安企神

金融科技行业

数据防泄漏解决方案

面向互联网银行 · 消费金融 · 支付机构 · 保险科技

让敏感数据在授信范围内流动，让每一次调用都有据可查

目录

01　项目背景 1

02　需求分析 2

03　方案设计 3

04　解决方案 4

05　方案优势 9

06　方案价值 10

公司简介 11

01　项目背景

对金融科技公司而言，最值钱的资产往往不在机房里，而在数据中台和策略库里：几亿条客户标签、一套套调优多年的风控规则、一份份贷前贷后的审批数据。模型可以重训，系统可以重建，唯独这批数据一旦流出，黑产拿到的是可以直接变现的"原料"，欺诈损失与监管处罚会在同一个周期内找上门。

与这份价值形成反差的，是数据在业务链路里的流动方式。一笔贷款从进件、审批到贷后管理，数据要在业务系统、数仓、报表平台、外包坐席之间往返十几次；一次营销活动，名单要从数仓导出、加工、下发到电销终端。业务的效率建立在"数据随手可得"之上，风险恰恰藏在这份便利里：没有人能随口说清，此刻有多少份带身份证号和银行卡号的明细，正以明文躺在多少台电脑上。

监管与合规的要求也在收紧。金融监管总局 2024 年发布的《银行保险机构数据安全管理办法》要求数据分类分级、落实"谁管业务、谁管业务数据、谁管数据安全"的责任制，并把数据安全风险纳入全面风险管理；JR/T 0197-2020 将金融数据划分为五级；《个人信息保护法》对最小必要收集提出硬约束。这几年因客户信息泄露被通报、罚款甚至暂停业务的案例并不少见——数据保护已经不只是防黑产的生意问题，而是直接关系牌照与业务资格的合规问题。

金融数据资产的三点特征

01　数据密度极高	02　变现链条极短	03　协作方极多
一张宽表就涵盖身份、卡号、额度、行为，单条记录即可拼出完整画像。	带卡号的名单拿到即可用于欺诈或转卖，损失直接兑现。	外包催收、电销坐席、数据供应商、建模伙伴都要接触数据，协作面越广，边界越难守。

金融数据的安全不是"限制业务干活"，而是把数据从产生到销毁的每一次流转都纳入可控范围：谁能看、能不能导、发出去之后还能不能追。方案要做的，是把这些零散的防护动作收敛到一套加密规则、一个管理平台、一份可核查的记录上。

02 需求分析

结合业务形态与监管要求，我们把数据防泄漏的共性问题归纳为五个方面。它们并非彼此孤立，而是同一条数据链路上的不同环节：敏感数据散落在终端，从多条通道流出，事后又说不清楚。

敏感信息在终端明文落盘，权限与密级是两张皮

- 审批件、征信报告、标签明细以明文存放在业务终端，与日常文件混放，落盘之后系统权限就管不到了。
- 报表平台导出的宽表在本地反复加工、拆分、转发，导出有日志，导出之后的流转没有。
- 制度上按密级划分了查阅范围，终端上却缺少对应的执行动作，保密要求与实际管控是两套体系。

对外协作环节多，数据一出手就收不回来

- 电销与催收外包都需要下发客户名单，Excel 一发，转发、留档、二次售卖无从约束。
- 与数据供应商、联合建模伙伴的数据交换频繁，接口之外还依赖大量人工传递。
- 外包驻场人员自带设备接入办公网络，接入即可接触业务数据，边界形同虚设。

数据加工链路长，副本在中间环节反复复制

- 数仓与报表平台的数据导出到本地后二次加工，再经群聊、网盘分发，副本散落多台设备。
- 测试与演示环境直接使用真实客户数据，脱敏靠手工，环境成了第二生产库。
- 运营与客服场景的批量名单在多台电脑之间来回传递，正本与副本早已分不清。

人员流动与账号共用，风险信号难以预警

- 核心岗位离职前的批量导出、集中压缩、改名外发，往往在提离职之前就已完成。

- 坐席与运营账号存在共用现象，出了事难以定位到具体的人。
- 非授权查询客户信息是典型的风险事件，靠人盯人几乎不可能发现。

审计举证能力跟不上监管节奏

- 操作记录散落在业务系统、数仓、网关、终端各处，缺少按数据维度的统一检索入口。
- 监管检查问到"这份名单被谁导出、发给了哪家外包"，往往只能人工排查，答复周期以天计。
- 监管要求的风险评估、监测与处置记录，缺少终端侧的常态化数据支撑，报表靠临时拼凑。

03 方案设计

金融数据的安全问题，本质是三句话：数据不受控、出口不受限、行为不留痕。方案围绕一条主线展开——让敏感数据在授信范围内自由流动，离开这个范围就失去价值，每一次流转都留下可核查的记录。

围绕这条主线，方案以"一个平台、三道防线"组织能力：加密解决"拿走也打不开"，外发管控解决"传不出去"，审计溯源解决"查得到、说得清"。

一个平台 · 三道防线

防线	能力	目标	说明
防线 01	数据加密	可用不可带走	名单、审批件、策略文件在办公内网自由流转，离开授信环境即为乱码
防线 02	外发管控	带不走	外发、传输、打印、截屏，逐条出口设审批与策略
防线 03	审计溯源	查得到	记录、检索、报表与取证，把"说不清"变成"拿得出"

三条设计原则

- 先分级、再授权——对齐 JR/T 0197 五级分级，按数据密级而非部门定权限。低密级岗位打不开高密级文件，跨条线协作以授权代替解密，避免"一把钥匙开所有门"。

- 一个客户端、一个管理端，不动业务系统——业务终端只装一个客户端，加密在驱动层完成，业务系统、报表平台、征信接口的调用方式一律不变。管理侧只有一套后台，按条线、职场、岗位分组批量下发策略。
- 管控精度与数据价值匹配，能灰度、能回退——只对命中规则的文件加密，公开物料保持原样；上线先核心条线后全量，性能有基线、异常可单机回退，安全不以拖慢放款与审批为代价。

实施路径：三步走

第一步 · 敏感数据摸底	第二步 · 核心条线试点	第三步 · 全量推广与制度固化
扫描全网终端与共享目录，识别含个人金融信息的文件，把五级分类与岗位权限逐一对上。	选取风控与电销条线先行部署，跑通加密、外发、审计三条主链路，同步完成性能基线测试。	覆盖总部、异地职场与外包驻场终端，策略集中下发，与数据安全制度、检查应答预案逐条对应。

04 解决方案

方案能力围绕敏感金融数据的加密防泄漏展开，解决"数据怎么管"的问题。全部能力共用一个客户端与一个管理平台，按需启用、逐步扩展。

1.1 金融敏感数据透明加密

数据的价值在内容本身，而不在它存在哪个目录。第一个动作是让文件"带锁"：加密在驱动层完成，保存即密文，在授信环境内正常打开、编辑、流转，离开授信环境就是一堆乱码。

加密模式与适用场景

加密模式	适用岗位与场景	实际效果
透明加密	风控、审批、数据分析等核心岗位	新建保存即密文，内网正常使用，外发为乱码

加密模式	适用岗位与场景	实际效果
智能加密	客服、运营等需读取、少外发的岗位	按程序与文件类型判定，命中敏感规则才加密
只读	对外合作方案、培训与宣导材料	可看不可改、不可另存，防止二次扩散
落地加密	外包回传数据、渠道与供应商来件	落到本机即转为密文，转发到别处无法打开
不加密/只解密	公开物料适合不加密、管理岗适合只解密	保持原有习惯，由外发审批等手段兜底

实施要点

- 按岗位分配模式：核心业务与风控岗位启用透明加密，敏感明细落盘即密文；行政、HR 等岗位用智能加密；对外材料设为只读；外包回传与第三方来件用落地加密。
- 国密算法与分级密钥：采用 SM3/SM4 算法，密钥分级管理，满足等保测评与商用密码应用安全性评估要求，为现场检查提供可说明的技术口径。
- 例外清单可维护：业务系统安装目录、征信接口程序等经审批加入例外，避免误伤业务运行。



1.2 加密网关与数据链路对接

金融科技的骨架是数据链路：业务库、数仓、报表平台、文件服务器、对账与报送通道。加密如果让报表导出变慢、让对账文件出错，就一定会被业务人员绕开。所以第二个动作是把加密嵌进链路，而不是加在链路之外。

加密网关：服务器明文，终端密文

通过与数仓平台、报表系统、文件服务器及业务系统免硬件对接，服务器侧始终是明文，终端侧始终是密文——上传自动解密，下载自动加密，不改变访问地址，不改变导出与查询动作。

环节	状态	说明
服务器区	明文	数仓、报表平台、文件服务器以明文存储与计算，加工与统计不受影响
加密网关	转换	上传解密、下载加密，无需专用硬件，与现有系统直接对接
业务与运营终端	密文	数据落地即密文；离网授权到期失效；外发须经审批

为什么强调"不改流程"

业务场景最常见的失败，不是技术不行，而是安全措施拖慢了取数之后，业务人员想出各种变通：先解密再干活、用私人网盘中转、把明细贴到在线文档里。方案把加密动作放在文件系统的读写路径上，业务人员感知到的只是"数据还是那份数据"，变通的动机自然就消失了。

1.3 数据外发与交付管控

金融科技公司不可能与外界绝缘：名单要下发外包，报表要报监管与合作方，数据要跟供应商交换。管控的目标不是"不许发"，而是"按规矩发"——事前有审批，事中有约束，事后有记录。

三类外发场景，同一套策略

场景	管控方式
邮件白名单外发	向已备案的合作方、集团与监管报送邮箱发送时自动放行，其余外发仍需申请审批
受控外发交付	生成受控文件——限定打开次数与有效期、绑定设备、禁止另存、页面显示水印，原文件不作解密，打开行为留痕
外包协作下发	外包终端纳入授信范围但限定条线与目录，只能接触本项目数据，任务结束授权即回收

实施要点

- 审批分级：一般材料外发由条线负责人审批，涉及核心策略与批量名单的外发升级至数据安全归口部门，驳回则拒绝输出并记录原因。
- 离网办公：出差、驻场、居家可通过审批获得离网授权，到期自动失效，避免"带回去就失控"。
- 交付收尾：项目结束或外包退场时回收授权、吊销密钥，已交付的受控文件到期自动打不开。



1.4 敏感数据与分级

做加密之前先回答三个具体的问题：哪些文件含个人金融信息，它们躺在哪些机器上，现在是不是明文。

从发现到处置的四个环节

环节	动作
01 数据源	终端与共享目录：名单明细、审批件、征信报告、报表文件、策略与模型文件、压缩包
02 识别	内容识别引擎：身份证号、银行卡号、手机号组合特征，征信报告版式指纹，风控策略文件指纹与关键词
03 定级	对照 JR/T 0197 五级与内部密级目录打标，形成敏感数据台账
04 处置	给机密文件补加密、告警、阻断外发，纳入对应条线与密级

实施要点

- 扫描定位：扫描指定终端与共享目录，列出含敏感内容的文件及其加密状态，文件服务器上的历史存量同样覆盖。
- 分级策略：核心策略文件、普通业务数据、公开物料对应不同的加密强度、外发策略与审批层级，让管理精度与数据价值匹配。
- 避免过度管控：只对命中规则的文件加密，公开材料保持原样。管控越精准，配合度越高，制度才不会被绕过。

1.5 数据安全审计与泄露溯源

中大型金融科技公司动辄数百上千台终端，一天产生的操作记录数以万计。审计的价值不在于"都记下来"，而在于要的时候找得到，从海量记录里定位到那一条。

从采集到取证的链路

环节	说明
统一采集	文件创建、修改、删除、复制、重命名，外发、打印、剪贴板等与数据流转相关的操作，客户端缓存，断网续传
检索	按人、时间、条线、关键词、文件类型组合检索，从一条记录还原整条事件链
输出取证	审计报表、事件链条、监管检查佐证、法务取证材料

留痕的意义在于"能解释"

一次监管检查中被问到"上个月下发给外包的名单有没有扩散"，如果只能回答"我们查一下"，结果往往已经是失分。能当场调出记录、说清路径、指明责任人的团队，在监管与合作伙伴眼里的可信度完全不是一个量级。

- 全量留痕：数据文件的每一次落盘与流转逐条记录，与加密、外发策略联动，异常动作即时告警。
- 异常信号：非授权时段批量查询客户信息、离职前集中导出、向个人邮箱或网盘发送，命中即预警。
- 事件链还原：从一条外发记录顺藤摸瓜，还原"谁、在什么时间、用什么方式、带走了哪些数据"的完整链条。

05 方案优势

金融科技机构选型时最常问的三个问题是：会不会拖慢业务、要不要改现有系统、出了事能不能拿出证据。对应的答案，构成了这套方案的基本盘。

优势	说明
加密不影响业务体验	加密在驱动层完成，导出、加工、上报的动作与从前一致，业务人员几乎感知不到
兼容：数据链路全适配	与业务系统、数仓、报表平台、文件服务器协同工作，导出与批量作业不因

优势	说明
	加密中断
密不离数：保护跟随文件走	加密属性随文件移动，复制、重命名、打包后仍是密文，不依赖某个目录或某台服务器
分级：密级与岗位双轨授权	按数据密级与岗位范围双重授权，低权限打不开高密级文件，解密走审批留档
合规：对标监管办法与测评	访问控制、安全审计、数据保密性措施可映射监管办法与等保 2.0 条款，支持国密算法
轻量：旁路部署，平滑推广	不改造现有网络，客户端静默安装，按条线分批推进，不打断业务节奏

06 方案价值

价值	具体表现
敏感数据"可用不可带走"	名单、审批件、策略文件在授信范围内自由流转，离开即为乱码，"拷一份带走"从技术上失效
协作"效率不打折"	授权范围内该通的都通：条线协作、跨线授权、链路流转全部照旧，安全没有成为额外负担
人员与外包流动"有底线"	离职、转岗、外包退场时授权与密钥同步回收，受控交付物到期自动失效，数据资产不随人员流失
取证"有据可依"	加密、外发、流转记录可以当场调取，监管检查、客户尽调与法务维权都有了底气

这四条价值指向同一件事：把依赖保密协议、人盯人的数据保护方式，换成可持续运行的技术机制。制度写在制度文件里，机制跑在数据链路上，两者合起来才叫"管得住"。

公司简介

石家庄安企神网络科技有限公司成立于 2015 年，是一家以研发信息安全类产品以及提供相关服务为主营业务的技术驱动型公司。

安企神软件是由该公司研发的终端安全管理系统，打造全生命周期一站式信息安全整体解决方案平台，集文档加密、电脑行为审计、终端安全管理、网络准入控制、敏感内容识别、IT 运维管理等 200+功能于一体，有效防护不当办公行为造成的数据泄露。

安企神软件深耕终端安全与数据防泄密领域十余年，拥有 300 余家合作伙伴，服务万余家政企客户，累计覆盖终端超 1000 万台，广泛应用于政府、金融、运营商、制造、能源、教育、医疗等行业的大型知名单位和机构，涵盖衣食住行各行各业。

ANQISHEN
400-666-2563
www.wgj7.com
河北·石家庄
安企神软件®