安企神

政府单位行业

数据防泄漏

与终端安全管理解决方案

面向党政机关 · 事业单位 · 政务服务中心

让政务数据在内网安全流转，让每一次操作有据可查

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

第一部分 以数据防泄漏为导向 5

第二部分 以终端安全管理为导向 12

05 方案优势 13

06 方案价值 14

公司简介 15

01　项目背景

数字政府把政务服务搬到了桌面上。“一网通办”“跨省通办”“一网统管”的背后，是户籍、社保、医保、不动产、税务、市场监管等高频数据，在成千上万台办公电脑上被调阅、编辑、打印和上报。数据从机房走向终端，防护的重心也随之从网络边界移到了每一台电脑的硬盘里。

监管的尺子同样在变。除《网络安全法》《数据安全法》《个人信息保护法》之外，《保守国家秘密法》的修订、网络安全等级保护 2.0 的第三级要求、商用密码应用安全性评估，以及政务数据分类分级的推进，都把责任压到了数据处理的具体环节。检查方式同样在变：过去看制度是否上墙，现在直接调终端日志——谁在什么时间插了 U 盘、拷了哪些文件、打印了几份、发往了哪个邮箱，一条一条对。

现实情况往往并不对称。多数单位的投入集中在机房与边界：防火墙、入侵检测、堡垒机、日志审计一应俱全。而一份尚未标密、内容却相当敏感的统计报表，可能就躺在某台窗口电脑的桌面上，随时可以被复制、打印或者拍照带走。终端是数据的最后一公里，也常常是防护最薄弱的一公里。

政务数据资产的三点特征

01　价值密度高	02　责任链条清晰	03　出口高度分散
一份名册、一张报表，背后往往是数万人的身份信息与法人信息，泄露一次即构成群体性风险。	谁采集、谁使用、谁负责，制度上是明确的，一旦出事就必须能说清、能举证。	窗口、科室、乡镇站所，打印、拷贝、拍照，几乎无法仅靠流程约束。

说到底，政务终端的安全不是“再装一个软件”，而是把数据从产生到归档的每一次流转都纳入可控范围：谁在用、能不能拷、能不能打、能不能发、发出去之后还能不能追。方案要做的，是把这些零散的管控动作收敛到一套规则、一个平台、一份可核查的记录上。

02　需求分析

结合党政机关、事业单位与政务服务中心的终端环境，我们把共性问题归纳为五个方面。它们并非彼此孤立，而是同一条链路上的不同环节：文件散落在终端，从多条出口流出，事后又说不清楚。

敏感文件散落在终端，谁能看、谁能拷、谁能发没有统一口径

- 公文、报表、名册、案卷、调研数据以明文存放在个人电脑，命名与归档各行其是，同一份材料在不同终端存在多个版本。
- 科室之间习惯用 U 盘、即时通讯、邮件互传，文件一旦离开内网便处于完全失控状态。
- 定密与标密在制度上有要求，终端上却缺少可执行的技术动作，标识与管控成了两套体系。

输出通道多而分散，打印、复印、扫描、刻录最难管

- 打印无审批、无留痕、无水印，红头文件、会议材料、干部名册往往在打印环节流出。
- 复印、扫描、光盘刻录等离线输出长期处于监管盲区，事后既查不到内容，也定位不到人。
- 窗口与综合科室的打印机多人共用，出问题时只能追溯到“这台机器”，无法追溯到经办人。

一机两用与违规外联，让网络边界形同虚设

- 终端私接互联网、私搭无线热点、私接路由器，内外网隔离被一根网线绕开。
- 维修、外包、上级检查等外来设备接入内网缺乏校验，接入即等于获得内网访问能力。
- 跨网文件交换依赖人工 U 盘摆渡，既无审批也无记录，是保密检查中最常见的扣分项。

审计留痕不全，检查时说不清

- 日志分散在网关、服务器、业务系统各处，缺少统一检索入口，事件回溯基本靠人工排查。

- 面对“谁、在什么时间、用什么方式、带走了哪些文件”的追问，往往只能给出模糊判断。
- 报表靠临时手工汇总，难以支撑日常监督、季度通报与专项检查的常态化要求。

点位多、终端杂、运维力量薄弱

- 市、区县、乡镇（街道）、村（社区）多级部署，终端形态从办公 PC 到窗口一体机、笔记本、虚拟机。
- Windows 与国产操作系统并存，补丁、软件、口令的管理标准难以统一。
- 运维人员少、点位分散，故障处理靠跑现场，批量安装与策略下发效率低。

03 方案设计

政务终端的安全问题，本质是三句话：数据不受控、通道不受限、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——让数据始终处于可控状态，让每一次流转都可追溯，让管控动作落在既有办公流程之内。

围绕这条主线，方案以**“一个平台、四道防线”**组织能力：加密解决“带走也没用”，通道管控解决“带不走”，终端治理解决“从哪台机器带”，审计溯源解决“带走了能查到”。

一个平台 • 四道防线

防线 01　数据加密	**可用不可带走**	核心文件在内网自由流转，离开授信环境即为乱码。
防线 02　通道管控	**带不走**	外设、打印、外发、截屏与拍照，逐条出口设策略。
防线 03　终端治理	**摸得清**	资产、软件、补丁、外设与准入，一台终端一张底账。
防线 04　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

- **分区分域、分级授权**——按科室与业务系统划分安全域，按敏感程度划分密级。低密级账号打不开高密级文档，跨部门协作以授权代替解密。
- **一个客户端、一个管理端，管理员分级分权**——终端侧只装一个客户端，管理侧只有一套管理端，一个后台即可纳管全部终端。终端按科室、楼层、区域分组，策略按组批量下发；管理员分超级管理员与普通管理员，普通管理员只能管理指定分组的终端、只能使用被授权的功能模块，运维、安全与审计的职责由此分开。
- **不改变办公习惯，才能落地**——加密在驱动层完成，新建、编辑、保存的动作与从前一致；打印、流转、公文会签的路径不变。安全应当隐形在流程里，而不是增加新的填报负担。

实施路径：三步走

第一步　核心科室试点	第二步　分批推广	第三步　制度固化
选取办公室、综合科与涉密岗位先行部署，跑通加密、打印、外发三条主链路。	按层级推送客户端与策略，乡镇站所统一纳管，运维在平台上远程完成。	策略与保密制度、等保整改项逐条对应，形成可核查的常态化闭环。

04　解决方案

方案能力分为两组：第一组以数据防泄漏为导向，解决“文件怎么管”；第二组以终端安全管理为导向，解决“机器怎么管”。两组能力共用一个客户端与一个管理平台，按需启用、逐步扩展。

第一部分　以数据防泄漏为导向

1.1　政务文档透明加密

政务文件的价值在内容，而不在它存在哪个文件夹。所以第一个动作是让文件本身“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、编辑、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	办公室、综合科、涉密岗位	新建保存即密文，内网正常使用，外发为乱码
智能加密	需频繁读取、较少外发的岗位	按程序与文件类型判定，命中敏感规则才加密
只读	对外交接件、下发给基层的材料	可看不可改、不可另存，防止二次扩散
落地加密	上级来文、外部报送文件	落到本机即转为密文，转发到别处无法打开
不加密 / 只解密	领导阅文终端、专用输出终端	保持原有习惯，由打印、外设等手段兜底

实施要点

- **按岗位分配模式**：核心科室启用透明加密，文件新建即密文；需读取但少外发的岗位可用智能加密；对外交接件设为只读；上级下发与外部来文用落地加密。
- **国密算法与分级密钥**：采用 SM3/SM4 算法，密钥分级管理，满足商用密码应用安全性评估对数据存储机密性的要求。
- **密级与安全域**：跨科室不可见、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：**文件在终端始终是密文，出口决定结果**——内网授信终端与授权应用内正常打开、编辑、流转；经 U 盘、邮件、截图、拍照等非法出口离开，得到的只是乱码，或被直接阻断并留下行为记录。

1.2 公文流转与业务系统对接

政务办公的骨架是流程：起草、审核、会签、印发、归档。加密如果让流程变慢，就一定会被绕开。所以第二个动作是把加密嵌进流程，而不是加在流程之外。

加密网关：服务器明文，终端密文

通过与 OA、公文传输、档案、门户及业务系统免硬件对接，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**，不改变访问地址，不改变业务流程。

服务器区（明文）	加密网关	内网办公终端（密文）
OA · 公文传输 · 档案 · 门户，业务数据以明文存储与流转；文件服务器 / 共享目录按目录设定加密与解密规则。	无需专用硬件；与现有系统对接；上传解密、下载加密。	文件落地即密文；离线授权到期失效；外发须经审批。

为什么强调“不改流程”

实践中最常见的失败，不是技术不行，而是流程被拖慢后员工想出各种变通：拍照、抄录、用私人邮箱中转。方案把加密动作放在文件系统的读写路径上，用户感知到的只是“文件还是那个文件”，变通的动机自然就消失了。

外发与离线

- **邮件白名单**：向指定的上级单位、协作单位邮箱发送时自动解密，其余外发仍需申请审批。
- **受控外发**：确需向外部单位提供材料时，生成受控文件——限定打开次数与有效期、绑定设备、禁止打印、页面显示水印，原文件不作解密，打开行为留痕。
- **离线办公**：出差、下乡、居家可通过审批获得离网授权，到期自动失效。



1.3 打印与输出管控

打印是政务场景里最容易被忽视的出口，也是检查中最难解释的一环。文件在硬盘里是密文，落到纸面上就再无技术约束——能做的只有三件事：事前管住谁有权打，事中让纸面带上痕迹，事后留得下打过的内容。

打印全流程管控

环节	动作
第一步　发起申请	说明用途与份数，指定打印机
第二步　审批	科室负责人 / 保密办审批，超限升级审批；驳回则拒绝输出并记录原因
第三步　输出	强制叠加水印，限定设备
第四步　归档留痕	记录操作人、时间、终端信息

四类输出通道，同一套策略

打印	复印	扫描	光盘刻录

审批 · 水印 · 内容留存	设备管控 限制	外设白名单 · 操作审计	授权使用 · 记录留档

实施要点

- **水印可追溯**：纸面叠加姓名、工号、时间与终端编号，既能警示，也能在文件流出后锁定到人。
- **内容可复核**：不仅记录“打印了几页”，还留存打印文档快照，回答“打印了什么”。
- **窗口场景适配**：窗口与大厅的共用打印机按岗位绑定，谁打印、打了几份，一目了然。

一个常见误区

不少单位把“禁止使用 U 盘”当作主要手段，却对打印环节几乎不设防。实际检查中，从打印机旁的废纸篓里翻出材料，比从 U 盘里拷走文件要容易得多。输出侧的管理，往往才是最短的那块板。

打印管控也最容易“一阵风”：刚上线时严格审批，两个月后因为影响效率被要求放开。可持续的做法是把粒度做细——哪些文件必须审批、哪些只需留痕、谁有豁免权限，先写进制度再落成策略，而不是一刀切。管得住又用得顺，制度才留得下来。

1.4 敏感内容识别与分类分级

分类分级是政务数据治理的起点，但落到终端上，首先要回答三个很具体的问题：哪些文件里有敏感内容，它们躺在哪台机器上，现在是不是明文。

从发现到处置的四个环节

01 数据源	02 识别	03 标记	04 处置
终端与共享目录：文档、表格、PDF、压缩包、图片	内容识别引擎：关键词、正则、证件号、文件指纹、图片 OCR	敏感文件清单：位置、类型、密级、当前是否加密	补加密 · 告警，阻断外发，纳入分级

常见敏感特征（规则库可自定义）

身份证号　手机号码　社保 / 医保编号　银行账号　详细住址　案件与卷宗编号　内部会议纪要　“不予公开”字样　领导批示与签报　执法笔录　未发布的统计数据　人员编制与薪酬

识别不是目的，分级才是

很多单位做过一轮敏感文件扫描，得到一份长长的清单，然后就没有然后了。清单本身不产生价值，价值在于把清单变成规则：哪些目录必须加密、哪些岗位只能只读、哪些文件外发必须走审批。识别是起点，分级与策略才是终点。

- **扫描定位**：扫描指定终端或共享目录，列出含敏感内容的文件及其加密状态；服务器上的历史数据同样覆盖。识别规则可按科室、按业务单独设定，避免一套规则管所有部门。
- **分级策略**：一般数据、重要数据、核心数据对应不同的加密强度、外发策略与审批层级，让管理精度与数据价值匹配。
- **避免过度管控**：只对命中规则的文档加密，普通材料保持原样。管控越精准，员工配合度越高，制度才不会被绕过。

1.5　行为审计与事件定位

一个市级单位动辄数千台终端，一天产生的行为记录数以万计。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。

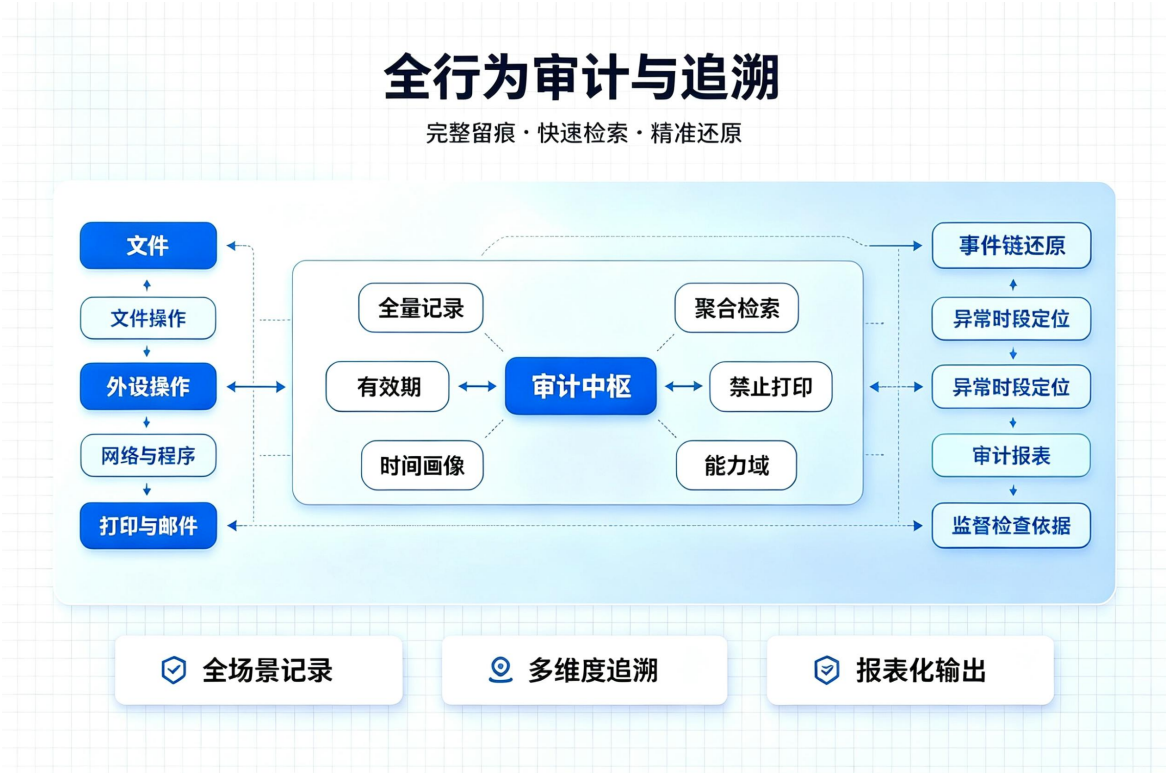
从采集到取证的链路

统一采集	索引存储	聚合检索	输出取证
文件操作、U 盘、打印、邮件、即时通讯、网页、程序、剪贴板；客户端缓存，断网续传	结构化入库，分级留存	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	审计报表 · 事件链条 · 检查佐证 · 责任认定

留痕的意义在于“能解释”

一次检查中被问到“这份文件是怎么出去的”，如果只能回答“我们查一下”，结果往往已经是扣分。能当场调出记录、说清路径、指明责任人的单位，和被动的单位，整改成本完全不是一个量级。

- **全量记录**：文件创建、修改、删除、复制、重命名，U 盘插拔与拷贝，打印、邮件、即时通讯、网页、程序、剪贴板与远程操作，逐条留痕。
- **聚合检索**：按人、时间、关键词、文件类型组合检索；从一条外发记录顺藤摸瓜，还原整条事件链。
- **时间画像**：单台终端一天的行为时间轴，异常时段一目了然，不必逐页翻日志。
- **报表输出**：按科室、人员、事件类型生成审计报表，可直接用于日常监督、季度通报与专项检查。



1.6 屏幕与成像防护

加密挡住了文件，却挡不住一部手机。屏幕是终端上最后一道、也最容易被忽略的出口——尤其在阅文室、会议室和政务大厅的窗口前。

三类屏幕出口，三层应对

出口 01　肉眼与相机	出口 02　截屏与录屏	出口 03　复制与拖拽
阅文、会议、窗口前拍照即带走	一键保存、一键转发，无痕扩散	一段文字、一个号码，三秒完成
应对：屏幕水印（姓名 · 工号 · 时间，拍照即留痕）	应对：截屏管控（全局禁用 / 仅遮蔽密文，普通页面不受影响）	应对：剪贴板与拖拽管控（复制即脱敏，禁止拖到外部程序）

一个真实的场景

窗口工作人员用手机拍下屏幕上的办事群众信息，转发到一个几百人的工作群里——这不是恶意窃密，却同样是个人信息泄露。这类行为既无法用法条约束，也很难靠人盯人发现，只能靠技术手段在动作发生的瞬间拦下来。

屏幕防护的另一层价值是威慑。当员工知道屏幕上始终带着自己的名字与时间，随手拍一张这个动作本身就会变得犹豫——这比事后追责更有效，也更少伤及正常工作氛围。

- **防手机拍照**：软件与摄像头联动，检测到拍照动作立即锁屏，同时抓拍现场画面并截取当前屏幕，两图对照即可锁定人与内容。
- **水印内容可定制**：按岗位显示姓名、工号、部门与时间，纸张、屏幕、打印三类水印可分别设定，形成一致的视觉约束。
- **不打扰正常办公**：截屏仅在加密文档区域遮蔽，日常截图、演示与培训不受影响，避免因“太麻烦”而被要求关停。
- **与打印、外设联动**：屏幕、纸张、外设三类出口用同一份水印模板，追责时不必再拼凑不同系统的记录。



第二部分　以终端安全管理为导向

数据之所以能被带走，前提是有终端可以承载。终端本身管不清——资产不明、软件随意、外设失控、谁能入网没门槛——数据防线就成了空中楼阁。所以第二组能力落在“机器”上：先摸清有什么，再决定允许做什么。

2.1　资产台账与变更报警	全网资产扫描，自动生成软硬件台账；内存、硬盘、网卡、外设发生更换即时报警。资产异动不再靠人工核对，报废、调拨、私拆都有据可查。
2.2　软件标准化与正版化	企业软件库统一分发，禁止安装来源不明程序；支持全网安装与全网卸载；盗版软件自动识别并可远程清理，降低版权纠纷与供应链风险。
2.3　外设与移动介质	U 盘按禁用、只读、只写、白名单四种方式授权；加密 U 盘只能在授信终端打开；光驱、蓝牙、USB 外设分类管控，物理出口逐一收口。
2.4　违规外联与网络准入	终端私接外网立即告警并可阻断；准入网关同时校验用户身份、设备身份与安全状态，合规才入网；IP 地址与设备分布可视化。

2.5　跨网文件交换	内外网隔离环境下，文件经申请、审批、摆渡、留痕几步完成交换。谁在什么时候交换了哪个文件，全程可查、原始文件可追溯。
2.6　备份、补丁与远程运维	文件删除与修改自动备份，配合文档防勒索；补丁统一管控、弱口令强制整改；远程协助与批量分发，让基层运维不必再跑现场。

合规才入网：准入控制的三道校验

接入请求	终端发起接入：有线 · 无线 · 便携设备
① 用户身份校验	账号口令 · 认证入网
② 设备身份校验	终端注册 · 外来设备识别
③ 结果处理	合规放行；不合规终端进入隔离区整改

05　方案优势

政务单位选型时最常问的三个问题是：要不要改网络、会不会影响办公、检查时能不能拿出东西。对应的答案，构成了这套方案的基本盘。

一体化：一个客户端，一个平台	加密、审计、管控、准入、跨网交换在同一客户端内实现，不必为每类需求装一套系统、维护一套账号体系。
闭环：事前、事中、事后	事前以加密预防，事中以通道阻断，事后以审计取证。三段能力串成一条链，而不是各自独立的工具箱。
合规：对标等保与密评	按等保 2.0 三级要求设计访问控制、安全审计与数据保密性措施，支持国密算法，可直接映射测评项。
兼容：信创环境统一纳管	Windows 与国产操作系统、不同品牌终端在同一平台管理，策略与操作逻辑保持一致，替换系统

	不等于丢掉管控。
分权：多级管理台与角色分离	市、区县、乡镇分级授权，策略统一制定、分级下发；运维、安全、审计角色分离，责任边界清晰。
轻量：旁路部署，平滑推广	不改造现有网络结构，客户端静默安装，可按科室分批推进，试点到全覆盖不打断日常办公。

06 方案价值

数据“可用不可带走”	核心文件在单位内部自由流转，离开授信环境即为乱码。加密不改变办公习惯，却让“拷一份带走”这条路从技术上失效。
出口“可管可查”	打印、外设、外发、屏幕四类出口都有策略与记录。堵住的不是某一个漏洞，而是最常见的几条泄密路径。
检查“有据可依”	日志、报表与事件链可以当场调取，把“说不清”变成“拿得出”。一次检查不必再动员全单位翻台账。
运维“从跑腿到平台”	资产、软件、补丁、故障在同一个平台上处理，乡镇站所不必等运维上门，基层信息员的工作量明显下降。

这四条价值指向同一件事：把过去依赖人盯人、依赖临时检查的管理方式，换成可持续运行的技术机制。制度写在纸上，机制跑在终端上，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®