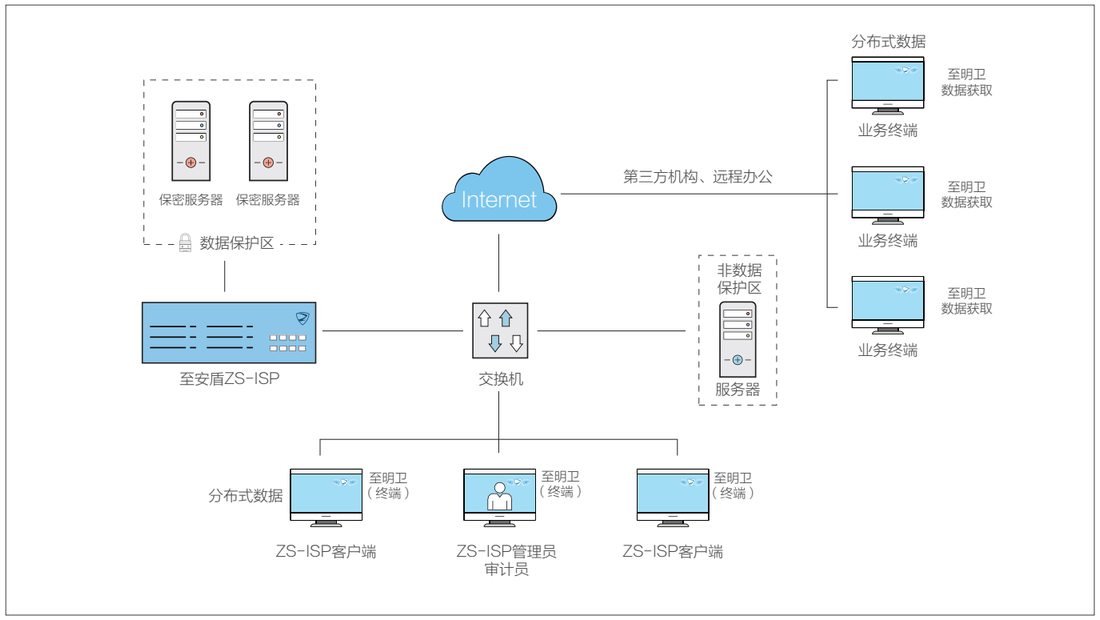
至安盾®+至明卫®——核心数据保护，终端风险监控分析

至明卫®是部署于终端、服务器和云主机等设备上的监控软件。探针对分布式数据进行全方位不间断监控，采集用户行为，形成用于分析的系统日志。探针通过分析展示系统动态及数据流向，绘制数据资产地图，对于违规用户行为实时报警，对I/O外设进行智能管理。

针对集成电路企业的复杂部署环境，服务器、用户终端、第三方机构和远程办公等同时需要数据保护时，通过至安盾隔离管控集中式数据，至明卫监测分布式数据，两者联合部署为企业核心数据资产提供完善保障。



部分客户

紫光展锐 UNISOC　ZTE中兴　君正 Ingenic　Allwinner Technology　Cambricon 寒武纪　INTERNATIONAL GREEN CHIP 英特格灵芯片　MEMSIC　SG-T 智芯公司

HGrace 華虹宏力　兆芯　Brite semiconductor　灏起科技 MontageTechnology　华大北斗 ALLYSTAR　中国科学院微电子研究所　Empyrean 华大九天

扫码关注志翔

北京志翔科技股份有限公司　电话：010-82319123　北京市海淀区学院路35号世宁大厦1101
www.zshield.net　邮箱：sales@zshield.net　邮编：100191

Solution
解决方案

志翔科技集成电路行业安全解决方案

兼顾数据安全与高效研发，守护集成电路企业核心竞争优势

亮点

- 分区隔离，保护核心数据安全
- 利用桌面虚拟化，杜绝数据下载到本地
- 严格的数据文件审批流程，提升可管控性
- 快速查找日志记录，实现安全事件过程追溯
- 图形渲染加速，提升远程带宽利用率
- 负载均衡+集群模式，提升可靠性与体验
- 两步部署，五分钟上线，与现有系统无缝集成

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，企业所面临的信息安全风险也日益严峻。特别对于集成电路行业而言，信息安全关乎企业的核心竞争力。因此，如何保护企业最核心的资产——IP知识产权，有效防范企业核心业务数据泄漏，避免成为下一个数据违规事件的焦点，已成为企业持续保持市场竞争力的最大挑战之一。

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基于体系化设计，平衡考量核心数据安全，和企业研发与办公实际需求。以至安盾®ZS-ISP为核心，设置统一入口，彻底隔离数据与终端，数据不落地，以视频流的形式交互流转，严防外泄。结合终端部署的至明卫®，让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。为集成电路企业远程办公、多地协同研发、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。

挑战

- 集成电路设计制造的环节多、分工细，内部人员和外包商的违规或高危行为监管难度大，数据泄漏风险高；
- 断网等物理隔离方案僵化，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；
- 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；
- 虚拟桌面等解决方案虽然能满足远程办公需求，但成本高，部署复杂，且叠加安全产品极易带来不兼容和稳定性差等问题。

需求

1. 对本地和远程终端程序使用，和访问数据等行为进行隔离和授权管理，禁止未授权行为；
2. 对用户操作，及网络文件传输等行为，进行监控和审计记录；
3. 按需对核心数据分区隔离及统一管控，方便本地、多地、外包等多研发场景下对数据的访问与操作，兼顾安全与研发效率；
4. 建立完善的审批、审计机制，对数据的存取进行统一监控管理。一旦发生数据泄露事故，可对数据访问过程进行完整、全方位、快速的追溯；
5. 安全管控的同时，能满足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；
6. 性价比高，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

通过设立统一入口的方式，利用技术手段集中管控企业办公、研发、运维人员，以及外包服务商等多场景下的数据访问与操作。方案以数据为防护核心，以身份和权限作为新的防护边界，基于体系化设计，兼顾数据安全保护、研发效率以及办公体验，满足集成电路设计流程中个环节数据保护的需求。

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，杜绝泄密。

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，且内置版图渲染优化，节省企业带宽，提升用户体验，满足外包公司远程登录服务器办公需求，并具备严格的审计机制，一键统计外包绩效功能。

确保GDS文件等资料的安全

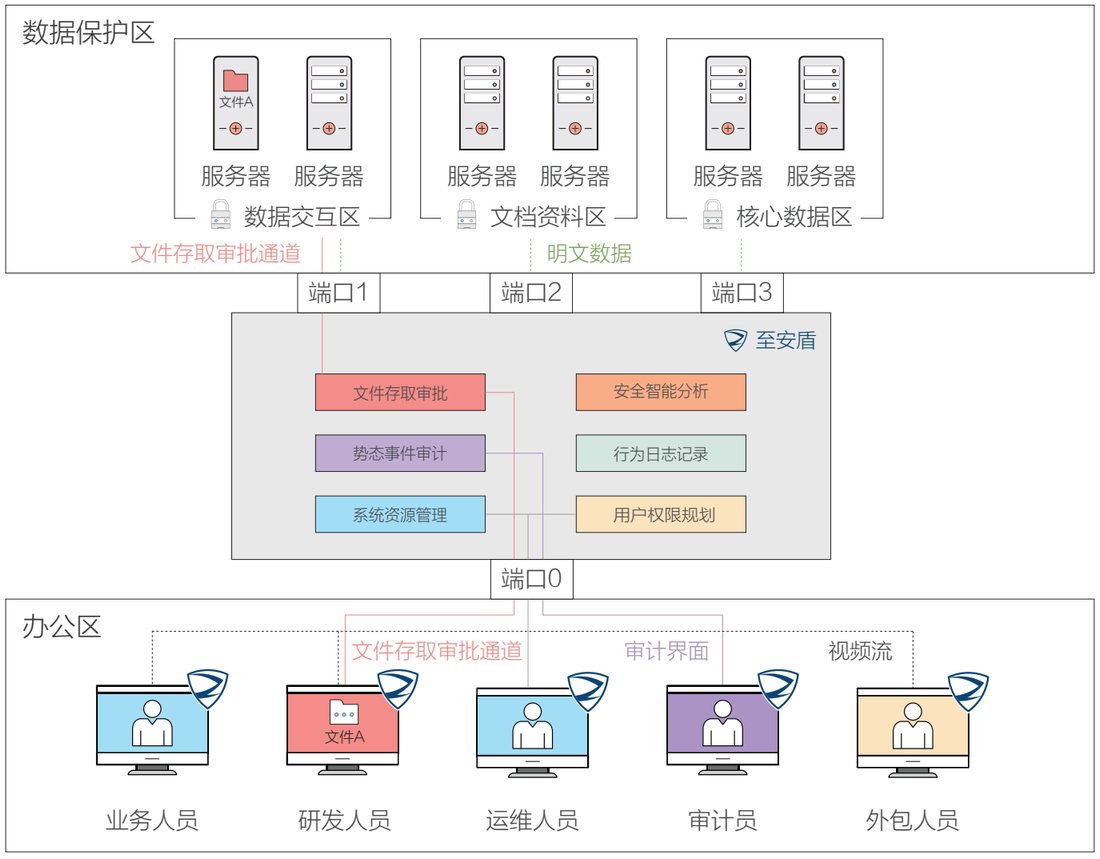
人工审批导出GDS文件，交由工厂流片。人工审批的审批人和责任人一致，能极大的保证关键文件导出过程的安全。记录导出文件，相关日志存储10年，以备审计和事件追溯。

“在管理外包服务供应商的数据交互方面，志翔的方案简单安全，单台设备部署就能优化原有的IT架构，并在一些流程上可配置进行自动操作，有效的节约了管理成本。”

—— 展讯

至安盾®ZS-ISP——设置统一入口，隔离核心防泄漏

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。至安盾集成了隔离、审批、审计、事件告警等多种功能，支持远程访问及办公场景，主要针对集中式数据存储的IT基础架构。



系统设置管理

企业可自定义和设置数据保护级别和访问权限

行为日志记录

系统可自动记录所有文件及数据的访问记录和用户行为

文件存取审批

只有满足特定访问规则和权限所要求的用户，才能获取相应文件

态势事件审查

提供可视化审计界面，根据日志进行安全态势展示和风险评估

“至安盾理想地支持了我们总部与多个分支研发中心并行工作，并确保数据安全的需求。在面临断网和其他突发事件时，至安盾的安全远程办公模式对确保研发进度非常重要。”

—— 英特格灵