域智盾软件®

IC设计行业

数据防泄漏解决方案



CONTENTS/目录

01 项目背景 ---------- 3

02 面临问题 ---------- 4

03 需求分析 ---------- 5

04 解决方案 ---------- 6

05 方案价值 ---------- 11

06 系统架构 ---------- 12

07 公司简介 ---------- 12

一、项目背景

1.1 行业现状

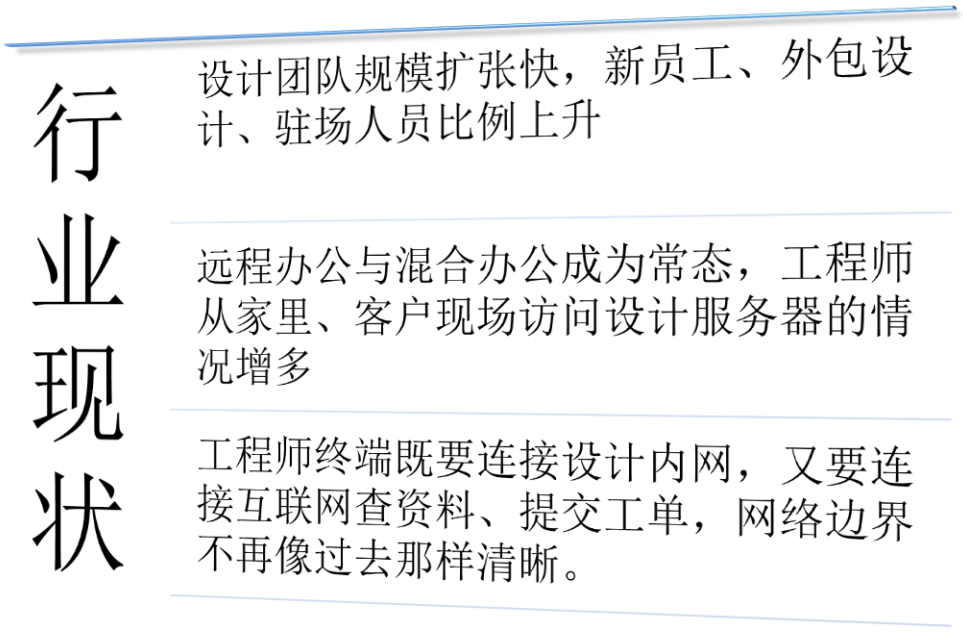
IC 设计行业是典型的知识密集型行业，企业的核心资产集中在代码、版图、网表、验证环境、工艺库、设计规格书与客户交付文件。一款芯片的设计周期往往持续数年，团队从前端设计、验证、后端版图、时序收敛到流片、封测需要多部门协同，外部还涉及晶圆厂、封测厂、IP 授权方、EDA 工具供应商与客户。

随着国内 IC 设计企业数量快速增长，行业内同时出现几个明显趋势：

一是设计团队规模扩张快，新员工、外包设计、驻场人员比例上升；

二是远程办公与混合办公成为常态，工程师从家里、客户现场访问设计服务器的情况增多；

三是工程师终端既要连接设计内网，又要连接互联网查资料、提交工单，网络边界不再像过去那样清晰。



在这样的环境下，设计数据外流的路径不再只是“有人把文件拷走”，还包括：外发到公共仓库、通过聊天工具外传、外包人员泄密、远程打包等。

1.2 相关法律条文

IC 设计企业作为数据处理者与关键信息基础设施相关行业参与者，需要对齐以下法律法规

与标准要求。

法律层面

- 《中华人民共和国网络安全法》：按等保要求履行安全保护义务，核心落地点是日志留存不少于六个月、重要数据备份与加密。
- 《中华人民共和国数据安全法》：重要数据处理者须明确数据安全负责人和管理机构。
- 商业秘密与软件著作权：源代码与设计文档首先定性为商业秘密(《反不正当竞争法》)，自主研发软件可依《计算机软件保护条例》主张软件著作权。防泄漏系统的加密、外发审批、行为审计功能直接服务于商业秘密“保密性”要件的维持与侵权追溯。

国家标准与行业要求

- GB/T 22239-2019 第三级：需映射身份鉴别、安全审计、数据保密性、集中管控四项控制项。

NDA 中的保密与审计配合条款

- IC 设计企业与晶圆厂、封测厂、IP 供应商及客户签署的保密协议，通常约定：设计数据的保密范围与使用限制、交付物的使用边界、以及安全事件发生后的审计配合义务。

二、面临问题

- 外发通道分散：邮件、即时通讯、个人网盘、代码托管平台、U 盘、手机、打印构成多条外流路径，安全团队无法同时监控。
- 外包与驻场人员管理薄弱：外包设计工程师接入企业环境后，访问范围、项目边界、离场回收缺乏技术手段，主要靠合同约定。
- 软件合规风险突出：工程师在工作电脑上安装未经授权的 EDA 破解工具、盗版设计软件、远程控制软件，既带来合规风险，也引入病毒与后门。
- 资产台账与现场不一致：IC 设计企业终端更新换代快、服务器与工作站混布，IT 部门对“网络里有什么设备、装了什么软件、谁在用”缺乏实时视图。
- IT 运维压力大：几百到上千台设计终端的补丁、软件分发、远程协助、资产盘点依赖人工逐台处理，效率低且容易遗漏。
- 事件发生后无法快速定位：发生疑似数据外流时，IT 与安全部门无法快速溯源泄密者。

三、需求分析

面对上述真实现状，企业在规划数据防泄漏与终端管理体系时，需要先回答几个问题：

- 如何满足相关法律法规的要求？
- 如何找出所有敏感文件？
- 如果有人批量拷贝文件，企业是否能在当天发现？
- 本公司有多少台终端、分别在哪些部门、装了哪些软件、有多少台长期未打补丁？
- 发生一起疑似数据外流事件时，从告警出现到完成定位、止损、举证，需要多长时间？

这些问题指向的不是某一款单点工具，而是一套覆盖数据、终端、行为与运维的体系。围绕 IC 设计行业的真实工作方式，企业至少需要在以下几个方面获得针对性能力：

- 设计数据本身在终端侧可控可读、离开授权环境即密文。
- 外发与外传通道可识别、可阻断、可审批、可追溯。
- 外包、远程、离职等人员变动场景前置管控，而不是事后追查。
- 软件合规、上网行为、终端资产与 IT 运维在同一套体系中完成，不再叠加多套工具。



四、解决方案

4.1 方案概述

域智盾软件由服务器端、管理端与客户端三部分组成。服务器集中管理策略、存储审计日志；管理端向安全、IT、合规管理员提供统一的操作界面；客户端部署在员工电脑上，执行管理端下达的策略。

4.2 IC 设计数据防泄漏

4.2.1 文件透明加密

对 RTL、GDSII、LEF/DEF、网表、验证脚本、工艺库、设计规格书等指定格式文件，自动加密。员工日常打开、编辑、提交的操作方式不会发生改变，文件一旦被复制到 U 盘、个人目录、文件传输助手，即为乱码，无法打开。

针对大文件，可以将其放入沙箱内存储（在电脑上划分一个虚拟安全空间），沙箱内文件呈不加密状态，故而不会影响操作流畅度；将文件移至沙箱外，文件呈加密状态，在不影响操作流畅度的同时，实现文件的高安全保护。

4.2.2 划分安全区域

按项目组、部门、外包团队划分不同安全区域。

A 项目组文件只有本组成员可以查看，其他项目组即便私存也无法打开查看。

问题：如何让 A 项目组的文件 B 项目组能看，但是 B 项目组的文件，A 项目组看不到？

解决方案：设置密级即可，B 项目组用“绝密”级别，A 项目组用“秘密”级别，即可实现这一效果。

4.2.3 异常行为报警

当终端检测到短时间内大量文件被拷贝、被打印时，实时向安全团队推送报警。

4.2.4 外发通道立体管控

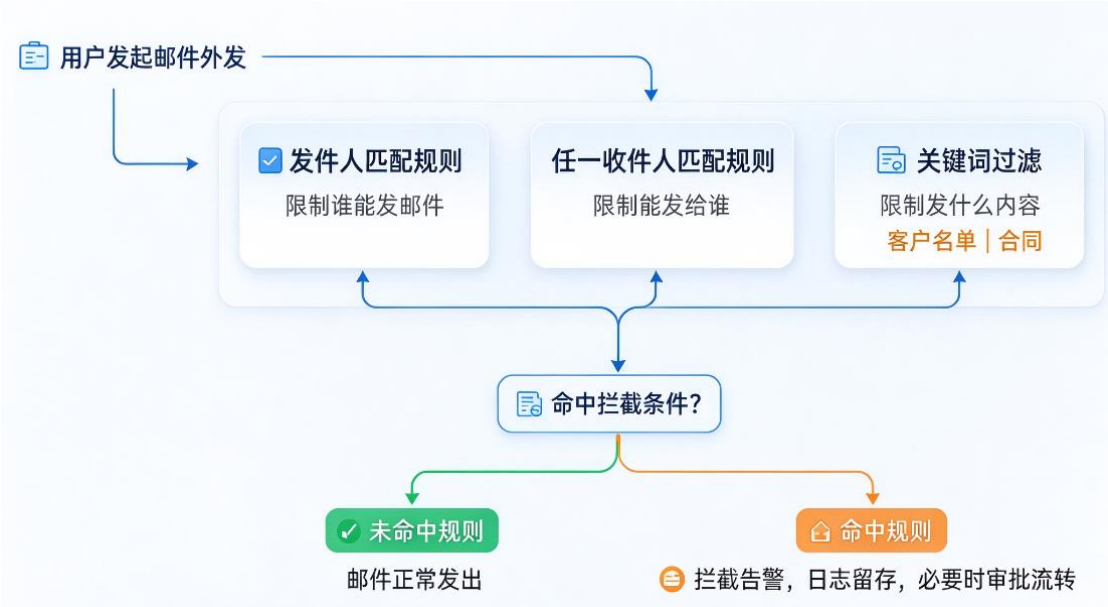
- 邮件外发

通过发件人匹配规则、收件人匹配规则或关键词过滤，细化拦截条件，限制特定类型的邮件发送行为。

发件人匹配规则：限制谁能发邮件；

任一收件人匹配规则： 限制能发给谁；

关键词过滤：限制发什么内容，比如禁止发送含“客户名单”、“合同”等词的邮件。



- 应用程序

可以禁止指定程序发送文件，将微信、QQ、网盘、浏览器、钉钉等程序添加进库，用户无法通过这些程序外传文件。

外发审批：确需对外发送的文件，需要走审批，待管理员通过后，方可正常外发。

- HTTP 上传文件控制

工作模式有两者，分别是禁止以下 URL 上传、允许以下 URL 上传，目的是限制网页端的上传操作。

- 防删除、篡改文件

设置文件操作权限，比如禁止新建、删除、重命名、拷出、拷入、移出、移入。

设置文件自动备份，备份模式有文档删除时备份、文档修改时备份、手动备份等，可以快速找回删除、篡改的文件。

4.2.5 多种水印类型

包括文字水印、点阵水印、图片水印、二维码水印，即使被手机翻拍也可定位责任人。

4.2.6 离线与远程办公管控

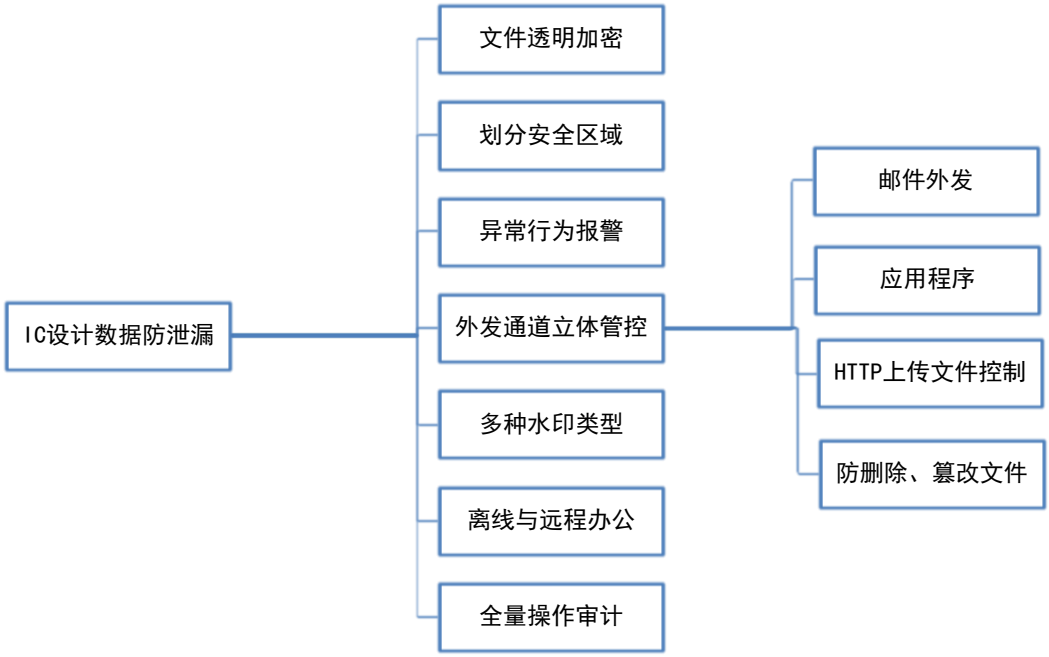
员工居家办公、出差时，终端上的加密策略与文件权限继续生效，在指定时间内可正常打开加密文件，超时无法访问。

4.2.7 全量操作审计

对设计文件的打开、编辑、另存、复制、外发尝试、打印、删除动作进行全量记录，按员工、

项目、终端、文件、时间形成可检索的审计日志，留存周期按企业合规要求配置。

即便是断网，也会记录相关操作，待重新联网后自动同步最新策略与审计记录，不影响工程师继续工作。



4.3 终端操作行为管理

4.3.1 软件合规管理

支持对 Windows 软件、Linux 软件及安卓应用进行统一资产盘点，覆盖终端软件的安装与运行状态。

可查看软件名称、版本号、所属公司、安装率、安装数量及安装包等关键信息。

支持右键操作：删除软件信息、发起全网卸载、查看安装该软件的客户端列表。

4.3.2 企业软件库

管理员可将经过安全检测的软件安装包上传至企业软件库，员工仅能通过软件库安装程序，阻断官网、应用商店等外部下载渠道，从源头降低私自拷贝安装包带来的盗版与病毒风险。

4.3.3 上网行为管理

支持配置网站黑白名单策略，对终端可访问的网站范围实施精细化管控。白名单模式下仅允许访问指定网站，黑名单模式下阻断指定网站访问，两种模式可按部门或终端灵活启用，有效限制与工作无关的网络访问，降低恶意站点与数据外传风险。

4.3.4 办公效率分析

在不侵犯员工个人隐私的前提下，按部门、按岗位统计终端使用时长、应用使用分布、上网类别分布，输出时间画像、效率概览，帮助部门负责人识别软件使用不均衡、利用率不足等管理问题，为后续采购与人员配置提供数据参考。



4.4 全网资产管理

IC 设计企业的资产盘点难点在于：

- 工作站、服务器、办公终端、临时接入设备混杂；
- 工作站硬件配置高、更新换代快；
- 外包与访客设备频繁临时接入。

解决方案

自动资产发现：所有接入企业网络的终端自动识别并入库，记录 IP、MAC、操作系统、硬件配置、所属部门、使用人。

硬件变更感知：硬盘更换、内存加装、网卡变更、外接设备长期接入等动作实时上报，资产台账与现场状态保持一致。

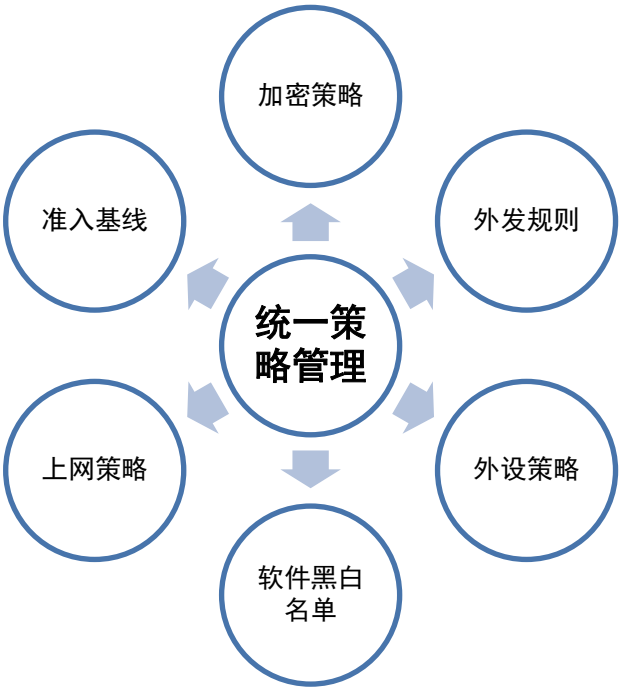
软件资产盘点：自动采集终端上安装的软件清单，包括软件名、版本号、公司、安装率、安

装数、安装包等。

4.5 IT 高效运维

4.5.1 统一策略管理

加密策略、外发规则、外设策略、软件黑白名单、上网策略、准入基线全部在同一控制台配置，按部门、岗位、项目组差异化下发，避免在多套工具之间切换。



4.5.2 批量软件与补丁分发

- 批量软件分发

支持按部门、终端组或指定客户端进行批量软件推送与卸载，无需逐台远程操作或跑现场。

典型场景包括：新工具全员补齐安装、特定部门定向推送、统一推送标准版本等。

- 补丁分发管理

后台一键扫描全网终端，统计已安装与未安装补丁清单，按高危、重要、可选等级别筛选需要下发的补丁。

分发时可自定义策略：指定部门或终端范围、设置安装时间段或弹窗提醒。

4.5.3 远程协助与终端维护

- 远程协助

远程连接提供多种模式，管理员按实际需求选择：

交互模式：双方均可操作，适合手把手教员工操作或协同排障；

旁观模式：仅查看屏幕，不干扰被控端操作，适合巡检或先观察再决定是否介入；

兼容模式：适配不同系统环境或老旧设备，提升连接稳定性；

独占模式：管理员独占操作权，被控端无法操作，专治紧急故障或需要连续操作的场景；

无人值守：第一次需要员工同意，之后不需要。

- 终端维护

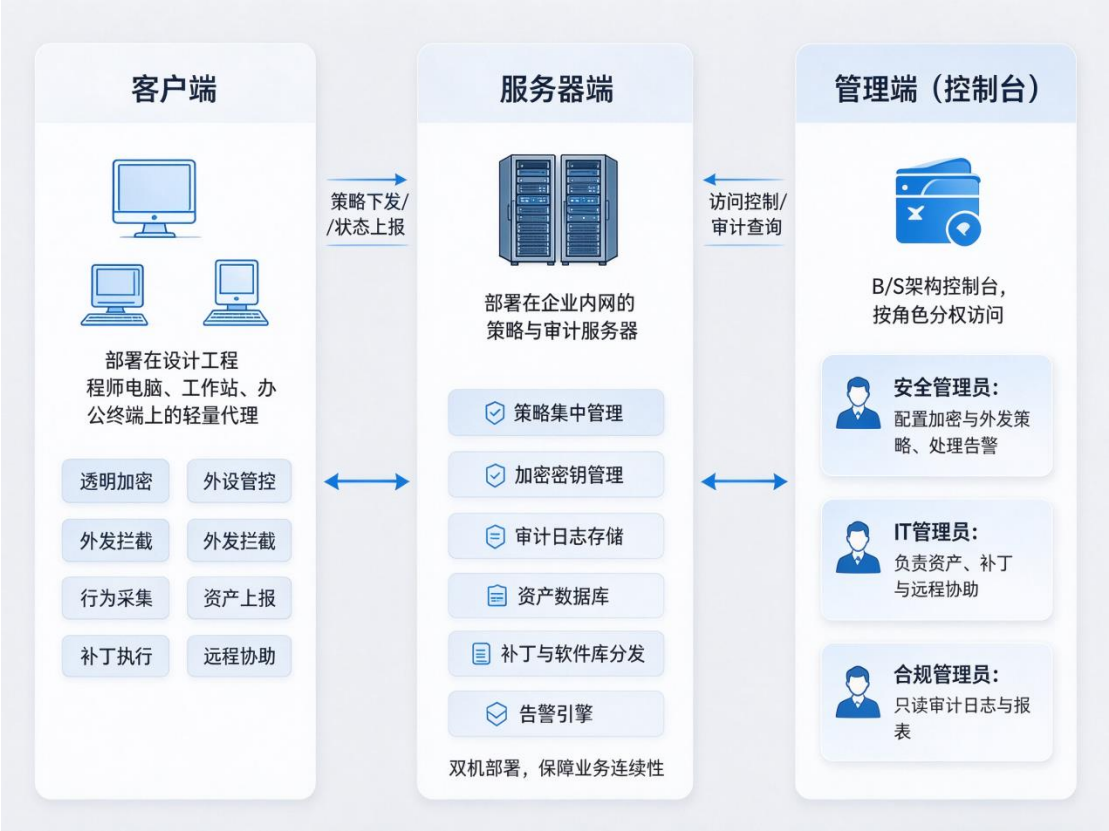
远程操作：支持远程关机、重启、锁定计算机，若终端支持网络唤醒，管理员可在软件内发送开机指令，无需到工位操作；

关键信息安全：禁止修改 IP 地址、MAC 地址，避免因私改 IP 引发的地址冲突，以及通过换 IP 绕过上网策略、访问受限资源的行为。

五、方案价值

- 泄露追溯从“查几天”压缩到“小时级”，追溯过程不依赖多系统日志拼凑；
- 高风险场景前置拦截，权限跟着组织走，不依赖人工逐项清理；
- 核心设计资产锁定在受控边界内，设计文件自创建起即处于加密状态，离开授权环境后无法正常打开；
- 把法条要求翻译成可举证的技术动作，面对监管检查或客户审计，可直接导出策略清单与操作记录，而非临时补材料；
- 运维动作收敛到一个界面，资产盘点、补丁分发、软件部署、远程排障不再分散在多个工具中切换；
- 安全数据反哺管理决策，哪些软件长期闲置、哪些网站占用工时、哪个部门终端风险集中，采购审批与团队管理有了可量化的参照。

六、系统架构



七、公司简介

河北中视新研软件开发有限公司，自成立起便锚定终端安全与数据防泄密赛道。

➢ 十余年研发积淀，兢兢业业的奋斗史

从驱动层加密引擎的第一行代码写起，研发团队在终端安全领域持续投入十余年，产品从单一的文件加密工具，逐步扩展为覆盖上网行为审计、终端安全管理、文件透明加密、网络准入控制的完整体系，每一次版本迭代都踩在客户实际需求与合规要求的变化节点上。不追求概念先行，而是把驱动层稳定性、EDA 工具兼容性、大规模终端并发管理这些“硬骨头”逐个啃下来。

➢ 3000000+终端稳定运行，与时俱进的辉煌史

累计支持超过 300 万台终端稳定运行，是十余年研发投入与现场打磨叠加出的结果。等保 2.0 落地时，审计留存与身份鉴别能力同步补齐；数据安全法实施后，分类分级与重要数据

管控模块跟进；信创替代推进中，国产操作系统与国密算法适配按期交付。三百万终端的持续运行，既是规模数字，也是十余年“兢兢业业做产品、与时俱进跟需求”的注脚。

如需进一步了解公司产品，或希望结合自身终端规模与合规要求做针对性评估，欢迎拨打客服热线 400-097-8770，由专人对接沟通。

