

Zero Trust Network Access (ZTNA) and SASE



The requirement

Public sector organisations increasingly rely on cloud services, remote working, and third-party platforms to deliver critical services.

As access patterns become more distributed, traditional network security models based on perimeter controls are less effective at protecting users, applications and data.

Clients need to reduce risk from credential compromise, unauthorised access, unmanaged devices, and legacy connectivity solutions. They also require secure access that supports modern delivery, including hybrid cloud adoption, supplier access and operational continuity.

There is a growing requirement to implement Zero Trust Network Access (ZTNA) and Secure Access Service Edge (SASE) approaches that enforce least privilege access, improve network resilience, and provide consistent security controls across users and locations, including IoT-connected environments where applicable.

Redesmere's solution

Redesmere provides ZTNA and SASE services to help organisations design, implement and operate secure access to applications and services.

We help clients to modernise network access using identity-driven controls, context-aware policies, and secure connectivity patterns which are aligned to public sector governance and security requirements.

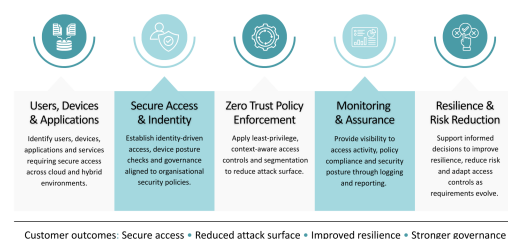
Our service supports the design and delivery of resilient, scalable network architectures across cloud and hybrid estates, enabling secure access for staff, partners and suppliers without expanding the attack surface.

We help organisations move from legacy remote access models to a Zero Network Trust Access approach that improves security, simplifies operations, and supports long-term transformation goals.

A key component of our service focuses on developing the capabilities and teams our clients need to onboard new network technologies and services. This component of the service provides a suite of organisational and people-development capabilities designed to complement and enhance the adoption, optimisation, and ongoing management of cloud services.

Our teams are multi-disciplinary with significant expertise in cloud strategies, business architecture, technical architecture, network architecture, cloud transformation, digital transformation, programme turnaround, programme control, delivery enablement and independent assurance.

SERVICE DELIVERY OVERVIEW



Customer outcomes: Secure access • Reduced attack surface • Improved resilience • Stronger governance

When to use these services?

The service supports the design, implementation, and operation of secure network access using Zero Network Trust Access principles. It enables organisations to control access to applications and services based on identity, context and risk, rather than network location,

improving security and resilience across cloud and hybrid environments.

Clients use the service to modernise or replace legacy remote access and perimeter-based network models, reducing exposure to unauthorised access while improving the experience for users, suppliers and partners.

The service supports secure access to cloud-hosted and on-premise applications, with appropriate governance and audit.

Where access requirements span multiple applications, user groups, or environments, the service provides a consistent access control layer. This reduces complexity, improves oversight, and supports secure connectivity as services and organisational needs evolve.

What are the benefits?

- » Reduced risk from unauthorised access and credential compromise
- » Improved security posture through least privilege and continuous verification
- » More resilient and scalable access to critical services
- » Improved user experience through consistent secure access
- » Reduced dependency on legacy remote access solutions
- » Stronger governance through policy control and reporting
- » Increased operational continuity and reduced downtime risk
- » Improved alignment to public sector security and assurance needs
- » Future-proof access models that support cloud adoption and change

How we work

We tailor our services to our clients' specific requirements, agree the objectives and outcomes that are to be achieved, and document these in formal Statements of Work (SoWs).

An integral part of each SoW is the implementation plan for the services which

sets out how the objectives and outcomes are to be achieved as a series of epics.

The vast majority of our client engagements are outcome-based arrangements, with milestone-based payments that are linked to the achievement of the objectives and outcomes set out in the SoWs.

We maintain detailed plans throughout each engagement which we use to review progress and to reprioritise work with our clients on a regular basis.

A key component of most of our implementation plans is "Service Transition" which we use from the outset of each engagement to plan and manage any offboarding activities.

Our services are usually provided during normal business hours. However, we recognise that some cloud transformation activities need to be performed out of hours and at weekends which we are happy to incorporate into the service.

We are able to operate using our own or our clients' tooling, cloud and Office 365 infrastructure.

What is distinctive about us?

Redesmere's core proposition is that:

- » Our small multi-disciplinary teams are hand-picked for each individual client engagement.
- » We have the skills, track record and gravitas to make a real difference.
- » Our people have extensive experience of digital transformation, delivery and cloud implementation programmes.
- » Our independence means that we do not have any conflicts of interest to get in the way.
- » We are able to provide our services through time and materials, fixed price or output-based contracts, when appropriate.

How to contact us?

e: hello@redesmere.com

t: +44 1625 810180

w: <https://redesmere.com>