

IT 外包安全解决方案

助企业实现数据安全和效率共赢

亮点

- 💡 数据不落地，严控IT外包数据泄露风险
- 💡 多场景带宽自研优化算法，提高综合带宽利用率
- 💡 多重性能优化，外包综合效率平均提升近300%
- 💡 具备严格的审计机制，一键统计外包绩效
- 💡 支持多种IT环境、技术平台和外包模式
- 💡 接入快捷、应用高效，内部管理成本至少降低30%

行业背景

企业常将IT、人力资源或设计等非主营业务委托给专业服务公司管理和运维，IT外包帮助企业减少成本，快速获取所需技术、经验与资源，提升自身效率，更专注于其核心业务创新，但同时也带来诸多数据安全风险。据权威统计，近48%的企业内部数据泄露与第三方服务有关，如何更安全的使用IT外包服务，是企业面临的难题之一。

志翔科技IT外包安全解决方案，依托志翔领先的“无边界”和“零信任”安全理念，专门针对解决企业业务系统和IT研发外包所面临的监管复杂、泄密风险高等安全风险，及满足外包团队远程安全接入等业务开展需求。

方案以“保护数据、防止泄密、接入安全、提升效率”为出发点，围绕核心数据为中心进行统一安全和业务管控，有效解决了传统IT外包安全方案对IT外包方过度束缚所带来的诸如：内外工作割裂、资源浪费，工作效率和质量低下等问题，让IT外包商在保证高服务效率与质量同时，避免误碰安全红线。方案部署快捷、简单易用，让企业得以大大减少在IT外包监管上的精力投入，打消安全顾虑。

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

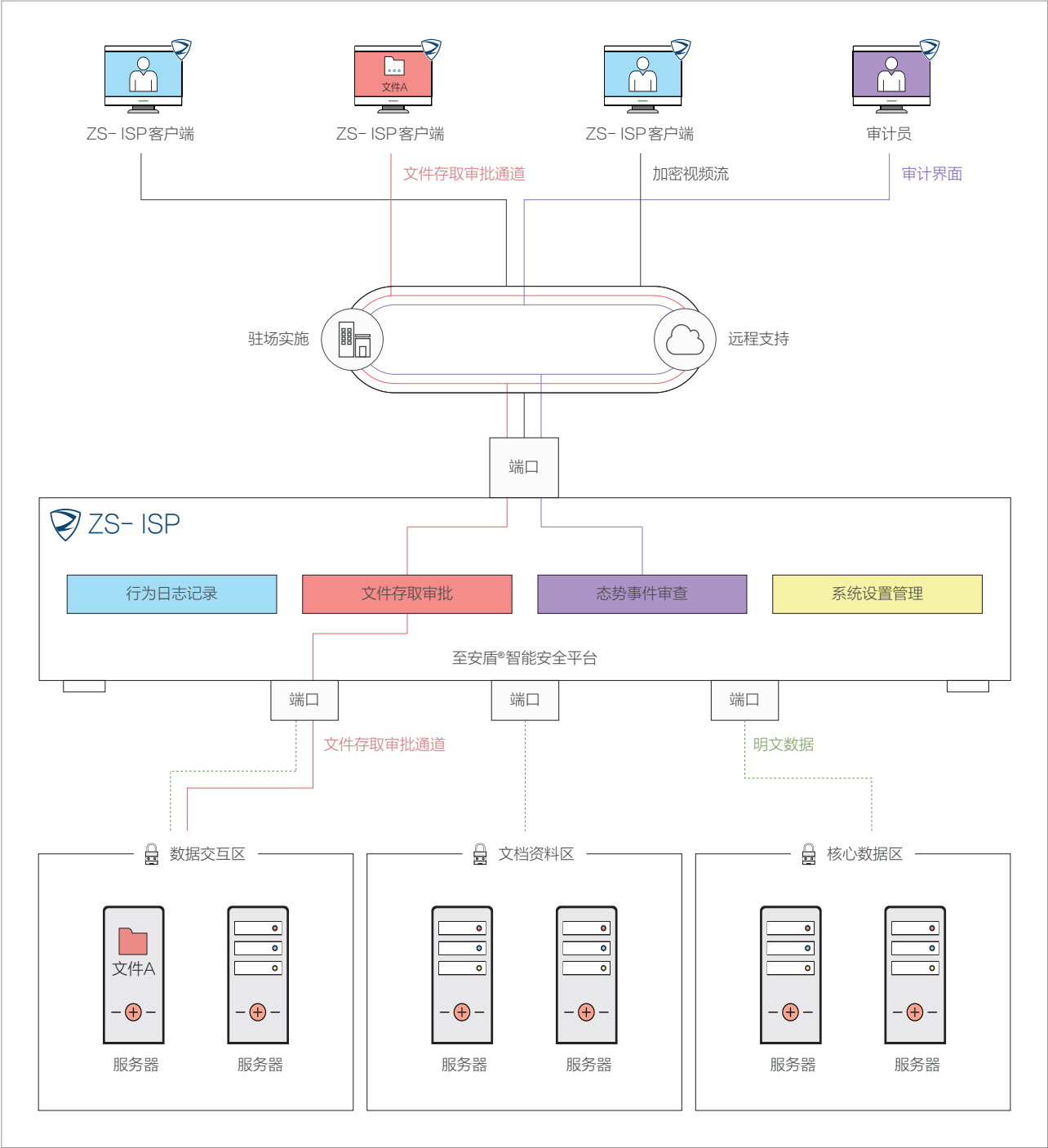
地址：北京市海淀区学院路35号世宁大厦1101

邮编：100191

方案部署

企业按需划分出IT外包服务保护区，串联部署志翔科技至安盾®ZS-ISP智能安全平台，隔离保护区与外包人员。外包人员在终端电脑上安装至安盾ZS-ISP客户端，通过登录客户端进行数据访问和办公。方案支持驻场及远程访问等多场景。

无需IT改动，几步即可快速部署上线，业务不中断；用户经客户端接入，不改变现有工作体验；集群部署，服务器负载运行可视化，IT运维可按需灵活分配资源、弹性扩展。



方案功能

志翔科技IT外包安全解决方案以至安盾ZS-ISP智能安全平台作为业务、办公的统一入口，划分和隔离数据保护区与办公区。保护区内数据以视频流的形式传输至外包人员终端被访问和操作，数据不落地。方案对所有外包人员进行集中管控，全面监控用户行为，可视化外包服务状态，实时预警可疑行为。根据企业需求，方案可支持多个外包项目保护区划分与访问控制配置。同时，提供智能审计机制，快速统计外包绩效，有效提高外包工作效率节省资源投入。

🔒 隔离保护

- 隔离外包与内部环境，外包工作在隔离区进行，并保存至隔离区，降低数据泄露风险。
- 隔离区中提供完整验证环境，确保外包工作质量可控。
- 日志全记录，数据访问操作行为随时可审计。

⚙️ 管理提升合规可视

- 智能审批文件存取，减少人工环节，降低沟通管理成本。
- 可视化评估外包服务与当前安全状态；项目验收有依据，保质提效。
- 兼顾外包管控与内控合规要求。

满足多行业外包场景需求



志翔IT外包安全解决方案适用于：

IT系统建设及业务外包、系统集成支持、驻场服务支持、IT远程支持、系统定制开发、系统运维外包等多种外包服务模式。

方案支持多种IT环境；支持Windows、Linux等多种研发模式；适配主流IT外包及研发安全架构，兼容现有终端安全模式。

支持多种服务器虚拟化模式，和Windows、Linux、MacOS等多种终端接入。