安企神

汽车行业

终端安全管理解决方案

面向整车研发 · 零部件制造 · 试验检测 · 销售服务企业

让每一台终端可信，让每一份数据可管，让每一次操作可查

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.....5

05 方案优势.....9

06 方案价值.....10

公司简介.....11

01 项目背景

一款新车从造型创意走到交付，要经过概念设计、工程开发、试验验证、供应商定点、试制量产、上市销售一整条链路。上千名研发人员在终端上绘制三维模型、调整整车控制器标定参数、分析路试与碰撞数据；生产端上千台工控机与制造执行系统终端支撑着焊装、涂装、总装的节拍；销售端成百上千家经销商的门店电脑里沉淀着客户订单、金融资料与售后记录。一家车企的信息资产，就这样分散在研发网、生产网、办公网和经销商体系四类环境里，承载它的不是几台服务器，而是数以千计、形态各异的终端。

这些终端上的数据，恰恰是车企最贵的家底。一套全新车型的造型数据与工程图纸动辄投入数亿元；三电系统的标定参数、自动驾驶算法的训练数据集，是几轮冬测夏测换来的经验；客户名单与成交价格体系，则直接关系到价格政策的执行。设备可以再采购，一次车型数据的大面积外流却没有任何办法补救——对手拿到的不只是文件，还有你两三年的开发投入和踩过的坑。

合规的压力同样具体。《汽车数据安全管理若干规定（试行）》对重要数据提出了识别、备案与出境评估要求；两项汽车信息安全强制性国家标准已发布并进入实施倒计时；面向海外市场的企业还要面对 UN R155/R156 网络安全与软件升级管理体系认证；集团内部审计、客户审厂、供应商评审也都在看同一件事——你能不能拿出记录。而《数据安全法》《反不正当竞争法》与等级保护 2.0 对访问控制、安全审计的规定，最终都要落在终端上才能执行。

泄密的路径也在变得隐蔽。设计文件打包上传个人云盘、路试数据拷进随车笔记本带回、把算法问题贴到技术论坛求助、经销商销售人员离职时带走整份客户档案、供应商拿到图纸后转发给更下一级——这些动作单看都不刺眼，连起来就是一条完整的输出链路。

现实投入却常常不对称。车企愿意为产线设备和试验台架付高价，安全预算却排在后面；更重要的是，安全方案一旦影响产线节拍、拖慢仿真计算、打断测试采集，业务部门第一时间就会要求撤掉。所以这个行业的安全建设，第一约束不是功能多少，而是"不碰产线、不打扰研发"。

汽车行业终端资产的三点特征

01 资产形态跨域	02 泄露即不可逆	03 生态边界长
研发工作站、产线工控机、测试采集终端、门店 PC 形态迥异，任何一类管不住，防线就有缺口。	车型数据、标定参数一旦流出无法召回，新车上市节奏与差异化卖点随之失守。	数据要在 Tier1/Tier2 供应商、经销商、检测机构、路试外包团队之间往复，协同方越多，边界越不封闭。

汽车行业的数据安全不是"再装一套软件"，而是让每一台终端都成为可信的承载点：终端上有什么、谁在用、能打开什么、能带出什么、带出之后能不能追。方案要做的，是把散落在各基地、各网域的管控动作，收敛成一套规则、一个平台、一份可核查的记录。

02 需求分析

结合整车企业、零部件企业与经销体系的终端环境，我们把共性问题归纳为五个方面。它们不是五个独立的缺口，而是同一条链路上的五个环节：终端摸不清，数据管不住，出口收不严，事后说不清。

终端底账不清，多基地多类型终端并存

- 研发工作站、产线工控机、试验采集终端、门店收银与销售 PC 并存，操作系统从 Windows、Linux 到工控专用系统跨度极大。
- 内存、硬盘、外设被更换或私拆没有记录；员工私装软件、私接随身 WiFi，IT 团队往往在出问题之后才知道。
- 集团多个基地、多家子公司各管各的，底账对不齐，安全策略就无从谈起。

研发与生产数据散落终端，版本与权限混乱

- 三维模型、工程图纸、BOM 清单、标定数据在个人工作目录、共享盘、试制车间之间反复拷贝，同一份数据存在多个"最新版"。

- 研发网、办公网、生产网之间边界靠约定维持，跨网拷贝无人校验。
- 试制车间的终端既连着产线设备，又插着工程师的 U 盘，是最容易被忽略的交叉点。

对外通道多，供应链与销售体系各有各的出口

- 定点与开发阶段要向 Tier1/Tier2 供应商发放图纸与技术协议，量产后要与供应商往复传递变更与质量数据。
- 经销商体系要下发价格政策、培训资料，又持续回传客户订单信息；认证检测、展会宣传、媒体试驾各有各的数据出口。
- 数据量大、批次频繁，靠邮件附件和移动硬盘传递，发出去就失控。

移动与远程场景存在管理真空

- 路试车队常年在外，采集终端随车流动，脱离内网后传统边界防护基本失效。
- 驻厂支持、供应商现场、展会现场都要带终端接入客户或现场网络。
- 销售人员流动办公，客户资料存在个人终端上，丢失与外带无从约束。

审计与举证能力薄弱，合规应对吃力

- 日志分散在文件服务器、域控、网关、经销商系统各处，缺少按项目、按基地维度的统一检索入口。
- 监管检查或客户审厂问到"这份图纸发给过哪些供应商""这些客户数据被谁导出过"，只能人工排查，答复以天计。
- 数据安全测评要的台账靠临时手工整理，无法常态化。

03 方案设计

汽车行业的终端安全问题，本质是三句话：终端不受控、出口不设防、行为不留痕。因此方案不追求功能堆叠，而是围绕一条主线展开——让每一台终端成为可信的承载点，让每一份数据的进出有边界，让每一次操作可回溯。

围绕这条主线，方案以"一个平台、三层防护"组织能力：终端治理解决"摸得清"，数据防护解决"带不走"，审计溯源解决"查得到"。

层次	能力	解决的问题	实际效果
第一层	终端治理与准入	摸得清	资产、软件、补丁、外设、准入，一台终端一本账
第二层	数据加密与出口管控	带不走	加密、外发、介质、打印、屏幕，逐条出口设策略
第三层	行为审计与溯源	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

- **按基地分域、按角色授权**——以基地与网域为隔离单元，研发、生产、办公、经销商各成安全域；域内再按岗位细分权限，产线终端只允许运行授权程序，销售终端打不开研发目录，跨域协作以授权代替解密。
- **一个客户端、一套管理端，不改变业务节奏**——终端侧只装一个客户端，Windows 与 Linux 同源；研发人员的编译仿真、产线设备的采集上报方式一律不变。策略由总部统一制定，按基地分级下发。
- **性能与稳定优先，能灰度、能回退**——上线前在试验环境做性能基线测试，按项目组灰度部署，异常可单机回退；产线终端的策略变更安排在停线窗口执行。安全的底线是不影响生产节拍与研发节点。

实施路径：三步走

第一步 试点先行	第二步 全域推广	第三步 制度固化

第一步 试点先行	第二步 全域推广	第三步 制度固化
选一个车型项目组与一条产线试点，跑通加密、外发、审计主链路，完成性能基线测试。	覆盖各基地研发、生产、办公终端，经销商体系轻量接入，策略由集团集中下发。	把策略与保密制度、供应商协议、合规应答逐条对应，形成可季度复核的闭环。

04 解决方案

方案能力分为两层：第一层是终端安全治理，解决"数据靠什么承载、从哪台机器进出"；第二层是数据防泄漏，解决"数据本身怎么管"。两层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 以终端治理为基础

这一组能力回答"承载点可不可信"：先摸清每一台终端，再收住软件、外设与入网资格，为数据防护打好地基。

1.1 资产台账与硬件变更监控

全网扫描自动生成软硬件台账，终端型号、配置、使用人、归属基地一目了然；内存、硬盘、网卡、外设发生更换即时报警，调拨、私拆都有据可查。对于车企多基地、多子公司的现状，台账支持分级查看、统一汇总，集团安全部门随时能回答"我们有多少台终端、都在哪、谁在用"。

1.2 软件标准化与补丁管理

办公软件、CAD/CAE 工具统一分发与授权管理，禁止私装来源不明程序；对破解版工具远程清理——这不仅是安全问题，工业软件厂商的侵权索赔近年来已成车企的现实风险。补丁统一检测、统一分发，弱口令强制整改；工位机与产线终端分组管理，避免一刀切。

1.3 网络准入与违规外联

准入网关对入网终端校验用户身份、设备身份与安全状态，未注册设备、健康状态不达标的终端一律拦在网外。私接互联网、私搭热点、私用随身 WiFi 立即告警并可阻断，研发网、生产网、办公网之间的违规跨接逐条留痕，把"靠约定维持的边界"变成"技术上可执行的边界"。

1.4 远程运维与终端保障

多基地终端集中在同一平台运维，故障远程协助处理，异地基地不必等总部派人上门；文件删除与修改自动备份，配合防勒索策略，产线终端与研发终端的数据多一层兜底。



第二部分 以数据防泄漏为核心

这一组能力回答"数据本身怎么管"：从加密、外发、介质、聊天与邮件、屏幕出口到敏感识别与行为审计，十个动作串成一条从产生到归档的链路，任何一个环节都不单独成立。

2.1 文档透明加密

数据的价值在内容，所以第一个动作是让文件本身带锁：三维模型、工程图纸、标定参数、算法文件在保存时自动加密，加密在驱动层完成，员工在授信环境里打开、编辑、编译、仿真的习惯完全

不变；文件一旦离开授信环境，打开就是乱码。加密采用 SM3/SM4 国密算法，密钥按基地与密级分级管理，既满足合规对存储机密性的要求，也为认证审核提供可说明的技术口径。

加密模式	适用岗位与场景	实际效果
透明加密	造型、车身、三电、算法等核心研发岗	新建保存即密文，内网正常使用
智能加密	试验、质量、采购等读取多、外发少的岗位	命中敏感规则才加密，避免误伤
只读	发给供应商与经销商的受控资料	可看不可改、不可另存
落地加密	供应商回传数据、检测机构报告	落到本机即转密文，转发他处无法打开
不加密	公共资料、已公开宣传物料	由外发与审计手段兜底

2.2 供应链与经销商外发管控

管控的目标不是"不出去"，而是"出去的那一份可控"。外发走"申请、审批、受控、留痕"四步：申请人说明用途、接收方与有效期，项目负责人分级审批；生成受控文件限定打开次数与有效期、绑定设备、禁止打印、叠加水印；谁在何时发给谁、对方打开了几次，全程留痕并可回溯。

三类典型场景：供应商图纸发放按项目建立白名单通道，交付清单与审批单一一对应，防止"多给了一份不该给的图"；经销商体系的价格政策与培训资料以受控文件下发，到期自动失效；认证与展会资料分密级处理，可公开的照常使用，涉密的走审批。

2.3 移动介质与输出通道

通道	主要风险	管控方式
U 盘与移动硬盘	整目录打包带走	禁用、只读、专盘专用三种授权，加密 U 盘仅授信终端可打开
打印与复印	图纸、报价单外流	审批、水印（姓名、工号、时

通道	主要风险	管控方式
		间）、内容留存
光盘刻录与蓝牙	交付两用，事后无记录	授权使用、操作留档
试制车间接口	标定数据、固件被读出	编程器与调试工具白名单，操作留痕

2.4 聊天、邮件与屏幕出口

即时通讯与网页邮箱的外发行为逐条审计，向个人邮箱、网盘发送敏感文件自动阻断或告警；邮件白名单放行已备案的供应商与经销商邮箱，其余外发需审批。屏幕是最后一道出口：屏幕水印叠加姓名、工号与时间，评审会上随手拍屏即留痕；截屏、录屏工具按策略管控。当员工知道屏幕上始终带着自己的名字，随手外发的动作本身就会变得犹豫。

2.5 敏感内容识别与分类分级

扫描研发终端、共享存储与文件服务器，按规则识别敏感文件：车型代号与项目命名、工程图纸特征、标定数据格式、VIN 与客户信息特征、人脸与地理位置字段等；命中的文件打上密级标签，形成敏感文件台账，再按台账补加密、限权限、管出口。识别是起点，把清单变成策略才是终点。

2.6 行为审计与离职风险预警

统一采集文件操作、外设使用、打印、邮件、即时通讯、网页、程序运行、剪贴板、远程操作等行为记录，客户端缓存、断网续传；按人、时间、项目、关键词组合检索，从一条记录还原整条事件链。三类信号重点预警：离职流程发起前的批量下载与集中压缩；非工作时段的异常外发与审批驳回后的换道重试；跨项目访问核心目录与高频使用截屏工具。监管检查或客户审厂时，报表与事件链可以当场调取，把"我们查一下"变成"记录在这里"。



05 方案优势

优势	说明
一体化：一个客户端，一个平台	加密、审计、介质管控、准入、运维在同一客户端实现，不必为每类需求装一套系统、维护一套账号
不碰产线：不动业务工具链	驱动层加密、编译仿真与产线上报方式不变；工控环境专项适配，策略可灰度、可回退
分域：按基地与网域隔离	研发、生产、办公、经销商各成安全域，跨域越权在客户端侧即被拦住，贴合集团化组织方式
可举证：对标体系与监管要求	访问控制、安全审计、数据保密措施可映射等级保护 2.0 与汽车数据安全规定条款，支持国密算法
可扩展：多基地统一纳管	总部与各基地在同一平台分级授权，策略统一制定、分级下发，运维、安

优势	说明
	全、审计角色分离

06 方案价值

价值	具体表现
终端"一本账"	资产、软件、外设、入网资格集中呈现，多基地底账对得齐，变更随时可查
数据"可用不可带走"	核心文件在授信环境自由流转，离开授信环境即为乱码，研发习惯不变而"拷走一条路"失效
出口"可管可查"	介质、打印、外发、聊天、屏幕逐条设防，堵住最常见的几条泄密路径
合规"拿得出"	台账、报表、事件链当场可调，监管测评、客户审厂、内部追责不必再动员全公司翻记录
运维"从跑腿到平台"	资产、补丁、故障在同一平台处理，几个人的 IT 团队也能管住上千台终端

这五条价值指向同一件事：把过去依赖保密协议、依赖人盯人的管理方式，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。



400-666-2563

www.wgj7.com

河北·石家庄

安企神软件®