志翔科技
ZSHIELD INC

零信任安全解决方案

零信任、无边界，为企业应用与数据安全提供全面保护

客户价值

满足安全合规要求：符合企业系统安全建设、等保及数据安全法等相关的安全合规管理要求。

加固企业数据安全防御体系：配合既有边界和终端等安全产品，进一步加固企业数据安全防御体系，规避传统VPN等系统存在的权限分配和并发能力不足，及安全漏洞多等问题。

收敛业务暴露面减少攻击：零信任可收敛业务系统暴露面，隐藏实际业务系统IP和端口，可有效防止端口扫描、漏洞扫描等工具发起的渗透攻击，提升在HW行动等场景中的防御水平。

提升企业用户身份和环境治理水平：通过统一账号、多因素认证，提高用户身份认证的强度和精度；利用持续终端环境检查评价加强员工终端的安全水平和安全意识，从而提升企业整体身份和环境治理水平，减少网络攻击和数据泄露风险。

服务客户

紫光展锐 UNISOC · Cambricon 寒武纪 · 长江存储 YANGTZE MEMORY · Empyrean 华大九天 · Maxscend · BES 恒玄科技

比特大陆 BITMAIN · 兆芯 · H-Grace 華芯宏力 · 君正 Ingenic · 金升阳 MORNSUN · 华大北斗 ALLYSTAR

NOVOSENSE 纳芯微电子 · xiaomi · NIO 蔚来 · 国家开发银行 CHINA DEVELOPMENT BANK · 昆仑银行 Bank of Kunlun

亮点

高性能和安全增强：控制中心和安全网关均采用高可靠性设计，保障用户高并发场景的连接稳定性，传输快，延迟小。增强的身份认证等安全特性大大提高攻击门槛

易用灵活的策略引擎：基于ABAC机制的策略引擎可灵活配置出不同策略结构，支撑不同行业客户需求，便捷的用户和资源管理为系统运维提供便利

弹性按需扩展：安全网关采用注册机制调度分配，按不同网络区域和业务提供不同网关建连，系统不下线即可快速按需扩展网关能力

轻量部署广泛兼容：客户端轻量级部署和运行，系统资源占用少，兼容第三方终端安全产品，支持各类终端设备访问不同类别的应用资源

基于零信任架构的网络接入、应用访问控制和数据保护

志翔科技“零信任、无边界”解决方案遵循零信任安全架构设计，符合行业零信任标准，支持Web应用、隧道应用、桌面、网盘等多种业务资源的接入访问体验，为企业构建统一访问的无边界应用和数据安全防护体系。方案可广泛应用于政府、金融、高科技等行业的远程办公、研发和运维等接入场景。

云计算、5G、物联网等技术发展推动移动办公等新应用的落地，企业数字化转型进程加速推进，企业的业务架构和网络环境不断演进和快速变化，传统的安全体系已经难以适应和满足其需求：

- 远程办公、多方协同办公等成为常态，企业面临应用访问需求复杂化，内部资源暴露面不断扩大等风险。
- 各种设备（BYOD、合作伙伴设备）、各类人员接入大大增加安全管理难度，带来诸多不可控的安全风险。
- 高级威胁攻击频发，带来边界高筑墙的安全防护逻辑不再适用。

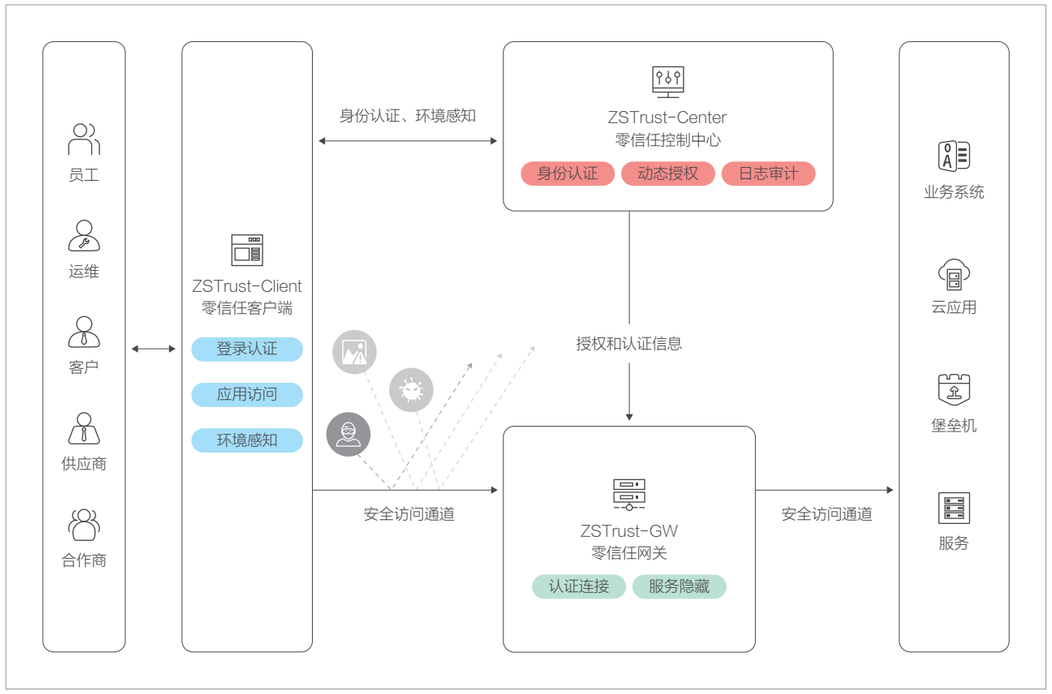
关注志翔

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

志翔科技零信任解决方案

方案以志翔至锐联®ZS-Trust零信任访问控制系统为核心，并包含多个灵活可选的安全模块组件。

至锐联®ZS-Trust零信任访问控制系统是基于零信任理念架构设计的软件定义边界产品，通过统一应用门户，基于身份建立最小权限访问，支持多种业务资源的接入访问体验，可为多行业客户在无边界网络环境中构筑安全、高效、稳定的办公网络。



零信任安全模块、组件

零信任控制中心：零信任控制中心是整个系统的安全大脑，负责管理各安全应用模块，进行授权认证、安全规则策略的制定、下发、控制和动态调整，并监控整个系统运行状况和业务动态。控制中心持续不间断地收集控制区域所有的操作信息、日志、报警，与安全事件联动进行智能分析和审计，并可视化呈现。

零信任网关：零信任网关是整个系统的策略执行点，负责建立访问主体与资源之间的安全访问通道。基于SPA单包授权，网关在“网络隐身”的状态下，可仅针对授权客户端建立加密传输通路。同时，基于访问控制模型，网关可对用户的访问行为进行持续监测、动态身份认证和权限判定，从而为企业构建持续、可信的网络访问环境。

零信任客户端：零信任客户端是访问主体的访问行为发起端，为访问主体提供用户登录和资源访问的界面。客户端支持用户通过多种认证方式向控制中心认证并获得授权的业务资源。同时客户端持续对终端设备环境进行检测和准入认证，限制仅“可信”的设备才被允许接入网络，并有相应安全措施防止数据的窃听、篡改和泄露。

方案部署

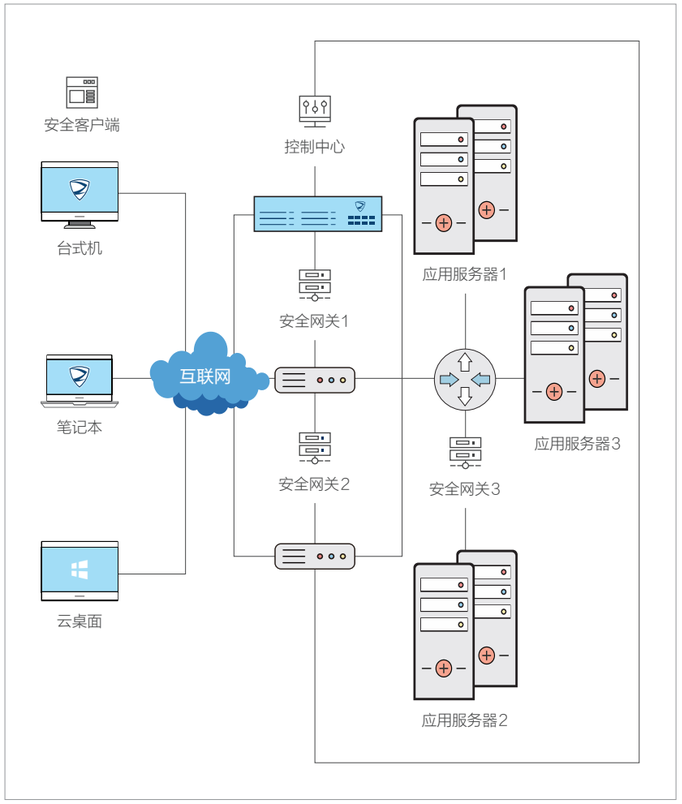
统一身份管理：对用户进行统一管理和身份认证，对接企业的已有身份认证系统等，仅允许认证用户访问授权资源。

最小授权原则：配置访问者和资源之间的细粒度、最小访问权限的策略，建立用户的终端准入规则，动态调整授权用户访问资源的权限。

安全代理网关：基于SPA单包授权，建立起可信客户端授权资源之间的加密连接通道，实现业务资源的“网络隐藏”。

终端环境感知：基于检测策略，客户端持续对终端设备的环境进行感知和度量，仅允许“可信”的设备才能访问资源。

精细审计运维：提供详细的用户认证、资源访问和系统运行的审计日志，便捷的用户和资源维护管理功能。



应用场景

远程办公
- 远程研发和办公
- BYOD，替换VPN
- 最小权限/动态授权

远程运维
- 运维人员权限管控
- 远程协作
- 数据防泄漏保护

攻防对抗
- 业务隐藏
- 不暴露任何端口
- 避免攻击

终端加固
- 终端持续监测管控
- 动态授权
- 应用准入访问

数据防泄漏
- 数据授权访问
- 终端安全措施
- 动态环境评估

合规改善
- 安全体系加固
- 终端环境评估治理
- 满足合规要求