安企神

IT 互联网行业

研发代码加密解决方案

面向互联网企业 · 软件研发团队 · 外包与远程协作场景

让源代码在研发链路内自由流动，让每一次流转都有迹可循

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.....10

06　方案价值.....11

公司简介.....13

01　项目背景

对互联网企业而言，最值钱的资产往往不在机房里，而在开发机的代码仓库里。一行行源码、一套套算法模型、一份份架构设计文档，凝结的是团队数月甚至数年的研发投入。产品可以迭代，服务器可以重建，唯独源码一旦流出，竞争对手拿到的是可以直接编译、直接运行的"半成品"，领先窗口会被瞬间抹平。

与这份价值形成反差的，是代码在研发过程中的流动方式。一个功能从需求评审、编码、提交、代码评审、持续集成、测试验证到发布交付，要在几十台开发机、多个代码仓库和若干协作平台之间往返数十次。研发的效率建立在"代码随手可得"之上，而风险恰恰藏在这份便利里：没有人能随口说清，此刻公司有多少份未发布的源码正以明文状态躺在多少台电脑上。

监管与合规的要求也在逼近。除《网络安全法》《数据安全法》之外，网络安全等级保护 2.0 对重要数据的保密性提出了明确要求，软件供应链安全逐渐进入采购与投标的评审项，越来越多的甲方在合同里写入了源码保护与保密审计条款。对研发团队来说，代码保护已经不只是"防同行"的生意问题，而是直接影响商务资格的合规问题。

互联网代码资产的三点特征

01　价值高度集中	02　流转链路极长	03　泄露后果即时
一个核心仓库就是一整条产品线的竞争力，泄露一次即伤及根本。	从 IDE 到 Git、CI/CD、测试、交付，代码每天要经过几十次落盘与传输。	代码拿到即可编译运行，不存在"看不懂用不上"的缓冲，损失直接兑现。

说到底，研发代码的安全不是"限制开发人员干活"，而是把代码从编写到交付的每一次流转都纳入可控范围：谁能改、能不能传、能不能发出去、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

结合互联网企业研发组织的实际环境，我们把代码防泄漏的共性问题归纳为五个方面。它们并非彼此孤立，而是同一条研发链路上的不同环节：代码散落在开发机，从多条通道流出，事后又说不清楚。

源码以明文状态散落在开发机上，没有统一的管理口径

- 工程源码、配置文件、数据库脚本、接口文档以明文存放在个人电脑，与个人文件混放，版本杂乱。
- 同一项目的代码分散在本地目录、共享目录、个人网盘与聊天记录里，谁也说不清"正本"在哪。
- 制度上有保密要求，终端上却缺少可执行的技术动作，保密协议与实际管控是两套体系。

协作通道多而分散，代码从每一条缝里都能流出去

- 向 Git 仓库推送只是众多出口之一：邮件附件、即时通讯传文件、网盘中转、截图粘贴，条条可达。
- 开发人员本地拉取完整仓库后，整个项目历史连同所有分支都躺在个人电脑里，一次拷贝即全量带走。
- 个人云开发环境、在线代码片段工具的普及，让"复制一段核心逻辑"这个动作几乎不留下任何痕迹。

外包与远程协作规模大，交付环节最容易失控

- 外包团队、众包测试、自由职业者参与开发，代码交付只能靠口头约定与保密协议约束。
- 驻场人员自带设备接入研发网络，接入即可访问代码资产，边界形同虚设。
- 项目结束后，交付出去的源码是否被二次扩散、是否还留在对方机器上，甲方乙方都说不清。

人员流动快，离职带走代码难以防范

- 互联网行业年流动率高，核心研发的每一次离职都是一次潜在的代码外流。

- 离职前的集中下载、私有仓库镜像、个人邮箱备份，往往在提离职之前就已完成。
- 没有技术手段的情况下，公司很难证明"他带走了什么"，维权举证极其困难。

事后追溯能力弱，出了事拿不出证据

- 代码操作记录散落在 Git 平台、文件服务器、办公终端各处，缺少统一检索入口。
- 面对"这份源码是什么时候、被谁、用什么方式传出去的"的追问，往往只能给出模糊判断。
- 安全事件复盘靠人工拼凑，难以支撑法务取证、客户审计与内部通报的常态化要求。

03 方案设计

研发代码的安全问题，本质是三句话：代码不受控、出口不受限、行为不留痕。因此方案不追求功能项的堆叠，而是围绕一条主线展开——让代码在授信的研发环境里自由流动，离开这个环境就失去价值，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"带走也没用"，外发管控解决"传不出去"，审计溯源解决"带走了能查到"。

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	源码与设计文档在研发内网自由流转，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

- **按项目分级分域，按角色授信授权**——按产品线与项目组划分安全域，按代码敏感程度划分密级。非本项目成员打不开高密级仓库文件，跨组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，管理员分级分权**——研发终端只装一个客户端，管理侧只有一套管理端。终端按项目组、办公区、办公地分组，策略按组批量下发；安全、运维与审计角色分离，普通管理员只能管理授权范围内的终端与功能模块。
- **不改变研发习惯，才能落地**——加密在驱动层完成，新建、编码、保存、提交的动作与从前完全一致；IDE、Git、构建、调试的路径不变。安全应当隐形在研发流程里，任何拖慢发版节奏的设计都会第一时间被绕开。

实施路径：三步走

第一步 · 核心项目组试点	第二步 · 分批推广	第三步 · 制度固化
选取核心产品线与算法团队先行部署，跑通编码、提交、构建三条主链路。	按项目组推送客户端与策略，异地办公与驻场终端统一纳管，运维远程完成。	策略与保密制度、交付合同条款逐条对应，形成可核查的常态化闭环。

04 解决方案

方案能力围绕代码加密防泄漏展开，解决"代码怎么管"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 研发源码透明加密

代码的价值在内容本身，而不在它存在哪个目录。所以第一个动作是让代码文件"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、编译、提交、流转，一旦离开授信环境，打开就是一堆乱码。

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	核心研发、算法团队	新建保存即密文，内网正常使用，外发为乱码
智能加密	行政、测试、运维等需读取，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	对外交付物、公开 SDK 与文档	可看不可改、不可另存，防止二次扩散
落地加密	外包回传代码、第三方交付文件	落到本机即转为密文，转发到别处无法打开
不加密/只解密	管理岗适合只解密、离职人员适合不加密	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**：核心研发与算法岗位启用透明加密，源码新建即密文；测试、运维等岗位可用智能加密；对外交付物设为只读；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对数据机密性的要求。
- **项目域与密级**：跨项目组默认不可见、越级打不开，解密必须走审批，审批过程本身留档。

一句话概括：代码在研发终端始终是密文，出口决定结果——授信终端与授权工具内正常打开、编译、提交；经邮件、网盘、即时通讯等非法出口离开，得到的只是乱码，或被直接阻断并留下记录。

1.2 加密网关与研发工具链对接

研发的骨架是工具链：IDE、Git/SVN、代码评审、持续集成、制品库、测试环境。加密如果让构建变慢、让流水线报错，就一定会被开发人员绕开。所以第二个动作是把加密嵌进工具链，而不是加在工具链之外。

加密网关：服务器明文，终端密文

通过与 GitLab、SVN、制品库、文件服务器及项目管理平台免硬件对接，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，不改变仓库地址，不改变提交与拉取动作。

环节	状态	说明
服务器区	明文	代码仓库、制品库、文档服务器以明文存储与流转，构建与索引不受影响
加密网关	转换	上传解密、下载加密，无需专用硬件，与现有系统对接
研发终端	密文	代码落地即密文；离线授权到期失效；外发须经审批

为什么强调"不改流程"

研发场景最常见的失败，不是技术不行，而是安全措施拖慢了提交与构建之后，开发人员想出各种变通：先解密再干活、用私人仓库中转、把代码贴到在线片段工具里。方案把加密动作放在文件系统的读写路径上，开发人员感知到的只是"代码还是那份代码"，变通的动机自然就消失了。

编译、构建与持续集成

加密文件在授信环境内可被编译器、解释器、构建工具正常读取，本地调试、单元测试、打包构建的体验与从前一致。流水线从明文的代码仓库取件，构建产物按既有规则处理，不会出现"密文进了制品库"之类的链路事故。

1.3 代码外发与交付管控

互联网企业不可能与外界绝缘：对外交付源码、给客户部署包、向合作方提供接口文档、给外包下发开发任务，都是必要动作。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	向指定的合作方、客户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项目域，只能接触本项目代码，任务结束授权即回收

实施要点

- **审批分级**：小范围文档外发由项目经理审批，核心仓库相关材料外发升级至安全负责人，驳回则拒绝输出并记录原因。
- **离线办公**：出差、居家、现场驻场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**：项目结束或人员离场时回收授权、吊销密钥，已交付的受控文件到期自动打不开。



1.4 代码资产识别与分级

做加密之前先回答三个具体的问题：哪些文件是代码或设计资产，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：源码工程、脚本、配置、设计文档、接口文档、压缩包
02 识别	内容识别引擎：代码特征、文件类型、项目标识、关键词与文件指纹
03 处置	补加密、告警、阻断外发，纳入对应项目域与密级

实施要点

- **扫描定位**：扫描指定终端与共享目录，列出含代码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。识别规则可按产品线单独设定，避免一套规则管所有项目。
- **分级策略**：核心算法、普通业务代码、公开组件对应不同的加密强度、外发策略与审批层级，让管理精度与代码价值匹配。
- **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，开发人员的配合度越高，制度才不会被绕过。

1.5 加密审计与泄露溯源

一家中大型研发企业动辄数百上千台开发终端，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、剪贴板等与代码流转相关的操作，客户端缓存，断网续传
聚合检索	按人/时间/关键词/文件类型组合检索，时间画像定位异常时段
输出取证	审计报表、事件链条、客户审计佐证、法务取证材料

留痕的意义在于"能解释"

一次客户安全审计中被问到"上一版本的源码交付出去之后有没有扩散"，如果只能回答"我们查一下"，结果往往已经是商务失分。能当场调出记录、说清路径、指明责任人的团队，和被动的团队，在客户眼里的可信度完全不是一个量级。

- **全量记录：**代码文件的每一次落盘与流转逐条留痕，与加密、外发策略联动，异常动作即时告警。

- **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、带走了哪些文件"的完整链条。
- **报表输出：**按项目组、人员、事件类型生成审计报表，可直接用于内部通报、客户审计与合规检查。



05 方案优势

研发团队选型时最常问的三个问题是：会不会拖慢开发、工具链兼不兼容、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。

加密不影响研发体验	加密在驱动层完成，编码、提交、构建、调试的动作与从前一致，开发人员几乎感知不到加密的存在
兼容：研发工具链全适配	与主流 IDE、Git/SVN、CI/CD、制品库协同工作，构建与流水线不因加密中断

密不离码：保护跟随文件走	加密属性随文件本身移动，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：项目域与密级双轨授权	按产品线划分安全域，按代码价值划分密级，跨域不可见、越级打不开，解密走审批留档
合规：对标等保与密评	按等保 2.0 要求设计数据保密性与安全审计措施，支持国密算法，可直接映射测评项
轻量：旁路部署，平滑推广	不改造现有研发网络，客户端静默安装，可按项目组分批推进，试点到全覆盖不打断发版节奏

06 方案价值

代码"可用不可带走"	源码在公司内部自由流转，离开授信环境即为乱码。加密不改变研发习惯，却让"拷一份带走"这条路从技术上失效
协作"效率不打折"	授权范围内该通的都通：组内协作、跨组授权、工具链流转全部照旧，安全没有成为研发的额外负担
人员流动"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，代码资产不随人员流动而流失
取证"有据可依"	加密、外发、流转记录可以当场调取，把"说不清"变成"拿得出"，客户审计与法务维权都有了底气

这四条价值指向同一件事：把过去依赖保密协议、依赖人盯人的代码保护方式，换成可持续运行的技术机制。制度写在合同里，机制跑在研发链路上，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®