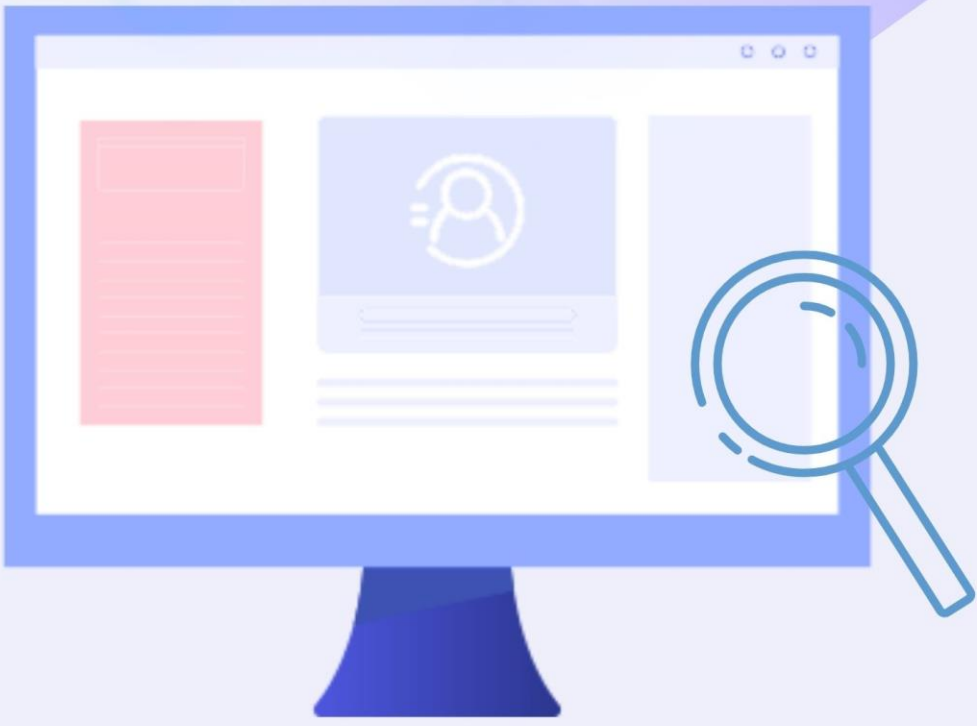
域智盾软件®

金融科技行业

数据防泄漏解决方案



CONTENTS/目录

01 行业背景 ---------- 3

02 面临问题 ---------- 3

03 法律要求 ---------- 3

04 方案设计 ---------- 4

05 解决方案 ---------- 4

06 方案优势 ---------- 7

07 方案价值 ---------- 8

08 系统架构 ---------- 9

09 公司简介 ---------- 9

一、行业背景

金融科技企业服务于银行、证券、保险、支付等持牌机构，日常处理大量客户身份信息、账户与交易数据、风控模型、信贷审批材料、产品定价方案与核心系统源代码。与传统金融机构相比，金融科技企业人员结构更年轻、研发与运营团队混合办公、远程与混合办公比例高，外部合作方与驻场开发人员多，数据在员工电脑、测试环境、共享盘与协作工具之间流转频繁，一旦外泄可能触发监管处罚，引发舆情风险，冲击金融业务稳定与品牌信誉。

本方案面向金融科技公司、金融软件服务商与互联网金融企业，围绕终端数据防泄漏构建一体化防护体系。

二、面临问题

金融科技业务线上化、平台化发展，高价值敏感数据采集、流转、共享场景持续增多。

- ？ 高危站点、违规通讯易引发窃密风险，审计难落地
- ？ U 盘、邮箱、网盘、即时通讯工具外发文件，缺乏拦截与审批
- ？ 员工出差、远程办公时终端脱离企业内网，本地数据处于失控状态
- ？ 监管要求趋严，需完整终端操作留痕，满足审计溯源合规需求

三、法律要求

- 2017 年《中华人民共和国网络安全法》（原版）：网络运营者应采取监测、记录网络运营状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。
- 2019 年《网络安全等级保护基本要求》（GB/T 22239）第三级及以上对终端管控、审计留存、外发控制的相关要求。
- 2020 年《中国人民银行金融消费者权益保护实施办法》，明确应依法开展职责范围内的金融消费者权益保护工作，依法保护金融消费者合法权益。

四、方案设计

本方案以“金融数据在终端侧全程可控”为出发点，从以下角度构建整体能力：

- 以员工岗位与业务系统为边界

按研发、运营、客服、风控、合规、外包等岗位划分数据访问权限，最小必要授权，避免跨岗位越权访问。

- 以不影响业务效率为前提

加密与管控动作在驱动层与系统层完成，员工在授权业务系统内的操作方式保持不变。

- 以事件可追溯为交付标准

所有文件操作、外发动作、外设接入、权限变更集中留痕，事件发生后可按人、按机、按文件、按时间还原全过程。

五、解决方案

5.1 文件透明加密

对终端上的客户资料、交易数据、风控文档、源代码等指定类型文件自动加密。在授信环境下，文件正常使用，员工日常操作方式不变；文件离开授信环境后即为密文，无法通过 U 盘、邮箱、网盘带走。

5.2 敏感文件报警

支持自定义敏感词库，可对截屏内容、窗口标题、网页搜索内容、文件名、打印文档标题、AI 提问、邮件正文、聊天消息、网页标题、屏幕画面进行敏感词识别；支持对压缩包、Word、图片、TXT 等多类文件深度扫描，统计文件内敏感词命中次数。

5.3 文件操作记录

完整记录文件操作日志，涵盖客户端、操作用户、所属部门、操作类型（新增/删除/修改/查看/重命名）、源路径、目标路径、文件大小、审计时间等信息。

实际问题：公司有 300 名员工，每人每天操作约 50 次文件，每日可产生 15000 条日志。如何快速定位高风险文件操作？

解决方案：域智盾软件支持按员工、部门、时间、关键词检索审计日志，可快速定位高风险文件操作。

5.4 禁止程序发送文件

按企业实际情况指定禁止发送文件的程序清单，包括邮箱客户端、网盘客户端、浏览器、微信、企业微信、QQ、钉钉等。终端通过这些渠道外传文件时，系统弹出警告框、阻止文件外传操作，从程序层面切断最常用的外发通道。

5.5 文件操作权限

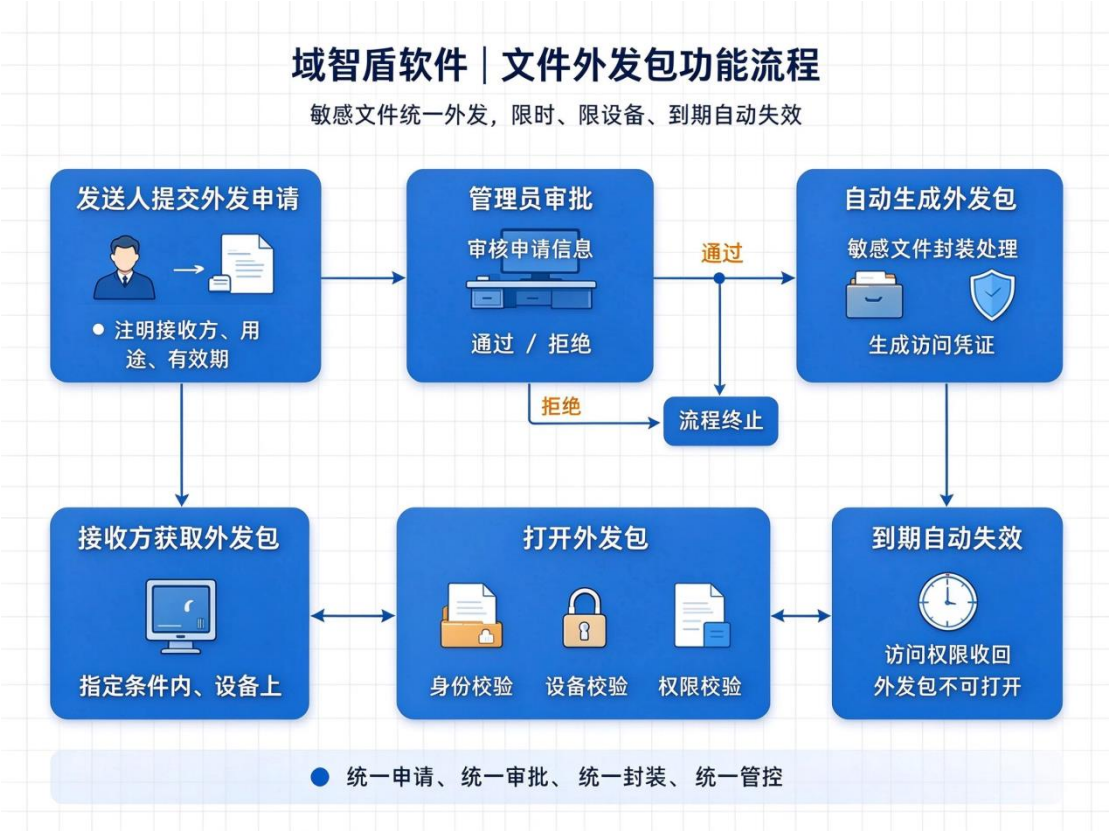
按部门、岗位、角色授予不同的文件操作权限，包括只读、可读可写、禁止另存、禁止打印、禁止外发、禁止拷贝到外接存储等。非授权人员即使接触到文件本身，也无法打开或复制内容。

5.6 外设管控

支持对光驱、刻录设备、蓝牙、红外、串口、并口、无线网卡、USB 无线网卡、PCMCIA、1394、便携式存储设备等外设进行权限管控；同步监测违规外联、私建热点、私自修改网络配置等异常行为，一旦识别即刻阻断并触发告警，适配金融科技行业内网安全管控要求。

5.7 文件外发包

对确需对外发送的敏感文件，通过外发包机制统一处理：发送人在客户端提交外发申请，注明接收方、用途、有效期；管理员审批通过后自动生成外发包；接收方在指定时间内、指定设备上方可打开，到期自动失效。



5.8 邮件防泄密

针对金融科技行业邮件传输涉密风险，系统提供两类邮件安全管控策略，兼顾业务协同与数据防泄密需求。

邮件白名单：发往白名单内对象的加密文件可自动解密，保障对外合规业务邮件正常流转。

邮件发送拦截管控：可基于发件人、收件人、邮件内容敏感关键词设置细化过滤条件，对违规邮件进行拦截，防范客户信息、交易资料、风控文档等敏感数据通过邮件外泄。

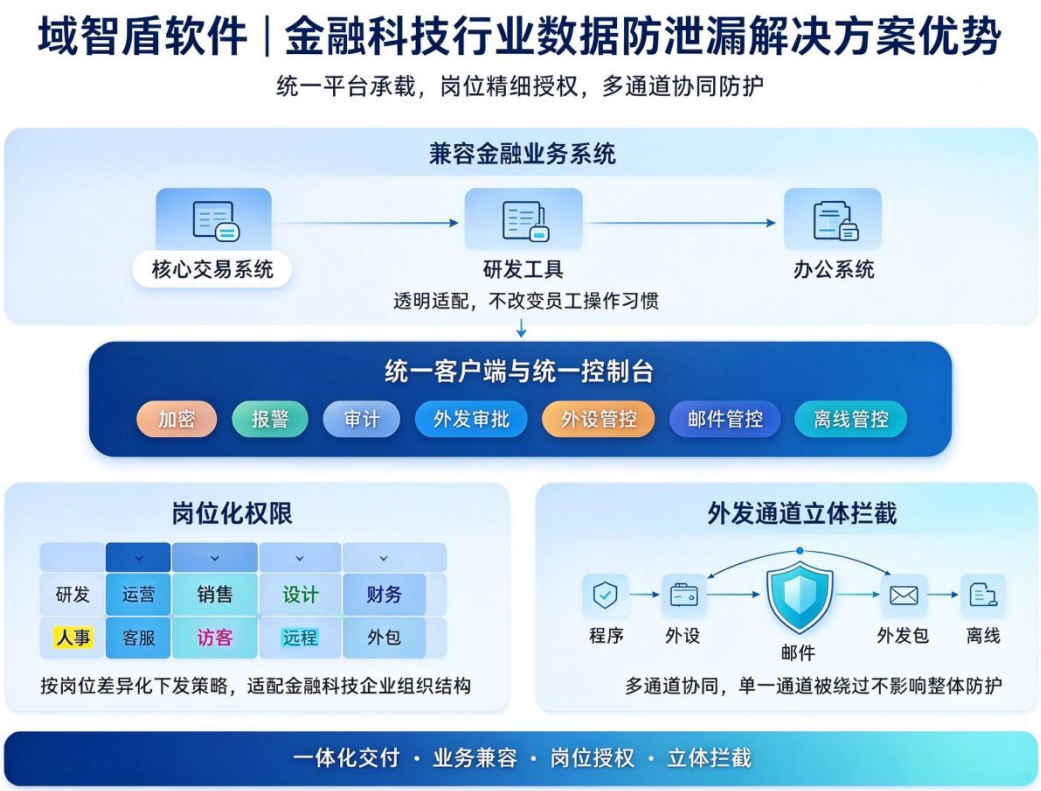
5.9 离线管控

面向金融科技行业员工外勤、携笔记本出差拜访客户场景，可开启离线使用模式。管理员可预先设定离线有效期(例如 3 天),在有效期范围内,终端可离线正常访问加密的客户资料、业务文档；离线时限到期后，加密文件自动无法打开。



六、方案优势

- 一体化交付：加密、报警、审计、外发审批、外设、邮件、离线在同一客户端与同一控制台完成。
- 兼容金融业务系统：对核心交易系统、研发工具、办公系统做兼容适配，不改变员工操作习惯。
- 岗位化权限：按研发、运营、客服、风控、合规、外包等岗位差异化下发策略，适配金融科技企业组织结构。
- 外发通道立体拦截：程序、外设、邮件、外发包、离线多通道协同，单一通道被绕过不影响整体防护。



七、方案价值

- 合规价值：契合个人金融信息保护、金融数据分级分类、等保三级等监管规范，支撑常态化合规核验。
- 业务价值：筑牢客户信息、交易流水、风控算法、核心源码的防护屏障，规避数据外泄引发的客户维权、监管罚没、业务声誉受损等重大风险。
- 管理价值：推动数据安全管理制度落地为终端侧可落地、可量化的管控策略，助力安全合规团队实现全域数据资产可视、可管、可控。
- 效率价值：敏感内容识别、外发审批、风险溯源等流程线上闭环，释放安全团队效能。
- 风险价值：实现数据外泄风险隔离，支持快速溯源定位、及时止损、留存取证依据。

八、系统架构



九、公司简介

河北中视新研软件开发有限公司，坐落于河北石家庄，是专注于终端数据安全领域的自研型软件服务商。公司深耕内网终端管控、文档加密、数据防泄漏技术研发，自主打造域智盾软件，面向金融科技、先进制造等对数据合规有高要求的行业，提供全链路、可落地的数据安全治理方案。

公司具备完善的软件著作权、信息安全体系资质，配套全周期技术支撑与本地化服务，持续为金融科技企业筑牢客户信息、交易数据、风控资产的安全防线，护航数据要素合规流转。

官方网站 yzdsaas.com

电话： 400-097-8770

地址： 河北省石家庄市

——以终端为落点，覆盖客户数据、交易数据与研发资产

域智盾软件®