

至安盾® 智能安全平台

云计算、物联网等新技术的快速发展带来了企业IT架构的变革和业务日渐云化，员工能够随时随地访问集中化、高价值的业务数据。如何应对上云和云上的数据安全问题，同时兼顾安全与效率，成为企业发展中必须解决的大问题。

零信任安全，无边界工作

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，创新性的通过三道安全防线和五大安全策略，为企业构建立体防护机制。“零信任安全”模式，即将任何访问者与业务系统和数据隔离。“无边界工作”模式，让任何人和设备可灵活接入至安盾，通过至安盾方能对业务和数据进行安全访问。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的生产环境，保障工作效率。

产品优势



三道安全防线

通过统一入口访问控制、自有安全接入协议DPD、自带安全专用防火墙等三道安全防线，打造身份可信、安全、统一接入的业务空间环境，围绕核心数据的流向来构筑完善的安全机制。



五大安全策略

从三权分立、安全分区、文件存取管控、报警预警和审计追溯等五个方面，建立多层次可视化的安全策略体系，结合大数据安全分析技术，完整清晰的管理和掌控企业安全状态。

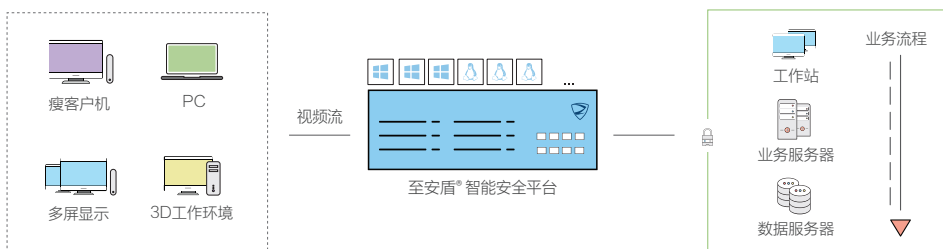


部署简便，优化效率

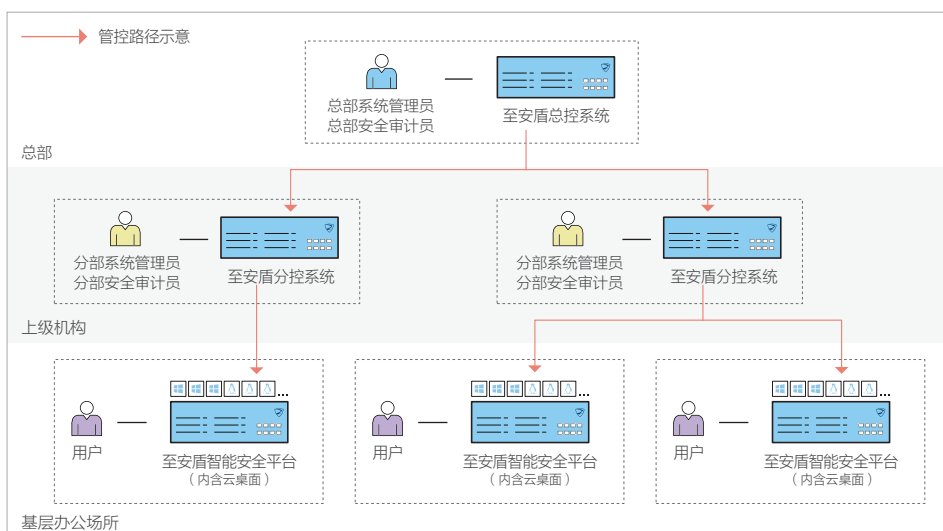
基于VDI技术的安全云桌面部署简便，能够细粒度分配运维、研发以及设计的桌面权限与性能，并针对制图3D等专业计算需求进行专门优化，用户体验卓越。

部署方式

安全云桌面部署：至安盾将保护区内的关键数据与用户相隔离，防止恶意软件和人为操作导致的非信任连接和数据泄露风险。用户通过终端登录至安盾桌面，数据不落地，以视频流的形式经桌面传输到终端，为政企打造安全统一的业务环境。

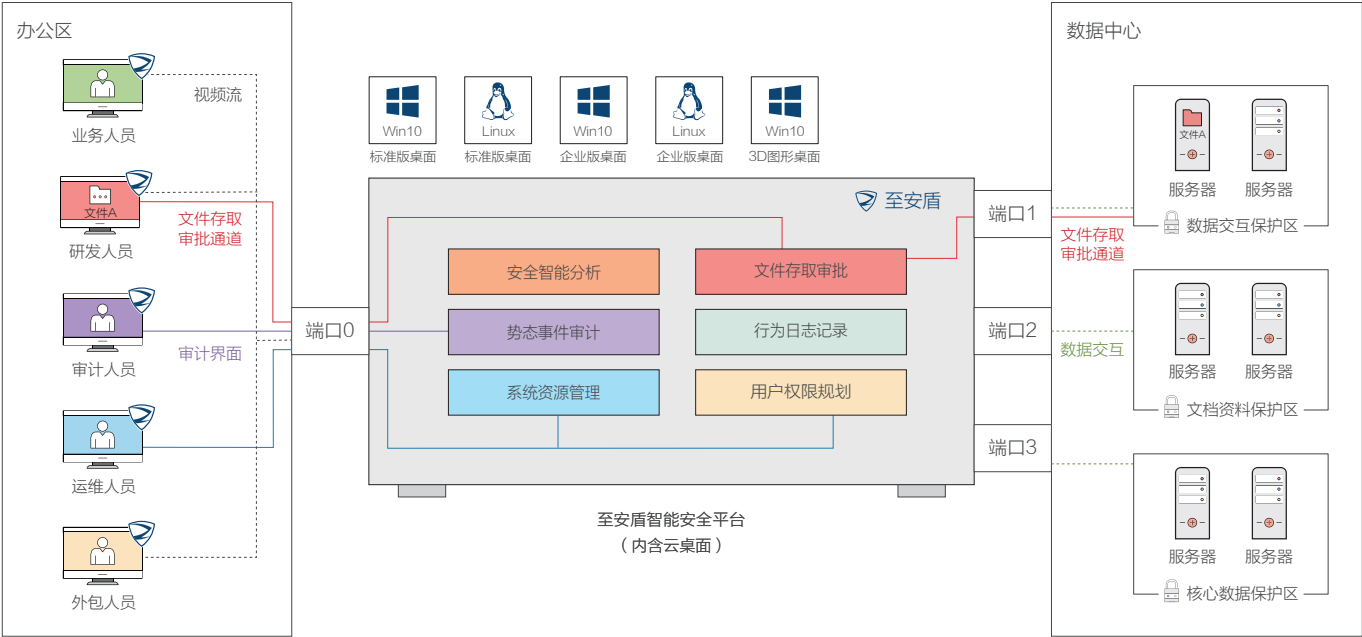


多地多级分布式部署、统一管控：针对多层级管理的大型政企机构，至安盾支持多级多地分布式部署来提升业务承载能力。在基层通过本地桌面就地接入业务和办公；在上级机构和总部，部署分控和总控设备，多级统一管理，在统一管控的基础上，避免集中部署带来的性能瓶颈。



核心功能

至安盾以安全访问控制、安全接入协议等为基础，结合云桌面服务，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。



桌面交付：向用户交付虚机和应用，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。

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。

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、虚拟机管理、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。

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

安全分区：内置动态网络构建模块，可同时管理并严格隔离多个数据保护区。用户对保护区的访问可动态分配和管理。

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：sales@zshield.net

北京市海淀区学院路35号世宁大厦1101
邮编：100191