

志翔可信工作域管控平台

安全与高效的科研生产力支撑平台

在科研场景中终端 CPU、操作系统、科研软件、外设等因素交织，数据交互复杂且频繁，极易引发数据泄漏风险。目前，多数机构仍以网络安全为主要防护手段，对数据安全防护不足。

志翔科技可信工作域管控平台应运而生。平台依托分区隔离、安全工作空间、访问管控、数据安全交换和安全审计五大核心模块，打造“数据可见、可用、不可带走”的全方位防护体系，以数据不落地的安全保障，为科研团队构建可信的数字化工作环境，有效解决复杂科研场景下的数据安全难题。

志翔可信工作域管控平台基于“逻辑隔离+动态防护”双重机制，将核心业务系统、关键科研数据与办公终端彻底隔离，从源头降低恶意入侵、误操作等风险。用户可通过客户端软件或瘦客户机等方式接入可信工作域。平台以加密视频流的形式将可信工作域画面实时传输至终端，实现数据全程“不落地”，既保障安全，又提供统一高效的科研办公体验。

产品亮点

场景化精准防护

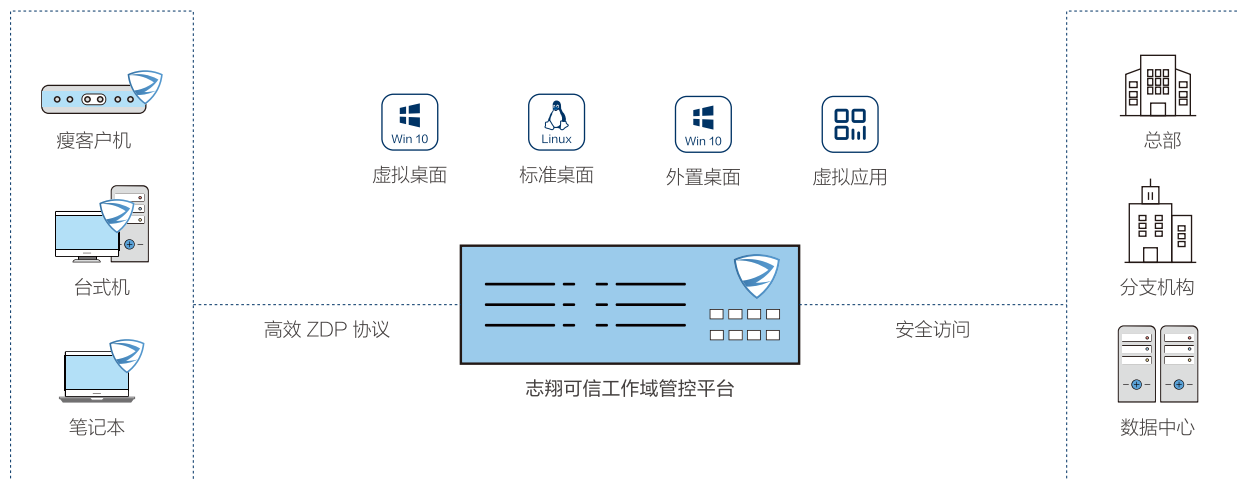
针对科研场景中软硬件多样、数据交互频繁等特点设计，更贴合科研机构实际需求。

安全与便捷兼顾

优化科研人员操作体验，简化访问权限申请流程，实现“数据带不走，科研不停顿”。

性能卓越，体验流畅

针对高清图像、4K 视频处理等特定优化。自研 ZDP 协议，画面传输时延 < 50ms，色彩还原度接近本地。



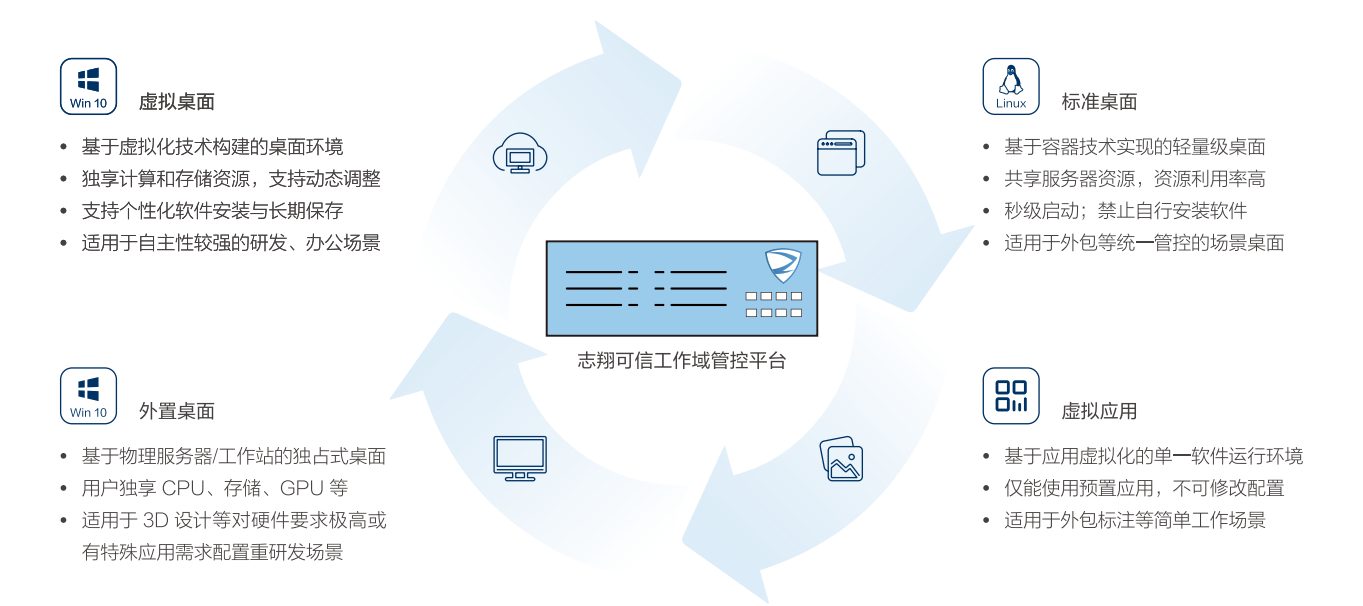
应用场景与价值

志翔可信工作域管控平台广泛适用于医疗、高科技、制造等行业的科研与开发环境。平台为企业提供：

- 全方位可信防护体系：满足合规与安全要求；
- 安全与高效并重的科研环境：让安全不再是限制，科研人员专注创新；
- 一站式统一平台：覆盖访问控制、安全工作空间、传输、审计等科研工作数据管控全场景。

核心功能

志翔可信工作域管控平台以精细化访问控制、高效访问协议、智能内容检测为核心，结合安全分区隔离与全流程安全审计，构建覆盖数据存储、使用、交换等全生命周期的安全防护体系。平台提供虚拟桌面、标准桌面、外置桌面和虚拟应用桌面等多类工作空间，可统一管理、灵活调度、快速按需部署，满足科研、设计、办公等不同工作场景需求。



专用安全访问协议：自研 ZDP 协议，深度适配工作空间访问与跨域文件交换场景。实现数据面与控制面双重加密及动态密钥，全程“数据不落地”；安全高效访问，图像优化、低带宽占用；跨域协同体验优化，远程工作流畅。

精细化访问管控：基于“时间-地点-角色-终端”四维策略授权鉴权，支持应用级资源和使用者细粒度权限配置，严格执行“最小权限”原则。

终端访问安全管控：内置防截屏引擎，精准识别各类截屏工具并阻断。对终端访问工作空间的画面叠加明水印与盲水印，支持拍照截屏等双重溯源。外设接入严格认证管控，杜绝 USB、光驱、外接硬盘等非法操作，确保文件在终端侧“不留痕、不泄露”。

数据流转审批：建立跨区域、部门的数据流转管控机制，数据在不同可信保护区之间传输需通过自动规则校验或人工审批流程。全程记录流转日志，支持流转文件自动备份，满足追溯与合规要求。

数据电子围栏与追溯：通过电子围栏划定文件使用范围，确保重要数据不可流转出受控环境。快速回溯文件流转路径，精准定位数据泄露责任源。

灵活部署，集中管控，广泛兼容：支持多层级分布式部署，分部利用本地资源本地部署，总部统一管控与调度整体系统，本地化效率与全局管控兼得。平台提供的适配环境可广泛支持科研常用数据分析、仿真模拟、绘图设计类软件兼容性要求，满足科研人员专业需求。

志翔可信工作域管控平台——让您的科研工作更安全、更简单、更高效。



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