

Secure Network & Identity Services

Design and deployment of secure, identity-driven and segmented network environments

Secure Network & Identity Services provides specialist support to help public-sector organisations control access to their networks, reduce cyber risk, and protect critical services. The service covers the design and deployment of Network Access Control (NAC), network segmentation, and firewall solutions, delivered individually or as part of a single, integrated engagement.

The service is suitable for on-premises, cloud and hybrid environments and supports secure network modernisation, Zero Trust adoption, and compliance-driven security improvement programmes.

NAC Design Services

Design of Network Access Control solutions to manage who and what can connect to the network. This includes defining identity- and device-based access policies, integration with directory and authentication services, and producing logical designs aligned to organisational security requirements.

NAC Deployment Services

Deployment and configuration of NAC platforms and policies across wired, wireless and remote access networks. This includes integration, testing, phased rollout and handover to ensure controlled and reliable enforcement of access decisions.

Segmentation Design Services

Design of network segmentation models to limit lateral movement and protect critical systems. This includes analysis of traffic flows, definition of segmentation boundaries, and production of designs aligned to business services and risk profiles.

Segmentation Deployment Services

Implementation of segmentation controls across network infrastructure, including configuration of VLANs, routing and access rules. The service supports safe migration, validation of connectivity, and production of as-built documentation.

Firewall Design Services

Design of perimeter and internal firewall architectures to protect users, systems and data. This includes policy design, rule-base optimisation, resilience planning, and alignment with identity and segmentation controls.

Firewall Deployment Services

Installation and configuration of firewall solutions, including policy implementation, rule migration, testing and cutover support. The service ensures firewalls are operationally ready and aligned to governance and audit requirements.

Outcomes for Buyers

- Improved control over user, device and application access
- Reduced attack surface through effective segmentation
- Consistent security controls across hybrid environments
- Clear documentation and operational handover
- Support for compliance, audit and assurance activities