产 品 技 术 白 皮 书

安企神

文档透明加密技术

白 皮 书

让核心文档加密无感

让数据资产安全常在

石家庄安企神网络科技有限公司

2026 年 11 月 · V1.0

序言 3
一、行业现状 3
1.1 数据泄露的代价越来越高 3
1.2 泄密路径防不胜防 3
1.3 从"事后防泄"到"事前加密"成为共识 4
二、技术介绍 4
2.1 方案概述：驱动层加密内核 + 授信环境 4
2.2 加密机制：从打开到落盘的全自动闭环 5
2.3 六种加密模式：按岗位适配，而非一刀切 6
2.4 加密生效范围：程序与格式自主配置 7
2.5 安全区域：密钥分区的部门隔离 7
2.6 防泄密外围管控：堵住加密之外的出口 8
2.7 部署与管理 8
三、方案创新与价值 9
3.1 从"事后防泄"到"事前加密"的机制创新 9
3.2 从"一刀切"到"分区分岗"的模式创新 9
3.3 从"管控体验对立"到"无感透明"的价值创新 9
3.4 客户价值小结 9
四、落地方法论 10
4.1 五阶段实施路径 10
4.2 培训与制度共建 10
4.3 合规与隐私边界 10
4.4 常见顾虑与回应 11
五、典型应用场景与服务保障 11
5.1 行业场景 11
5.2 服务保障承诺 12
六、资质与认证 12
七、未来展望 12
版权说明 13
免责声明 13

序言

设计图纸被员工随手发到个人网盘、报价单通过私人邮箱外带、离职员工把多年积累的方案打包带走——这些场景几乎每周都在企业真实上演。更让管理者头疼的是，传统的"封端口、禁网盘"式管控，管得住通道却管不住文件本身：文件一旦以明文形态存在，复制、转发、截图总有防不住的瞬间。数据安全的关键，正在从"看住出口"转向"看住文件"。

安企神给出的答案是：让加密无处不在，让员工毫无感知。文件在企业内部创建、打开、编辑、流转的每一个环节都处于加密状态，员工不需要任何额外操作；而文件一旦离开授信环境，就是一份无法打开的乱码。《安企神文档透明加密技术白皮书》系统阐述安企神软件在文档透明加密方面的技术设计、六种加密模式、密钥分区与防泄密配套管控，帮助企业在"防得住"与"用得顺"之间找到平衡点，让核心数据从源头上处于受保护状态。

石家庄安企神网络科技有限公司成立于 2015 年，深耕数据安全与终端管理领域十余年，产品与服务覆盖万余家政企客户，终端管理规模超过 2 亿台。我们希望这本白皮书成为您规划文档加密体系时的实用参考。

一、行业现状

1.1 数据泄露的代价越来越高

一份核心图纸的流出，可能意味着一个研发项目的投入付诸东流；一份客户名单的外传，可能带来渠道与订单的双重流失；一次报价成本的泄露，可能让整个竞标功亏一篑。对知识密集型企业而言，文档就是资产，泄密就是直接的资产损失。而与有形资产不同，文档一旦流出便难以追回，事后追责挽回的损失也十分有限。

1.2 泄密路径防不胜防

文件是明文的，泄密的方式就层出不穷：直接把文件发到个人邮箱或网盘；把文档内容复制粘贴到聊天窗口；把机密内容拖拽到另一个文件；对着屏幕截一张图发出去；收到外部传来的机密文件后原封不动转手外发。通道可以一个个封堵，但只要文件本身不加密，每一条想象得到的缝隙都可能成为出口，防泄密变成一场永远打不完的"猫鼠游戏"。

1.3 从"事后防泄"到"事前加密"成为共识

《网络安全法》《数据安全法》与等级保护 2.0 对重要数据的保护提出了明确要求，越来越多的行业客户审厂与招投标也将数据加密列为硬性条件。与"封堵出口+事后追溯"的传统思路相比，对文档本身实施加密保护，从源头上保证"文件离开环境就不可用"，正在成为企业数据安全建设的首选路线。企业需要的是一套既加密彻底、又不干扰正常办公、还能按岗位灵活适配的加密体系。

二、技术介绍

2.1 方案概述：驱动层加密内核 + 授信环境

安企神文档透明加密方案由三个部分组成：部署在企业内网的服务器端承担策略下发、密钥管理与日志存储；常驻每台终端的客户端内置驱动层加密内核，在文件系统层面对指定格式文档实施自动加解密；管理员通过统一控制台完成模式分配、密钥规划与策略调整。

方案的核心概念是"授信环境"：凡是安装了安企神客户端并接入服务器的电脑，构成一个彼此信任的办公环境。在这个环境内部，加密文件可以正常打开、正常编辑、正常流转；一旦文件离开这个环境——被发到没有安装客户端的电脑、上传到外部网盘、通过私人渠道外传——呈现出来的就是一份无法识读的密文。

透明，是指不增加任何操作步骤。 员工不需要选择"要不要加密"、不需要输入密码、不需要改变任何使用习惯：打开文档时自动解密供编辑，保存关闭时自动加密落盘，加密与解密都在后台瞬间完成。保护是强制的、自动的，也是无感的。



图 1　文档透明加密总体架构

2.2 加密机制：从打开到落盘的全自动闭环

触发时机与日常体验。 当文档被打开、编辑、关闭时，加密内核自动完成加解密动作，员工全程无感知。需要说明的是，PDF 文件需要经过编辑后保存才会触发加密，CAD 图纸需要点击保存按钮才会落入加密状态——这与各格式软件的保存机制有关，不影响整体保护效果。

加密后的流转效果。 加密文件在授信环境内与普通文件没有任何使用差异：同事之间可以正常互传协作，版本来回修改不受影响；文件被非法外发到非授信环境后，打开即是乱码，任何工具都无法还原。

杜绝"收到即转发"的漏洞。 单纯的透明加密存在一个盲区：如果员工收到一份外部传来的机密文件后故意不打开、直接转发出去，文件始终处于未加密状态。落地加密机制补上了这

个缺口——机密文件只要到达本机，无论是否被打开编辑，都会立即被强制转入加密状态，"收到不打开、直接转发"的路径被彻底堵死。

全流程保护链。 从员工创建第一份文档开始，加密状态贯穿创建、编辑、保存、内部流转、外发管控的全生命周期；配合外发审批与解密申请流程，每一份文件的去向都有据可查。



图 2　文档透明加密生命周期

2.3 六种加密模式：按岗位适配，而非一刀切

不同岗位对加密的需求天然不同：研发部门既是数据生产者，文件必须全程加密；财务、行政等支撑部门更多是数据使用者，本机文件无需加密但要能打开加密文件；管理层需要随时随地查阅原始文件。安企神提供六种加密模式，管理员可在控制台按部门、按终端灵活指派：

透明加密。 面向数据生产岗位的默认模式：打开、关闭文档时强制自动加密，本机新建的文件全部落入加密状态，在授信环境内正常使用，离开环境即乱码。

智能加密。 面向支撑与管理岗位：本机新建的文件一律不加密，明文文件编辑保存后也不加密；但可以正常打开公司内部传来的加密文件，且编辑保存后文件始终保持加密状态。一句话概括——自己创建的文件不加密，别人发来的加密文件能打开、且始终加密。

只解密不加密。 俗称"老板模式"：适合企业所有者与高级管理层。加密文件在这类终端上打开、关闭之后自动解密，无需走解密申请流程，管理层查阅文件再无任何负担。

只读模式。 设置后终端对加密文件只允许阅读，不能修改、不能另存，适合需要知悉内容但不应留存副本的场景。

不加密模式。 关闭该终端阅读加密文件的权限：已加密的文件无法再打开，新建文件也不再加密。适用于突发情况下的应急收权——例如发现员工异常离岗倾向时，管理员可立即关闭其权限，避免损失扩大。

落地加密。 面向经常接收外部文件的岗位：文件到达本机即被强制加密，无论是否打开过，杜绝"收到机密文件后故意不打开、直接转发"造成的泄密。



图 3　六种加密模式按岗位适配

2.4 加密生效范围：程序与格式自主配置

加密并非对所有文件一刀切，而是按"应用程序 + 文件格式"精准生效。控制台内置的加密应用库覆盖办公文档、二维与三维图纸、源代码文件、音视频素材等常用类型，每一项对应特定的程序与文件后缀；勾选后，从这些程序中生成的对应格式文件将自动、强制加密，且这些文件再次用相同程序打开时可以正常二次编辑。

支持自主扩展，这是安企神的显著优势。 当企业使用的专业软件不在内置库里时，安企神支持由服务方协助添加，也支持向企业开放权限自主添加；而不少同类产品既不提供自主添加入口，也没有配套工具，导致企业核心业务软件始终游离在加密体系之外。

2.5 安全区域：密钥分区的部门隔离

加密文件能不能跨部门传阅，由密钥说了算。安企神在后台内置 50 把不同的加密密钥，管理员可自主规划：给销售部配 A 密钥、给财务室配 B 密钥，两个部门的加密文件便无法私自相互传阅，实现部门级的机密隔离；如果企业不需要内部分隔，将各部门统一为同一把密钥，加密文件即可在全公司范围内自由流转。

密钥由企业自主掌控、服务器端统一管理，加密策略的调整不需要更换文件、不需要重新加密存量数据，切换平滑无感。

2.6 防泄密外围管控：堵住加密之外的出口

文件加密解决了"文件外发即乱码"，但内容仍可能通过复制、拖拽、截屏等方式被带出。安企神围绕加密文件配套了一组外围管控：

加密剪贴板。 从加密文档中复制文字，粘贴到任何外部位置得到的都是一句"您复制的内容已被加密处理"，以粘贴方式批量带出机密内容的路径被切断。

禁止拖拽。 加密文件的内容被锁定，无法通过拖拽把机密内容拉取到其他文件或窗口，防止"拖一段、藏一处"的零散泄密。

截屏管控。 针对加密文件的截屏行为可配置两种表现：黑化窗口——截屏瞬间文档区域变黑，截到的只有一块黑幕；隐藏窗口——截屏瞬间文档自动最小化到任务栏，截到的只有空荡的桌面。文件发不出去，截图也带不走内容。

加密标识。 开启后加密文件图标左下角显示一把小绿锁，员工与管理员一眼即可区分加密文件与明文文件，避免误操作。

2.7 部署与管理

方案延续安企神一贯的轻量路线：服务器端支持本地私有化部署，密钥与加密日志全部留存企业内网；客户端安装体积小、驱动层加解密性能损耗低，日常办公与大型图纸编辑均无明

显卡顿；加密模式、密钥规划、外围管控策略在同一控制台一处配置、全网生效。企业无需组建专职安全团队，一名 IT 管理员即可承担日常运营。

三、方案创新与价值

3.1 从"事后防泄"到"事前加密"的机制创新

传统防泄密方案把精力放在"看住出口"：审计外发行为、封堵敏感通道、事后追查责任。安企神把保护前移到文件本身——文件在落盘的瞬间就已加密，出口再多，出去的也只是一份份乱码。加密不再依赖员工自觉，也不再依赖管理员盯防，而是由驱动层内核强制执行，从机制上消除了"文件以明文形态存在"这个最大的风险源。

3.2 从"一刀切"到"分区分岗"的模式创新

加密方案最常见的落地障碍是"一刀切"：全员加密，支撑部门抱怨影响办公；全面放开，研发部门等于裸奔。安企神用六种加密模式加密钥分区化解了这对矛盾：按岗位指派透明加密、智能加密、老板模式、只读、不加密、落地加密，按部门规划 50 把密钥的归属，加密强度与业务角色精准匹配——该加密的地方一个不漏，不该加密的地方一寸不多。

3.3 从"管控体验对立"到"无感透明"的价值创新

加密体系能否落地，最终取决于员工是否配合。透明加密把保护动作完全藏进文件的打开与保存之间，员工的操作步骤一步未增、习惯一成未变；智能加密与老板模式让支撑部门和管理层几乎感受不到加密的存在。管控与体验不再对立，方案上线阻力随之大幅降低。

3.4 客户价值小结

对数据生产部门，核心文档从出生起就处于加密状态，外发即乱码，泄露路径被釜底抽薪；对支撑与管理部门，业务协作不受影响，加密文件照样打开、照样编辑；对管理层，文件查

阅零负担，部门隔离与应急收权随手可得；对管理者整体，密钥与策略一个控制台统管，数据资产从源头上处于受保护状态。

四、落地方法论

4.1 五阶段实施路径

第一阶段"立项调研"：梳理部门构成、文档类型与高风险岗位，确定加密模式分配草案与密钥分区方案。第二阶段"部门试点"：选择研发等数据生产部门先行上线，验证加密对业务软件的兼容性与性能表现，收集格式误伤样本。第三阶段"策略调优"：依据试点反馈补充加密应用库条目、微调各岗位模式与外围管控强度，让加密策略贴合企业实际。第四阶段"分批推广"：按部门分批部署客户端并下发策略，每批稳定运行后再推进下一批。第五阶段"常态运营"：进入日常加密状态巡查、解密审批与月度报表机制，加密体系进入自我运转状态。



图 4　加密体系五阶段落地路径

4.2 培训与制度共建

工具只是底座，制度与习惯才是长效保障。实施过程中我们协助企业完成三项工作：一是管理员培训，覆盖模式分配、密钥规划、解密审批与报表解读；二是管理层简报，把部门隔离效果与应急收权机制讲清楚；三是员工宣导，用"操作零变化、文件更安全"的透明规则争取理解与配合，并同步把加密范围、外发审批流程写入保密制度。

4.3 合规与隐私边界

方案的加密范围严格限定于企业指定的工作文档格式，只针对业务文件生效，不触碰员工的私人文件与私人通讯内容；加密密钥由企业自主掌控、存储在企业内网服务器，外部厂商无法解密企业数据；解密与外发均走审批流程并全程留痕，每一次文件"出环境"都有据可查。企业应同步在保密制度中明确告知加密范围与审批规则，做到"告知在先、加密在后、最小够用"。

4.4 常见顾虑与回应

"会不会拖慢电脑？"——加密内核在驱动层完成加解密，单次动作毫秒级，日常办公与大型图纸编辑均无明显感知。

"文件会不会损坏或丢失？"——加解密伴随文件的打开与保存同步完成，策略调整与客户端异常均有容错与恢复机制，存量文件无需重新加密。

"员工离职带不走文件，正常业务往来怎么办？"——对外发文件走解密审批或外发授权，该出的文件按流程出，不该出的文件出不去。

"中途更换系统怎么办？"——密钥与策略由企业管理员掌控，支持平滑的方案切换与数据迁移评估，不会把企业数据锁死在单一产品里。

五、典型应用场景与服务保障

5.1 行业场景

行业	核心保护对象	加密方案要点
研发与制造企业	二三维图纸、源代码	透明加密全覆盖，图纸程序自主接入，落地加密防转发
金融与投资机构	客户资料、报价与合同	部门密钥隔离，剪贴板与截屏管控，只读模式对外协

设计创意机构	设计稿、素材库	透明加密+禁止拖拽，成品外发走审批
政务与事业单位	公文、涉密资料	密钥分区管理，加密标识区分密文，审计留痕
律所与咨询机构	案卷、项目文档	智能加密适配协作岗位，离职应急收权

5.2 服务保障承诺

安企神在全国拥有 300 余家合作伙伴，提供本地化实施与售后支持：产品支持 7 天全功能试用；单台授权低至 60 元起，按终端数量灵活授权；客服热线 400-666-2563 工作日 5 分钟内响应；针对加密兼容性提供专项验证支持，保障企业业务软件平稳接入加密体系。

六、资质与认证

安企神软件已通过 ISO9001 质量管理体系与 ISO27001 信息安全管理体系认证，核心功能模块取得多项计算机软件著作权登记；产品历经万余家政企客户的生产环境验证，终端管理规模超过 2 亿台，在政务、金融、制造、医疗、教育等行业形成了成熟的加密交付与运营经验。

七、未来展望

加密走向分级智能。

加密策略将从"按部门指派"进一步走向"按文件内容自动分级"：结合敏感内容识别，让不同密级的文件自动匹配不同的加密强度与流转规则，保护粒度更细、误伤更少。

加密与审计深度融合。

文档透明加密将与行为审计、AI 使用审计在统一平台上打通：加密文件被谁打开、被谁投喂给 AI、被谁尝试外发，全部纳入同一条行为链路，形成"加密保底、审计溯源"的双重防线。

密钥体系走向零信任。

"默认不信任、持续验证"的零信任架构将与加密体系融合，文件访问权限与设备身份、用户身份、环境风险动态绑定，授信环境的边界随风险等级实时伸缩。

密码应用走向合规化。

方案将跟进商用密码应用要求，支持更高强度的国密算法选项与密评配套能力，让加密体系不仅防得住，也经得起测评。

版权说明

本白皮书版权归石家庄安企神网络科技有限公司所有。未经书面许可，任何单位和个人不得以任何形式复制、转载、摘编本白皮书的部分或全部内容。安企神及本白皮书中提及的产品名称，是石家庄安企神网络科技有限公司的商标或产品标识。

免责声明

本白皮书内容基于产品当前版本整理，功能与界面可能随版本升级而调整，具体以实际交付版本为准。本白皮书仅用于向客户介绍产品技术与方案，不构成任何形式的合同承诺。因使用本白皮书内容而产生的任何直接或间接损失，石家庄安企神网络科技有限公司不承担相关责任。

如需了解更多产品信息或预约产品演示，请联系安企神客服热线 400-666-2563。