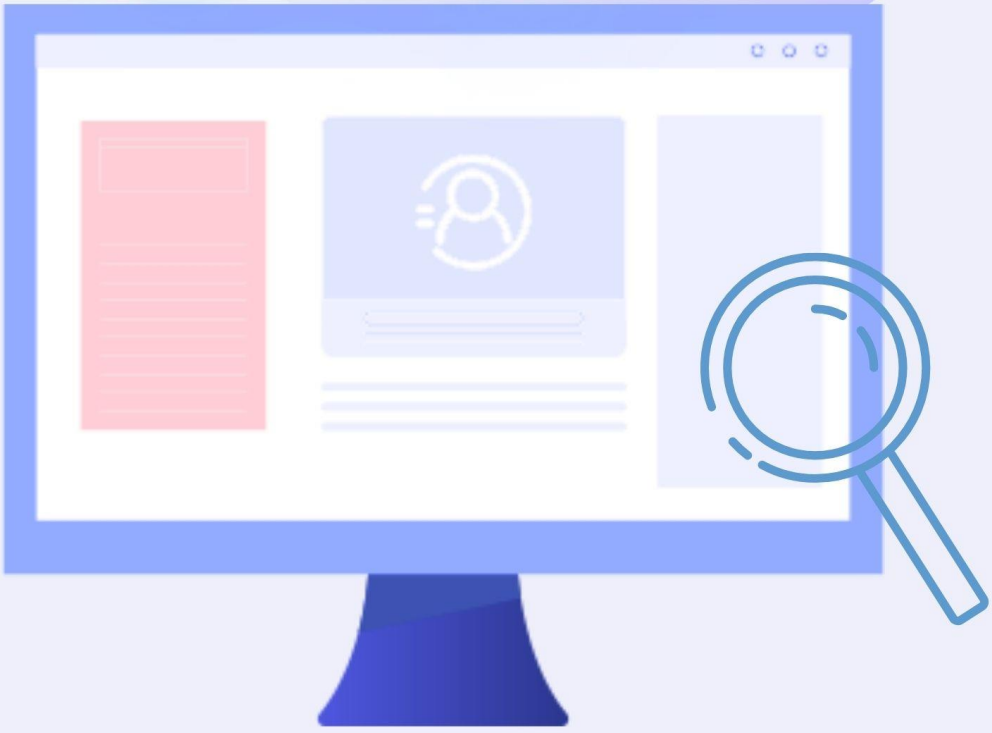
域智盾软件®

半导体行业

数据防泄漏&终端安全管理解决方案



CONTENTS/目录

01 项目背景 ---------- 3

02 方案概述 ---------- 3

03 典型场景防护设计 ---------- 4

04 实际效益 ---------- 9

05 架构概览 ---------- 9

06 公司简介 ---------- 10

一、项目背景

半导体行业核心资产以 IP 核、GDS 版图、PDK 工艺库、Verilog/VHDL RTL 代码、仿真工程、测试向量、良率数据、设备工艺参数、流片资料为主，文件体量巨大、专业格式特殊、研发协作链条长,业务场景与通用办公场景差异明显,衍生出大量区别于普通制造业的安全痛点：

- 核心数据资产价值高、格式特殊，通用加密产品兼容性不足；
- 人员结构复杂，并行项目多，多方协作带来跨主体数据泄露风险；
- 内网环境复杂，多类型终端、集群、哑终端增加管控难度；
- 风险识别依赖人工巡检，缺少针对高风险行为的自动告警，违规行为发生后不能及时干预；
- 终端基础安全与防泄密割裂，多个平台独立运行，策略容易冲突，形成防护短板；
- 行业监管要求叠加，需要满足《中华人民共和国数据安全法》《集成电路布图设计保护条例》、网络安全等级保护、出口管制、行业数据安全规范等多重要求。

上述风险点相互交织，单一安全产品或零散管控手段难以形成完整防护闭环，无法兼顾业务连续性、知识产权保护与多维度合规要求。

基于此，本项目部署域智盾软件，面向芯片研发全流程搭建适配半导体业务场景的安全管控方案，对核心敏感数据实施全链路防护，平衡安全管控与研发作业效率，满足行业监管与知识产权保护需求。

二、方案概述

域智盾软件采用统一管理架构，支持私有化部署，集文件透明加密、细粒度权限管控、外设端口管控、应用与网络管控、屏幕安全防护、敏感内容识别、外发审批、终端准入、主机基线加固、全链路审计等模块，兼容 Windows、Linux、Mac、信创系统，适配半导体研发工位、洁净车间终端、外协远程接入、外勤办公终端等差异化管控场景。

策略可根据项目周期、外协合作周期动态调整，兼顾半导体项目迭代快、多方协同复杂的业务特征，在不改变研发人员原有作业习惯、不降低研发效率的前提下，持续降低集成电路核心知识产权泄露风险，形成适配半导体产业特性的终端安全与数据防泄漏常态化管控体系。

三、典型场景防护设计

以下五个场景覆盖了半导体企业最常见的数据外流与终端失控路径。

1.内部人员主动泄密

工作情形：部分人员在转岗、离职前，将多个项目的 GDSII 文件、验证脚本从设计服务器批量复制到本地工作目录，再通过个人邮箱附件发到私人邮箱。这类行为往往发生在离职面谈之前，HR 与 IT 在泄密发生阶段才被通知，原始数据已经离开企业环境。

防护设计

- 加密剪贴板

当用户从加密文档中复制内容，粘贴至其他非授权程序、外部应用时，内容无法正常识别，会被替换为“您复制的内容已被加密处理”。

- 文件自动加密

当用户新建、保存、另存文件时，文件会自动完成加密，无需人工手动加密操作，脱离受控环境，文件变为乱码状态。同时，支持落地加密、全盘批量加解密、智能加密、只解密不加密、只读、不加密等多种模式，适配不同场景下的安全防护。

- 邮件防泄密

支持邮件外发精细化管控，基于发件人、收件人、邮件关键词设置过滤匹配条件，实现非合规邮件外发拦截，管控邮件外传风险。

针对正常合作交流，可以开启邮件白名单，将信任用户添加至白名单内，发往该邮箱的文件会自动解密，满足合规业务对外邮件交付需求。



2.工程师向外部供应商发送敏感文件

工作情形：举例，工程师电脑上有 10000 份文件，当需要把良率分析报告发给外设备厂商做技术对接时，会不会携带机密资料呢？

防护设计

➢ 文件外发包

支持对加密文件制作受控外发包，可自定义设置文件有效期、打开次数、打开密码、背景水印等信息。外发包脱离企业受控环境后仍受权限约束，可防止交付文件被二次转发、随意扩散，兼顾供应链协同业务与知识产权防护。

- 有效期设置：可设定外发包的生效截止时间，到达预设有效期之后，合作方将无法继续打开文件。
- 打开次数限制：可自定义允许打开的最大次数，达到设定打开次数后文件自动锁定。
- 打开密码：制作外发包时可设置独立打开密码，外部接收方需要输入正确密码才可访问文件。
- 背景水印：支持在外发包页面叠加自定义背景水印，用于泄密事件溯源取证。



➢ 敏感信息设置

敏感信息报警：支持企业自定义敏感词库，可录入“客户名单”、“机密” 等自定义关键词，当终端触发预设敏感词规则时，系统即时弹窗告警，并同步推送告警通知至管理员，实现涉敏行为实时预警。

敏感文件：展示识别出的所有敏感文件，记录信息包含客户端、所属部门、文件名、文件存储路径、命中敏感词、文件详情、文件修改时间，便于管理人员统一查看涉敏资产分布。

敏感文件审查：支持新建敏感文件审查任务，完成任务参数配置后，系统自动对终端存量文件执行批量审查。任务台账记录任务名称、任务创建时间、发起人、执行状态、任务总项数、已完成数量、审查关键词、涉敏命中情况，支撑企业定期开展存量涉密资产排查。

- 文件操作审计

完整留存文件新建、打开、修改、复制、剪切、删除、重命名、拷贝、打印等操作，日志集中存储且不可篡改，为安全事件溯源、合规核查提供依据。

3.多通道外传：U 盘、个人手机、即时通讯、打印

工作情形：企业存在多种旁路泄密通道，包含 U 盘、移动硬盘、微信、QQ、网盘、邮箱、手机拍照、打印等。单一文件加密无法覆盖全部外传通道，形成防护缺口，尤其半导体版图、工艺参数可通过打印、屏幕翻拍方式绕过文件加密管控。

防护设计

- U 盘管控

可以设置 U 盘的使用权限，比如禁止使用、仅读取、仅写入、允许使用等；

此外，还可以管控 USB 无线网卡、PCMCIA、光驱、刻录、蓝牙、红外、串口、并口、1394 设备、便捷式设备。

- 终端防拍照

对工位屏幕区域的手机拍摄行为进行实时检测，当识别到手机对准电脑屏幕进行拍摄时，系统将自动执行终端锁屏处置，阻断屏幕翻拍泄密行为。

模块支持自定义置信度阈值配置，管理员可根据业务场景灵活调整识别灵敏度：调高置信阈值，仅在高置信度确认存在拍照行为时才执行锁屏，降低误触发概率；调低置信阈值，一旦识别到疑似拍照行为立即执行锁屏。

- 程序外传管控

识别并拦截指定程序（企业微信、QQ、网盘、浏览器）的文件传输动作。

- 文档检测大屏

将所有事件统一汇入控制台告警中心，安全团队在一个界面上看到当天发生的全部外传动作，具体包括外传文件分类分布、文件趋势情况、外传文件途径分布、泄密事件详情描述等。



4.资产账实不符

工作情形：半导体企业终端数量大、人员流动频繁，IT 部门维护的资产台账与现场实际设备存在偏差，无法快速回答“这台电脑是谁的、装了什么软件、最近有什么变更”。

防护设计

- 基本信息

自动统计终端电脑的基本信息，包括操作系统、处理器、内存、主板、显卡、存储器、光驱驱动器、音频、网络等。

- 软件资产统计

自动采集全网终端已安装软件清单，统一汇总软件名称、版本号、发布厂商、安装数量、安装占比、安装包信息等资产数据，形成软件资产台账。支持右键操作，可执行软件信息删除、全网批量卸载指定软件、查询安装该软件的客户端，辅助管理员完成软件资产巡检与统一治理。

- 硬件资产统计

包含客户端名称、IP 地址、MAC 地址、操作系统、系统产品 ID、主机出厂日期、主机厂商、主机型号、硬盘容量、硬盘序列号、CPU 型号、内存容量，自动生成硬件资产台账，实现终端硬件资产可视化。

- 变更实时告警

硬件变更（新增硬盘、更换网卡、外接设备）与软件变更（安装新软件、卸载安全代理）实时上报，IT 在控制台直接看到资产变化。

5.违规软件与外来终端带来的安全事件

工作情形：员工在工作电脑上私自安装破解软件、远程控制工具、挖矿程序；外来设备（厂商笔记本、个人电脑）临时接入研发网，带入病毒或被横向利用。这类事件往往先由业务中断、数据异常被发现，事后倒查才发现源头是一台被忽视的终端。

防护设计

- 对终端上运行的程序做黑白名单控制，未经允许的软件不得启动，远程控制工具、P2P 下载工具默认拦截。
- 终端补丁集中下发，操作系统与常用业务软件的补丁缺口在控制台一目了然，避免长期暴露在已知漏洞下。
- 外来设备接入内网前必须经过准入认证与安全检查，未认证终端被隔离到修复区，仅可访问补丁与修复资源，无法直接访问内部网络。
- 违规外联、私改 IP、私接热点、安全代理被卸载等动作实时告警，安全团队在事件发生当天介入。



四、实际效益

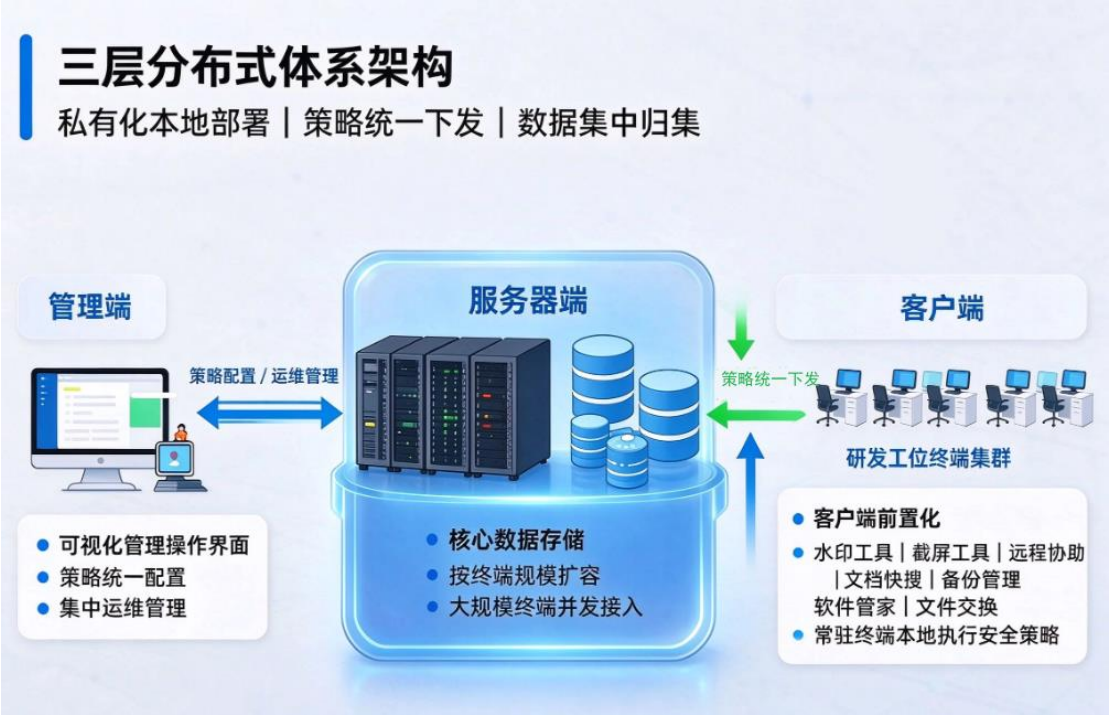
- 数据侧：核心数据全程加密，单点拷贝、拍照、外发不致整批数据外流。
- 合规侧：可直接对接客户审查、行业监管与等保测评，减少团队在材料整理上的重复投入。
- IT 运维侧：资产台账自动更新，补丁分发与软件管控集中完成，IT 部门从“被动响应工单”转向“主动发现异常”。
- 人员管理侧：离职、转岗、外包结束当日自动回收权限，避免在人员变动环节留下数据外流窗口。
- 事件响应侧：发生疑似数据外泄事件时，可秒级完成“谁、在什么时间、对哪份文件、做了什么动作、通过哪个通道”的完整还原。

五、架构概览

平台采用管理端、服务器端、客户端三层分布式体系架构，支持私有化本地部署，各组件职责独立、协同联动，策略统一下发、数据集中归集，可适配半导体企业多部门、多项目组、大规模研发工位的终端安全管控场景。

方案组成：

- 服务器端：负责存储核心数据，可根据终端规模扩容，支撑大规模终端并发接入。
- 管理端：提供可视化管理操作界面，实现全网终端安全策略统一配置与集中运维管理。
- 客户端：支持客户端前置化，提供水印工具、截屏工具、远程协助、文档快搜、备份管理、软件管家、文件交换，常驻终端本地执行管理端下发的安全策略。



核心优势：

- 统一策略引擎、统一数据库，降低管理员运维成本。
- 不改变研发人员原有作业习惯，保障芯片设计业务稳定运行。
- 界面简洁、功能清晰、操作简单、易用性强，节省用户学习成本。
- 策略可随项目周期，既实现跨项目越权访问防控，又不会对全部终端执行统一强管控。
- 支持本地私有化部署，不依赖公有云，适配数据安全法、出口管制、布图设计保护条例等合规要求。

六、公司简介

河北中视新研软件开发有限公司，总部位于石家庄，是国内专注于终端安全与数据防泄漏领域的软件企业。公司核心团队来自一线安全厂商，拥有自主研发的加密技术、敏感识别引擎与终端管理平台，旗下“域智盾软件”产品已在金融、半导体、医疗、汽车、能源等行业落地，服务客户覆盖上市企业、集团总部与关键信息基础设施相关单位。

公司交付的不是一套软件，而是一套可以让客户安全负责人在监管检查、客户审计、事件复盘时拿得出手的策略文档、审计记录与处置流程。客服热线 400-097-8770。

官方网站 yzdsaas.com

电话：400-097-8770

地址：河北省石家庄市

域智盾软件®