NSecsoft
安在软件

芯片研发集成电路设计企业
数据防泄密安全保护方案

目录

01

项目背景

数据安全挑战

集成电路（IC）设计行业作为国家战略性新兴产业的核心，是信息技术产业的基石。近年来，随着全球科技竞争的加剧和国家对集成电路产业的空前重视，中国IC设计企业迎来了快速发展的黄金时期。然而，伴随产业的蓬勃发展，IC设计企业所面临的数据安全挑战也日益严峻。这些企业以知识产权为核心竞争力，其研发投入巨大，技术成果高度集中于芯片设计图纸（EDA文件）、源代码（如RTL代码、验证环境）、工艺制程数据、仿真验证结果以及流片文档等高价值数字资产。一旦这些核心数据发生泄露，不仅可能导致企业数亿甚至数十亿的研发投入付诸东流，更会严重损害企业的市场竞争力、商业信誉，甚至威胁国家信息安全。

当前，IC设计企业的数据防泄密需求呈现出以下特点：

1. 核心资产价值极高：芯片设计文件、源代码、工艺文档等是企业的生命线，其价值密度远超一般行业，任何形式的泄露都可能带来毁灭性打击。

2. 研发流程复杂且工具链多样：IC设计流程涉及数十种专业EDA工具，这些工具生成的文件格式各异，且数据流转频繁，传统安全方案难以无缝集成和有效管控。

3. 内外部协作频繁：设计、验证、流片、封装测试等环节常涉及与第三方IP供应商、代工厂、测试服务商等外部伙伴的紧密协作，数据外发需求多，供应链安全风险突出。

4. 人员流动性大且权限管理复杂：研发人员是核心数据的创造者和使用者，其高流动性、离职风险以及复杂的权限管理，使得内部泄密成为一大隐患。

5. 新兴技术带来新风险：生成式AI等新技术的应用，在提升效率的同时，也可能无意中将敏感设计片段输入公共系统，或在内部训练模型中“记忆”并重建敏感数据。

面对上述挑战，构建一套精准、高效、合规的集成电路设计企业数据防泄密安全保护方案，已不再是可选项，而是保障企业创新成果、商业机密及市场地位的战略性需求。本方案旨在通过引入先进的数据防泄漏技术和综合安全管理措施，从数据全生命周期角度，为IC设计企业提供全方位、深层次的数据安全防护，确保核心知识产权的机密性、完整性和可用性。

02

面临问题

集成电路（IC）设计企业在数据防泄密方面面临着多重复杂且严峻的挑战。这些问题不仅源于其核心数据资产的极高价值，也与行业特有的研发流程、人员管理以及技术环境紧密相关。以下是IC设计企业当前面临的主要数据安全问题：

1. 核心数据资产的高价值性与脆弱性

核心数据资产风险

IC设计企业的核心知识产权资产，如芯片设计图纸（EDA文件）、源代码（RTL代码、验证环境）、工艺制程数据、仿真验证结果以及流片文档等，是企业竞争力的核心基础。这些数据一旦泄露，可能导致企业数亿研发投入付诸东流，并严重影响市场地位。然而，这些高价值资产却异常脆弱：

- **明文存储风险：**多数IC设计企业的研发部门使用EDA、VCS、Design Compiler等专业工具进行开发，产生的源代码和设计文档多以明文形式存储在员工终端电脑上。这种存储方式使得员工可以轻松通过USB设备、网络传输等方式外发核心文件，企业几乎无法有效监控和阻断。

- **服务器数据暴露：**IC设计企业普遍使用SVN、GitLab等版本控制系统集中存储设计资料，员工仅凭账号密码即可自由访问并下载整套项目代码库。更重要的是，这些系统通常缺乏文件操作审计和防扩散控制，导致核心数据在下载后处于完全失控状态。

- **开发环境风险：**IC设计流程中涉及数十种专业工具，包括Pro/E（三维设计）、Ansys（仿真）、Cadence（布局布线）等复杂软件环境。这些工具生成的过程文件（如中间数据、日志）同样包含敏感信息，但往往被排除在传统数据保护方案之外。同时，编译后的可执行程序需要正常外发用于芯片烧录，这一关键节点若缺乏安全保护机制，极易成为数据泄露的突破口。

2. 员工操作与权限管控的复杂性

IC设计企业的核心知识产权资产，如芯片设计图纸（EDA文件）、源代码（RTL代码、验证环境）、工艺制程数据、仿真验证结果以及流片文档等，是企业竞争力的核心基础。这些数据一旦泄露，可能导致企业数亿研发投入付诸东流，并严重影响市场地位。然而，这些高价值资产却异常脆弱：

终端操作风险突出：

- **非合规渠道外发：**员工普遍通过私人邮箱、微信、QQ等非授权通讯工具传输设计图纸和代码片段。

- **移动存储滥用：**尽管多数企业禁止私人U盘使用，但员工仍可通过小型移动设备（如微型SD卡）轻易导出数GB的设计资料。研发人员为调试目的使用U盘拷贝代码至非授权设备的现象几乎成为行业常态。

- **物理泄密途径：**设计图纸被拍照外泄的事件频发，尤其是实验室和晶圆厂环境中的手机摄像行为，企业通常无法精准定位泄密源头。

- **烧录权限失控：**研发人员可随意通过COM口进行芯片烧录操作，缺乏操作审批与行为审计机制，使得未经验证的设计版本可能被烧录至芯片中带离公司。

权限管理困境：核心设计部门与其他部门（如测试、生产）之间的数据隔离机制普遍缺失，导致非授权人员可能获取并打开敏感设计文件。更严重的是，当员工岗位变动时，其历史访问权限往往得不到及时调整，形成“权限冗余”现象。

3. 技术环境与供应链的特殊挑战

技术环境与供应链挑战

IC设计企业面临的技术环境复杂性远高于普通行业，这为终端安全和数据安全带来了独特挑战。从工具链到设计方法学，再到供应链协作，每个环节都潜藏着特殊风险点。

- **开发工具链兼容性难题：**IC设计流程依赖数十种专业软件工具，涵盖从架构设计、RTL编码、逻辑综合到物理实现的完整链条。这些工具包括但不限于VisualHDL（架构设计）、VCS（仿真验证）、IC Compiler（布局布线）、Dracula（版图验证）等。每个工具生成的文件格式和进程行为各异，导致传统数据安全方案难以无缝集成：加密可能中断编译流程，管控策略可能阻碍仿真任务。某设计企业部署加密系统后，发现时序分析工具因无法读取加密中间文件而运行失败，严重延误了项目进度。

外包与供应链风险：

IC设计企业通常将EDA工具运维、IP验证、后端实现等环节外包给专业服务商，这创造了多个关键风险点。

- **EDA供应商远程接入：**如Synopsys、Cadence等供应商工程师需定期接入客户内网进行软件维护。传统VPN方式授予了过宽的访问权限，运维人员可能接触核心设计数据。

- **第三方IP整合：**设计过程中大量复用第三方IP核，这些组件可能包含未公开漏洞或后门。某头部企业发现，其使用的PCI控制器IP中存在隐蔽数据导出函数，可能泄露芯片内部状态。

生成式AI应用带来的新风险：

当工程师使用ChatGPT等工具优化Verilog代码或调试脚本时，可能无意中将设计片段输入公共AI系统。更复杂的是，企业内部训练的AI模型可能“记忆”并重建训练数据中的敏感设计模式。行业专家警告：“使用客户的设计数据准备训练集时，数据所有权边界变得模糊，AI生成的优化方案可能包含多个客户的IP特征”。

综上所述，针对集成电路设计企业的业务特点和核心数据资产，构建一套精准、高效、合规的数据防泄漏体系，已不再是“锦上添花”，而是保障其创新成果、商业机密及市场地位的战略性需求。

03

方案设计

芯片研发数据安全

针对集成电路（IC）设计企业面临的严峻数据防泄密挑战，本方案基于Ping32数据防泄漏解决方案的核心能力，结合IC设计行业的业务特点和核心数据资产，构建一套精准、高效、合规的数据安全防护体系。该方案旨在从数据全生命周期角度，实现对芯片设计数据（EDA文件、源代码、工艺数据等）的精准防护、实时响应与深度溯源，确保核心知识产权的机密性、完整性和可用性。

Ping32智能防护

智能防护是本方案的基础，通过在IC设计研发、测试和流片过程中，对核心数据进行源头控制和透明加密，确保数据在产生之初即具备安全属性，并贯穿其整个生命周期。这包括对芯片设计图纸、源代码、工艺制程数据、仿真验证结果等关键数字资产的保护。

1. 芯片设计文件与源代码透明加密

IC设计企业的核心知识产权高度集中在芯片设计文件（EDA文件）、源代码（如RTL代码、验证环境）及工艺文档中。这些文件是企业研发投入的结晶，一旦泄露将造成巨大损失。Ping32采用驱动级透明加密技术，确保这些核心资产的安全。

- **EDA文件实时无感知加密**：针对IC设计研发部门广泛使用的EDA工具（如VCS、Design Compiler、VisualHDL、Cadence、Synopsys等），Ping32透明加密技术能够对这些工具创建的各类设计文件（如.hfss, .ads, .cadence等）进行实时、无感知加密。当研发人员在授权环境下访问这些文件时，系统自动解密，不影响其正常使用和操作习惯。一旦加密文件离开授信环境（即未安装加密客户端的电脑），通过U盘、网络等方式传输到外部环境，打开时将显示为乱码，从而有效保护了核心设计文件的安全。

- **源代码加密防护**：对于RTL代码、验证环境等源代码文件，Ping32确保研发人员在编写、编辑和保存时，文件自动加密。这使得研发人员可以保持原有的编码习惯，如新建文件、编辑、保存，即可实现源代码文件的加密。文件一旦离开安装加密客户端的电脑，在外部环境中将无法正常查看，有效防止源代码泄露。

- **工艺文件加密**：对工艺制程数据、PDK（Process Design Kit）等关键工艺文件进行加密保护，确保这些敏感数据在存储和流转过程中的机密性。

2. 代码库与设计资产安全管理

IC设计企业的核心知识产权高度集中在芯片设计文件（EDA文件）、源代码（如RTL代码、验证环境）及工艺文档中。这些文件是企业研发投入的结晶，一旦泄露将造成巨大损失。Ping32采用驱动级透明加密技术，确保这些核心资产的安全。

- **上传下载加密解密：**针对基于B/S（浏览器/服务器）或C/S（客户端/服务器）架构的代码库和资产管理系统（如GitHub、SVN等），Ping32部署解密网关。当研发人员从代码库下载源代码或设计文件到本地终端时，文件将自动加密；当加密文件需要上传到代码库进行版本管理或共享时，系统将自动解密。这保证了代码库中的文件始终保持明文状态以便正常使用，而下载到本地终端的文件则受到加密保护，有效防止了本地文件失控导致的数据外泄。

核心文档
加密保护

- **权限精细化管理：**结合企业现有的身份认证和权限管理系统，Ping32可实现对代码库和设计资产的精细化访问控制。例如，可以限制特定人员只能下载加密文件，而无权上传或修改；或者根据项目组和角色，分配不同的文件访问和操作权限，确保最小权限原则的实施。

3. 编译与烧录安全

IC设计流程中，编译和烧录是关键环节，涉及将源代码转化为可执行固件并写入芯片。这些环节若缺乏安全控制，可能导致未授权的固件版本被烧录，或源代码在编译过程中意外泄露。

- **本地编译过程管控：**Ping32对IC设计研发中常用的编译环境（如Keil/GCC/Maven等）进行授权和管控。系统能够识别编译过程中的核心代码文件，并对其进行加密保护，同时允许非核心的中间文件保持明文状态，以确保编译流程的顺畅进行。这在保证源代码安全的同时，最大程度地减少了对研发效率的影响。

- **编译服务器防护：**对于集中式编译服务器，Ping32安全网关功能可确保加密文件在上传至编译服务器时自动解密，编译完成后下载到本地终端时再次加密。这保证了编译服务器能够正常处理明文代码，而最终生成或下载的固件和相关文件则受到加密保护，防止在传输和存储环节被非法获取。

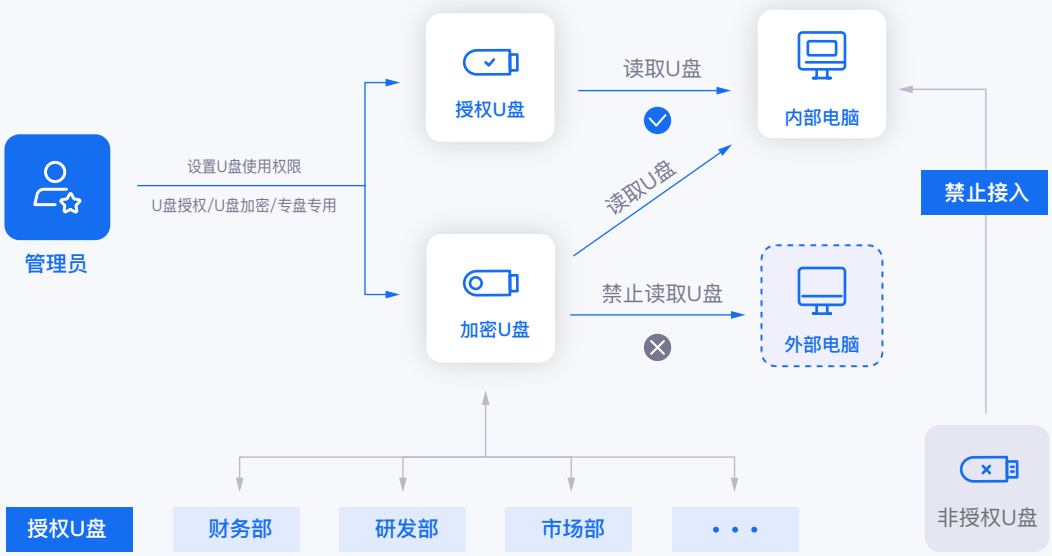
- **烧录安全控制：**Ping32对研发终端的通信端口（如COM口、USB等）进行精细化管控，仅开放必要的烧录接口。同时，对授权的烧录工具进行加密授权，确保只有通过授权工具才能进行芯片烧录。在烧录过程中，文件通过烧录工具打开时自动解密，整个过程对用户无感知，且无明文文件产生，显著降低了源代码在烧录环节泄露的风险。

4. 离网办公与移动设备安全

IC设计研发人员常因出差、现场调试或居家办公等原因，需要在非公司网络环境下工作。此时，如何保障加密文件的持续安全和策略的有效执行是重要挑战。

- **离线策略与补时功能：**Ping32提供离网补时功能，允许管理员预设离线时间。当研发人员离开公司网络环境时，在设定的安全时长内仍可正常打开和编辑加密文件。同时，所有文件外发管控策略将同步下发到终端，并持续生效，不会因终端离线而失效。这确保了即使在离线状态下，敏感数据也受到持续保护，并能有效拦截非授权外发行为。

- **专用加密U盘管控：**为满足调试、数据传输等需求，企业可为研发人员配备专用加密U盘。这些U盘在离开企业内部指定环境后，其中的文件将自动加密且无法正常读取，有效限制了U盘在企业外部的非法使用。同时，系统对U盘的接入和文件拷贝行为进行审计，记录详细的读写日志，确保移动存储介质的安全合规使用。



Ping32实时响应

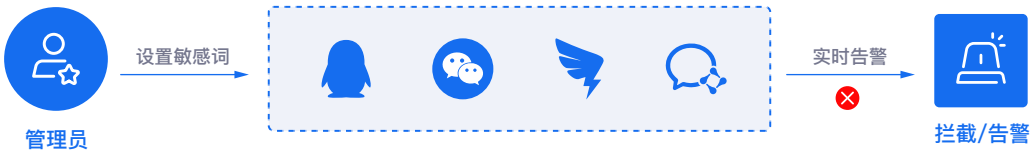
实时响应能力是数据防泄漏体系的关键组成部分，它确保了在数据面临潜在泄露风险时，系统能够及时发现、告警并采取阻断措施。这对于IC设计企业相关的商业机密、供应链数据和客户项目信息的保护尤为重要。

1. 商业机密文件外发管控

IC设计企业在日常运营中，涉及大量的商业机密文件交互，如与合作伙伴的合同、财务报表、采购清单、市场分析报告等。这些文件往往包含敏感的商业信息，需要严格控制其外发流向。

- **敏感内容分析与审批流程：**Ping32通过集成敏感内容识别技术，对通过邮箱、网盘、即时通讯软件（如企业微信、钉钉、QQ等）进行的文件外发行为进行实时监测。系统可预设敏感词库、正则表达式或文档指纹，一旦检测到外发文件中包含敏感内容（如合同编号、客户名称、报价信息、核心技术参数等），将立即触发告警或阻断。对于合规的外发需求，系统支持配置审批流程，员工需提交外发申请，经相关负责人审批通过后方可外发，并可设置外发文件的有效时间和访问权限，确保文件在授权范围内安全流转。

- **网络途径全面管控：**除了常见的邮件和网盘，Ping32还能对浏览器上传、FTP传输、蓝牙共享等多种网络外发途径进行全面管控和审计，确保所有可能的数据外发通道都在监控之下，防止“绕道”泄密。

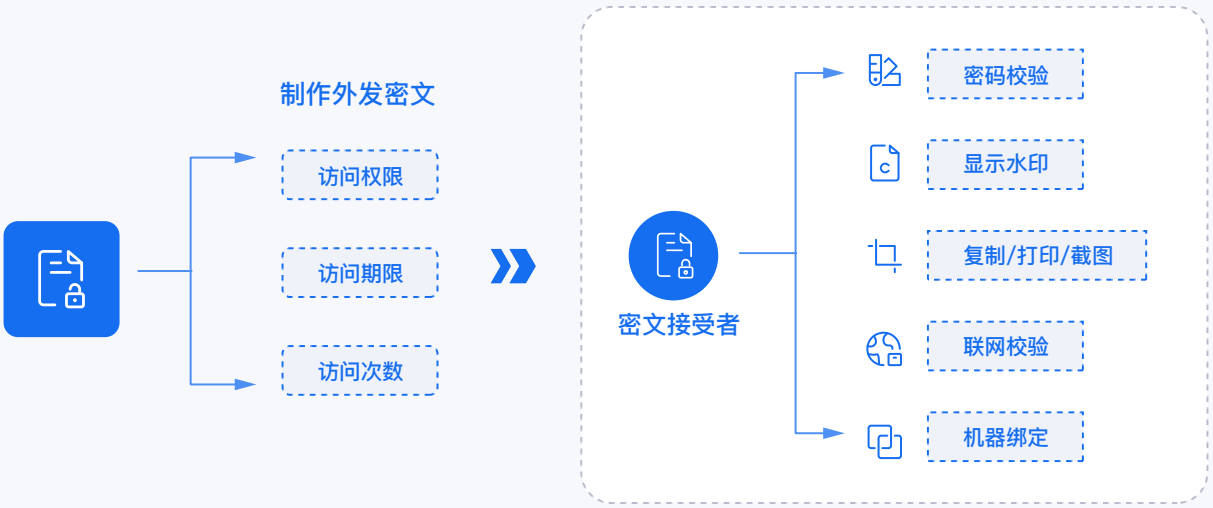


2. 供应链与合作方文件交互安全

IC设计企业的研发和生产涉及复杂的供应链协作，包括IP供应商、代工厂、测试服务商等。与这些外部合作方共享技术文档（如设计规范、测试报告、接口协议）是不可避免的，但必须确保信息安全。

- **文件外发包（Temporary Access）：**针对需要与外部合作方共享敏感技术文档（如GDSII/OASIS文件、PDK、测试规范等）的场景，Ping32提供“文件外发包”功能。企业可以将加密文件打包成外发包，并对接收方设置精细化的访问权限，例如：

  指定时间限制：设置文件在特定时间段内有效，过期自动失效。
  指定打开次数：限制文件被打开的次数，超过次数后无法继续访问。
  禁止操作限制：禁止接收方进行打印、复制、粘贴、截图等操作，防止二次泄露。
  水印显示：在外发文件中动态显示接收方信息水印，便于追溯。 这确保了即使文件被外发到外部环境，其内容和使用方式仍在企业的严格控制之下。



- **云盘与存储介质管控：**严格禁止员工将芯片设计图纸、源代码、工艺制程数据等核心资产上传至未经授权的公共网盘（如百度网盘、阿里云盘等），通过策略配置实时阻断此类行为。同时，对外部U盘、移动硬盘等存储介质的接入进行严格管控，仅允许授权设备接入，并对所有读写操作进行详细记录和审计。

3. 打印与屏幕截图合规

在IC设计研发过程中，打印和屏幕截图是常见的操作，但也极易成为数据泄露的途径。本方案通过精细化控制，确保这些操作的合规性。

- **打印行为管控与审计：**对包含敏感信息的IC设计相关文档（如设计报告、测试报告、专利文档等）的打印行为进行严格管控。系统通过敏感内容识别技术，实时监测打印任务，一旦检测到敏感内容，可自动阻断打印或要求员工提交打印申请。所有打印操作都将被详细记录，包括打印内容、时间、操作人员、终端设备等信息，形成完整的审计日志，便于事后追溯和责任认定。同时，可阻断虚拟打印机操作，防止通过虚拟打印生成文件进行泄密。

- **屏幕截图与水印防护：**在涉及敏感数据的操作界面或文档中，强制显示动态水印，水印内容可包含操作人员的身份信息和时间戳。同时，系统可阻止未经授权的屏幕截图工具（如QQ截图、微信截图、系统自带截图工具等）对敏感区域进行截取，或对截图内容进行模糊化处理，有效防止通过屏幕截图方式进行数据泄露。

Ping32深度溯源

深度溯源能力是数据防泄漏体系的最后一道防线，它确保了在发生数据泄露事件时，企业能够迅速定位泄露源头、追溯泄露路径，并进行有效取证，为事件响应和责任认定提供关键支撑。这对于IC设计企业这种核心技术资产价值极高的行业尤为重要。

1. 泄密追踪与文件备份

对IC设计企业相关的核心技术文件（如芯片设计图纸、源代码、工艺制程数据、仿真验证结果、流片文档等）和核心商业文件（如客户合同、IP授权协议、供应商协议等）进行全生命周期的操作审计和泄密追踪。

- **操作行为全面记录：**系统详细记录所有与敏感文件相关的操作行为，包括文件的创建、修改、复制、粘贴、删除、重命名、打开、打印、外发等。记录内容涵盖操作时间、操作用户、源文件路径、目标路径、操作类型等详细信息。这为构建完整的文件流转路径提供了基础数据。

- **脱离终端行为触发备份：**当敏感文件出现脱离授权终端的行为时（例如，被拷贝到U盘、上传到非授权网盘、通过邮件外发等），系统将自动触发文件备份功能，将原始文件内容进行留存。这使得即使文件被成功外泄，企业也能保留一份原始副本，便于后续的取证分析和内容比对。

- **文件内容与上下文关联：**泄密追踪不仅记录操作行为，还能关联文件的内容变化和上下文信息，例如，记录文件在不同版本之间的修改差异，或者文件在不同应用中被打开和处理的记录，从而更全面地还原泄密事件的发生过程。

2. 聚合搜索与智能分析

面对IC设计企业海量的终端操作日志和数据流转记录，快速、精准地定位敏感信息和异常行为是深度溯源的关键。Ping32的聚合搜索功能提供了强大的数据分析能力。

- **多维度审计记录聚合：**系统能够聚合来自多个维度的审计记录，包括但不限于：网站访问记录、即时通讯记录、邮件审计记录、文件操作记录、文件外发记录、剪切板操作、屏幕截图记录、打印记录、移动存储设备使用记录等。这些分散的日志数据被统一收集、存储和管理，形成一个全面的安全事件视图。

- **关键词与正则表达式检索：**管理员可以通过输入关键词（如芯片型号、项目名称、IP核名称、敏感技术术语等）或使用正则表达式，在海量审计数据中进行高速、精准的检索。系统支持对文件内容（包括Word、Excel、PDF、CAD等常见文档格式的正文内容）、图片内容（通过OCR技术识别）、压缩包内部文件内容进行深度检索，确保不遗漏任何潜在的泄密线索。

- **智能关联与异常行为识别**：通过对聚合数据的智能分析，Ping32能够识别异常行为模式，例如：短时间内大量敏感文件被拷贝、非工作时间进行敏感操作、频繁尝试访问受限资源等。这些异常行为将触发告警，并可自动生成事件报告，帮助安全管理员快速发现潜在的泄密风险。

- **可视化报表与溯源路径**：系统提供可视化的报表和图表，直观展示数据流转路径、高风险用户、敏感文件分布等信息。当发生安全事件时，管理员可以根据聚合搜索的结果，快速构建泄密事件的时间线和操作链，精准定位到是哪个终端、通过什么途径、在哪个时间点、由哪个用户泄露了哪些数据，为内部稽查和责任认定提供有力支撑。

通过上述智能防护、实时响应和深度溯源三大核心能力，Ping32数据防泄漏解决方案为IC设计企业构建了一个从源头到终端、从事前预防到事后追溯的全方位、立体化数据安全防护体系，有效保障了企业核心资产的安全，维护了企业的市场竞争力。

04

方案优势和价值

Ping32芯片研发集成电路设计企业数据防泄密安全保护方案，是针对IC设计行业核心知识产权保护的特殊需求而量身定制的综合性解决方案。它通过深度融合技术防护与管理策略，为企业带来了显著的优势和价值，确保了核心技术资产和运营数据的安全，并提升了整体业务的韧性。

精准防护与源头治理

针对性强：方案充分考虑IC设计研发的特点，对EDA文件、源代码、工艺制程数据、仿真验证结果等核心数字资产进行精准识别和保护。不同于通用型防泄漏方案，本方案能够深入到行业特有的文件格式和工具链，实现更细粒度的控制，有效应对IC设计流程中的复杂性和多样性。

出生即安全：通过驱动级透明加密技术，在数据产生（如代码编写、设计绘图）的源头即实施加密，确保核心资产从创建之初就具备安全属性。这种“源头治理”模式避免了数据在后续流转中因未加密而产生的风险敞口，真正实现了“数据不落地，安全不离线”，从根本上杜绝了数据泄露的隐患。

全流程可控与效率平衡

数据流转全生命周期管控：方案覆盖数据从创建、存储、传输、使用到销毁的全生命周期，严格管控数据流转的关键节点，包括文件外发、打印、代码库交互、编译烧录、供应链协作以及移动存储介质使用等，形成闭环管理。这确保了核心数据在任何环节都处于受控状态。

无感知加密与效率优化：采用无感知透明加密技术，研发人员在授权环境下操作加密文件时，无需手动解密，保持了原有的工作习惯和效率。同时，通过对非核心文件明文化、编译环境精准授权、离线策略等灵活配置，最大程度减少了安全措施对核心研发和生产效率的影响，实现了安全与效率的平衡，确保业务连续性。

风险可视与深度溯源

全方位风险洞察：通过强大的聚合搜索和审计分析能力，将海量的终端操作日志、文件流转记录、网络行为数据等进行统一收集、关联分析。这使得企业能够从碎片化的信息中快速识别潜在的泄密风险，变“事后补救”为“事前预警”和“事中响应”，显著提升了安全响应速度。

精准定位与责任追溯：当发生安全事件时，系统能够提供详细的操作日志和文件流转路径，结合OCR技术对图片内容进行识别，以及对压缩包内部文件的穿透检索，帮助企业快速定位泄密源头、追溯泄密路径，明确责任人，为内部稽查和法律取证提供有力支撑，有效降低了事件处理的复杂性。

提升合规性与品牌声誉

满足行业合规要求：本方案有助于IC设计企业满足日益严格的行业监管要求和国家网络安全法律法规（如《网络安全法》、《数据安全法》、《个人信息保护法》等），特别是针对高科技和关键信息基础设施领域的合规性要求，降低合规风险。

增强客户信任与市场竞争力：在IC设计领域，数据安全是客户和合作伙伴选择供应商的重要考量因素。通过实施本方案，企业能够向客户展示其对数据安全的高度重视和有效防护能力，从而增强客户信任，维护并提升品牌声誉，进而提升市场竞争力。

规避经济与法律损失：有效防止核心技术和商业机密的泄露，避免因知识产权被窃取而导致的巨额研发投入损失、市场份额流失以及潜在的法律诉讼和罚款，直接保护企业的经济利益。

统一管理与简化运维

一体化平台：Ping32提供统一的平台，整合了文件加密、数据防泄漏、终端行为管控、敏感内容识别、软件合规管理和审计等多种功能，显著降低了企业采购、部署和管理多套独立安全系统的复杂度和成本，实现了安全管理的集中化和高效化。

集中化策略配置：通过统一的可视化管理平台，管理员可以根据角色、部门、项目等维度灵活配置和下发安全策略，实现集中化管理，大大简化了运维工作，提升了安全策略的执行效率和一致性。

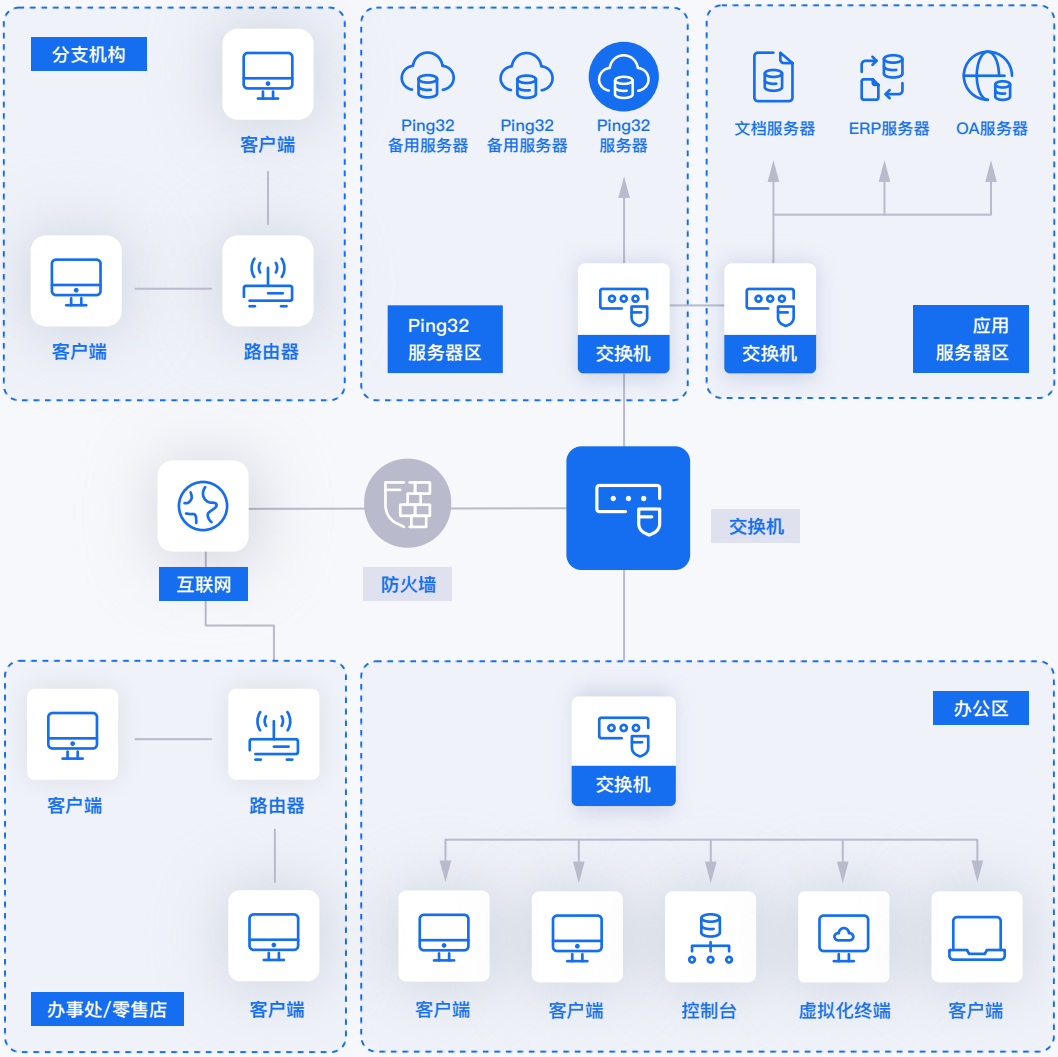
综上所述，Ping32芯片研发集成电路设计企业数据防泄密安全保护方案不仅仅是技术工具的堆砌，更是围绕IC设计企业核心资产和业务流构建的、有明确对抗目标的纵深防御体系。它直接服务于企业保护创新成果、规避商业与法律风险、维护市场地位的战略需求，为IC设计行业的健康、可持续发展提供坚实的安全基石。

05

系统架构

Ping32数据防泄漏解决方案采用C/S（客户端/服务器）架构设计，并结合了云服务与本地部署的混合模式，以满足IC设计企业对数据安全、隐私保护、高效运维和灵活部署的综合需求。整个系统主要由客户端模块、服务器模块和控制台模块组成，协同工作以实现对IC设计企业相关数据的全面防护。

系统架构图



1. 客户端模块

客户端是部署在IC设计企业内部所有需要受控的终端计算机上的核心组件。它负责执行由服务器下发的各项安全策略，并实时采集终端计算机的运行数据和操作日志，然后加密上传至服务器。

2. 服务器模块

服务器模块是整个系统的核心大脑，通常部署在企业内部的物理服务器或私有云环境中。它负责存储和管理所有安全策略、接收和处理客户端上报的审计数据，并向客户端下发管理指令。

3. 控制台模块

控制台是供网络管理员、 企业负责人用来管理终端计算机， 审计操作使用。管理者通过控制台设置管理策略， 查看日志和各项统计信息。 控制台操作界面简洁易用， 支持多个管理员不同权限登录。

通过上述架构设计，Ping32解决方案为IC设计企业构建了一个高效、可靠、易于管理的综合数据防泄漏平台，全面保障了企业核心资产的安全。

06

总结

Ping32芯片研发集成电路设计企业数据防泄密安全保护方案，是针对当前IC设计行业面临的复杂数据安全挑战而量身定制的综合性解决方案。它超越了传统的被动防御模式，构建了一个集“智能防护、实时响应、深度溯源”于一体的主动防御体系，旨在全面保障IC设计企业核心知识产权的全生命周期安全。

本方案的核心价值在于其对IC设计行业特性的深刻理解和精准覆盖。从EDA文件、源代码、工艺制程数据等核心研发资产的透明加密，到代码库、编译烧录环节的安全管控，再到商业机密文件外发、供应链协作、离网办公等场景的实时响应，以及最终通过聚合搜索实现对泄密事件的深度追踪和责任认定，Ping32解决方案在每一个关键环节都提供了切实可行的防护措施。它不仅有效封堵了数据泄露的各种途径，更在保障安全的前提下，最大限度地兼顾了研发和生产效率，实现了安全与业务的和谐统一。

通过实施Ping32芯片研发集成电路设计企业数据防泄密安全保护方案，企业将能够：

- **筑牢核心资产防线：**确保芯片设计相关的核心技术资料、设计图纸、源代码等知识产权免受非法窃取和泄露，保护企业的创新成果和核心竞争力。

- **实现全流程透明审计：**对研发人员操作、文件流转、软件使用等行为进行可视化追溯，提升内部管理规范性，降低内部风险。

- **规避泄密多重损失：**有效防止因数据泄露导致的经济损失、法律风险、客户信任流失和品牌声誉受损。

- **提升合规性水平：**满足国家和行业对集成电路数据安全日益严格的合规要求，为企业的可持续发展提供坚实保障。

- **简化安全运维：**通过一体化平台和集中化策略管理，显著降低安全运维的复杂度和成本，提升安全管理效率。

总之，Ping32芯片研发集成电路设计企业数据防泄密安全保护方案不仅仅是一套技术工具，更是IC设计企业在数字化转型浪潮中，应对数据安全挑战、维护国家信息安全、保障社会稳定运行的战略性选择。它为IC设计行业的健康、安全、可持续发展奠定了坚实的基础。

公司简介

山东安在信息技术股份有限公司成立于2014年，是一家以研发信息安全类产品及提供相关服务为主营业务的技术驱动型公司。是中国领先的、拥有完全自主知识产权的信息安全产品和服务解决方案专业提供商。

安在软件自主研发的Ping32终端安全管理系统，构建了全生命周期的一站式信息安全产品与整体解决方案平台，包括文档透明加密、办公行为审计、操作管控、敏感内容识别、终端系统安全、运维管理等功能，有效防护由于不正当的办公行为造成的数据泄漏。

Ping32凭借优异的信息安全管理方案以及良好的用户体验受到广泛好评。被广泛应用于政府、金融、军工、运行商、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，为国内10000多家用户，超过200万台终端提供安全保障。

400-098-7607
nsecsoft.com

济南
高新区经十路7000号汉峪金谷
金融交易中心6层

NSecsoft
安在软件

Contact us : design-team@nsecsoft.com