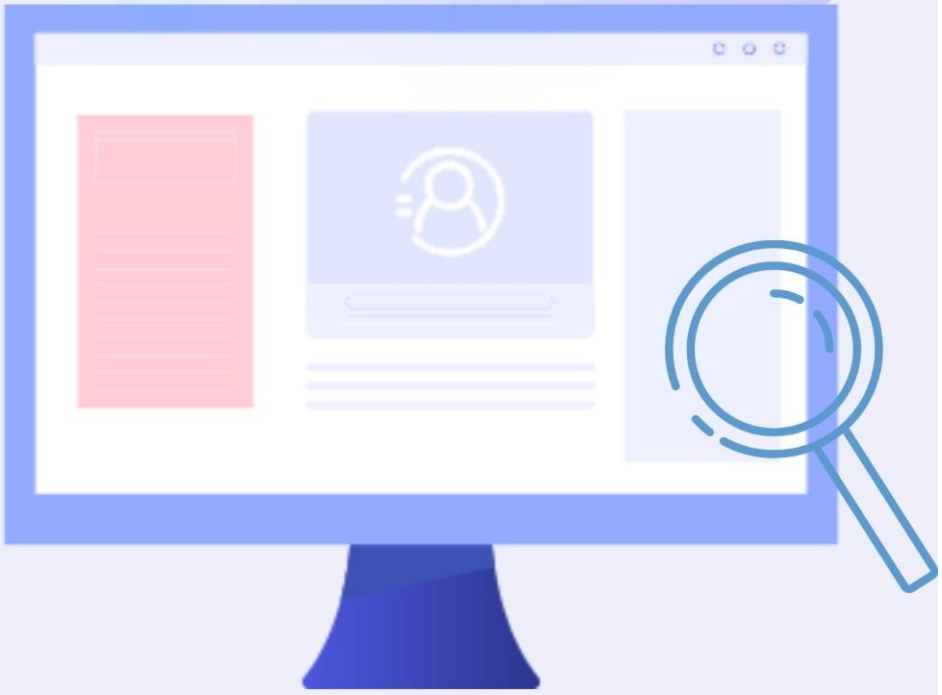
域智盾软件®

制造行业

文档防泄密解决方案



CONTENTS/目录

01 项目背景 ---------- 3

02 面临问题 ---------- 3

03 方案设计 ---------- 4

04 方案优势 ---------- 7

05 方案价值 ---------- 7

06 系统架构 ---------- 8

07 公司简介 ---------- 3

一、项目背景

制造企业在实际用工中持续产生电子文档、三维数模、工艺参数等高价值核心资产，此类文件贯穿研发、工艺、生产、供应链全流程，是企业的核心竞争要素。仅依靠员工守则与管理制度，缺乏技术层面的系统性防护屏障，机密文档泄密风险持续存在。一旦发生泄密事件，企业将面临技术优势丧失、合规处罚及举证困难的叠加后果。

二、企业面临问题

制造企业在文档防泄密层面通常面临以下典型问题：

- 设计图纸、工艺文件以明文形式存储于员工终端，通过 U 盘拷贝、网络传输、邮件外发等途径可轻易带离企业。
- 设计评审、生产看板、工艺参数展示等场景中，屏幕内容暴露于多人视野，可通过系统截屏或手机拍照将敏感信息转化为图片外传。
- 向供应商、外协厂、客户发送文件，对方后续的转发、复制、打印行为会脱离发送方管控，易引发二次泄密。
- 制造企业终端数量多、分布广，依靠人力难以统计所有敏感文件，难以及时发现违规行为。



三、方案设计

设计出发点

本方案以“文档全生命周期可控”为出发点，覆盖文档从创建、存储、流转、外发到销毁的完整过程，在保障业务效率的前提下，对核心数据实施分级、分场景的精准防护，确保涉密文档“拿不走、打不开、传不出、赖不掉”。

解决方案

文档加密

1. 透明加密机制

员工在授权终端上正常编辑、保存文档时，系统在后台自动完成加密，不影响原有操作习惯。加密文档在授权环境内可正常打开、编辑、打印，脱离授权环境后呈现乱码，有效防止文件被非法带离后内容泄露。

2. 格式全覆盖

支持制造行业常用文档格式的加密保护，可加密的后缀包括：

- 日常办公类：DOC、DOCX、WPS、XLS、PPT、PDF、VSD、TXT、RTF、ODT、OTT、MPP 等；
- 图片设计类：PSD、CDR、CPT、ZPR、INDD、AI、AEP 等；
- 图纸设计类：DWG、DWT、DWF、PLA、PRG、PWJ5、PRJ、EXB、JDP、ZMX、RP、IDS 等；
- 三维设计类：3DS、MAX、DE、IDW、ASM、DRW、PRT、CEX、DXF、LTS、Z3、ICS、PVS 等；
- 电子电气设计类：PRJGRP、SCH、STP、DDS、CPM、LDS、ASC、BPMN2 等；
- 编程开发类：C、CPP、JAVA、PY、JS 等常见开发语言文件；
- 另有打印组件类、压缩软件类、浏览器、影音编辑、单片机开发、仿真计算等。

注：若有企业自研软件，可联系厂商开放权限协助添加或自主添加。

3. 外发管控

文档需外发时，须经审批流程。外发文件可附加打开次数、有效期、打开密码、禁止打印、禁止截屏等限制，接收方在限定条件下方可查阅，超期或超次自动失效。

终端设备管理

对制造企业终端设备实施统一、细粒度的外设与接口管控，封堵非授权数据出口。

1. 外设端口管控

提供禁止使用、仅读取、仅写入、允许使用四类权限，精细化管控企业 U 盘的使用权限

2. 移动设备管控

限制打印机、移动硬盘、光驱、蓝牙设备、红外设备、串口、并口、无线网卡、手机连接数据线等各类设备，避免绕过。

3. 网络外联管控

对终端的多网卡、VPN、热点共享等行为进行监控与限制，防止终端通过非授权网络通道向外传输数据。

屏幕管控

针对屏幕截取与拍照泄密这一制造行业高发风险，构建“预防—威慑—追溯”三位一体的屏幕防护能力。

1. 屏幕水印

支持点阵水印、图片水印、文字水印、二维码水印、隐式水印。水印覆盖全部应用窗口或指定应用窗口，正常观看不影响内容辨识，但拍照或截屏后水印信息清晰可读，增强拍照取证的可靠性。

2. 截屏管控

对截屏行为实施策略化管控：

- 禁止使用系统截屏快捷键及第三方截屏工具；
- 对指定应用（如加密文档阅读器、图纸查看器）禁止截屏；
- 设置截屏行为，截屏时加密窗口会黑化或最小化，终端无法截取加密信息。

3. 终端防拍照

对于高涉密区域终端，可开启终端防拍照功能，检测到手机拍照行为，立马触发锁屏策略，降低通过拍照方式泄露屏幕内容的可能性。

文档安全备份

为防止文档因误删除、勒索软件加密、终端故障或恶意破坏而丢失，域智盾软件提供文档安全备份能力。

1. 自动备份策略

对指定目录、指定类型文档在修改、删除等操作时自动触发备份，备份文件存储于安全服务端，保留多个历史版本，支持按时间点恢复。

2. 备份范围可控

研发设计文档、工艺文件、财务数据等核心资料强制备份；临时文件、个人文档可排除在外，避免存储资源浪费。

3. 快速恢复

管理员或授权用户可快速恢复指定文档的历史版本，恢复操作记录完整日志，确保备份数据不被滥用。

敏感数据识别

通过内容识别技术，自动发现和分类制造企业内的敏感文档，为精细化管控策略提供依据。

1. 敏感信息报警

企业可自定义敏感词库，当员工电脑中触发敏感词时，立即弹窗报警并通知管理员。

2. 敏感文件

显示所有部门内的敏感文件，记录客户端、所属部门、文件名、文件路径、敏感词、详情、文件修改时间等信息。压缩包、word、图片、txt 等都能扫描出来。

3. 敏感文件审查

创建敏感文件审查任务，软件会自动审查所有符合要求的文件。

文件操作审计

对终端上的文件操作行为进行全量记录，为安全事件调查和合规审计提供数据支撑。

1. 全量操作日志

记录文档的创建、读取、修改、重命名、删除、复制、移动等操作。

2. 外设与网络传输审计

记录通过 USB 设备拷贝、网络共享上传、邮件发送、即时通讯工具外发等行为。

3. 打印审计

记录打印行为，包含打印文档名称、页数、打印机、打印时间，可根据策略对敏感文档的打印操作实施审批或阻断。



四、方案优势

部署优势

轻量化本地私有部署，业务数据留存于用户自有环境，数据可控。服务器数据库一键式安装，轻量部署，使用 mysql 数据库，大型用户支持对接 oracle。

售后服务

周一至周六技术支持支撑到晚上 21:00，周日、节假日各岗位均有值班的企业。随时支持客户的需求，急客户之所急。

合规支撑

方案设计与日志留存机制满足《中华人民共和国网络安全法》《中华人民共和国数据安全法》及制造业相关保密管理要求，审计报表可直接用于内部合规检查与外部审计。

五、方案价值

1. 筑牢核心知识产权防线，守护企业技术根基

构建覆盖文档全生命周期的系统性防护屏障，将电子文档、三维数模、工艺参数等核心资产

纳入可控、可管、可追溯的安全域，从源头遏制技术外溢，守护企业技术壁垒与竞争优势。

2. 构建供应链协同安全底座，提升合作信任层级

实现外发文件流转的可控化、可追溯化管理，确保核心数据在供应链上下游流转中始终处于企业安全边界之内，强化企业作为可信合作伙伴的资质背书。

3. 强化安全治理效能，实现事件精准溯源

依托屏幕水印、操作审计与行为日志的多维证据链，将泄密事件调查从被动排查升级为精准定位，实现责任到人、追溯到端、取证有据。

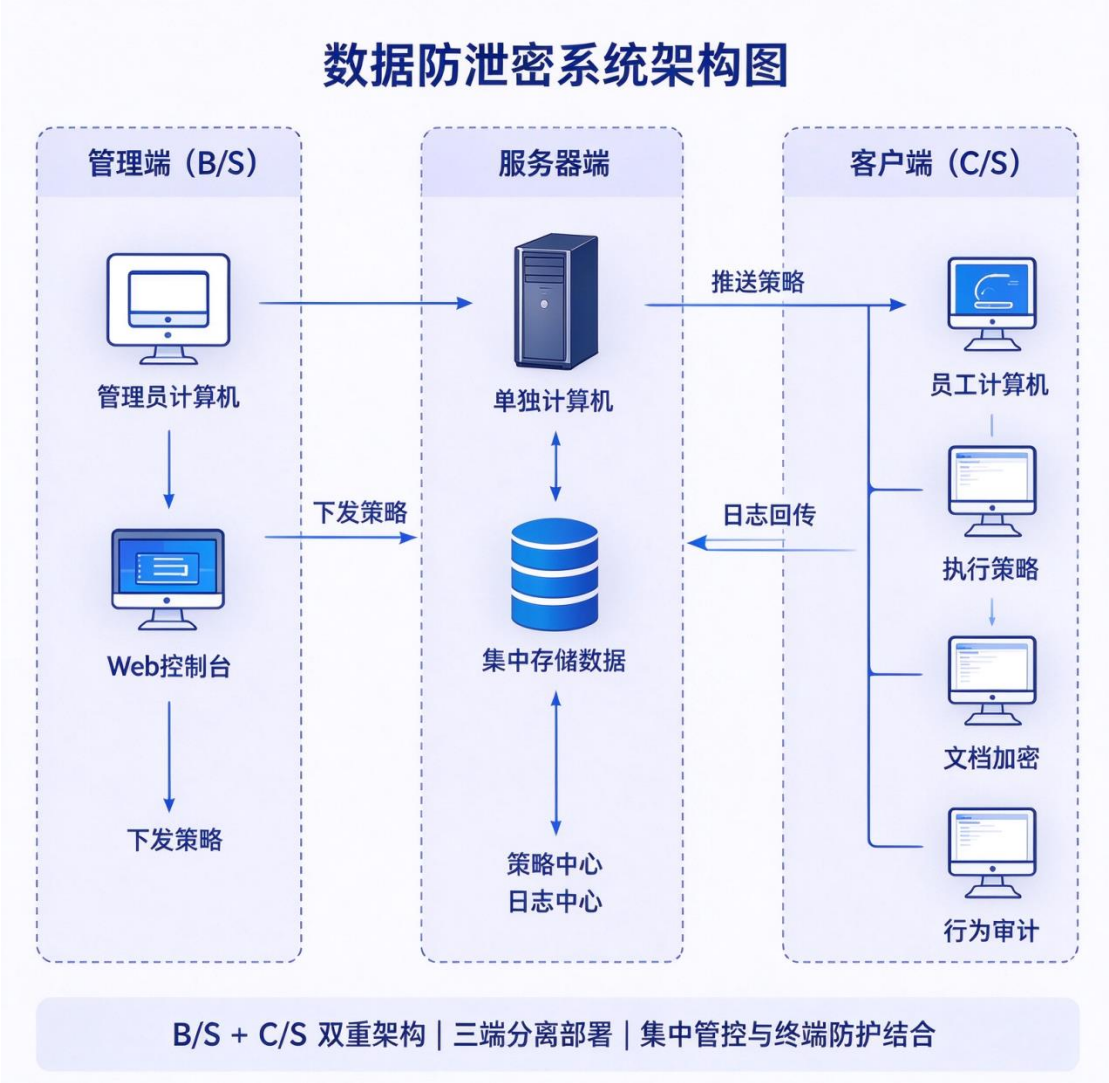
4. 夯实合规管理基础，支撑企业行稳致远

以完整审计日志与敏感数据识别记录为依托，为等保测评、行业保密检查及客户安全审核提供可验证的数据支撑，将合规要求内化为常态化管理能力。

六、系统架构

支持 b/s、c/s 双重架构，由服务器端、客户端、管理端构成。

- 服务器端：安装在单独计算机上，集中存储数据。
- 客户端：安装在员工计算机上，执行策略。
- 管理端：安装在管理员计算机上，下发策略。



七、公司简介

河北中视新研软件开发有限公司是一家以研发信息安全产品及提供相关服务为主营业务的技术驱动型公司，总部位于河北省石家庄市。公司拥有完全自主知识产权的信息安全产品与解决方案，专注于终端安全、文档加密、网络准入等领域，为国内企业用户提供专业的信息安全产品与终端安全管理整体解决方案。

域智盾软件为该公司旗下终端安全与数据防泄密产品品牌，已与 300 余家合作伙伴建立协同生态，累计服务政企客户逾 10000 家，支撑超 300 万台终端稳定运行。

产品覆盖终端安全系统、文件加密软件、网络准入设备等方向，致力于帮助制造、设计、政府及企事业单位保护核心数据资产，降低信息安全风险。

官方网站 yzdsaas.com

电话：400-097-8770

地址：河北省石家庄市

域智盾软件®