志翔科技
ZSHIELD INC

至锐联® ZS-Trust 零信任访问控制系统

云计算、大数据、移动办公等推动企业数字化转型进程加速，带来企业业务架构和 IT 基础架构的升级迭代。远程协同让企业业务开展更加高效、便捷，但同时各类设备、人员和应用的接入，带来访问场景复杂化和内部资源暴露面扩大化，也进一步加大安全运营的管理难度，让企业面临新的安全风险。传统的边界安全理念和防护手段如部署边界安全设备、仅简单认证用户身份、静态和粗粒度的访问控制等显得捉襟见肘、难以应对。

零信任持续验证，构建无边界安全体系

至锐联® ZS-Trust 零信任访问控制系统（以下简称：至锐联）是基于无边界、零信任理念架构设计的安全接入管控产品。至锐联利用 SPA 等单包认证网络隐身技术，通过在互联网或企业网建立基于授权终端和针对特定资源的虚拟网络安全边界，根据用户身份和策略提供最小访问控制权限，并以灵活严密的安全机制和加密安全连接，管理调控用户的接入访问，从而减少网络访问的安全隐患。至锐联支持多种业务资源的接入访问体验，致力于为企业构建安全高效、灵活易用的统一安全访问体系。

产品优势

策略灵活 运维便捷

基于 ABAC 机制的策略授权体系，可针对不同角色用户灵活配置最小访问授权，满足不同行业客户需求；简单易用的用户和资源管理设计为系统运营提供便利。

安全可靠 性能高效

系统的认证模块、网关和资源均采用服务隐藏设计，大大降低业务系统暴露面，减少攻击风险。高可靠性设计保证高并发场景下的连接稳定性和弹性扩展能力，数据传输高效，访问延迟小。

轻量部署 兼容性广

支持多种终端设备通过各类应用对不同业务不同协议的应用资源进行访问；客户端轻量级部署和运行，对系统影响小，可广泛兼容第三方终端安全产品。

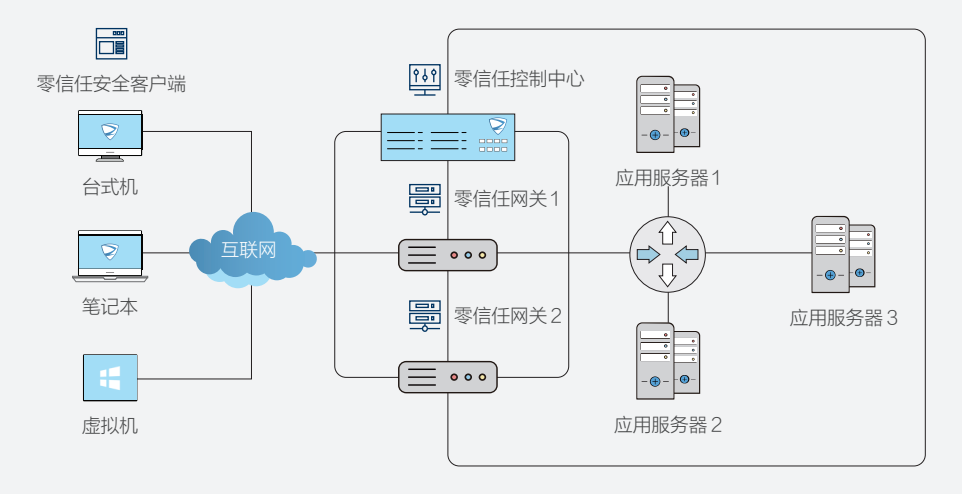
产品部署

至锐联遵循标准的零信任架构设计，包含控制中心、网关、客户端三个组件：

零信任控制中心：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、安全策略控制、终端设备和资源状态监控等。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，利用大数据技术进行可视化智能分析和审计。支持软部署或软硬件一体部署于企业内网或 IDC 等。

零信任网关：网关采用软部署或软硬件一体的方式部署于访问主体和业务资源之间，如内网边界或业务服务器上，为两者建立通道。网关基于 SPA 单包授权并在“网络隐身”的状态下，通过安全加密、服务隐藏等为可信客户端访问授权业务资源提供安全传输通道，为企业构建持续、可信的网络访问环境。

零信任客户端：客户端则安装于台式机、笔记本、虚拟机等各类终端主机上，为访问主体提供用户登录和资源访问的界面，支持用户通过多种方式身份认证并访问授权的业务资源。同时，客户端持续对终端设备环境进行检测和准入认证，“可信”设备方可允许接入网络和访问资源。



核心功能

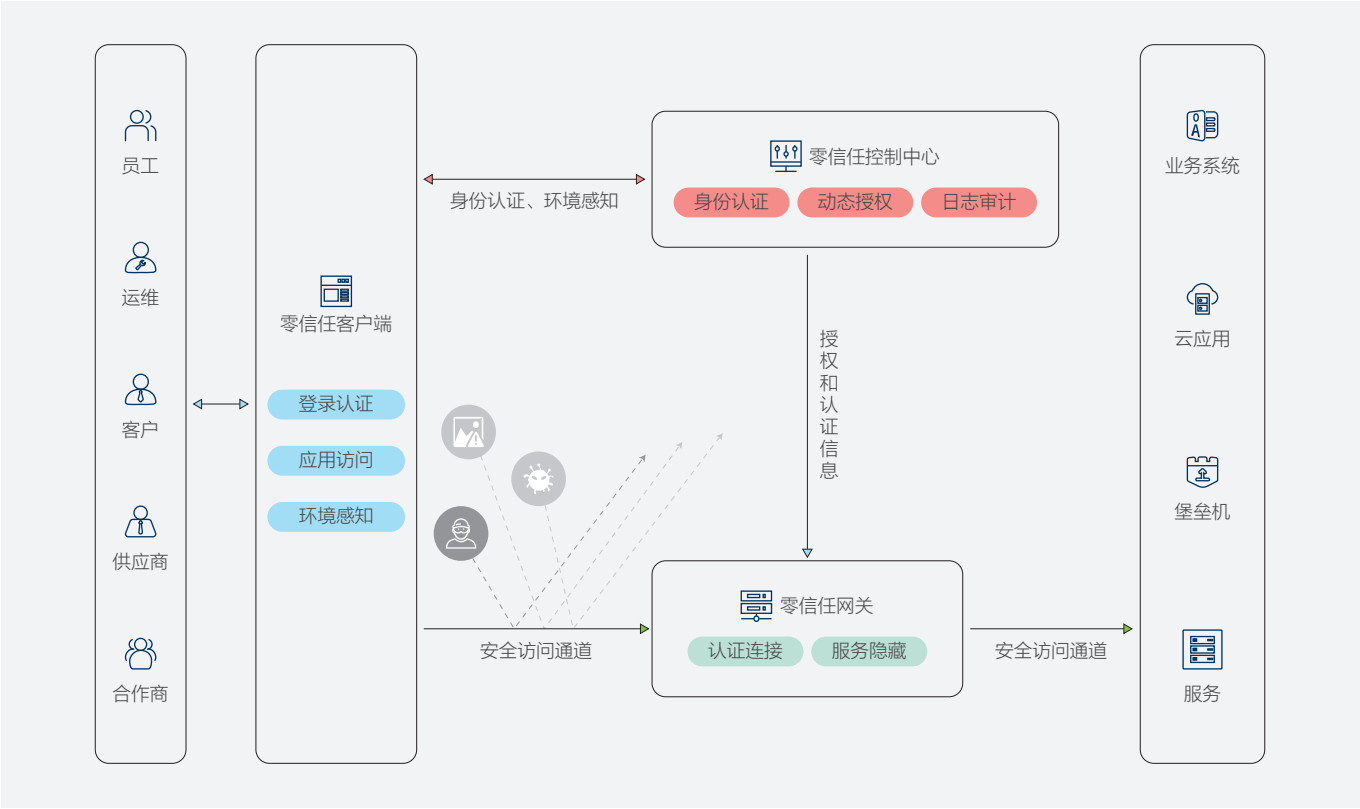
至锐联遵循零信任安全架构设计并具备增强数据安全能力，客户可按需进行灵活的策略配置和网关弹性扩展。至锐联兼容各类第三方安全软件，支持Windows 、Linux和Mac等操作系统，其核心功能包括：

统一身份认证：可对接企业的现有身份认证系统等平台，对用户进行统一管理和身份认证，认证用户仅可在鉴权后访问授权资源。

安全代理网关：基于SPA单包授权，为可信客户端和授权资源之间建立加密连接通道，从而实现业务资源的“网络隐藏”。

精细运营审计：对用户认证、资源访问和系统运行态势等采集详细的审计日志，并提供全面分析。支持对用户和资源的便捷维护管理，有效支撑企业IT运维管理。

智能端点感知：基于安全态势的检测策略，客户端持续对终端设备的环境进行感知和度量评估，仅允许“可信”设备访问授权资源。



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