SNO
A smarter tomorrow.

MANAGED SECURE ACCESS SERVICE EDGE (SASE) SERVICE FOR ENTERPRISE AND PUBLIC SECTOR CUSTOMERS

UNIFIED SECURE ACCESS AND NETWORKING FOR MODERN, DISTRIBUTED ORGANISATIONS

Specialist Network Operations

Service Overview

SNO's Managed Secure Access Service Edge (SASE) service provides enterprise and public sector customers with a fully managed, cloud-delivered secure access and networking solution that converges network connectivity and security into a single, policy-driven service.

The service enables secure, high-performance access to applications, data and services for users, devices and locations, regardless of where they are located. While simplifying operations and reducing the complexity of managing multiple point solutions.

Designed for organisations modernising their networks to support hybrid working, cloud adoption and distributed operations, SNO's Managed SASE service delivers consistent security enforcement, centralised policy control and optimised connectivity, without the cost and operational burden of managing complex infrastructure in-house.

The service supports users, branch locations, remote workers and cloud environments, providing a unified operational model that improves visibility, reduces risk and strengthens service resilience.

What You Get

Unified Secure Access and Networking

SNO's Managed SASE service converges networking and security capabilities into a single, cloud-managed architecture.

- Secure access to applications and services for users, devices and sites, regardless of location.
- Policy-based enforcement applied consistently across all access methods.
- Integrated networking and security controls delivered as a unified service.
- Centralised visibility across users, traffic, applications and security posture.

Always-On Protection with Integrated Threat Intelligence

Security controls are continuously enforced using real-time inspection and globally sourced threat intelligence.

- Continuous inspection of user and application traffic.
- Protection against known and emerging threats.
- Automatic updates to security services without operational disruption.
- Risk-based enforcement aligned to active threat campaigns targeting enterprise and public sector organisations

Secure Access Policy Management & Customer Communications

SNO provides end-to-end ownership of secure access policy design, implementation and ongoing management through a structured service model designed to minimise disruption and ensure consistent enforcement.

Each customer is supported by a named Service Delivery Manager (SDM) or NOC Team Lead, who acts as the single point of accountability for service operations, incidents and changes. All service activities are managed through SNO's Service Desk, ensuring governance, traceability and consistent communication.

Service updates, incidents and changes are communicated in line with agreed service levels and customer impact. All actions are logged within SNO's Service Management platform, ensuring transparency, auditability and compliance readiness.

SNO's primary objective is to maintain secure, reliable access to business-critical applications while preserving performance and user experience.

Automated Enforcement with Expert Oversight

The Managed SASE service combines automated policy enforcement with expert operational oversight.

- Centralised, policy-driven access control.
- Automated enforcement of security and routing policies.
- Analyst oversight for complex access, performance or security events.
- Coordinated control across users, devices, branches and cloud environments.
- Root Cause Analysis (RCA) for high-impact service or security incidents.

Access Use Case & Policy Playbook Management

Secure access and networking operations are delivered through structured use cases and operational playbooks.

- Predefined and custom access policies aligned to customer risk profiles.
- Secure onboarding workflows for users, devices and locations.
- Continuous tuning of policies based on usage patterns and threat trends.
- Documented operational playbooks to ensure consistent, repeatable service delivery.
- Alignment with recognised security and networking frameworks.

Policy-Driven Control & Governance

The service operates within a governed, auditable framework aligned to customer policies and compliance requirements.

- Role-based access control (RBAC) aligned to least-privilege principles.
- Centralised policy definition and enforcement.

- Segregation of duties across operational and administrative roles.
- Full audit trail of access events, policy changes and administrative actions.

Configuration & Change Management

SNO delivers the Managed SASE service under a formal Configuration and Change Management framework to ensure consistency, control and auditability throughout the service lifecycle.

Configuration Management includes:

- Establishment of secure baseline access and security policies.
- Centralised management of access rules, routing and inspection policies.
- Continuous validation to detect misconfiguration or drift.
- Secure documentation and version control of configurations.

Change Management ensures:

- Risk and impact assessment prior to implementing changes.
- Expedited handling of emergency changes impacting service availability or security.
- Full change logging, validation and post-implementation review.

Reduced Risk & Improved Access Security Posture

The Managed SASE service actively reduces operational and security risk by:

- Enforcing consistent access policies across all users and locations.
- Reducing exposure caused by unmanaged or implicit network trust.
- Improving visibility into application usage and access behaviour.
- Simplifying the security architecture by consolidating multiple controls.

Built for Resilience and Performance

SNO's Managed SASE service is designed to support always-on, mission-critical access.

- Resilient, cloud-delivered service components.
- Optimised routing for application performance.
- Secure handling of access logs and telemetry.
- Business Continuity and Disaster Recovery (BCDR) planning and testing.

Seamless Integration with Your Environment

Where required, the service can integrate with existing enterprise platforms, including:

- Identity and access management systems.
- Endpoint and device management platforms.
- Cloud and SaaS applications.
- Logging, monitoring and service management tools.

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

Clear Reporting & Audit Readiness

Service Performance & Operational Metrics

- Visibility into secure access coverage and policy effectiveness.
- Monitoring of service performance, availability and user experience.
- Trend analysis to identify access risks or performance bottlenecks.
- Review of SLA adherence as part of regular service reporting.

Reporting cadence

- Monthly service and incident reporting
- Quarterly executive reporting
- Annual or on-demand compliance and audit reporting

Service Levels (At a Glance)

SLA Metric	Target
Policy Enforcement Availability	99.9%
Incident Response	< 30 minutes
Change Implementation	As agreed
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 incidents, service requests and operational queries related to the Managed SASE service. Ensures consistent intake, prioritisation, tracking and governance of all customer interactions via SNO's Service Desk.
Security Incident Management	24x7x365	Manages secure access, connectivity, performance and security incidents to minimise business impact by restoring secure connectivity as quickly as possible using a structured, repeatable incident lifecycle aligned with agreed service levels.
Escalation Management	24x7x365	Ensures functional and hierarchical escalations are executed within defined KPIs to maintain response momentum and service assurance.
Security Access Monitoring	24x7x365	Continuous monitoring, correlation and analysis of access activity, traffic flows, policy enforcement, security events and service health across users, devices, sites and cloud environments.
Policy & Use Case Management	Included	Development, tuning and ongoing management of secure access policies, use cases and enforcement rules aligned to customer risk profiles, access requirements and evolving threat and usage patterns.

Automated Policy Enforcement & Orchestration	Included	Execution of automated and semi-automated access, security and routing policies to ensure consistent enforcement, rapid containment of access issues and reduced operational overhead.
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, supports service optimization and acts as an escalation point for complex technical matters and acts as an escalation point during core working hours.
SLA Management	Included	Definition, monitoring and reporting of service availability, incident response, resolution targets and policy enforcement performance aligned with Managed SASE 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 and review of service performance, user experience and access efficiency to ensure service objectives are met and to support future capacity and demand planning.
Availability Management	Included	Ensures the Managed SASE service delivers agreed levels of availability and resilience to support business-critical access and connectivity requirements.
Change Enablement / Release Management	Included	Controls changes to access policies, security rules, routing configurations and platform updates to minimise risk while maintaining service stability and compliance.
Service Request Management	Included	Handles standard access, onboarding, configuration and operational service requests through defined workflows as part of business-as-usual service delivery.
Problem Management	Included	Identifies root causes of recurring access, performance or security incidents and implements corrective actions to reduce future risk and operational impact.
Security Governance & Risk Management	Included	Oversees risks related to secure access, data protection, confidentiality and availability of services, controls and operational processes within the Managed SASE service.
Asset, User & Access Profile Management	Included	Maintains visibility and lifecycle control of users, devices, sites and access profiles to ensure consistent policy enforcement and accurate service coverage.
Configuration Management	Included	Maintains controlled, auditable access and security configurations including baselines, change tracking, version control and configuration integrity monitoring.
Service Reporting	Included	Comprehensive monthly reporting covering incidents, service performance, SLA adherence, access trends and operational insights across all Managed SASE service elements.

Why Choose SNO's Managed SASE Service for Enterprise and Public Sector?

SNO's Managed SASE service delivers secure, high-performance access without the complexity of traditional network and security architectures. By converging secure connectivity, policy-driven access control and expert operational management into a single managed service, SNO enables enterprise and public sector organisations to modernise securely, reduce risk and support flexible working. While allowing internal teams to focus on their core mission with confidence.