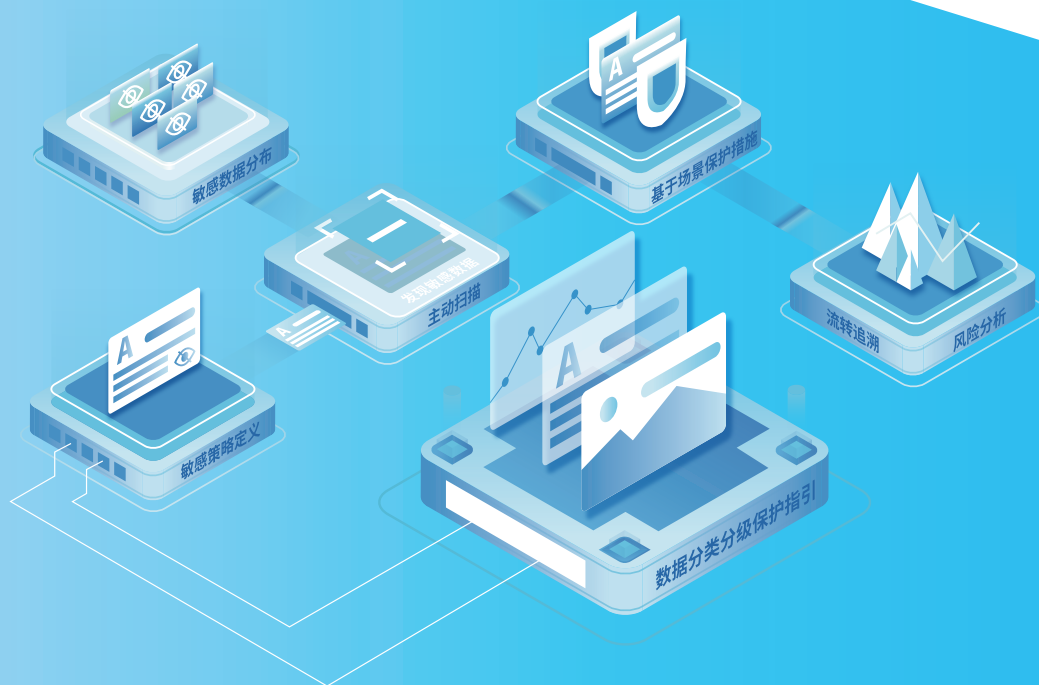


# UniDLP数据防泄露系统

开创业内以场景驱动的非结构化数据安全整体解决方案



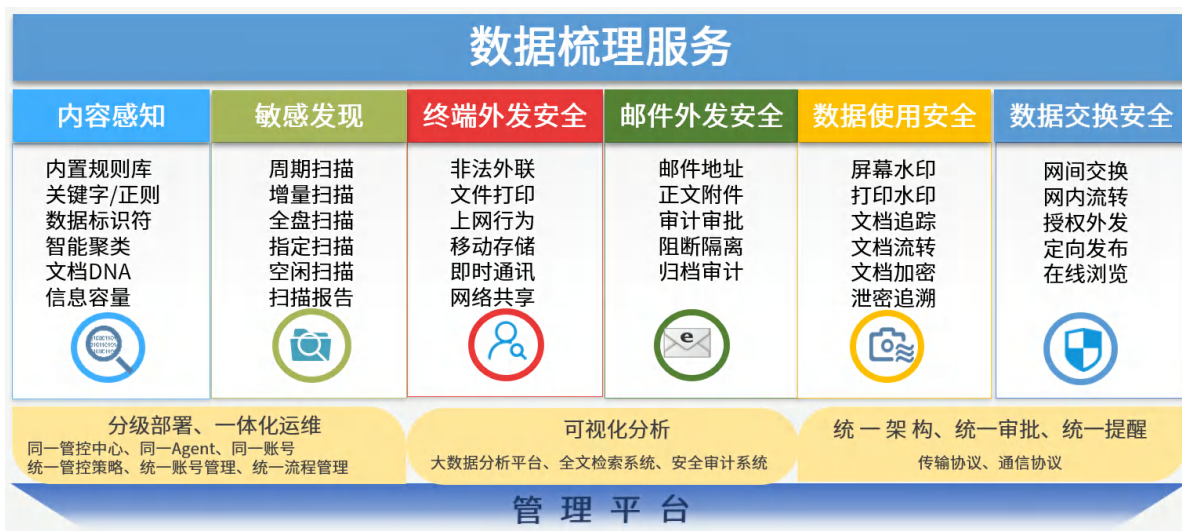
# UniDLP数据防泄露系统

## 产品概述 Product overview

联软数据防泄露系统(简称:UniDLP)以终端数据发现和数据分类分级为基础,采取用户权限控制、文件内容识别、文档透明加解密、数据安全隔离、数据安全流转、网络应用和外设管理、业务数据访问控制、水印和隐写等多种技术手段组合,通过数据活动监测、数据访问控制、数据风险评估、数据审计溯源,以业务场景为驱动保护企业所有员工终端的数据资产和数据活动,实现客户终端数据防泄露或泄露后追踪溯源。



## 产品方案 Solutions



## 数据分类分级

- ▶ 通过数据梳理服务和终端数据探针,对企业典型数据进行调研,通过半自动化的梳理工具对数据进行分类分级,并对数据面临的风险进行评估,帮助企业制定数据安全方案。

## 数据特征识别

- ▶ 支持对文档、源代码、图片等文件进行文件源格式识别,并基于关键字、正则表达式、数据标识符、智能聚类、文档相似度、唯一标记、流转记录、信息容量等方法对内容进行感知,实现对文档所属类别、级别的判定以及数据血缘关系、分布地图、风险态势等分析。

## 数据安全保护

### 数据风险识别

- ▶ 在用户无感知的情况下对终端硬盘数据进行扫描,生成敏感数据分布图和敏感数据使用图,对潜在风险进行识别;
- ▶ 对已确定的敏感数据提取文档DNA或隐藏标签,全网搜索跟此文档有血缘关系疑似敏感数据,实现风险提前防范。

### 数据活动监测

- ▶ 对USB拷贝、共享、网盘、IM、邮箱等行为进行全方位审计;
- ▶ 对文档的创建、流转过程进行完整审计;
- ▶ 对业务系统的访问、下载数据进行记录和标记;
- ▶ 基于文档类型、大小、类别、等级以及涉及的用户、部门、行为进行可视化展示。

### 数据访问控制

- ▶ 对外设、网络应用、用户、设备以及数据类别、级别进行灵活的策略设置;
- ▶ 对第三方、合作伙伴的数据进行打开次数、时长、水印、打印权限等限制;
- ▶ 文档透明加解密在手机端查看加密的文件;
- ▶ 内置专家规则,对违规外发等明确的泄露行为进行及时阻断、提示和告警;
- ▶ 基于用户画像,对违规访问、异常下载、滴漏外传、对抗式外发批量的恶意泄露等行为进行实时分析和动态策略应对。

### 数据泄露追溯

- ▶ 在截屏、拍照、打印时附加明文、隐形、隐藏等多种水印,一旦泄露可追溯源头;
- ▶ 对文档的创建、流转、外发、分布等进行全方位记录,一旦泄露,可全面分析定位;
- ▶ 通过屏幕录像,对研发、设计、客服等敏感岗位进行全过程还原。

## 产品适用场景 Application scenarios

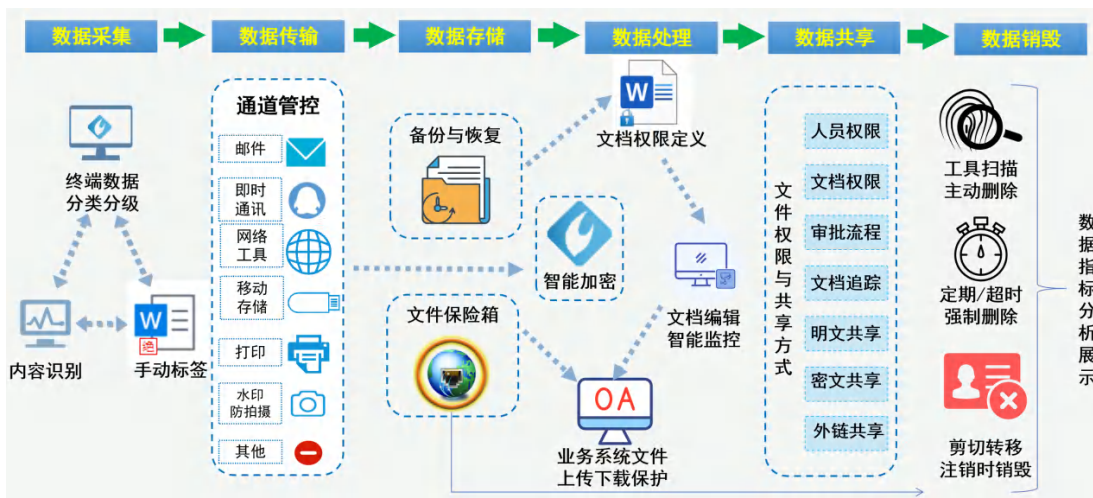
### 1、基于数据安全体系的数据安全合规建设

建设“数据安全管理体系、数据安全技术体系、数据安全运营体系”三大体系，通过规划数据安全战略、完善数据安全管理制度及组建数据安全团队，利用丰富的识别、发现技术完成对数据分类分级管理，并基于场景化需求、差异化技术灵活实现不同数据有效管控和安全对抗，保证办公效率的同时实现数据安全，最后基于终端敏感审计及事件管理持续完善数据运营。



### 2、基于数据生命周期对散落在终端的海量非结构化数据进行分类分级保护

建设基于“数据生命周期”的数据防泄露系统平台，实现对终端上非结构化数据的“采集、传输、存储、使用、分享(外发)、销毁”全流程保护。



### 1、及时发现敏感数据资产分布情况

通过敏感文件审计策略,发现留存在员工终端的敏感数据资产,并进行分类分级展示。



### 2、实时掌握敏感数据外发使用情况

实时展示企业敏感数据的使用情况,评估数据泄露风险。



### 3、终端数据权限控制“权限最小够用”原则

根据数据传输通道与泄露风险,组织决策数据权限控制策略(如:提醒、审计、告警、阻断、审批等),基于用户角色调整策略下发和执行优先级。



### 4、监控预警与追踪溯源

系统自动搜集高频外发敏感数据的用户行为,主动预警给数据安全管理员。管理员结合审计信息和适度的屏幕截图或录像,开展日志查询与数据溯源,给业务部门输出安全报表用以了解数据安全风险管控结果。

数据安全 / 数据泄露防护 / 常用信息查询 / 数据外发预警监控

在 预警方案 中查询 请输入

已选择0条数据

序号	预警方案	预警类型	预警描述	状态
1	USB外发文件预警	文件读写操作审计预警	1天内外发超过25个敏感四级文件-邮件预警	启用
2	即时通讯审计预警	即时通讯审计预警	1小时内外发超过5个敏感文件-邮件预警	禁用
3	敏感文件留存预警	敏感文件审计预警	终端发现敏感文件超过100个-邮件预警	启用
4	频繁打印预警	打印监控预警	1小时内打印超过5个敏感文件-邮件预警	启用

## 产品特点 Features

- ▶ 帮助企业梳理数据资产, 识别数据泄露风险;
- ▶ 防止敏感数据泄露, 保护企业数据资产;
- ▶ 在数据泄露后提供快速有效的追溯手段;
- ▶ 基于场景进行方案设计, 实现数据安全同时保障数据流转高效。

## 方案优势 Advantages

### 以场景驱动, 最大限度保障业务效率

- ▶ 通过数据梳理, 针对不同类型用户、数据类型、使用环境, 评估数据面临的不同风险, 通过多种技术手段组合实现对应不同场景的最佳方案, 实现安全保护的“度”与业务效率的最佳平衡。

### 创新技术更优保护

- ▶ 全面文件识别、多重内容感知技术, 突破内容识别技术性能瓶颈, 特有的文档追踪、信息容量检测可针对业务数据从源头上进行保护;
- ▶ 通过明文、隐形、隐藏等多种水印技术, 并基于业务系统、敏感文档进行触发式加载, 保障用户体验的同时, 针对拍照、打印、截屏等泄露行为快速定位责任人;
- ▶ 提供文档水印发布系统, 在方便文档发布的同时防止数据的下载、拍照、截屏泄露;
- ▶ 针对高权限账号进行透明审计, 防止高权限账号被恶意使用 (仅限专用版);
- ▶ 针对敏感业务系统的数据字段在显示前进行脱敏处理 (仅限专用版)。

### 内置高速数据处理引擎, 快速追溯与定位

- ▶ 数据引擎支持并行计算与横向线性扩展, 实现海量审计数据的高速存储、计算和分析。

### 方案成熟, 应用范围广

- ▶ 在金融、制造、医疗、企事业等各个行业有大量可验证的大规模部署案例及最佳实践。

## 部分典型客户 Some Typical Customers










**服务热线:400-6288-116**

地 址:深圳市南山区粤海街道科兴科学园A2栋9层

邮 编:518057

电 话:0755-86219298

传 真:0755-86148550

网 址:<https://www.leagsoft.com>



获取专家支持



知晓最新资讯