访问、用户点滴下载/浏览客户数据、用户异常登录、非工作时间违规访问客户数据等情况。

4.6 数据流向动态展示

系统支持实时动态展示敏感数据流向地图，并种颜色标识不同的事件严重性；同时支持按照数据的分类分级属性、业务部门、业务系统、传输协议等，对事件进行统计。

4.7 策略管理

NDLP 支持灵活高效的策略，能够适应各种敏感数据检测要求和响应要求。同时提供多个预置策略模板，帮助用户快速满足业务和和法规需求。同时支持策略的批量导出和导入，对策略进行备份和再次复用。

4.8 事件报表与仪表盘

系统支持支持友好丰富的事件报表功能，提供了集中展示事件的仪表盘，内置的通用型报表和仪表盘；

- 支持报表、仪表盘的自定义；
- 支持事件报表的高级查询，批量审计，归档，导出，附件批量下载任务；

- 支持立即下载报告，将报告发送到邮箱，指定计划任务创建报告并发送邮箱；
- 支持生成的报告文档类型包括：zip、pdf、word，方便管理员及领导查看。

5 产品特点

5.1 灵活的系统部署模式

NDLP 可采用交换流量镜像旁路方式，支持在各类局域网、云环境、虚拟云桌面以及虚拟环境中部署，且对用户网络零影响，可为绝大部分网络环境提供网络层涉敏数据的安全保护。

NDLP 还支持以软探针方式部署，以软探针 agent 方式部署到采集端，为企业在无交换设备修改权限情况下的公有云设施等条件下的部署提供解决方案。

5.2 符合自主可控要求

系统完全兼容国产化硬件和操作系统环境，功能、性能、可靠性等经过权威测评认证，满足不同网络环境用户使用场景。

支持的国产化硬件平台，包括鲲鹏服务器、飞腾服务器；支持国产操作系统银河麒麟 V10 等。

5.3 智能驱动精准高效

世平网络数据泄露防护系统对数据的内容进行识别和匹配，精准的数据匹配模型对于数据的准确定位和检查起到决定性作用，也是评判检查系统一个重要指标。

- **专业模型库**

世平信息结合多年保密行业的从业经验，梳理和总结保密行业涉敏数据特征，将涉敏数据特征转化为机器语言并按一定的逻辑关系组合，形成保密行业涉敏数据检查模型库。同时，还可以根据各单位的涉敏数据特殊性灵活配置专属规则。

- **人工智能助力**

系统内置基于主题模型的分类算法，可对现有涉敏文件进行自动分类。在

分类的过程中，使用中文分词技术，提取各类涉敏文件的特征，再通过人工审核后形成各行业或重大事件的涉敏文件特征库。

6 产品应用价值

通过部署 NDLP，可有效提升网络层面数据安全的防护能力，防止人员有意或无意将敏感信息文件通过网络进行外发，防止敏感信息通过网络被泄露。NDLP 的应用价值包括：

- 对网络中传输的数据进行管控，采用审计及告警等处理方式，保障敏感数据的安全使用；
- 实现对网络传输中非法获取敏感数据行为的审计与监控，及时发现数据的误用、滥用、窃取等行为并告警，防止敏感数据通过网络泄露；
- 实现对业务系统的监控和审计，对业务系统中的数据查询、下载、修改、导入、导出等行为进行监控与审计（身份、数据、行为绑定）；
- 基于用户访问内容进行用户行为审计（HTTP/HTTPS 协议）与监控，包括用户数据过量访问、用户点滴下载/浏览客户数据、用户异常登录、非工作时间违规访问客户数据等情况，并及时上报异常行为，提升业务系统的安全性。

7 典型应用

7.1 场景 1 镜像旁路部署

NDLP 通过旁路接入交换机镜像口，对途经该交换机所有镜像流量（需要被查方配合配置）进行实时捕获，及时发现涉敏数据通过各类网络通道的违规外发行为。

NDLP 的网络部署如下图所示，不影响用户原有网络拓扑，部署快速、方便。

系统典型部署如下图所示。

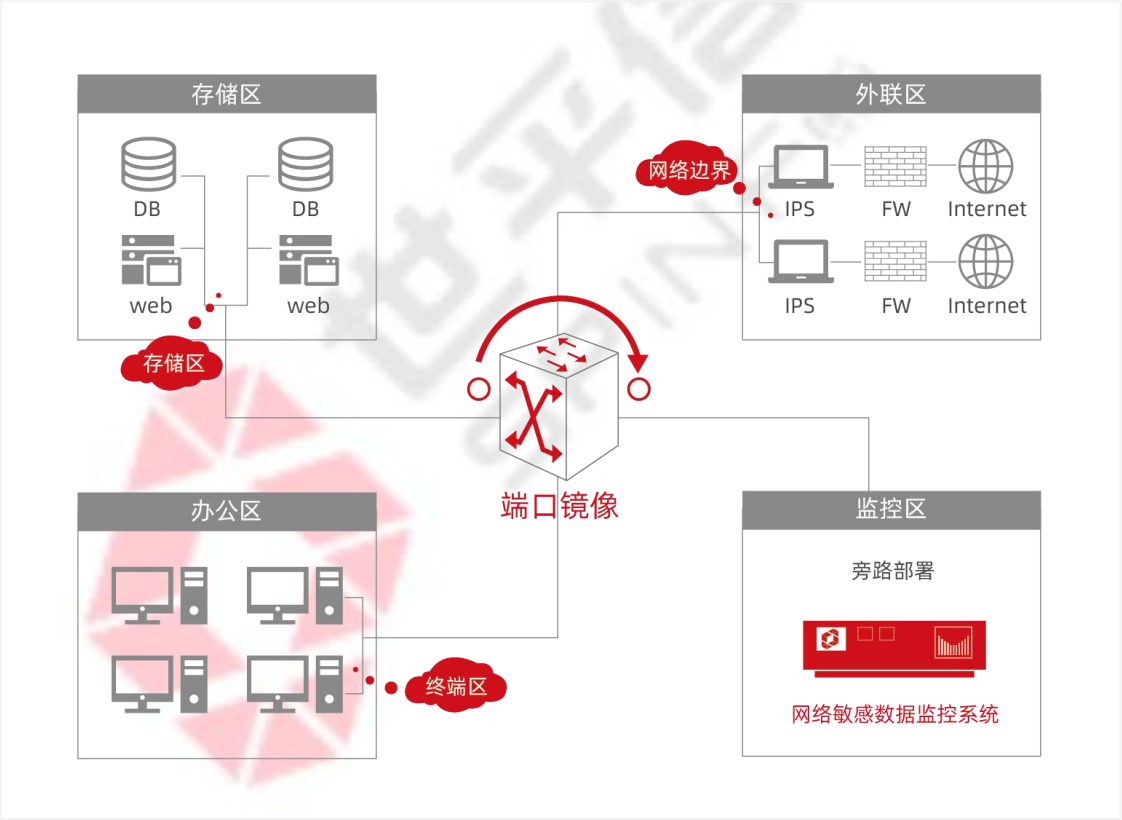

图 7-1 网络数据泄露防护系统部署示意图

8 产品形态规格

产品名称与型号		规格参数
网络数据泄露防护系统 SIMP-NDLP	初级版	提供网络监控功能 适应用户数：500 用户以内 性能：400Mbps
	中级版	提供网络监控功能 适应用户数：1000 用户以内 性能：1Gbps
	高级版	提供网络监控功能 适应用户数：2000 用户以内 性能：2Gbps
	旗舰版	提供网络监控功能 适应用户数：4000 用户以内 性能：3Gbps

9 技术支持

杭州世平信息科技有限公司各地分部/办事处地址及联系方式如下：

杭州总部

地址：杭州市西湖区西斗门路 3 号天堂软件园 D 幢 3 楼

电话：0571-56082888

传真：0571-56089102

西安子公司

地址：西安市雁塔区西电科技园 E 座 10 楼

电话：029-89199377

传真：029-89199377

北京子公司

地址：北京市海淀区上地东路颐泉路 2 号楼 711 室

电话：010-62962820

传真：010-62962820

山东子公司

地址：山东省济南市高新区会展西路 88 号 1 号楼 1-3134 室

电话：0531-88989380

传真：0531-88989380

湖南分公司（覆盖湖北省）

地址：湖南省长沙市芙蓉中路三段 420 号华升大厦 15 楼

电话：0731-85234695

传真：0731-85234695

广州分公司

地址：广州市天河区科华街 251 号乐天创意园 A2 栋 3016 室

电话：020-61868027

传真：020-61868027

四川分公司

地址：成都市青羊区八宝街 90 号九龙商务楼

电话：028-65214782

传真：028-65214782

杭州世平信息科技有限公司

SHIPINGINFORMATIONTECHNOLOGIESCO.,LTD.

总部地址：浙江省杭州市西湖区西斗门路 3 号天堂软件园 D 幢 3 层

邮政编码：310012

客服热线（24 小时）：4001006790

公司邮箱：marketing@shipinginfo.com

技术支持邮箱：support@shipinginfo.com

网址：www.shipinginfo.com