产 品 技 术 白 皮 书

安企神

数据防泄密系统

白 皮 书

让核心数据在每一次日常操作中
都安全可控

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：数据泄露是企业绕不开的经营风险 3
1.1 泄密威胁全景：风险藏在日常操作里 3
1.2 合规压力：数据安全已成法定义务 4
1.3 传统手段的局限：制度管不住，单点工具防不全 4
二、技术介绍：数据全生命周期四层防护体系 4
2.1 方案概述：围绕数据流转构建闭环防护 4
2.2 事前防御：把风险扼杀在发生之前 5
2.3 事中控制：让办公电脑只能用于办公 5
2.4 事后追溯与文件恢复：每一步都有据可查、有备可用 5
2.5 核心能力详解 6
2.5.1 透明加密：无感防护，内外有别 6
2.5.2 截屏防护：堵住最隐蔽的窃密通道 6
2.5.3 外设与打印管控：守住物理端口 7
2.5.4 终端数据防泄漏：主动发现敏感数据 7
2.5.5 行为审计与桌面管理：全程留痕 7
2.5.6 终端安全与网络准入：从入口筑基 7
2.5.7 跨网文件交换：隔离网络间的安全通道 7
2.6 管理协同：双模式管理与审批流集成 7
三、方案创新与价值 8
3.1 轻量部署：低负担的工程化设计 8
3.2 无感防护：安全不以牺牲效率为代价 9
3.3 一体化平台：200 余项功能，防护不留缝隙 9
四、落地方法论 10
4.1 分步实施：试点先行，降低切换风险 10
4.2 培训与制度共建：交付不只是装软件 10
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 11
5.1 行业应用场景 11
5.2 跨行业客户实践 12
5.3 服务保障：长期贴身的技术支持 12
六、资质与认证 12
七、未来展望 13
版权说明 13
免责声明 13

序言

数字化办公让企业的图纸、源代码、报价单、客户资料等核心资产，以电子文档的形式沉淀在每一台办公电脑上。与此同时，一次拷贝、一张截图、一次网盘上传，都可能让多年积累的成果在几分钟内流出企业。对今天的组织而言，数据安全已不再是 IT 部门的技术议题，而是直接关系经营底线的管理议题。

本白皮书面向企业经营者与决策层，系统分析数据泄露威胁与合规压力，介绍安企神以"事前防御、事中控制、事后追溯、文件恢复"为主线的数据全生命周期防护体系，并就技术架构、部署方式、实施路径、服务保障与采购模式给出决策参考，帮助企业在不改变办公习惯的前提下，把核心数据的主动权掌握在自己手中。

一、行业现状：数据泄露是企业绕不开的经营风险

1.1 泄密威胁全景：风险藏在日常操作里

多数企业将安全预算投向防火墙与杀毒软件，用于抵御外部攻击。但大量实际案例表明，数据泄露更多源自内部：离职员工用 U 盘批量带走研发图纸与客户资料，员工把报价单发到个人社交账号，涉密文档被随意打印带出公司，甚至通过手机翻拍屏幕即可轻松窃取。这些行为不需要高深技术，却最难防范。

内部泄密的典型渠道可归纳为四类：

- **物理端口外泄**：私人 U 盘、移动硬盘、蓝牙等外设接入拷贝，是最常见也最难监管的通道；
- **线上渠道外发**：聊天软件、邮箱、个人网盘上传，原图发送、压缩包转发等形式多样，人工巡查几乎无法覆盖；

- **截屏与拍摄**：截屏工具、录屏软件、OCR 文字识别乃至手机翻拍，让传统文件加密形同虚设；
- **违规打印**：涉密文件被私自打印带走，纸质形态脱离管控视野。

一次核心数据外泄，带来的可能不只是直接经济损失，还包括客户信任崩塌、订单流失、多年研发投入付诸东流，以及难以取证追责的维权困境。

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。缺乏体系化的数据安全防护，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：制度管不住，单点工具防不全

面对上述威胁，多数企业现有手段存在明显短板：

- **制度与保密协议**：只能约束自觉的人，挡不住恶意行为，且缺少技术取证手段，事后难以追责；
- **人工巡查**：效率低、有死角，跟不上多样化的泄密方式；
- **单点工具**：只装杀毒、只管 U 盘、只做加密，各管一段、形成防护缝隙——加密挡不住截图，管控拦不住打印。

企业真正需要的，是一套覆盖数据全生命周期、技术与管理一体的体系化方案。

二、技术介绍：数据全生命周期四层防护体系

2.1 方案概述：围绕数据流转构建闭环防护

安企神数据防泄密系统的核心设计理念，是围绕数据流转的完整链条构建闭环防护，把风险控制在每一个环节，而不是依赖某一种单点工具。体系由四道防线组成：事前防御把风险扼杀在发生之前，事中控制让办公电脑只能用于办公，事后追溯让每一个操作都有据可查，文件恢复则保障数据在极端情况下仍可找回。

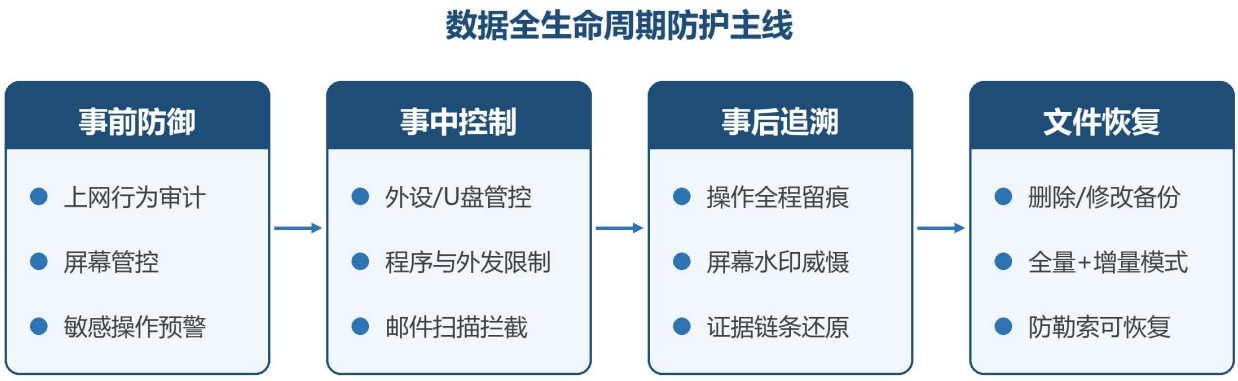


图 1　数据全生命周期四层防护主线

2.2 事前防御：把风险扼杀在发生之前

通过上网行为审计、屏幕管控与敏感操作预警等手段，及时发现员工的违规倾向与不良行为，在泄密发生之前预警干预。防线的重心从"亡羊补牢"前移到"未雨绸缪"。

2.3 事中控制：让办公电脑只能用于办公

全面接管终端电脑的权限与操作：U 盘与外设管控、程序运行限制、邮件扫描拦截、打印管理、禁止违规外发、限制软件安装。管理哲学是"有限制的自由"——企业授信环境内办公不受影响，违规通道则被逐一封堵。

2.4 事后追溯与文件恢复：每一步都有据可查、有备可用

系统自动留存完整的操作记录：屏幕截图、文件操作、拷贝行为、访问网址、外发记录。一旦发生泄密事件，管理者可以还原操作链条、定位责任人，为追责维权提供真实证据。

同时提供文件删除备份、修改备份、指定类型备份与全盘备份，支持全量与增量两种模式。即使遭遇误删、勒索加密或恶意破坏，企业数据也能恢复如初。

2.5 核心能力详解

2.5.1 透明加密：无感防护，内外有别

透明加密是整个方案的核心。企业核心文档在后台自动完成加密，全程静默运行：员工在公司授信电脑上正常打开、编辑、流转文件，办公习惯完全不变；而文件一旦脱离授信环境被私自外传，呈现的只是乱码，无法读取。

加密体系支持透明加密、智能加密、落地加密、断网加密、全盘加密等多种模式，配合分级密钥管理，可按部门与涉密等级灵活配置；文件外发需走申请解密等规范流程，兼顾安全与协作效率。

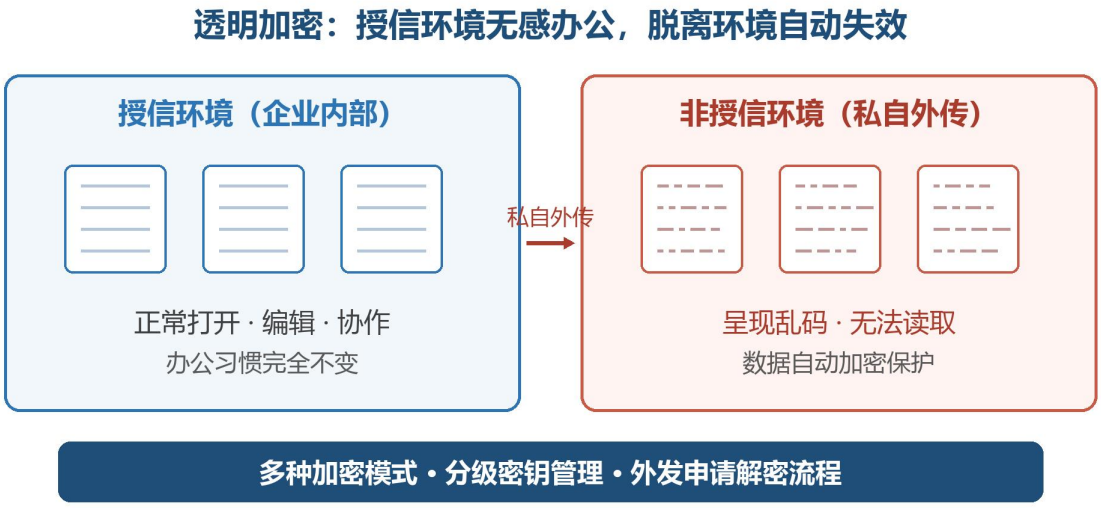


图 2　透明加密内外有别示意

2.5.2 截屏防护：堵住最隐蔽的窃密通道

针对截屏、录屏与 OCR 识别窃取，提供差异化防护策略：高涉密场景可全局禁用截屏录屏工具；一般场景可采取精准防护，涉密内容被强行截取时画面自动遮蔽，同时规避 OCR 提取，日常沟通不受影响。

2.5.3 外设与打印管控：守住物理端口

对 USB 存储设备与各类外设实施精细化权限管理，禁止私人设备随意接入拷贝，仅授权办公专用设备使用；打印行为同样纳入管控，杜绝涉密文档被私自打印带出。

2.5.4 终端数据防泄漏：主动发现敏感数据

支持对终端进行敏感文件扫描与敏感信息报警，配以文档检测大屏，让管理者对企业敏感数据的分布与流动一目了然;同时提供文档防勒索与文件操作备份能力,防止数据被恶意破坏。

2.5.5 行为审计与桌面管理：全程留痕

对网址访问、程序使用、文件操作、打印、邮件等行为完整记录，配合屏幕水印、程序水印、打印水印等威慑手段，形成"行为可查、责任可追"的管理闭环。桌面管理模块统一管控壁纸、通讯、右键菜单、定时锁屏等细节，规范办公环境。

2.5.6 终端安全与网络准入：从入口筑基

终端安全管理提供非法外联管控、软硬件变化报警、补丁统一管控、弱密码强制修改、文件与消息批量分发、远程协助等能力；网络准入控制则实现全网资产扫描与设备台账管理，做到"入网必认证、合规才入网"，把不可信设备挡在门外。

2.5.7 跨网文件交换：隔离网络间的安全通道

对存在内外网隔离需求的企业，提供受控的跨网文件交换能力，交换全程留存记录、自动杀毒、原始文件可追溯，在保障隔离的前提下满足必要的业务流转。

2.6 管理协同：双模式管理与审批流集成

系统支持按计算机、按用户两种维度管理，适配固定工位与移动办公等不同形态；内置完善审批流程，支持委托审批与批量审批，可免费对接钉钉、企业微信、飞书等第三方平台，融进企业既有协作习惯，让防泄密策略在业务流程中自然落地。



图 3　防泄密治理闭环

三、方案创新与价值

3.1 轻量部署：低负担的工程化设计

一套安全方案是否好用，部署成本与运行负担是关键考量。安企神在这方面有明确的工程化设计：

- **本地私有化部署**：服务器与数据库部署在用户自有环境，业务数据留存于企业内部，数据主权完全可控；采用 MySQL 数据库一键式安装，大型用户可对接 Oracle；
- **B/S 与 C/S 双架构**：C/S 架构侧重底层安全防护，保障系统自身安全；B/S 架构支持网页直接登录管理，无需安装管理端，便捷易用；
- **客户端轻量化**：安装包约 80M，标准环境下安装约 10 秒；测试环境 CPU 占用约 5%、峰值不超过 8%，策略全开内存占用一般不超过 100MB，对终端性能影响较低（实际表现受硬件配置与策略影响存在差异）；
- **全平台兼容**：兼容 Windows、Linux、Mac 及信创系统，满足国产化与信创环境要求；
- **持续迭代**：依据市场需求与客户反馈按需更新，通常 1 至 2 个月发布一个版本，功能新增与问题修复并举。

3.2 无感防护：安全不以牺牲效率为代价

传统数据安全手段常常要求员工改变习惯：换存储路径、走审批才能看文件、加密后协作困难。安企神的透明加密与策略管控在后台静默运行，员工在授信环境内的日常办公与正常协作完全不受影响；只有在数据试图脱离受控环境时，防护才真正"现身"。安全与效率由此不再是一道二选一的题。

3.3 一体化平台：200 余项功能，防护不留缝隙

安企神软件集文档加密、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 余项功能于一体。加密、外设、截屏、打印、外发、审计、备份等能力在同一平台内联动，避免了多套单点工具之间的防护缝隙与重复投入，也让管理策略得以全局统一。

四、落地方法论

4.1 分步实施：试点先行，降低切换风险

安企神建议按"试点先行、分步推广"的原则实施部署：优先选取部分终端开展试点，沉淀实施经验、统一配置流程后，再向全网其余分区推广落地。这一路径可以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　数据防泄密分步实施路径

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，内容涵盖平台操作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

数据防泄密的落地必须兼顾管理诉求与员工合法权益。安企神的策略体系支持按部门、岗位与涉密等级差异化配置：涉密岗位从严管控，普通岗位仅做必要留痕；管理端操作与审计记录本身亦有权限与日志约束，确保"监控工具"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，而非对立面。

4.4 常见顾虑与回应

"加密会不会影响办公效率？" 透明加密静默运行，授信环境内打开、编辑、协作与未加密时无差别；客户端资源占用低，标准环境 CPU 约 5%、内存不超过 100MB。

"员工会不会反感被管控？" 策略按岗位差异化配置，普通办公不受影响；屏幕水印等威慑手段本身即降低了违规动机，管理阻力随使用逐步下降。

"已有业务系统能否兼容？" 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，融入既有协作习惯。

"上线会不会冲击业务？" 试点先行、分步推广的实施路径，让企业在小范围验证后再全网铺开，切换风险可控。

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泄密路径差异明显，安企神的防护策略可按行业特点灵活组合：

行业	核心资产	典型防护场景
研发/制造	设计图纸、工艺文档	图纸透明加密，外发乱码；打印与 U 盘双重管控
软件/互联网	源代码、技术方案	代码文件加密，禁止违规外发，离职期重点监控
金融	客户资料、业务数据	敏感信息识别报警，操作全留痕，满足合规审计
医疗	患者数据、科研资料	数据分级授权访问，外设管控，防泄露可追溯

教育/科研	课题成果、试题资料	分级密钥管理，截屏防护，跨部门权限隔离

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

数据安全是一场持续的攻防演进：AI 工具的普及带来新的数据外传路径，远程与混合办公让边界更加模糊，信创与国产化进程则对安全体系的适配性提出更高要求。

安企神将持续在三个方向投入：一是深化敏感内容识别与智能预警能力，让系统从"记录行为"进化到"理解风险"；二是完善信创环境与跨网交换场景下的防护方案，跟随国产化与混合办公趋势；三是把十余年服务上万家政企客户沉淀的防泄密经验，转化为可复用的行业策略模板，让企业在上线之初即站在成熟实践的起点上。

数据是企业的核心资产，而泄密风险藏在每一次日常操作里。与其在事故发生后追悔，不如在风险发生前布防。

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。