志翔科技
ZSHIELD INC

内网办公安全解决方案

方案价值

- 防止数据和文件泄露
- 阻断非法终端接入内网
- 简化安全运维，降低运维成本

方案亮点

- 安全的接入协议，彻底的网络防护
- 严密的数据保护，完善的数据流转
- 强大的审计追溯，智能的安全预警
- 分布式网络部署，统一的安全管理
- 高可靠稳定运行，高性能业务支撑

内网办公安全解决方案基于至安盾®智能安全平台。该装置功能强大，不仅提供安全云桌面实现人与业务系统、数据的隔离，而且装置本身基于业界领先的安全技术构建，支持三权分立、安全分区、数据流转、报警预警和审计追溯等五大安全策略，以及嵌入式防火墙、访问控制、安全接入协议等三道安全防线。

至安盾智能安全平台支持分布式部署和统一安全管理。可直接在办公场所的机房实施云桌面服务器的分布式部署，利用本地带宽有效保障各部门工作人员与协作单位人员的接入带宽需求，解决了集中式云桌面部署地的带宽需求无法满足的问题。同时，至安盾采用了高性能的I/O架构，支持基于高性能SSD的镜像加载和多硬盘、多I/O的用户数据访问，有效解决I/O瓶颈问题。通过在上级机构和总部部署分控和总控设备，进行集中监测和管控，实现统一安全管理。

关于志翔科技

志翔科技是国内创新型的大数据安全企业，致力于为政企客户提供核心数据保护和业务风险管控两个方向的产品及服务。志翔科技打破传统固定访问边界，以数据为新的安全中心，为企业构筑兼具事前感知、发现，事中阻断，事后溯源，并不断分析与迭代的安全闭环，解决云计算时代的“大安全”挑战。志翔科技是2017年IDC中国大数据安全创新者，2020年数世咨询评选的中国网络安全百强企业，并获中国网络安全产业联盟（CCIA）“2020年中国网络安全成长之星”（CCIA成长之星），以及赛博英杰《2020年中国网络安全十大创新方向》代表厂商。2019-2020年，志翔科技的至明产品连续两年入选Gartner《云工作负载保护平台市场指南》。

更多信息

如欲了解有关志翔科技至安盾®ZS-ISP、至明®ZS-ISA安全探针产品的更多信息，请联系您的志翔科技销售代表，或访问官方网站：www.zshield.net

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

业务痛点

办公电脑被盗用

恶意人员可能利用办公人员离开工位的空档，操作电脑进行数据窃取或数据破坏，甚至通过该电脑向全网传播木马。

端口管控困难

办公区域人员流动较大，针对串口、并口、USB等接口的非法设备接入，缺乏有效的管控手段，存在数据泄露风险。

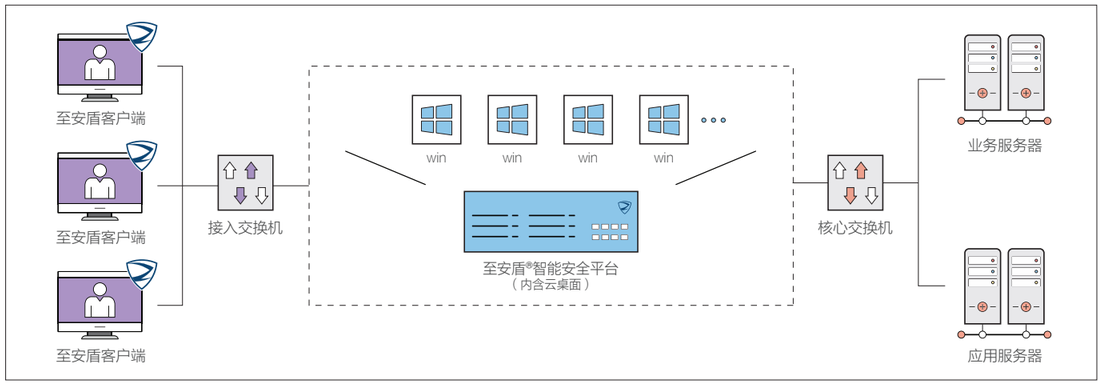
非法设备接入网络

若非法设备通过办公区域的网络接入电力公司网络，可能造成数据泄露、系统破坏、木马种植和传播等。

运维管理成本高

由于PC用户修改桌面环境的需求各有不同，桌面标准化难以实现；且PC分布在各个办公区域，运维安全与成本平衡困难，运维成本高。

解决方案



云桌面接入和业务系统隔离示意图

数据隔离保护

至安盾使用安全虚拟化技术，业务操作者所在的终端区只能看到视频，从而实现数据不落地，数据与业务操作者隔离的安全效果，同时不降低工作效率。

数据流转审批

数据流转审批支持不同用户和业务区域之间数据传送机制，在人工、自动或者各种组合策略的审批流程下，实现数据流转管理和效率提升。

运维安全监管

系统所有操作日志自动上报，各级分控审计所有下级日志，总控审计全网操作日志。基于此达成对运维安全的实时监管，可对下级运维充分授权并同时保证系统安全。从而解决因监管不到位、有安全担忧而无法给下级充分授权，导致运维效率低下的痛点。

安全接入控制

通过自有DPD协议，实现可信接入；支持用户、时间、访问来源和接入类型的四元组管控策略。该协议还能支持低带宽工作环境，同时具有最佳的外设兼容性。

实时报警预警

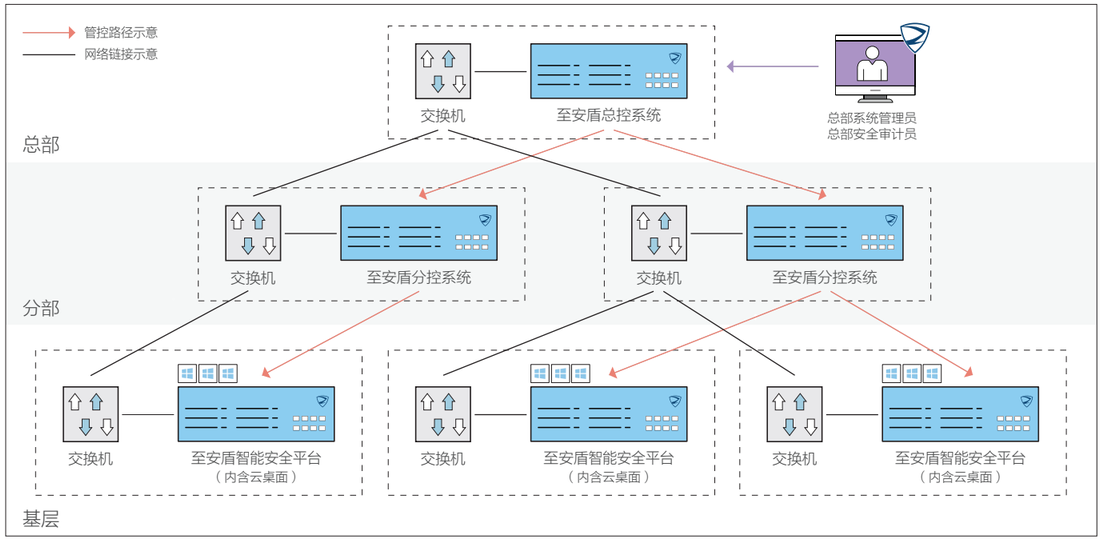
实时监控整个系统，发现违规操作，立刻产生安全告警，系统随之采取阻断等相关措施。针对多级部署场景，支持统一配置各级报警策略以及各级告警实时上报。

集群部署支持

云桌面支持N+M模式集群部署，可将一台服务器之上的云桌面虚拟机动态迁移至其他服务器；用户的数据在集群系统中可靠热备；任何单机节点退出服务，集群服务不降级。

部署方式

在基层办公场所分布式部署至安盾智能安全平台，就地提供办公接入服务；在上级机构和总部部署分控和总控设备，实现数据访问路径和管控路径的分离，并实现多级统一管理。



内网办公安全部署拓扑图

功能优势

安全性

桌面与应用全部运行在服务器上，集中进行安全管控。数据和文件等与客户端桌面隔离，实现不落地访问方式。制定严格的访问策略，控制用户对桌面应用的访问权限。实现日志安全留存，支持合规审查和事件追溯。

可靠性

集群架构保证服务可用性，不存在直接影响整体架构问题的单点故障。系统级硬件冗余，功能组件支持高可用性，单元功能组件出现故障不影响用户使用。提供主动监控服务，建立报警机制、负载共享和故障切换机制，实现无缝转移负荷。

可扩展性

支持Windows、Linux等不同操作系统终端的接入。支持远程应用、会话桌面、增强桌面等多种云桌面模式。可从容应对云桌面扩容以及IO性能需求和带宽需求增加等方面带来的压力。

用户体验

内置云桌面提供与PC机一致的使用体验。用户可使用各种配置的硬件设备访问桌面或应用，如笔记本、PC机和瘦客户机等。系统管理员统一进行系统维护和应用软件升级等工作，用户仅需专注本职工作。

场景及案例

内网办公安全解决方案适用场景丰富，可灵活运用于内网办公接入、研发网络、合作伙伴对接等场景的安全加固，保证业务系统和数据安全。该方案已在政府、科技、教育、电力等行业进行部署，实现了办公网络和研发网络的PC桌面替换和安全加固。