SNO
A smarter tomorrow.

MANAGED ZERO TRUST NETWORK ACCESS (ZTNA) SERVICE FOR ENTERPRISE AND PUBLIC SECTOR CUSTOMERS

IDENTITY-DRIVEN, APPLICATION-LEVEL SECURE ACCESS

Specialist Network Operations

Service Overview

SNO's Managed Zero Trust Network Access (ZTNA) service delivers secure, identity-centric access to applications and services without exposing the underlying network. Designed for organisations adopting cloud services, hybrid working and modern security architectures, the service replaces traditional perimeter-based access models with a zero-trust approach.

The Managed ZTNA service ensures users and devices are continuously verified before access is granted, with access decisions based on identity, device posture, context and application sensitivity. Access is provided at the application level rather than the network level, significantly reducing attack surface and lateral movement risk.

Backed by SNO's experienced security and network operations teams, the service provides end-to-end ownership of design, deployment, policy management, monitoring and incident response, enabling organisations to adopt zero trust securely without operational complexity.

The service is purpose-built for enterprise and public sector organisations that require strong access controls, auditability and secure access to internal, cloud and third-party applications.

What You Get

Identity-Driven, Application-Level Access

The Managed ZTNA service enforces access based on who the user is, the security posture of their device and the application being accessed.

- Application-level access without exposing the internal network.
- Continuous verification of user identity and device posture.
- Context-aware access decisions based on location, risk and behaviour.
- Least-privilege access aligned to zero-trust principles.

Secure Remote and Hybrid Workforce Access

SNO designs and operates resilient WAN architectures that maximise availability and performance.

- Active-active use of multiple underlay connections.
- Seamless failover without user intervention.
- Optimised use of lower-cost broadband links alongside private circuits.
- Support for branch, campus, data centre and cloud connectivity.

Integrated Security & Policy Enforcement

Security controls are embedded directly into the access workflow.

- Strong authentication and continuous trust evaluation.
- Granular application access policies.
- Integrated inspection and enforcement of security controls.
- Alignment with zero-trust and defence-in-depth strategies.

Access Security Incident Management & Customer Communications

SNO provides full ownership of ZTNA-related security incidents through a structured Incident Management process designed to minimise risk and restore secure access rapidly.

Each incident is owned by a dedicated Service Delivery Manager (SDM) or NOC Team Lead, acting as the single point of accountability throughout the incident lifecycle. All incidents are managed through SNO's Service Desk, ensuring governance, traceability and consistent communication.

Situation updates are provided by the relevant security and operations teams, with Service Alerts and Status Updates distributed based on incident severity and business impact. All investigation, containment and remediation actions are logged in SNO's Service Management platform, ensuring transparency and audit readiness.

Lessons learned are reviewed and used to refine access policies, device posture checks and enforcement rules through the formal Change Management process.

Automated Enforcement with Expert Oversight

SNO's Managed ZTNA service combines automated access control with expert human oversight.

- Continuous evaluation of user and device trust.
- Automatic revocation or restriction of access when risk is detected.
- Analyst-validated alerts to reduce false positives.
- Expert-led investigation of access anomalies and policy violations.
- Formal Root Cause Analysis (RCA) for high-impact incidents.

Full ZTNA Lifecycle Management

SNO manages the complete lifecycle of the ZTNA service.

- Access architecture design aligned to application and user requirements.
- Structured onboarding of users, devices and applications.
- Centralised visibility into access activity, policy enforcement and compliance.
- Secure offboarding and decommissioning of users and applications.

Policy-Driven Control & Governance

Access behaviour is governed through auditable, centrally managed policies.

- Application-specific access policies.
- Role-based access control (RBAC) aligned to least-privilege principles.
- Device posture and compliance-based enforcement.
- Full visibility and traceability of policy changes.

Configuration & Change Management

SNO operates the Managed ZTNA service under a formal Configuration and Change Management framework to ensure access controls remain predictable, controlled and auditable.

Configuration Management includes:

- Secure baseline configurations for access policies and enforcement rules.
- Centralised management of users, applications and trust policies.
- Continuous validation to detect configuration drift or unauthorised changes.
- Secure versioning and documentation of all configuration items.

Change Management

All changes to ZTNA policies, configurations or enforcement logic are governed through SNO's formal Change Management process.

- Risk and impact assessment prior to implementation.
- Expedited approval for emergency security-driven changes.
- Full logging, tracking and post-implementation review.

Customers are provided visibility into material changes impacting access behavior, security posture or compliance.

Reduced Attack Surface & Access Risk

SNO's Managed ZTNA service reduces access-related risk by enforcing a zero-trust access model and limiting exposure of internal applications and services.

- Eliminates implicit trust by requiring continuous verification of user identity, device posture and access context.
- Restricts access to explicitly authorised applications, preventing unnecessary network visibility.
- Limits lateral movement through application-level segmentation and least-privilege access controls.
- Continuously re-evaluates access during active sessions and enforces policy changes where risk increases.

Built for Resilience and Continuity

SNO's Managed ZTNA service is designed to support always-on operations.

- Resilient access enforcement architecture.
- Continuous monitoring of service health and access availability.
- Business Continuity and Disaster Recovery (BCDR) planning and annual testing.

Seamless Integration with Your IT Ecosystem

Where required, the service can integrate with your existing tools and platforms, including:

- Identity and access management systems.
- Endpoint security and posture assessment tools.
- Network and security enforcement platforms.
- IT service management and ticketing systems.

** *Integration scope subject to separate scoping and agreement*.

Clear Reporting & Audit Readiness

Service Performance & Operational Metrics

SNO measures and reports on the operational performance of the Managed ZTNA service to ensure access control remains effective, predictable and aligned with agreed service levels. Reporting provides clear visibility into access enforcement, incident handling and service outcomes, supporting operational oversight, continuous improvement and audit assurance

Reported metrics include:

- Access success and failure trends.
- Policy enforcement and access decision metrics.
- Incident response and resolution timelines.
- Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).
- SLA adherence and service outcomes.

Trend analysis is included to identify recurring issues, capacity constraints and optimisation opportunities.

Reporting cadence

- Monthly operational reporting covering access activity, incidents and changes.
- Quarterly executive service reviews highlighting security posture and trends.
- Annual or on-demand audit and compliance reporting aligned to governance and regulatory requirements.

Service Levels (At a Glance)

SLA Metric	Target
Access Event Detection	< 5 minutes
Operational Response	< 30 minutes
Access Restriction	Immediate upon confirmation
Root Cause Analysis	< 7 days (High / Critical Incidents)
Reporting Delivery	As agreed

Operational Service Elements (At a Glance)

Service Element	Availability	Description
Service Desk Management	24x7x365	Acts as the single point of contact for all ZTNA-related incident reporting, service requests and operational queries. Ensures consistent intake, tracking and governance of all customer interactions.
Incident Management	24x7x365	Manages ZTNA security and access incidents to minimise business impact by restoring secure application access as quickly as possible. Incidents are handled using a structured, repeatable lifecycle aligned with agreed service levels.
Escalation Management	24x7x365	Ensures functional and hierarchical escalations are executed within defined KPIs to maintain response momentum, service assurance and stakeholder visibility.
Event Management	24x7x365	Proactive monitoring and handling of access events, alerts and anomalies generated by ZTNA telemetry, policy enforcement and device posture checks across the supported environment.
Account Manager	Mon-Fri 08:45-17:30	A named Account Manager provides commercial oversight and acts as an escalation point during core business hours.
Service Delivery Manager	Mon-Fri 08:45-17:30	A named Service Delivery Manager (SDM) is responsible for operational governance, SLA oversight, incident accountability, and service performance reporting and acts as an escalation point during core working hours.
Technical Account Manager	Mon-Fri 08:45-17:30	A named Technical Account Manager provides technical oversight of the ZTNA service, supports policy optimisation and acts as an escalation point for complex technical matters during core working hours.
SLA Management	Included	Definition, monitoring and reporting of response, resolution and service availability targets aligned with the Managed ZTNA service levels.
Customer Portal Access	Included	Secure access to SNO's service portal for incident logging, service requests, status visibility and reporting access.
Performance Management	Included	Continuous monitoring of access performance, policy enforcement and user experience to ensure service objectives are met and to support capacity planning and optimisation.
Availability Management	Included	Ensures the Managed ZTNA service delivers agreed levels of availability, secure access and resilience to support business-critical applications.
Change Enablement / Release Management	Included	Controls changes to ZTNA policies, access rules and platform updates to minimise risk while maintaining operational stability and policy compliance.

Service Request Management	Included	Handles standard operational requests as part of business-as-usual service delivery through defined request fulfilment workflows.
Problem Management	Included	Identifies underlying causes of recurring access or policy incidents and implements corrective actions to reduce future impact.
Security Management	Included	Oversees risks related to the confidentiality, integrity and availability of application access, user sessions and enforcement policies.
Asset Management	Included	Maintains visibility and lifecycle control of ZTNA devices, clients, applications and associated access assets, supporting secure onboarding and decommissioning.
Configuration Management	Included	Maintains controlled, auditable ZTNA configurations, including baseline policy definitions, change tracking and configuration integrity monitoring.
Release Management	Included	Ensures operational readiness for new ZTNA features, platform enhancements and policy updates while minimising service disruption.
Service Reporting	Included	Comprehensive monthly reporting covering access activity, policy enforcement, incidents, SLA adherence and service trends across all service elements.

Why Choose SNO's Managed SD-WAN Service for Enterprise and Public Sector?

SNO's Managed ZTNA service enables organisations to adopt zero trust without the complexity of operating access controls in-house. By combining identity-driven access, continuous verification and expert operational oversight, we help enterprise and public sector organisations reduce risk, support modern working practices and maintain strong governance, so secure access becomes an enabler, not a barrier.