SNO
A smarter tomorrow.

MANAGED ENDPOINT DETECTION AND RESPONSE (EDR) SERVICE FOR ENTERPRISE CUSTOMERS

ALWAYS-ON ENDPOINT PROTECTION FOR MISSION-CRITICAL ENVIRONMENTS

Specialist Network Operations

Service Overview

SNO's Managed Endpoint Detection and Response (EDR) service delivers enterprise-grade endpoint security designed for organizations that operate critical, regulated or high-availability environments.

Built on advanced, behaviour-based protection technology and backed by experienced security analysts, our Managed EDR service continuously prevents, detects, investigates and responds to cyber threats across servers, workstations and user devices. By combining real-time behavioural analysis, machine learning and global threat intelligence, we stop both known and unknown attacks before, during and after execution while maintaining business continuity and compliance.

The service is purpose-built for enterprise and public sector organizations that require strong security controls, clear auditability and dependable operational oversight.

What You Get

Prevention-First Endpoint Protection

Unlike traditional signature-based tools, SNO's Managed EDR service focuses on stopping attacks at runtime by analysing behaviour in real time.

- Continuous monitoring of endpoint activity including processes, memory, file systems, registry changes and network connections.
- Detection of malicious behaviour based on intent, not just known malware signatures.
- Protection against ransomware, fileless malware, exploits and zero-day attacks.
- Automated rollback of malicious changes, where supported

24/7 Monitoring with Integrated Threat Intelligence

Your endpoints are continuously monitored and analysed through centralized security analytics enriched with up-to-date threat intelligence.

- Real-time correlation of endpoint telemetry across your environment
- Continuous updates to detection logic without disruption to users
- Protection aligned to emerging threat campaigns targeting enterprise and public sector organizations

Security Incident Management & Customer Communications

SNO provides end-to-end ownership of security incidents through a structured Incident Management process designed to minimize business disruption and ensure rapid, controlled recovery.

Each incident is owned by a dedicated Service Delivery Manager (SDM) or NOC Team Lead, who acts as the single point of accountability throughout the incident lifecycle. All incidents are managed through SNO's Service Desk, ensuring clear governance, traceability, and consistent communication. The SDM or NOC Team Lead is also responsible for overseeing service performance during incidents, ensuring response activities remain aligned with agreed service levels and operational priorities.

Situation updates are provided by the relevant security and operations teams, and Service Alerts and Status Updates are distributed at appropriate intervals based on incident severity and customer impact. Every action taken during investigation, containment and remediation is logged in SNO's Service Management platform, providing full transparency, progress tracking and audit readiness.

SNO's primary objective is to restore secure operations as quickly as possible, prioritizing service restoration and containment before agreed service levels are breached, while maintaining security integrity and evidence preservation.

Lessons learned from incidents are reviewed and, where appropriate, used to refine endpoint configurations and prevention policies through the formal Change Management process

Automated Response, Expert-Led Incident Management

When a threat is detected, SNO combines automation with expert human oversight to respond quickly and effectively.

- Analyst-validated alerts to eliminate noise and prioritize real risk
- Immediate isolation of affected endpoints to contain threats while maintaining management access
- Automated termination of malicious processes and blocking of related behaviours
- Guided remediation workflows to restore systems to a known good state
- Formal Root Cause Analysis (RCA) for high-impact incidents, including attack path, affected assets, and prevention recommendations

Full Endpoint Lifecycle Management

We manage the entire endpoint security lifecycle to ensure consistent protection and visibility.

- Structured onboarding of lightweight EDR agents across supported devices
- Continuous visibility into protected, unprotected, and non-compliant endpoints
- Alerts for agent tampering, service interruption, or policy drift
- Secure decommissioning aligned with data retention and forensic requirements

Policy-Driven Control & Governance

Security controls are aligned with your operational needs and governance model.

- Granular security policies tailored to endpoint roles, user profiles, and environments
- Adaptive controls that respond dynamically to threat severity
- Role-based access control (RBAC) aligned with least-privilege principles
- Formal change and configuration management with full audit documentation

Configuration & Change Management

SNO operates the Managed EDR service under a formal Configuration and Change Management framework to ensure security controls remain consistent, controlled, and auditable throughout the service lifecycle.

All endpoint security configurations, policies, and platform settings are maintained as controlled configuration items within SNO's Service Management system and are managed in accordance with defined operational and security standards.

Configuration Management includes:

- Establishment of secure baseline configurations for endpoint protection, prevention policies and response actions aligned to customer requirements
- Centralized management of endpoint security policies across environments and device types
- Continuous validation of configuration integrity to detect drift, tampering, or unauthorized changes
- Secure versioning and documentation of all configuration changes for audit and compliance purposes

Change Management

All changes to endpoint security policies, configurations, or response logic are governed by SNO's formal Change Management process.

- Changes are assessed for risk, impact, and operational dependency prior to implementation
- Emergency changes related to active security incidents follow an expedited approval path with full post-implementation review
- All approved changes are logged, tracked, and documented, including change rationale, execution details, and validation outcomes

Where required, customers are provided with visibility into material configuration changes that may impact operational behavior, compliance posture or risk exposure.

This disciplined approach ensures endpoint security controls remain effective, predictable and aligned with both security objectives and operational stability.

Reduced Attack Surface & Risk Exposure

The Managed EDR service actively reduces endpoint risk by:

- Identifying and blocking high-risk applications, scripts, and execution paths
- Preventing exploit techniques and memory-based attacks
- Providing expert guidance aligned with recognized frameworks such as NIST and CIS

Built for Resilience and Continuity

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

- Secure storage of telemetry, alerts, and forensic data
- Resilient management and analytics components
- Business Continuity and Disaster Recovery (BCDR) planning and annual testing

Seamless Integration with Your Security Ecosystem

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

- Security analytics and logging platforms
- Identity and access management systems
- Network enforcement solutions
- Ticketing and incident management systems

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

Clear Reporting & Audit Readiness

Service Performance & Operational Metrics

- Monitoring of key service performance indicators including detection time, analyst response time, containment execution and incident resolution timelines
- Visibility into endpoint coverage, agent health and policy enforcement effectiveness
- Trend analysis to identify recurring performance bottlenecks or operational risks
- Review of SLA adherence and service outcomes as part of regular service reporting

You receive reporting designed for technical teams, executives, and auditors alike.

- Incident timelines and response summaries
- Threat trends and risk posture insights
- Endpoint coverage and policy compliance
- SLA and service performance metrics

Reporting cadence

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

Service Levels (At a Glance)

SLA Metric	Target
Threat Detection	< 5 minutes
Analyst Response	< 30 minutes
Endpoint Isolation	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 incident reporting, service requests, and operational queries related to the Managed EDR service. Ensures consistent intake, tracking and governance of all customer interactions.
Incident Management	24x7x365	Manages security incidents to minimize business impact by restoring secure operations as quickly as possible. Incidents are handled using a structured, repeatable incident lifecycle aligned with agreed service levels.
Escalation Management	24x7x365	Ensures both functional and hierarchical escalations are executed within defined KPIs to maintain response momentum and service assurance.
Event Management	24x7x365	Proactive monitoring and handling of security events and alerts generated by endpoint telemetry, analytics and threat intelligence sources 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, 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 response, resolution, and service availability targets aligned with the Managed EDR 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 service performance to ensure detection, response, and containment objectives are met and to support future capacity and demand planning.

Availability Management	Included	Ensures the Managed EDR service delivers agreed levels of availability and resilience to support business-critical operations.
Change Enablement / Release Management	Included	Controls changes to EDR policies, configurations and platform updates to minimize risk while maximizing security effectiveness and operational stability.
Service Request Management	Included	Handles standard operational requests as part of business-as-usual service delivery through defined request workflows.
Problem Management	Included	Identifies underlying causes of recurring incidents and implements corrective actions to reduce future risk and operational impact.
Security Management	Included	Oversees risks related to the confidentiality, integrity, and availability of endpoint data and security controls within the Managed EDR service.
Asset Management	Included	Maintains visibility and lifecycle control of endpoint agents and supported assets, supporting vulnerability identification and secure decommissioning.
Configuration Management	Included	Maintains controlled, auditable endpoint security configurations, including baseline definition, change tracking, and configuration integrity monitoring.
Release Management	Included	Ensures operational readiness for new EDR capabilities, policy updates and platform enhancements while minimizing disruption.
Service Reporting	Included	Comprehensive monthly reporting covering incidents, performance metrics, SLA adherence and service trends across all service elements.

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

SNO's Managed EDR service delivers enterprise-grade endpoint protection without the complexity of running your own SOC. By combining prevention-first technology, automated response and expert security oversight, we help enterprise and public sector organizations stay resilient, compliant, and protected against evolving cyber threats so you can focus on delivering your mission with confidence.