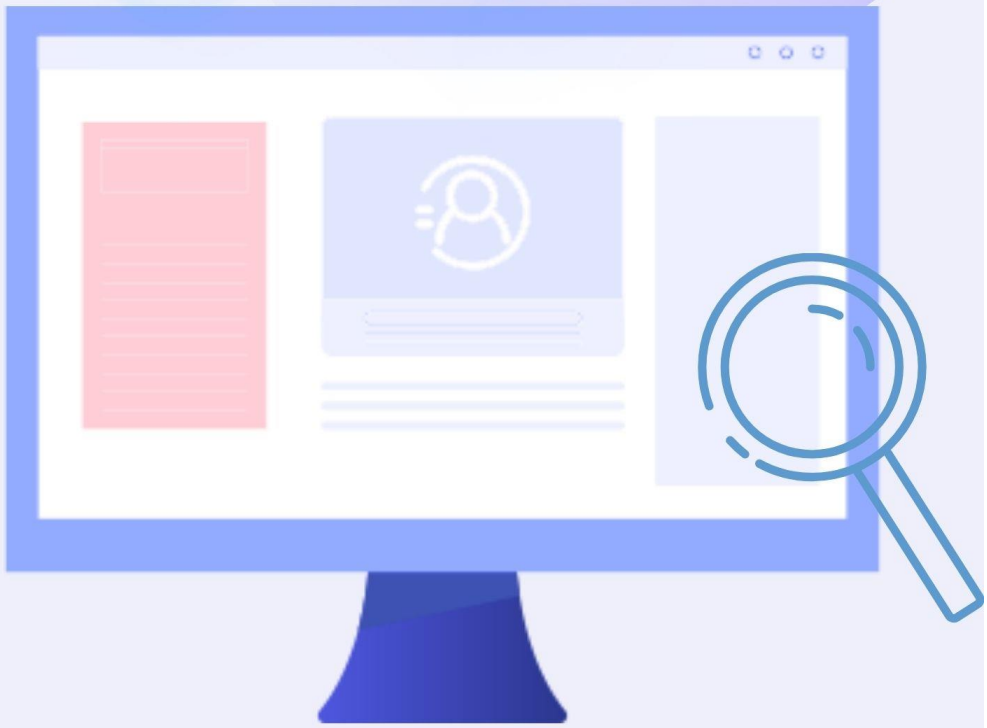
域智盾软件®

IT 互联网行业

研发代码加密解决方案



CONTENTS/目录

01 项目背景 ---------- 3

02 企业难题 ---------- 3

03 方案设计 ---------- 3

04 解决方案 ---------- 5

05 方案优势 ---------- 8

06 方案价值 ---------- 9

07 公司产品简介 ---------- 10

一、项目背景

随着业务发展，研发团队规模扩大、外包与远程办公比例上升、上下游协同增多，代码从研发内网外流到企业控制范围之外的风险显著增加。行业内已经发生多起因核心员工离职、外包人员离场、终端丢失导致的源代码外泄事件，相关企业不仅承担直接经济损失，还面临客户信任受损与监管合规压力。本方案面向 IT 互联网企业，围绕研发终端这一最后节点，构建覆盖代码全生命周期的加密与管控体系。

二、企业难题

结合 IT 互联网行业的研发场景，企业在代码保护方面通常面临以下问题：

- 源代码在员工本地工程目录、Git 克隆副本、构建缓存中大量存在，仓库权限无法约束本地文件。
- 研发人员通过 U 盘、私人网盘、个人邮箱、即时通讯工具将代码打包外发，缺乏统一拦截。
- 离职、调岗、外包离场环节没有技术手段阻止代码打包拷贝，管理制度难以落地。
- 电脑被拍照、手机翻拍屏幕、截屏、录屏即可带走代码片段，传统加密对图像化外泄无效。
- 不同部门、不同项目组之间代码权限边界模糊，研发人员可访问到与本职工作无关的仓库与目录。
- 剪贴板、拖拽、另存为等日常操作成为绕过仓库管控的通道，复制即可带走。
- 代码外发事件发生后缺乏完整审计记录，无法定位是谁、在什么时间、把哪部分代码带走。
- 研发终端硬盘损坏、误删、勒索病毒加密后，代码本地副本丢失，影响开发进度。

三、方案设计

本方案以“研发代码全生命周期可控”为出发点，从以下角度构建整体能力：

- 从事前、事中、事后、灾后四个阶段闭环设计

不依赖单一加密动作，而是在代码离开仓库之前先做好权限与区域隔离，在员工日常操作过程中持续阻断外泄通道，在事件发生后可完整追溯，并在终端故障时可恢复。

- 以部门与项目组为单位划分安全区域

按组织架构与项目边界设置安全区域，跨区域访问需要额外授权，防止研发人员将 A 项目代码拷贝到 B 项目环境或个人目录。

- 以不影响开发效率为前提

加密与管控动作在驱动层与系统层完成，员工使用 IDE、Git、构建工具的方式不变。

- 以证据链完整为交付标准

所有文件操作、外发尝试、截屏拍照行为、权限变更均留痕，事件发生后能够按人、按机、按文件、按时间还原全过程。



四、解决方案

4.1 事前防御

4.1.1 代码与文档透明加密

采用透明加密技术，对研发终端上的源代码、设计文档、接口文档、数据库脚本等指定类型文件自动加密。员工操作方式不变，文件离开授权环境，后即处于乱码状态，无法读取。

面向研发编程业务场景，系统兼容 Visual Studio、Eclipse、Matlab、Araxis Merge、ST Visual、Python、pycharm、WebStorm、Hbuilder、Phpstorm、Unity 3D、Cygwin、Clion、git、Zdevelop、Zdevelop、TESSY、nginx、HALCON、CS+ for CC 等主流开发工具，支持对工具进程及对应后缀文件加密防护。



该加密机制具备高防破解特性，经专项验证，通过重装系统、物理拆取硬盘等外部手段，均难以非法解密获取原始数据。

4.1.2 沙箱存储

针对体积庞大的代码工程文件，可开启沙箱存储功能，在终端构建独立虚拟安全隔离区。将代码文件置入沙箱内，以明文读写，不占用额外加解密算力，操作更加流畅；当文件被拷贝、

外发、移出沙箱外，文件自动变为加密状态，兼顾研发性能体验与源代码防泄露安全要求。

4.1.3 文件权限与部门权限控制

按部门、项目组、角色授予不同的文件访问权限，包括新建、删除、重命名、拷出、拷入、移出、移入等。非授权人员即使接触到文件本身，也无法打开或复制内容。

4.1.4 部门安全区域

在终端上划分安全区域，不同区域之间相互隔离。研发部文件运营部无法访问，反之亦然。如需访问，可以通过设置安全密钥、密级实现。

4.2 事中控制

4.2.1 终端防拍照

支持终端屏幕防拍照管控，系统可识别针对屏幕的手机拍摄行为，触发告警后立即执行终端锁屏，阻断拍摄操作，避免屏幕敏感信息被拍照外泄。

4.2.2 加密剪贴板

针对加密文件的内容进行管控，限制其复制粘贴行为。当终端从加密文件内复制代码片段时，粘贴到其他地方（微信、QQ、个人邮箱、记事本等）会显示“您复制的内容已被加密处理”。

4.2.3 禁止截屏与录屏

对敏感窗口启用截屏与录屏限制，当终端打开加密文件，进行截图、录屏等操作时，加密窗口会显示黑屏或最小化，阻断图像化外泄通道。

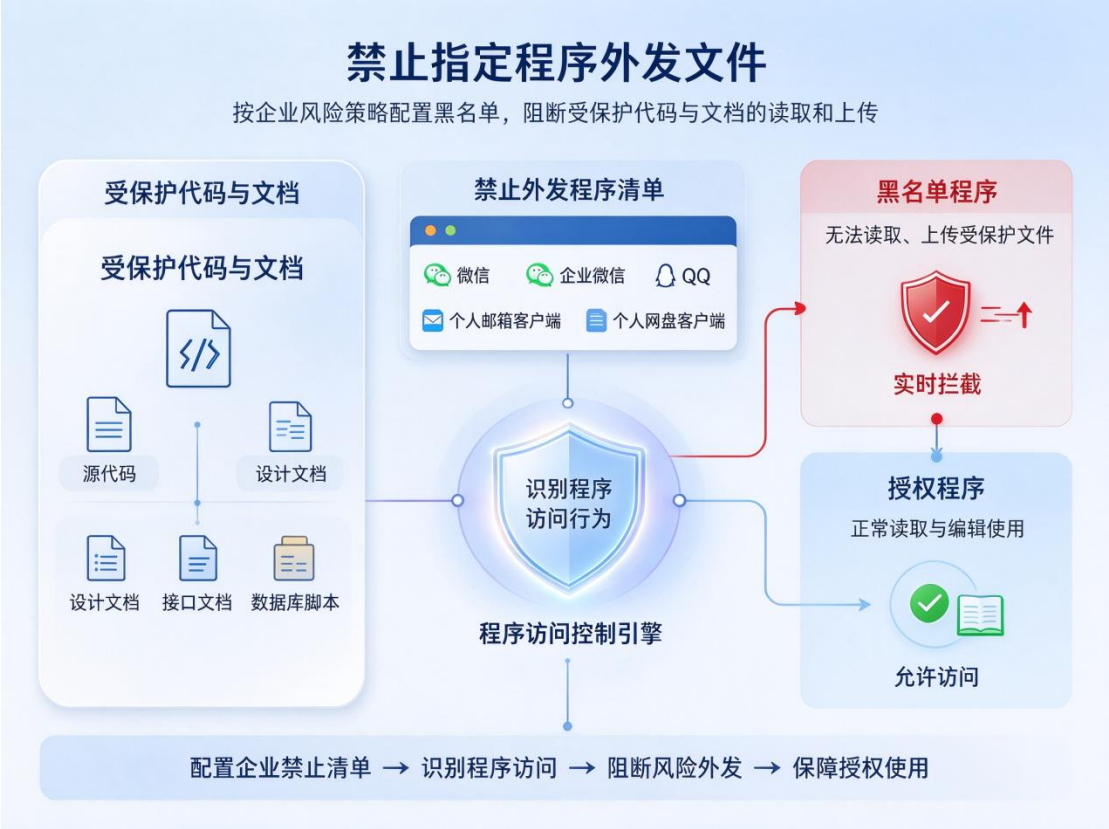
4.2.4 禁止拖拽

禁止将加密文件中的内容，直接拖拽到其他地方。

4.2.5 加密网关

面向 OA、CRM、ERP 等核心业务平台的文件上传、下载交互场景，系统提供加密网关功能，文件上传至指定业务系统时，触发自动解密机制，简化审批流程、保障业务连续性；从业务系统下载至终端本地的文件，将自动执行加密保护，防范客户敏感资料违规外泄。

4.2.6 禁止指定程序外发文件



4.2.7 敏感文件报警

敏感词支持自定义，审计的内容包括：窗口标题、网页搜索、文件名、打印文档标题、AI提问、聊天内容、邮件内容、网页标题、屏幕内容等，发现敏感行为会实时阻断并向管理员推送告警，安全团队可在事件发生当下介入。



4.3 事后溯源

4.3.1 终端操作审计

本地审计：文件操作、文件打印、应用程序、U 盘使用、USB 文件操作、剪贴板使用、刻录操作、设备使用、AI 文件操作、AI 调用程序；

网络审计：浏览网站、电子邮件、上传下载、AI 工具、网络搜索，留存周期可按合规要求配置。

4.3.2 水印溯源

支持点阵水印、二维码水印、图片水印、文字水印、隐式水印，可灵活布局在打印文件、电脑屏幕、应用程序、代码文件、截图内，依据外泄文件中的水印即可定位责任人，作为内部追责与外部举证的依据。

4.4 灾后恢复

支持文件删除时备份、文件修改时备份、手动备份，还可以根据文档类型、文档大小等条件灵活备份。终端发生硬盘损坏、误删、勒索病毒加密时，可从备份恢复到指定时间点，不影响后续开发进度。

五、方案优势

- 一体化闭环管控



- 对开发无打扰

开发工具的使用方式保持不变，程序员的办公流程保持不变，文件自动完成加密保护。

- 部署灵活

支持 Windows、macOS、Linux、信创等开发终端，兼顾离线办公，策略集中下发。

六、方案价值

☑可视可控 · 资产治理价值

推动代码安全管理由制度约束向技术落地转型，支撑安全、研发管理部门对全域代码资产的分布、流转、使用状态实现可视化、可管控，构建常态化的技术资产管控体系。

☑固本筑墙 · 知识产权价值

对核心算法、业务逻辑及产品源代码实施防护，有效规避人员离职、外包退场、终端遗失等场景下核心技术资产外泄风险，保障企业核心技术竞争力。

☑有据可依 · 合规保障价值

适配软件企业客户审计、融资尽调、等级保护测评等场景要求，实现源代码防护管控与操作

日志留存，满足相关安全与知识产权合规核查标准。

☑**减负提效·流程优化价值**

依托自动化备份、行为审计能力，降低研发、安全团队在资产盘点、安全事件溯源排查中的人工成本，释放团队精力聚焦核心业务。

☑**快速响应·风险兜底价值**

实现代码资产精细化隔离管控，杜绝单点违规操作引发批量代码外泄；发生安全事件时，支持小时级快速溯源、应急止损与取证举证，压缩风险影响范围。

七、公司实力

河北中视新研软件开发有限公司扎根河北石家庄，是专注终端安全领域的技术服务商。历经十余年技术沉淀，公司斩获软件产品认定、质量管理体系认证、AAA 级中国诚信企业家等多项权威认证。秉持开放共赢的合作理念，联动 300 余家渠道伙伴，面向全国服务一万余家政企单位，平台已承载 300 万台终端的常态化安全管控，以稳定可靠的产品能力守护政企数字资产安全。联系方式：400-097-8770。

