



Zero Trust Network Access (ZTNA) Health Check by WhiteSpider

WhiteSpider is an industry expert in enabling business transformation through the power of digital technologies.

Working across the globe, we design, deliver, and manage Software Defined technologies that transform IT operations, secure business infrastructure, and enhance user experience.

Service overview

WhiteSpider's Zero Trust Network Access (ZTNA) Health Check is a comprehensive, remotely delivered service designed to assess the security posture, architecture, and operational effectiveness of an organisation's ZTNA deployment.

As organisations move away from traditional VPN-based remote access toward identity-centric security models, ZTNA platforms have become a critical component of modern secure access architectures. However, as environments evolve, policies grow, and integrations expand, configuration drift, policy complexity, and visibility gaps can emerge.

Our ZTNA Health Check provides organisations with an expert review of their ZTNA environment to ensure it is aligned with Zero Trust security principles, vendor best practices, and operational requirements, while identifying opportunities to improve security, performance, and user experience.

The service supports both cloud-delivered ZTNA platforms and hybrid deployments, including integration with identity providers, endpoint posture services, and secure access service edge (SASE) architectures.

Scope and coverage

The ZTNA Health Check evaluates the entire secure access architecture, including:

- ZTNA gateway and broker configuration
- Identity provider integration (Azure AD / Entra ID, Okta, etc.)
- Authentication and multi-factor authentication policies
- Device posture and endpoint compliance validation
- Application segmentation and access policies
- Integration with Secure Web Gateway (SWG) or SSE platforms
- Logging, telemetry, and monitoring configuration
- User experience and connectivity performance
- Security policy architecture aligned to Zero Trust principles

Benefits

A WhiteSpider ZTNA Health Check can help you:

- ✓ **Stronger security posture:**
Ensure your secure access environment aligns with Zero Trust security principles and reduces exposure to identity-based attacks.
- ✓ **Improved risk visibility:**
Identify gaps in authentication, device posture validation, and access policy enforcement.
- ✓ **Maximise technology investment:**
Ensure you are making full use of the capabilities provided by your ZTNA platform.
- ✓ **Support strategic security initiatives:**
Strengthen your organisation's Zero Trust strategy and broader SASE or SSE adoption.
- ✓ **Improved access control management:**
Simplify policy structures and reduce complexity in application access configuration.
- ✓ **Enhanced monitoring and incident visibility:**
Ensure access activity is properly logged, monitored, and integrated into security operations workflows.
- ✓ **Optimised user experience:**
Identify configuration issues that may impact authentication performance or application access.
- ✓ **Future architecture readiness:**
Ensure the ZTNA platform is positioned to scale as your workforce, applications, and security strategy evolve.

What we do

WhiteSpider engineers perform a structured remote assessment using a combination of platform analysis, configuration review, policy evaluation, and best practice benchmarking.

The service is delivered entirely remotely using secure access methods and collaboration with your security and infrastructure teams.

- Our methodology includes:
- Architecture review of the ZTNA deployment
- Assessment of identity and authentication integrations
- Review of application access segmentation policies
- Evaluation of device posture validation mechanisms
- Analysis of logging, monitoring, and alerting configuration
- Security posture review against Zero Trust best practices
- Evaluation of user experience and performance factors
- Review of integration with broader security platforms such as SIEM, XDR, or SSE

Typical activities

Identity and access control

- Integration with identity providers
- MFA policy enforcement
- Conditional access configuration
- Role-based access models

Application access policies

- Application segmentation strategy
- Least privilege access enforcement
- Policy complexity and redundancy
- Application discovery and onboarding process

Device posture and endpoint security

- Endpoint posture validation
- Device trust mechanisms
- Endpoint compliance policies

Security architecture

- Alignment to Zero Trust principles
- Identity-centric access model validation
- Micro-segmentation effectiveness
- Integration with security monitoring platforms

Performance and user experience

- Gateway availability and resilience
- Authentication latency
- Application access performance

Monitoring and visibility

- Logging configuration
- Integration with SIEM/XDR platforms
- Alerting and incident visibility

Deliverables

Following the assessment, WhiteSpider provides a comprehensive PowerPoint presentation report tailored for both technical and executive stakeholders.

The report includes:

- ✓ Executive summary and overall security posture
- ✓ Executive summary and overall security posture
- ✓ ZTNA architecture overview
- ✓ Risk and health scoring across key categories
- ✓ Detailed findings and observations
- ✓ Security and operational improvement recommendations
- ✓ Best practice alignment guidance
- ✓ Prioritised remediation roadmap



Telephone: +44 20 3773 2380
E-mail: info@whitespider.com
Website: www.whitespider.com

