产 品 技 术 白 皮 书

安企神

保密沙箱技术

白 皮 书

让核心数据在受控工作空间里
隔离使用 · 源头加密 · 出口受控

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：防泄密的两难困局 3
1.1 痛点全景：文件锁得住，使用管不住 3
1.2 合规压力：数据安全已成法定义务 3
1.3 传统手段的局限：加密与易用难两全 4
二、技术介绍：隔离使用、源头加密、出口受控 4
2.1 方案概述：给核心业务划一块受控工作空间 4
2.2 工作空间隔离：一台电脑分出"两个世界" 5
2.3 授权程序绑定：业务软件天生"长在"沙箱里 5
2.4 边界处处设防：加密之后才是真正的开始 6
2.5 审批外发：带得出去、收得回来 7
2.6 沙箱日志联动审计：每一次"越界"都有画面 7
三、方案创新与价值 8
3.1 理念创新：从"加密一切"到"隔离使用" 8
3.2 体验创新：安全不以牺牲效率为代价 8
3.3 成本创新：管控收窄，负担更轻 9
四、落地方法论 9
4.1 分步实施：试点先行，降低切换风险 9
4.2 培训与制度共建：交付不只是装软件 9
4.3 合规与隐私边界：防护有度，管控有据 10
4.4 常见顾虑与回应 10
五、典型应用场景与服务保障 10
5.1 行业应用场景 10
5.2 跨行业客户实践 11
5.3 服务保障：长期贴身的技术支持 11
六、资质与认证 12
七、未来展望 12
版权说明 12
免责声明 13

序言

终端电脑上，核心数据的真正风险不是"被偷走"，而是"被正常使用着流走"。加密软件把文件锁住了，可文件总要先打开——打开的那一刻，另存一份、复制一段、截一张图，加密就形同虚设。

不少企业由此陷入两难：全盘透明加密"加密一切"，业务软件一多就出现打开报错、渲染异常，性能受损，误加密、误解密成为家常便饭；改用内容识别类防泄密，规则越配越细，误报也越拦越多，运维疲于奔命。防泄密防到最后，变成了和自家业务软件的拉锯战。

本白皮书面向企业经营者与决策层，介绍安企神保密沙箱以"隔离使用、源头加密、出口受控"为核心理念的防护体系：不再纠结"加密哪些文件"，而是直接给核心业务划出一块受控的工作空间，从使用的源头重建数据安全边界。白皮书同时就方案价值、落地路径、行业场景与服务保障给出决策参考。

一、行业现状：防泄密的两难困局

1.1 痛点全景：文件锁得住，使用管不住

企业的核心图纸、源代码、报价底稿都以电子文档形态流转在办公终端上。加密手段可以保证文件落盘为密文，但数据泄露真正发生的瞬间，几乎都发生在"打开使用"的过程中：复制到沙箱外、拖拽出去、截屏摄录、打印成纸、拷贝进外设。加密挡得住落盘，挡不住出口。

1.2 合规压力：数据安全已成法定义务

《网络安全法》《数据安全法》相继实施，等级保护 2.0 标准全面推行，企业对其掌握的数据负有明确的安全保护义务。对金融、医疗、政务、制造等敏感行业而言，数据防护能力

更是参与招投标、进入供应链体系的准入条件。缺乏体系化的防护方案，不仅面临泄露风险，也意味着合规短板。

1.3 传统手段的局限：加密与易用难两全

- **全盘透明加密**：对一切文件上锁，业务软件兼容性问题接连不断，大型 CAD 图纸、代码编译场景性能受损，误加密、误解密让 IT 部门疲于应付；
- **内容识别防泄密**：依赖规则匹配，规则越配越细、误报越拦越多，运维成本持续抬升；
- **制度约束**：要求员工"涉密文件记得存对地方"，等于把安全寄托在每个人的自觉上，文件散落在桌面、下载目录与传输记录里，管控无从谈起。

企业真正需要的，是一套既不干扰业务运转、又能从源头收窄风险的防护方案。

二、技术介绍：隔离使用、源头加密、出口受控

2.1 方案概述：给核心业务划一块受控工作空间

安企神保密沙箱的核心设计理念，是围绕核心数据的"使用过程"重建安全边界：在终端划出一个独立的受控工作空间，核心文件只在沙箱内创建、编辑、流转；授权业务程序启动即运行在沙箱环境内，其新建、编辑、另存的每一份文件都被圈在边界之内；数据一旦跨出沙箱边界，立刻自动加密，离开授权环境打开即是乱码。边界之外，出口策略、审批外发、日志审计逐项设防，形成"事前隔离、事中阻断、事后精准溯源"的完整闭环。



图 1　保密沙箱总体防护架构

2.2 工作空间隔离：一台电脑分出"两个世界"

沙箱在终端内划出两个互不干涉的区域：沙箱之内保持明文，员工照常双击打开、照常保存另存，大型 CAD 图纸、代码编译这类大文件也能流畅处理，不会被加密速度拖慢；文件一旦跨出沙箱边界，立刻自动加密成密文，在非授权环境打开就是乱码。

圈进去的只是核心图纸、源代码、报价底稿这类高密文件，不必给所有文件上同一把锁——该隔离的隔离，不该圈的不圈，管控面积收窄，兼容性风险与运维成本一起下降。

2.3 授权程序绑定：业务软件天生"长在"沙箱里

靠制度要求员工"涉密文件记得存进加密区"，等于把安全寄托在自觉上。保密沙箱走的是授权程序白名单路线：把 CAD、EDA、财务、开发等业务软件加入名单，这些程序启动即运行在沙箱环境内，它新建、编辑、另存的每一份文件天然被圈在沙箱边界之内，名单之外的程序碰都碰不到。

- 准入按程序授权，不靠员工自己"记得存对地方"；

- 新建、编辑、另存全部留在边界之内，跨出即加密；
- 员工操作习惯不变，上手没有学习成本，也不用刻意指定文件后缀。

数据从被授权程序接管的那一刻起就在边界之内，制度约束就此变成系统约束。

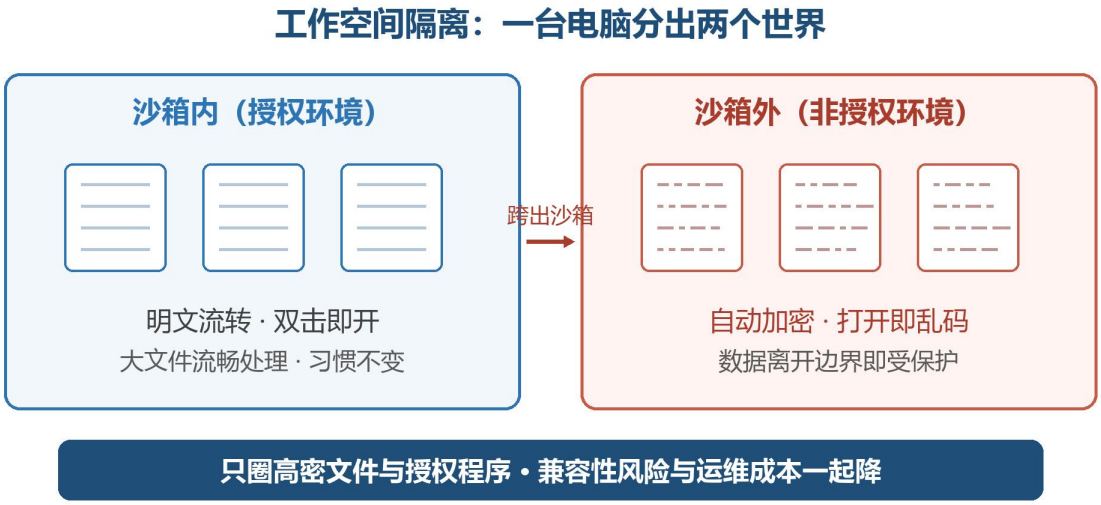


图 2　工作空间隔离：明文流畅办公，跨界自动加密

2.4 边界处处设防：加密之后才是真正的开始

"文件加密了"不等于"数据安全了"。文件在沙箱里是明文，打开的那一刻，泄密可能通过复制、拖拽、截屏、打印、外设任意一个出口发生。安企神在沙箱边界之外配合整套出口策略逐项设防：

- **剪贴与拖拽**：复制到沙箱外的剪贴内容自动加密，禁止将沙箱内文件拖拽出框；
- **截屏防护**：加密区域截屏变黑或窗口隐藏，堵住最隐蔽的窃密通道；
- **打印分级**：打印按程序与权限分级管控，杜绝涉密文档被私自打印带出；
- **外设管控**：U 盘按禁用、只读、只写、授权四档精细化管控；
- **沙箱防火墙**：整体阻断网络外传，只为内部协同需要的特定网段开例外——研发要与内部版本库通信就放行，往公网传就拦，每一次放开都留记录；

- **审批放行与水印**：关键出口支持审批放行，并叠加屏幕与文档水印，泄密源头可追溯到人。

防护由此从"锁住文件"延伸到"管住使用"，落在真正发生泄露的那个瞬间。

2.5 审批外发：带得出去、收得回来

完全不给出口，业务照样会绕路：传输工具传、网盘传、对着屏幕拍。堵住正常通道，只会把外发逼进失控的暗渠。保密沙箱配套外发审批流程：确需外发的文件提交申请，审批通过后按受控版本解密放行；每一次外发，谁申请的、谁批的、发给了谁，全程留痕。有路可走，有据可查，业务顺畅流转，风险始终在轨。

2.6 沙箱日志联动审计：每一次"越界"都有画面

传统审计只有一行"文件被复制"：发生在谁的电脑上、哪个软件里、操作了什么，无从还原，查案靠问人，结论靠推测。保密沙箱记录沙箱内文件进出、出口尝试、外发审批的全过程日志，覆盖创建、修改、复制、移动、删除、外发各环节，支持按人、按文件、按时间段快速检索；并可与终端屏幕记录联动，直接定位到越界操作瞬间的画面。"文字日志 + 画面佐证"的双重验证机制，让审计人员不再对着时间戳逐条比对，调查取证周期大幅缩短。



图 3　沙箱审计与溯源闭环

三、方案创新与价值

3.1 理念创新：从"加密一切"到"隔离使用"

传统方案纠结"加密哪些文件"，靠规则与后缀判断，误伤与漏防并存；保密沙箱把问题改为"核心业务在哪里发生"，直接对工作空间与授权程序设界。防护的锚点从文件属性转移到使用场景，规则数量大幅减少，误报与误加密从机制上被规避，防泄密不再是与业务软件的拉锯战。

3.2 体验创新：安全不以牺牲效率为代价

沙箱内保持明文流转，员工双击打开、保存另存与日常无异；大型 CAD 图纸、代码编译等大文件场景不受加密速度拖累。员工操作习惯完全不变，没有学习成本，也不需要刻意指定文件后缀——安全策略在后台生效，业务在明处顺畅运转。

3.3 成本创新：管控收窄，负担更轻

只圈高密文件与授权程序，管控面积收窄，带来三重收益：兼容性风险随管控范围同步下降；系统负担更轻，终端性能影响可控；策略配置与运维工作量显著减少。配合本地私有化部署、轻量客户端与免费对接钉钉、企业微信、飞书审批流，企业以更低的总体成本获得体系化防护。

四、落地方法论

4.1 分步实施：试点先行，降低切换风险

保密沙箱建议按"试点先行、分步推广"的原则实施：优先选取研发、财务等核心部门的部分终端开展试点，梳理应纳入沙箱的业务程序与文件范围，验证业务兼容性、统一配置流程后，再向全网其余分区推广落地。这一路径让企业在小范围内验证效果、优化策略，避免一刀切式上线带来的业务冲击。



图 4　保密沙箱分步实施路径

4.2 培训与制度共建：交付不只是装软件

厂商针对所采购的产品模块提供专项培训，内容涵盖沙箱策略配置、授权程序梳理与数据防泄漏实践经验，并可围绕企业数据安全管理制度建设开展交流，帮助企业把技术防护延伸为管理体系。

4.3 合规与隐私边界：防护有度，管控有据

沙箱防护的落地必须兼顾管理诉求与员工合法权益。策略体系支持按部门、岗位与涉密等级差异化配置：涉密岗位从严设界，普通岗位不做额外约束；审计记录与放行审批本身亦有权限约束与全程留痕，确保防护工具始终在制度授权范围内使用，成为合规经营与员工权益的双重保障。

4.4 常见顾虑与回应

"沙箱会不会影响业务软件运行？" 授权程序在沙箱内以明文方式正常运行，大型 CAD 图纸、代码编译等场景均可流畅处理；纳入沙箱的程序范围由企业自主梳理，逐个验证后再全网推广。

"员工会不会反感被管控？" 沙箱只圈定核心业务场景，日常上网、沟通、普通办公不受影响；屏幕水印与出口留痕本身即是威慑，管理阻力随使用逐步下降。

"业务文件确实需要外发怎么办？" 外发走审批流程，审批通过后按受控版本解密放行，全程留痕——既保住业务流转，也守住数据边界。

"已有业务系统能否兼容？" 授权程序白名单按企业实际业务定制，兼容 Windows、Linux、Mac 及信创系统，审批流可免费对接钉钉、企业微信、飞书。

五、典型应用场景与服务保障

5.1 行业应用场景

不同行业的核心资产与使用场景差异明显，保密沙箱可按行业特点灵活设界：

行业	沙箱内核心业务	典型防护场景
研发/制造	CAD/EDA 设计软件	图纸沙箱内明文流转，跨界自动加密，外设四档管控
软件/互联网	开发环境与版本库	代码只在授权程序内编辑，沙箱防火墙仅放行内部网段
财务/金融	财务与业务系统	报表底稿圈内管控，打印分级，审批外发全程留痕
设计/文创	设计与文档工具	加密区域截屏变黑，屏幕水印威慑，越界画面可溯源
教育/科研	课题与实验数据	按项目划界隔离，跨部门权限隔离，日志联动审计

5.2 跨行业客户实践

安企神的客户名单覆盖多个领域的头部机构，包括苏州华为技术研发有限公司、清河县中心医院、重庆大学、韩国产业银行支行、太极计算机股份有限公司等。这些跨行业的实际落地案例，验证了方案在不同办公形态与管理要求下的适应性。

5.3 服务保障：长期贴身的技术支持

- **专属工程师**：每个客户配备 1 名专属工程师全程负责售后服务；
- **多渠道响应**：提供电话、QQ、Email 等多种远程技术支持方式，工作日响应时间不超过 5 分钟；

- **长时值守**：技术支持覆盖周一至周六至晚间 21:00，周日与节假日各岗位均有值班；
- **持续升级**：软件版本升级与新产品发布均提供通告服务，保障系统持续保持最佳状态。

六、资质与认证

石家庄安企神网络科技有限公司成立于 2015 年，是一家以信息安全产品研发和相关服务为主业的技术驱动型企业，深耕终端安全与数据防泄密领域十余年：覆盖 200 余个行业细分领域，拥有 300 余家合作伙伴，服务政企客户上万家，产品广泛应用于政府、金融、运营商、制造、能源、教育、医疗等行业。

公司在质量与信息安全管理体系层面具备完整背书：已通过 ISO9001 质量管理体系认证与 ISO27001 信息安全管理体系认证，为河北省软件协会会员单位，获评纳税信用 A 级纳税人，并已入围多家中央及地方国有企业信息化供应商采购目录。这些资质为政企客户的采购合规性提供了直接依据。

七、未来展望

数据防泄密正在从"以文件为中心"走向"以场景为中心"：AI 工具的普及带来新的数据外传路径，混合办公让信任边界更加模糊，信创与国产化进程对防护方案的适配性提出更高要求。安企神保密沙箱将持续在三个方向演进：一是深化授权程序与业务场景的自动识别能力，让沙箱边界的划定从人工梳理走向智能推荐；二是完善沙箱与加密、审计、准入等模块的联动编排，形成按行业预置的策略模板，让企业上线即站在成熟实践的起点上；三是跟随信创与混合办公趋势，扩展跨终端、跨网络的受控工作空间方案。

让数据在沙箱里安心流转，让越界行为寸步难行。

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。未经本公司书面许可，任何单位或个人不得以任何形式复制、转载、摘编或传播本白皮书的全部或部分内容。

免责声明

本白皮书所载信息仅供参考，产品功能与性能参数可能随版本更新而调整，实际表现受部署环境、硬件配置与策略设置影响存在差异。具体功能与配置以双方签署的合同及最终交付的产品版本为准。

如需了解更多产品信息，可访问安企神软件官网获取免费安装包，或致电客服热线 400-666-2563 咨询。产品提供 7 天免费试用。