志翔科技
ZSHIELD INC

至安盾® ZS-ISP高效的数据安全防护体系

至安盾®智能安全平台基于“零信任安全，无边界工作”的安全理念，为企业构建数字化办公环境与立体安全防护机制。将访问者与业务系统和数据隔离，不再区分内外网，用户和设备完成身份权限认证后，经“无边界工作”模式，让任何人和设备只要有网络即可接入至安盾，至安盾方能对业务和数据进行安全访问。通过基于角色和业务的管控机制，至安盾确保操作者仅允许访问和操作权限内的业务系统与数据，为用户提供体验无降级，安全与高效兼得的生产环境。

产品优势

安全无忧

安全原生的桌面服务，杜绝数据泄露，无惧渗透攻击。

本地不留数据，防截屏，防拍照，防拷贝，严控外设。

内置防火墙功能，自有专利技术保证用户登录强安全管控。

性能卓越

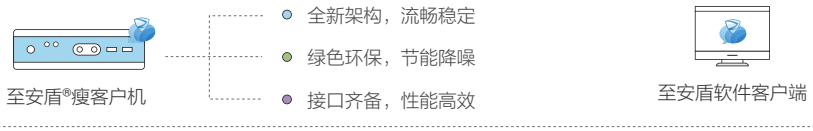
高性能存储架构，支持高并发存储访问。

用户体验精细优化，对高质量图像和视频显示效果好。

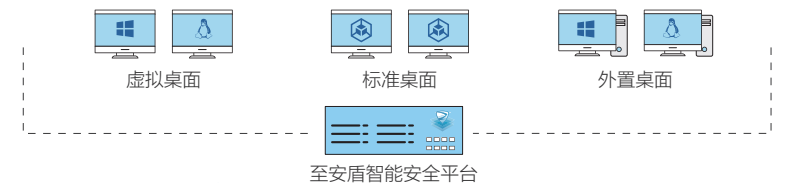
分支机构多地桌面资源共享，异地办公，本地体验。

产品组件

瘦客户机、软件客户端：用户通过至安盾客户端或专用瘦客进行数据输入（外设输入指令）和输出（接收视频流桌面），数据传输采用志翔自研的DPD桌面传输协议。适配多办公场景且不断优化的DPD协议，兼顾高用户体验、灵活操作、敏捷办公等多方面办公需求，让员工能专注于为企业创造价值，不再受限于终端本身的硬件故障或配置。

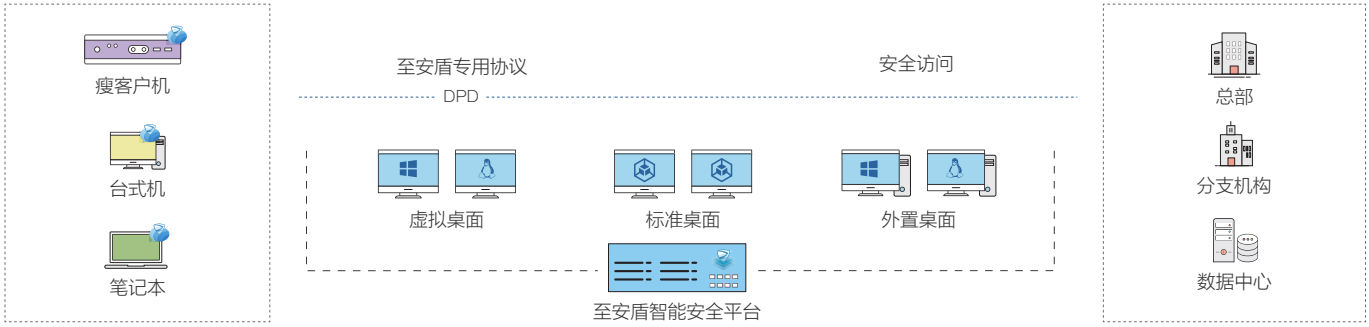


至安盾智能安全平台：至安盾智能安全平台为企业提供稳定可靠、性能高效的Windows、Linux安全工作环境。结合原生的智能安全管控机制，包括智能审批审计策略、可视化安全态势、安全事件溯源等功能，打造牢不可破的安全数字化工作环境。可与现有AD/LDAP/NIS系统无缝对接对接，根据用户权限灵活提供相应的配置与文件传输权限，进行批量管控。多重认证的登录方式，既安全又满足企业规范与合规要求；支持集群部署，有效防止因服务器故障导致的业务中断，确保安全无死角。



部署方式

至安盾智能安全平台将企业内部或数据中心的关键数据与用户进行隔离，能够有效降低恶意软件和人为操作导致的非信任连接和数据泄露风险。用户通过客户端软件或瘦客户机登录至安盾安全桌面，以视频流的形式将安全桌面的画面传输到终端，数据不落地，为政企打造安全统一的数字化办公环境。



核心功能

至安盾智能安全平台以安全访问控制、安全接入协议等为基础，结合安全桌面服务，建立多层次、可视化的安全策略体系，构筑适合多种角色和职能的业务空间环境，以安全、敏捷、高效的体验，为政企提供一站式解决方案。

安全桌面：提供安全桌面和应用，支持多种终端设备与操作系统。灵活管控镜像，提效率、降成本，并满足合规要求。

安全传输：基于DPD接入协议，实现数据面和控制信令的分离和安全传输，杜绝恶意攻击和非法接入等风险，保证数据不落地。

智能运维：对物理、虚拟和云环境提供动态个性化策略配置，简化用户管理、虚机管理、应用发布、资源配置等流程。

日志审计：收集、存储、关联分析并展示多种日志（系统、用户行为、数据流转等），助力智能运维和快速定位安全事件。

安全分析：基于大数据分析技术，对系统运行和用户操作产生的数据进行分析并展示，提供全面准确的安全态势信息。

终端管控：安全桌面内置防截屏功能，自定义水印防止通过拍照的形式进行数据获取，精细管控IO外设，文件不落地。

接入管控：基于时间、地点、角色和来源等提供灵活精细的控制策略，可对单个用户配置应用级的资源管控策略。

数据流转审批：通过自动和人工审批对数据文件在不同保护区之间的流转进行管控和记录，并支持备份流转文件。

事态报警：实时监控并对违规和可疑操作报警，可采取拦截阻断等措施，并以邮件、短信等多种方式通知管理员。

安全合规：可满足现行法律法规对关键数据隔离、权限管控、行为监控和操作审计的要求，助力企业信息安全体系建设。

扫码关注志翔

北京志翔科技股份有限公司
www.zshield.net

电话：010-82319123
邮箱：contact@zshield.net

北京市海淀区学院路35号世宁大厦1101
邮编：100191