

集成电路行业安全解决方案

零信任接入，兼顾数据安全和高效研发，守护集成电路企业核心竞争优势

随着市场竞争日益加剧，产业结构呈复杂化趋势，行业分工加速细化，企业所面临数据安全风险也日益严峻。特别对于研发周期较长、研发环节较多的集成电路行业而言，数据安全关乎企业生存和发展。如何保护企业最核心的资产—IP知识产权，有效防范数据泄露，在当下已成企业业务高效开展的最大挑战之一。

亮点

- 多区分区隔离，核心数据更安全
- 桌面虚拟化，数据不落地
- 自研多场景带宽优化算法，整体提升带宽利用率
- 严格文件流转/审批流程，技防替代人防，加强可控效率更高
- 负载均衡+集群模式，高可靠、可灵活扩展
- 两步部署，五分钟上线，无缝衔接现有系统
- 可视化日志记录，安全事件全过程可追溯

面向多种办公场景，统一入口严控数据安全

志翔科技集成电路行业安全解决方案综合考量核心数据安全，和远程接入等企业研发与办公场景的实际需求，为集成电路企业多地协同研发、远程办公、外包等多种应用场景，提供简单、易用、高效的核心数据资产保护解决方案。

方案采用模块化设计，企业可以按需灵活配置组合、弹性扩展：

- 方案以至安盾®ZS-ISP智能安全平台为核心，设置统一入口，隔离数据与终端，数据不落地，以视频流的形式实现交互操作，严防操作过程中的数据泄露。
- 所有文件的传输和流转需通过至锐通®ZS-DSE文件安全交换系统经严格的审批流程，以切片存储和加密隧道等多种手段，保证流转的全程可控、存储及传输等安全。
- 部署于终端的至明台®ZS-DSA数据防泄露产品，提供企业数据资产全景可视化，监控与分析用户行为与数据流向，预知风险、快速溯源。
- 同时，基于零信任架构设计的至锐联®ZS-Trust零信任访问控制系统可支持多种企业资源的接入访问，构筑安全、高效、稳定的远程接入安全网络，可全面增强企业远程接入安全。

服务客户



关注志翔

北京志翔科技股份有限公司
www.zshield.net

电话：400-819-8880
邮箱：contact@zshield.net

地址：北京市海淀区学院路35号世宁大厦1101
邮编：100191

挑战

- 集成电路设计制造的环节多、分工细，重要数据分布在内网终端上，缺乏监控和相应的安全防护措施，内部人员和外包商的越级分享等违规或高危行为监管难度大，数据泄露风险高。

- 文件存取审批和日志审计以人工为主甚至缺失，成本高、效率低，数据导出导入难管理，安全事件发生后难追溯。

- 断网等物理隔离方式僵化，无法满足高效研发、外包远程等协同工作需求，严重影响企业在激烈竞争环境中的技术创新效率；虚拟桌面和VPN等解决方案虽然满足远程办公需求，但成本高，部署复杂、权限管理困难，且叠加安全产品易带来不兼容和稳定性差等新问题。

需求

- 对本地和远程终端程序使用、访问数据等行为进行隔离和授权管理，禁止未授权行为。

- 对用户操作及网络文件传输等行为，进行全面监控和审计记录。

- 按需对核心数据分区隔离及统一管控，满足本地、多地和外包等研发场景下安全且高效的数据访问与操作体验。

- 建立完善的审批、审计机制，统一监控管理数据存取。发生安全事件，可快速追溯数据访问全过程。

- 安全方案不影响集成电路行业特有的版图制作、仿真等高性能处理工作的用户使用体验与效果。

- 部署简单，无需增加运维成本，尽可能少改变原有IT架构，缩短设备部署导致的业务中断时间。

志翔科技集成电路行业安全解决方案

方案以数据为防护核心，以身份和权限作为新的防护边界，采用体系化和模块化设计。通过设立统一入口，利用技术手段集中管控企业办公、研发、运维人员，以及外包服务商等在多场景下的数据访问与操作。满足数据安全防护、文件流转安全合规、远程接入安全增强等集成电路设计流程中各环节数据保护的需求，同时能很好兼顾研发效率及办公体验。

-  **FPGA可编程的EEPROM文件：**支持配置备份FTP服务器，通过绿色通道的数据文件可以自动备份，以备事后查看；所有自动导出都会在系统上留有日志，规避传统人工操作可能会产生的泄露风险。

-  **确保GDS文件等资料的安全：**人工审批导出GDS文件，交由工厂流片。人工审批的审批人和责任人一致，确保关键文件导出过程的安全。记录导出文件，相关日志可以长期存储和外部存储，以备审计和事件追溯。

-  **数据资产（文件、代码、图形）和业务操作：**通过至安盾隔离研发数据，管控数据存取流程，审计数据访问行为。整个业务流程以至安盾作为统一入口，实现集中管控，业务操作采用视频流方式交互，数据不落地，最大程度降低泄密风险。

-  **后端版图及其设计过程：**企业内部版图设计采用至安盾方案，安全性更高，且内置版图自研渲染优化算法和多场景自适应调节功能，节省企业带宽，提升用户体验，满足外包公司远程登录服务办公需求，通过严格的审计机制，可一键统计外包绩效功能。

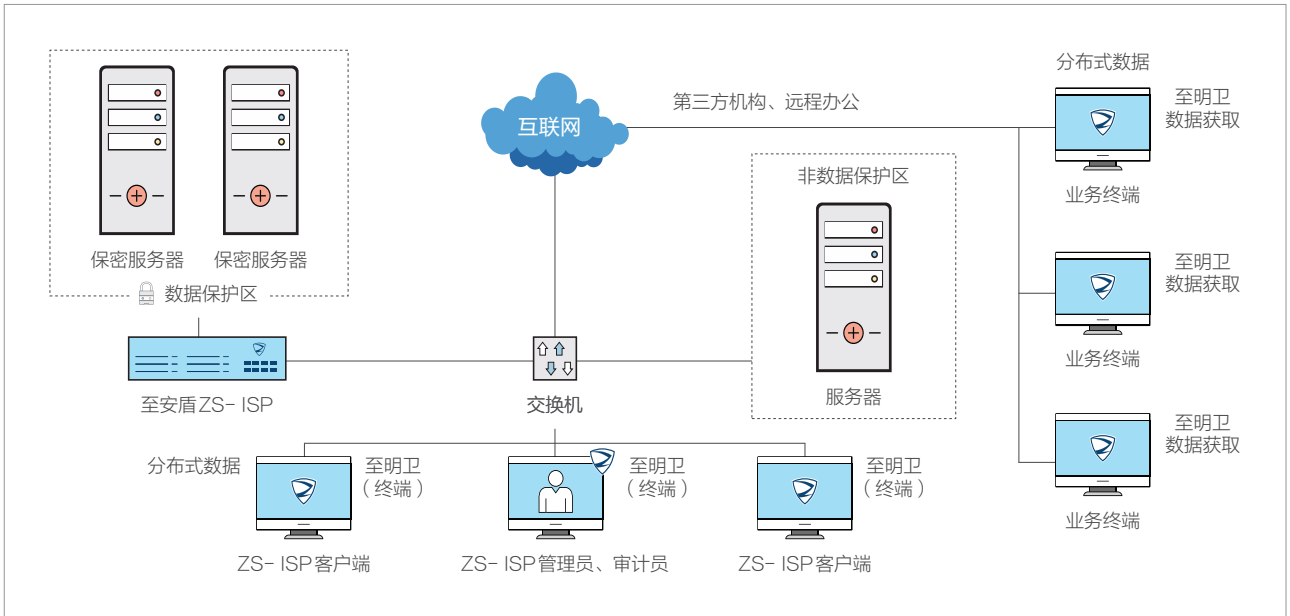
至安盾®ZS-ISP+至锐通®ZS-DSE+至明台®ZS-DSA

设置统一入口，隔离核心数据防泄漏；规范文件流转和审批流程，终端数据防护及监控

至安盾是软硬件结合的数据安全工作平台和管控系统，部署于用户终端与服务器/数据存储设备之间，成为企业数据存取、操作的统一入口。服务器上的操作以视频流显示在用户终端，从而做到数据与用户隔离，避免外泄。至安盾集成隔离、审批、审计、事件告警等多种功能，支持远程访问等多种办公场景，主要针对集中式数据存储的IT基础架构。

至明台®ZS-DSA是部署于终端、服务器和云主机等设备上的数据防泄漏与溯源系统。至明台融合智能文件内容识别和加密技术，通过平台策略扫描可发现散落在终端上的敏感文件，监控文件的使用和外发行为，根据预设规则实行加密或阻断等保护动作，实现对企业重要敏感文件的监控保护和行为审计。

针对集成电路企业复杂部署环境下，服务器、用户终端、外包商和远程办公终端等多方同时需要数据防护时，则可选择部署集至安盾、至锐通和至明台为一体的整体数据安全解决方案。方案通过至安盾隔离管控集中式数据，至锐通提供文件流转的合规审计和管控，至明台发现、监控和保护分散数据，三者各司其职、紧密配合为企业核心数据资产提供一站式完善保障。



- 系统设置管理自定义：**企业可自定义和设置数据保护级别和访问权限。

- 文件流转安全合规：**用户只能根据自身权限，遵循设置好的文件流转流程，经过审批后在权限许可位置获取相应的文件。

- 多种桌面形态可选：**支持虚拟桌面、Docker标准桌面和外置桌面等多种形态的桌面，用户可根据使用场景按需灵活选择。

- 多虚拟局域网接入：**支持多个虚拟局域网同时接入一套至安盾设备，设备内置防火墙功可保证各虚拟局域网的隔离性。

- 终端安全防护：**提供基于文件操作行为的安全管控，辅以透明加解密、网络管控、端口管控等，形成闭环安全管控环境。

- 行为日志全量记录：**系统可自行记录所有文件及数据的访问记录 and 用户行为。

- 事件审计可视化：**提供可视化审计界面，根据日志进行横向分析和展示，可辅助进行风险评估和事件溯源。