MISCO

Secure Access Service Edge (SASE)

Secure connectivity for a cloud-first world

Connect every user and location with consistent security and reliable

Modern networks are no longer defined by a single perimeter. Your users work everywhere, your applications live across data centres, SaaS, and cloud platforms, and your security has to keep up. Misco helps you simplify this complexity with a clear, unified approach to secure access service edge, giving you a smarter way to protect your organisation.

Why businesses are turning to SASE

Today's IT environments are more fragmented than ever. Applications have moved from the office to the cloud, remote and hybrid workforces have multiplied the number of access points, and threats increasingly rely on human focused attacks rather than traditional technical exploits. At the same time, organisations face pressure to meet governance frameworks such as ISO 27001, Cyber Essentials Plus, and GDPR, along with evolving legislation including NIS2 and the UK CS&R Bill.

This creates a landscape where multiple network edges, shifting compliance demands, and rising threat levels make it difficult to maintain a consistent security posture. Gaps appear, visibility drops, and attackers only need one weak point.

How SASE helps you reduce complexity

SASE brings networking and security together in a cloud delivered model, giving you one unified framework to protect users and applications everywhere.

With the right SASE strategy, you can:

- Apply consistent security across every edge, from branch to cloud to remote workers

- Support zero trust principles with identity-driven access

- Improve visibility into users, applications, and data movement

- Strengthen compliance reporting with clearer insights and control

- Remove duplicated tools and reduce operational overhead

- Detect and respond to threats faster with cloud-scale intelligence

- Support SaaS adoption and cloud migration with a more resilient network

When point products can still be the right fit

For organisations with strong in-house expertise or access to large MSP resources, a build-your-own approach can work well. This gives teams the freedom to deploy best in breed solutions from multiple vendors to meet specific connectivity and security requirements.

These solutions often include:

- SD WAN for inter-site connectivity and perimeter security
- Zero Trust Network Access for secure remote user access
- Layer 7 next-generation firewalls for a safe and compliant internet experience
- Data Leak Prevention for oversight and control of data leaving the organisation
- SecOps tools for log aggregation, investigation, and threat analysis
- Network and user visibility platforms to monitor uptime and end-user experience

This level of customisation can align closely with how the business operates, although each component needs careful evaluation. It is important to assess not only individual capabilities but also how well each tool integrates into the broader security stack. Without that alignment, new or overlapping tools can unintentionally introduce vulnerabilities that weaken the organisation's overall posture.

A point product strategy can also slow an organisation's ability to respond to emerging threats. Introducing new features or updating capabilities may take weeks or even months, reducing agility and placing more operational pressure on internal teams. Availability and latency requirements must also be considered, especially for organisations with a global footprint where design complexity increases significantly.

When a platform solution makes more sense

For organisations that do not want the complexity of integrating multiple point products, a Secure Access Service Edge platform offers a simpler path. SASE platforms can be ready to use out of the box or deployed quickly through dedicated cloud security instances.

Some platforms operate regionally, others globally, but all deliver a cloud like experience where the platform vendor handles feature interoperability, development, and maintenance. The customer or partner focuses on policy creation and managing sites and users.

Common SASE platform capabilities include:

- SD WAN for inter site connectivity and perimeter security
- Zero Trust Network Access for secure remote user connectivity
- Firewall as a Service for infrastructure protection and segmentation
- Secure Web Gateway capabilities such as:
    - Web filtering
    - IDS and IPS
    - DNS security
    - Next generation anti-malware
    - Remote browser isolation
    - Suspicious file sandboxing
    - CASB capabilities
- Data Leak Prevention for control of sensitive data
- SecOps tooling for log aggregation, investigation, and analysis
- Network and user visibility solutions to monitor performance and experience

This approach reduces the technical barriers to modern, secure connectivity. Customers and partners can focus on policy, usability, and outcomes rather than the operational workload of managing multiple systems. SASE platforms can suit a wide range of budgets, with options for SMBs through partner delivered managed SASE services.

Scaling also becomes simpler, allowing organisations to onboard new locations, users, and capabilities without delay.

MISCO

Why more organisations are choosing SASE

Many businesses are moving to SASE platforms for the same reasons they embraced digital transformation in the first place. SASE gives organisations the agility to adapt their connectivity and security quickly, aligning these capabilities with changing business demands. It delivers a consistent experience for every user in every location, helping teams stay secure, standardised, and compliant as threats evolve and regulations tighten.

This shift is driving rapid market growth. The SASE market is expected to grow from around 15 to 45 billion dollars in 2025 to more than 100 billion dollars by 2030 to 2032. Organisations are choosing SASE because it provides a clear and scalable way to solve modern connectivity and security challenges.

Find the right SASE path with support from Misco

Every organisation has unique traffic patterns, governance requirements, and application architectures. Misco helps you understand your current environment, uncover duplication or risk, and explore the SASE approach that best aligns with your goals.

Whether you want to simplify operations, improve compliance, or strengthen protection across cloud, data centre, and remote users, Misco can help you move forward with confidence.

Ready to explore SASE?

Speak with one of our specialists to discuss your environment and explore the available options.

Contact Misco
0800 368 9646 | sales@misco.co.uk

www.misco.co.uk/cms/managed-sase-services