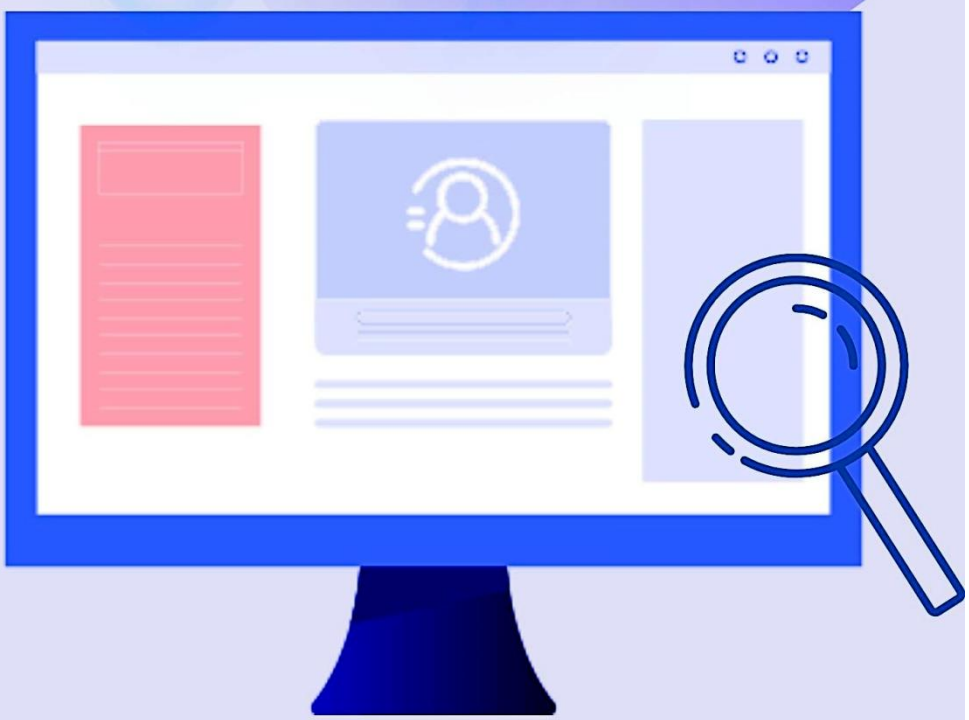
域智盾软件®

汽车行业

终端安全管理解决方案



CONTENTS/目录

01 项目背景 3

02 面临问题 3

03 方案设计 4

04 解决方案 4

05 方案优势 7

06 方案价值 7

07 系统架构 8

08 公司产品简介 9

一、项目背景

汽车制造业已进入以研发数字化、生产智能化和供应链协同化为主要特征的新阶段。核心资产主要以电子文档形式沉淀在员工办公电脑、工程工作站和生产车间终端上，以网络边界为核心的防护体系已难以约束数据本身的流向。

本方案面向汽车整车厂及零部件供应商，围绕办公网、研发网、生产网的实际场景，提出以终端为落点的一体化安全管理体系。

二、企业面临问题

结合汽车行业的业务特征，终端安全管理需要重点解决以下问题：

- 研发图纸、工艺文件在员工电脑本地长期留存，外发、拷贝与打印缺乏统一管控，离职、调岗环节易发生资料外流。
- 办公网与研发网之间通过 U 盘、手机热点、私人笔记本等路径违规外联，网络隔离策略被旁路。
- USB 外设、蓝牙、便携硬盘、手机接入缺乏审批与审计，测试数据通过普通外设被带出。
- 员工访问与工作无关的网站、运行与岗位无关的程序，既占用带宽又引入病毒与挖矿风险。
- 软件私自安装、硬件私换、IP 与计算机名私改，导致资产台账与实际终端不一致，事件发生后难以定位责任人。
- 操作系统与业务软件补丁长期不打，勒索病毒与远程漏洞利用直接进入内网。
- 外来设备随意接入内网，无准入校验即获得网络访问权限，存在横向渗透风险。
- 敏感文件发生外发时缺乏实时告警，安全团队往往在数据已经流出之后才被动响应。



三、方案设计

本方案以“终端全生命周期安全管控”为出发点，从以下角度构建整体能力：

- 以终端为落点，将管控动作直接落在员工日常使用的电脑上，策略统一生效，不依赖网络位置判断。
- 以身份与岗位为基准分配权限，不同角色在终端上获得差异化的访问、外发与外设权限。
- 以策略联动替代单点工具，上网行为、外设、加密、报警、补丁、准入等模块统一在一个控制台下发，避免多套工具各自为政。
- 以不影响业务为前提，驱动层与服务层实现，员工在授权软件内的操作方式保持不变。
- 以可审计、可追溯为交付标准，所有终端操作日志集中采集、留存可查，事件发生后能够按人、按机、按文件还原全过程。

四、解决方案

解决方案由九个相互联动的子模块组成，统一通过一个管理端配置。

上网行为审计

对员工终端的上网行为进行全量记录，包括访问网址、搜索关键词、网页标题、停留时长、上传下载流量，按部门、人员、终端维度生成报表。日志留存周期可按企业合规要求配置，满足内部审计与外部核查需要。

上网权限管控

按岗位配置网站访问策略，对与工作无关的网站类别（视频、游戏、购物、社交、网盘等）实施拦截；同时对终端上运行的程序进行黑白名单控制，未经允许的软件不得启动，从源头减少私自安装带来的风险。

数据防泄密

围绕文件的全生命周期提供三类能力：

加密模式：支持透明加密、智能加密、只解密不加密、只读、不加密等模式。

禁止程序发送数据：对微信、QQ、邮件客户端、网盘上传工具等指定程序发送文件的动作进行阻断或走审批流程，防止敏感文档通过即时通讯通道外发。

敏感文件报警：基于文件名、屏幕截图、窗口标题、网页搜索识别，发现敏感词时，实时向管理员告警并按策略阻断。

USB 外设管控

对 USB 存储设备、移动硬盘、手机、蓝牙、无线网卡、光驱、刻录、打印机等外接设备进行管控，所有外设接入与文件操作均留痕，解决 U 盘拷贝这一最高发的数据外流通道。

违规外联报警

对终端同时连接内网与外网、启用手机热点、私接无线路由、私自修改网络配置等行为进行实时监测，发现即阻断并向管理员推送告警。

硬件与软件变化报警

终端上线后自动采集硬件清单（CPU、内存、硬盘、网卡、外设）与已安装软件清单作为基线。发生新增硬件、更换硬盘、加装网卡、卸载安全软件、私自安装未授权程序等变化时，实时告警并记录，保证资产台账与现场一致。

电脑使用权限管控

对员工可能改变终端安全状态的操作进行限制，包括但不限于：禁止修改 IP 地址与计算机名、禁止使用注册表编辑器、禁止打开控制面板关键项、禁止添加与删除网络连接、禁止安装未授权驱动、禁用命令行敏感指令。

上述限制均按岗位差异化配置，不影响正常办公。

补丁管理

集中检测终端操作系统与常用办公软件的补丁缺口，按部门制定补丁下发计划，减少勒索病毒与远程漏洞利用对汽车内网的威胁，同时避免业务网因补丁兼容性问题受影响。

设备准入控制

所有接入企业内网的终端必须先经过安全检查：是否安装客户端、是否开启杀毒、补丁是否达标、是否存在违规软件。不满足基线的终端被引导至修复区，达标后才能访问业务系统，防止外来设备与个人笔记本直接进入内网横向移动。



五、方案优势

- 一体化交付：上网、外设、加密、报警、补丁、准入在同一客户端与同一控制台完成，避免多套安全软件叠加造成的冲突与运维成本。
- 策略联动：敏感识别、外发审批、终端阻断与告警形成闭环，识别结果直接驱动后续动作，而非仅做记录。
- 分级部署：支持按办公网、研发网、生产网分区分域下发策略，新增工厂、新入职员工可快速纳入管理。
- 轻量化运维：客户端安装包约 80M，策略全开内存占用一般不超过 100MB，资源占用是同类产品中最低。

六、方案价值

- 管理价值：将终端安全从制度要求转化为可执行、可考核的策略，安全部门对全公司终端状态实现可见、可控。
- 业务价值：保护研发图纸与工艺资料不外流，保障供应链协同中的数据可控，避免因泄

密事件导致的项目损失与客户索赔。

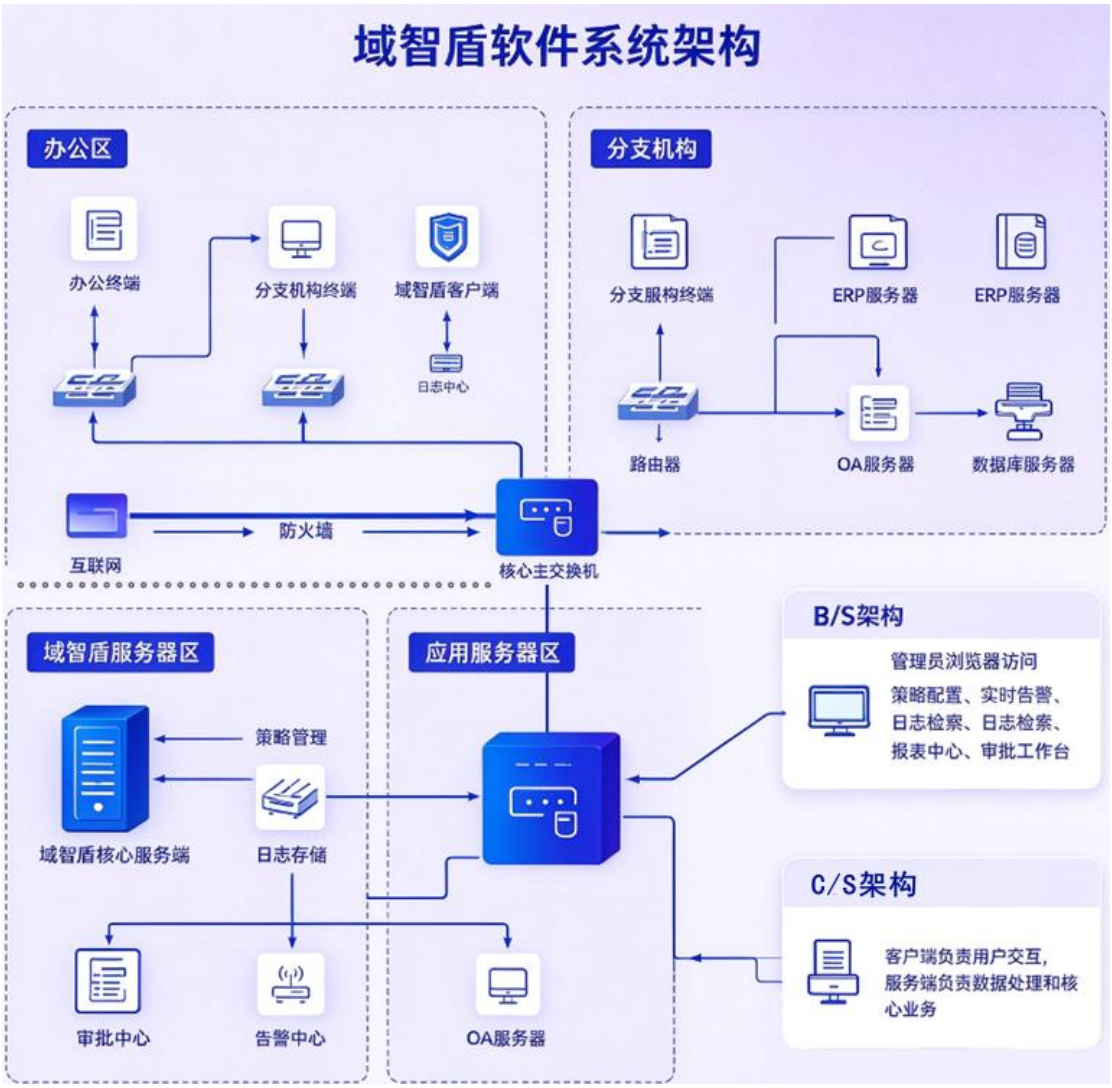
- 合规价值：满足《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》以及汽车数据安全管理相关规定对终端数据处理与日志留存的要求。
- 效率价值：外发审批、补丁分发、资产盘点等日常工作线上化，减少安全与团队的重复劳动。
- 风险价值：单点泄密不致整批数据流出，勒索病毒与漏洞利用可被提前阻断，事件发生后可在小时级完成定位与处置。

七、系统架构

系统采用双重架构结构，分别为：

B/S 架构（浏览器/服务器模式），提供策略配置、实时告警、日志检索、报表中心与审批工作台，管理员通过浏览器访问。

C/S 架构（客户端/服务器模式），客户端负责用户交互，服务器负责数据处理和核心业务。



八、公司产品简介

域智盾软件长期专注于终端安全与数据防泄漏领域，面向制造、汽车、能源、建筑、金融等行业提供终端一体化安全管理产品。产品覆盖上网行为审计、终端外设管控、文件透明加密、敏感数据识别、补丁分发与设备准入等能力，已在多家整车厂、零部件供应商与研发型企业落地。

河北中视新研软件开发有限公司，坐落于河北省石家庄市，聚焦终端安全技术自主创新，自研域智盾软件，问世十余年，始终坚持以合规为底线，持续迭代产品能力，提供从前期调研、方案设计、试点部署、上线运维、售后保障的全过程服务，联系方式：400-097-8770。

官方网站 yzdsaas.com

电话：400-097-8770

地址：河北省石家庄市

——以终端为落点，覆盖研发、生产与供应链全场景

域智盾软件®