UKCONNECT

SASE Product sheet

The network security challenge

Traditional network security models are struggling to keep up. There are vulnerabilities in remote working, secure data sharing is complex and an increased reliance on technology means widening attack surfaces. Couple this with siloed tech stacks, multiple vendors and difficultly in centrally managing security policies, network access for businesses is becoming increasingly challenging.

Secure Access Service Edge (SASE). The future of secure networking for businesses.

How does SASE work?

SASE is a simplified security approach that's easy to add onto your existing infrastructure, providing a rich security posture based on Zero Trust.

Single-vendor architecture

SASE seamlessly integrates with existing infrastructure. We can provide you with a full-stack, fully unified solution from hardware to network traffic management, optimisation and security.

Simple implementation

By adopting an incremental approach to your existing infrastructure, you can maintain security without the cost and complexity of undergoing a full 'rip and replace' of existing security architectures.

Zero Trust network in minutes

SD-WAN, Zero Trust processes and security are combined in a single, cellular-optimised architecture which is operationally proven, and ready to launch when you are.

Leveraging bonding and load balancing

Our in-house Network Operations Centre will monitor how traffic is sent across your network. We'll optimise and prioritise the delivery of business critical applications, and ensure an enhanced experience for all users.

- Full-stack, fully unified solution
- Simple procurement experience
- A rapid Zero Trust network – no site visit needed
- Cellular-optimised security architecture
- Commercially flexible, operationally proven
- 24/7 support from UK-based NOC
- Replaces legacy VPN architecture

SASE security components

A **Hybrid Mesh Firewall** (HMF) provides unified firewall protection across hybrid and cloud infrastructures.

Remote Browser Isolation (RBI) protects users and their devices through isolation technologies which secures data and other digital assets.

A **Secure Web Gateway** (SWG) protects against web-based threats and enforces unified internet usage policies while protecting against data loss.

A **Cloud Access Security Broker** (CASB) provides visibility and policy enforcement for cloud app usage and data.