联软科技
LEAGSOFT

技术白皮书

联软 UniDLP 数据防泄露系统

深圳市联软科技股份有限公司

2022 年 5 月

版权声明

免责条款

由于产品版本升级或其他原因，本白皮书内容有可能变更。联软科技留在没有任何通知或者提示的情况下对本白皮书的内容进行修改的权利。本白皮书仅作为使用指导，联软科技全力在本白皮书中提供准确的信息，但是不确保本白皮书内容完全没有错误，本白皮书中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

联系方式

用户支持邮箱：support@leagsoft.com

技术支持热线电话：400-6288-116

网址：http://www.leagsoft.com

目录

1 引言

1.1 背景

随着计算机和网络技术的飞速发展，越来越多的企业依托信息化的力量开展业务和拓展市场，因此大量数据被存储于计算机、网络存储设备中。大数据背景下，数据相当于企业的命脉，数据的价值更是不可估量的，也正因为如此，不少不法分子打起利用数据换取金钱的主意，数据安全正在面临来自多方面的威胁。近年来，数据泄露事件时有发生。数据泄密事件一般是由企业内部员工泄密引起或来自外部攻击。外部攻击例如木马、爬虫、勒索病毒等，内部攻击则是多样的，例如业务人员为牟利盗取数据、运维人员为泄愤破坏数据、内部员工在不知情的情况下将数据外泄等。美国电信巨头 Verizon 公司发布的由 81 个国家参与调研的《2020 年数据泄露调查报告 DBIR》显示，55%的数据泄露事件涉及有组织犯罪，30%的数据安全事件源自于企业内部。IBM Security 对全球 500 多个组织数据泄露时间深入分析发现后发布《2020 年数据泄露成本报告》，报告中显示，数据泄露事件给企业和组织造成的平均成本为 386 万美元。来自国际领先的隐私及信息管理调查机构 Ponemon Institute 的年度调查结果显示：信息泄漏事件的主谋已经不再单纯是网络黑客和恶意程序，更多的数据信息是被企业和机构的内部员工所泄漏或盗窃。与传统的外部盗窃相比，这种来自内部的恶意外泄更具有针对性，隐蔽性，给企业造成的损失也更大。因此，企业采取数据防泄露手段保护数据安全已刻不容缓。

1.2 政策

近年来，国家出台多部数据防泄露相关法规和政策，引导企业重视公司的数据资产。

《中华人民共和国数据安全法》中指出，数据处理包括数据的收集、存储、使用、加工、传输、提供、公开等。数据泄露防护贯穿整个数据的生命周期。低二十九条规定，开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取

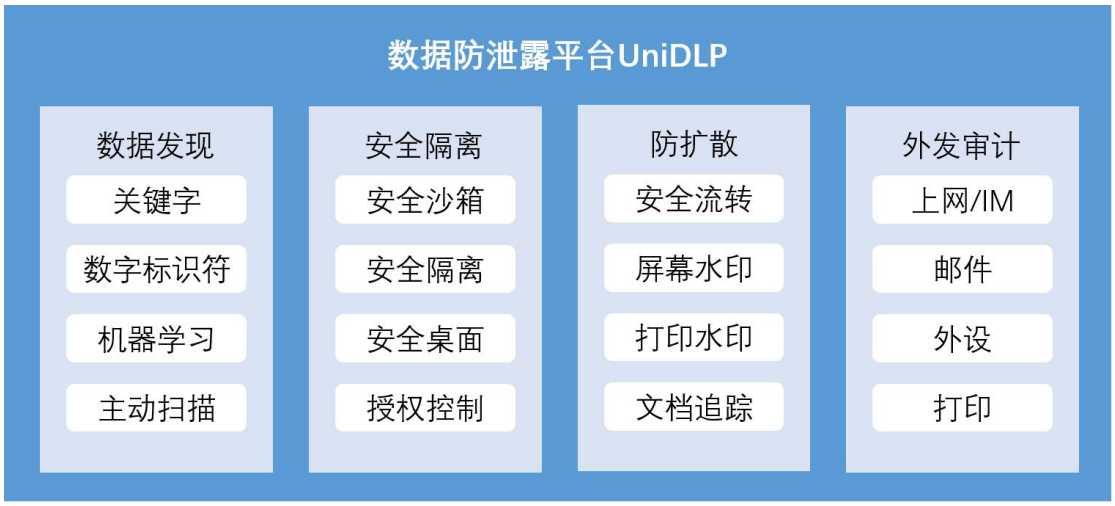
处置措施，按照规定及时告知用户并想有关主管部门报告。违反数据安全法，给他人造成损失将承担民事或刑事责任。

等保 2.0 三级等保（监督保护级，适用于地市级以上的国家机关、企业、事业单位内部的信息系统，例如涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统）中指出，应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析；访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可以行为等。

除此以外，《中华人民个人信息保护法》、《银行业金融机构数据治理指引》、《健康医疗信息安全指南》等法规和政策文件均阐述了数据防泄露治理的指导意见。

2 产品特点

联软科技股份有限公司（以下简称“联软科技”）推出的 LeagView 7000 数据防泄露产品（以下简称“UniDLP”）将网络接入管控、终端设备管控、DLP/沙箱/水印/数据流转管控/文档追踪/加密/行为与内容审计等数据管控技术有机结合，形成一个覆盖各行业各种场景的数据防泄露体系，防范敏感数据被从内部泄露或外来窃取。



1. 定义与发现

支持通过数据来源、文档内容来定义数据是否敏感，通过对文档格式的识别和文档内容的感知，实现对终端数据的智能分类、分级及可视化展现。

2. 控制与保护

通过外发通道管控、访问权限控制、文件加解密、安全计算环境隔离、数据安全流转、行为审计与追溯等功能与技术，打造完善的数据安全防护与信息防扩散系统。

3. 协同与联动

与安全数据摆渡系统协同，实现跨网或网内不同用户间的数据安全流转，通过与准入控制系统协同，实现资源访问控制。

4. 功能完整、方案成熟、大规模应用

功能完整：从准入控制到终端管控，从内容识别到数据保护，从行为分析到泄密预警，从网络到终端，从应用到内容，从已知风险管控到未知威胁发现；

稳定、易部署：不对文件染色，不改造业务系统，不影响应用访问速度，不指定文件系统类型、应用程序版本；

大规模应用：数据防护方案目前已在银行、证券、制造业、物流交通、政府、能源、电力等行业得到了广泛推广。

5. 以场景驱动，最大限度保障业务效率

针对不同类型用户、数据类型、使用环境，提供多种技术手段和方案供选择，实现安全保护的“度”与业务效率的最佳平衡

6. 内置大数据引擎，保障审计追溯效果

大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

7. 数据防扩散

以联软科技水印技术为基础的《信息防扩散解决方案》，能很好解决企业文档在流转过程中的扩散问题。该方案包括：

a) 明文、二维码、图片、矢量（隐形水印）等在内的多种水印生成方案；
b) 可以根据设备和用户信息自动生成上述不同类型的水印效果；
c) 可以将上述不同类型的水印，根据业务系统、文件敏感级别触发式的加载到设备的屏幕上以及打印件中；
d) 员工可以通过 Web 页面上传、发布、分享、外发企业文档，管理员可对员工上述的行为进行权限管控和水印方案制定；
e) 通过将企业业务系统与联软科技的水印服务器进行对接，将上述不同类型水印嵌入到业务系统页面和从业务系统下载的文档中。
f) 除了明文水印外，还有用户无感知的矢量水印，该技术为联软的专利技术；此外，还有用户不可见的数字盲水印，仅需将截图上传，进行隐水印码解析，即可实现信息泄露追溯；
g) 触发式加载：只有在访问关键的业务系统、编辑重要的文档、打开指定的应用时才加载水印，且最大限度将水印的影响降到最低；

3 行业实践方案

3.1 银行行业

1. 业务需求

银行通常地域分布广泛，终端设备数量多，敏感文件数量多且通常各办公终端均有分布。U 盘或移动硬盘使用量大，同时也是敏感文件外泄的重要途径。银行内部通常存在多张网络，不同网络之间传输数据流程复杂耗时较长。

2. 解决方案

总行部署统一的数据防泄露管控平台，若银行内终端数量较多可在各分行部署二级管控平台，二级服务器做双机热备，一是分散一级服务器压力，二是当一台服务器发生故障时不会影响业务的正常进行，同时数据在一级服务器统一展示，做到运营直观、高效。

UniDLP 平台内置了行业敏感规则模板，并支持只能聚类、文档 DNA 等敏感数据识别技术，可以帮助银行制定相关的敏感规则，通过敏感规则与外发通道管控相结合，实现敏感文件全生命周期监控，并针对文件的外发手段、时间、途径进行记录，做到可追溯。

针对银行内部移动存储介质进行注册，外来设备无法使用，对注册 U 盘的文件操作进行监控，另外可通过专用的安全 U 盘浏览器对特殊文件进行全方位防护。

对不同网络之间文件的流转，进行流转审批，审批通过后由专人负责文件流转操作，做到权限分离，操作留痕。

对屏幕添加矢量水印、明文水印达到震慑和防拍照、防截屏的目的，对文件添加图片水印、打印水印做到数据流转留痕，方便追溯的目的。

3.2 金融行业

1. 业务需求

金融行业移动办公终端数量多，通常办公终端离线后就无法有效地管控本地存储的文件，造成数据泄露的风险。中国证券业协会 2017 年 9 月 8 日发布

《证券公司合规管理实施指引》，明确了证券公司应当运用信息技术手段对工作人员电子邮件、即时通讯等职务通讯行为进行监测。

2. 解决方案

向办公终端推送安全助手，通过登录安全助手或获取域信息将终端设备与组织架构内人员进行绑定。通过安全助手向终端推送策略，对本地文件进行权限管理，同时监控邮件、网页、FTP 等外发通道，对文件进行读、写、外发等操作管控。

对客户端邮箱、网页邮箱、即时通讯工具进行监控，审计发送的文字、图片、文件等内容，并对发送的文件内容进行敏感扫描，同时对所有发送操作进行记录、存档，一旦发生泄露事件，即可通过存档的数据进行溯源。

针对特殊涉密岗位对屏幕操作进行录像、拍照等，一是起到震慑作用，二是通过录像和照片可以轻松对泄密事件进行溯源，可以有效防止泄密事件发生。

3.3 其他行业

1. 业务需求

制造业、交通运输业和医疗行业用户普遍对计算机软件、硬件的使用水平不搞，以及运维方面的管控措施不够全面，造成图纸、病志等信息泄露的不在少数。

由于信息化程度越来越高，许多企业存在员工自携或由公司发放智能设备、笔记本的现象，这些智能化移动终端可以随时连接网络，随时传输文件，可以通过多种方式对文件进行传输。

2. 解决方案

针对图纸、病志、客户基本信息等专用文件进行专门的敏感规则制定，再对这些特殊格式的文件进行进行敏感扫描，识别出敏感文件后将敏感文件进行加密，可有效地防止有意或无意的敏感文件外泄行为。

针对敏感文件的操作通过助手弹出提示的方式来提醒终端用户操作的后果，可以有效地防止由于对计算机使用不熟悉造成的数据丢失或外泄的风险。

通过禁用、或审计智能设备，对智能设备连接操作进行管理。通过封堵端口对传输协议进行阻断，例如 445 端口。通过设置 wifi 黑白名单对连接的网络

进行管理达到仅能连接指定网络的目的。