A boxxe Group Company

cisco Partner

Whitepaper

SASE for the distributed workforce:

A Guide to Secure Access Service Edge for the distributed workforce

Discover how SASE can unlock the full potential of your distributed workforce, while keeping the network robust and safe from advanced threats faced by remote and hybrid teams.

thisiscae.com

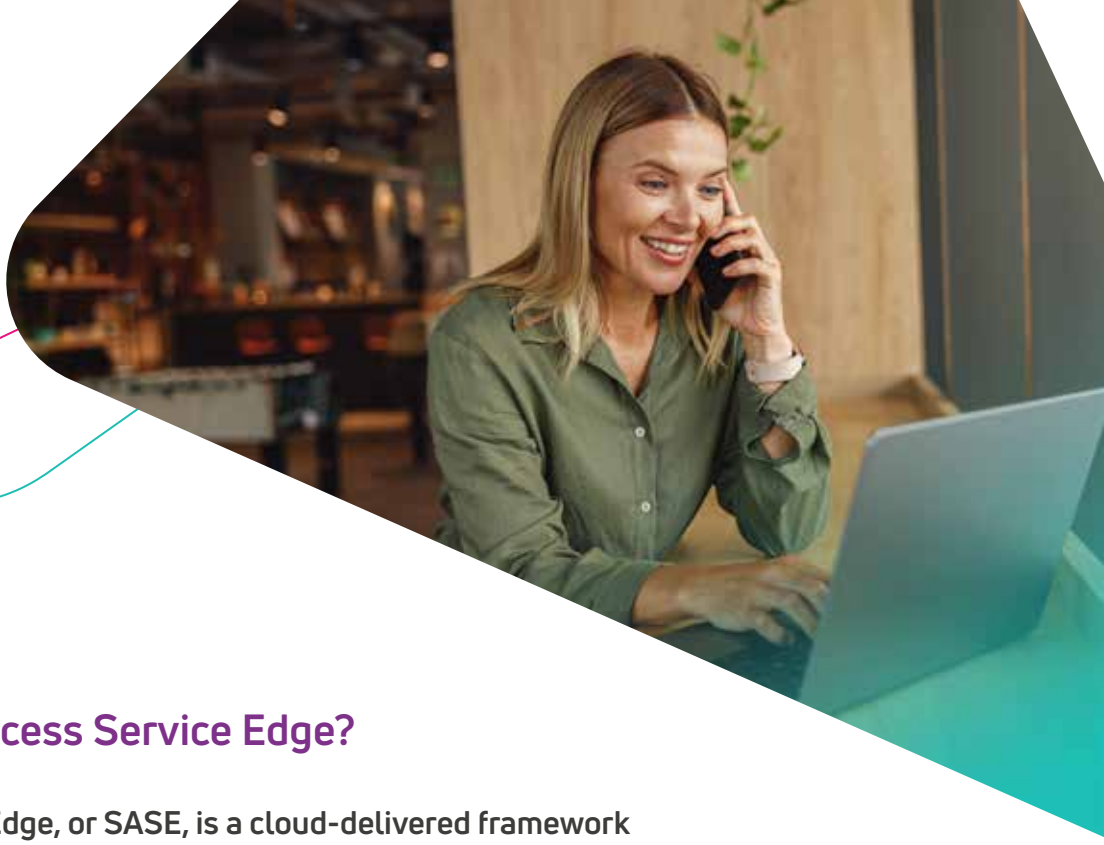
Introduction

The way we work has fundamentally changed. Employees are no longer tied to corporate offices and on-premises networks; they are working from home, co-working spaces, airports, and anywhere business demands. While this distributed model unlocks flexibility and productivity, it also introduces a new set of challenges for IT teams tasked with keeping users both secure and connected.

Traditional network and security architectures are not designed for a workforce that connects from everywhere. Routing traffic back through fixed points of presence often creates latency, slows down access to critical applications, and frustrates employees. At the same time, there's also an increased risk of breaches, data loss, and compliance failures.

The result is a difficult trade-off: organisations either compromise on performance to maintain security, or loosen controls to keep workers productive. Neither are a good option in today's environment.

This is where Secure Access Service Edge (SASE) comes in. By combining networking and security functions into a unified, cloud-delivered service, SASE enables enterprises to provide secure, high-performance access no matter where employees work. Instead of forcing traffic through legacy choke points, SASE delivers both security and connectivity at the edge, closer to users and applications, eliminating unnecessary latency while strengthening protection.



What is Secure Access Service Edge?

Secure Access Service Edge, or SASE, is a cloud-delivered framework that brings together networking and security into a single, unified service. Instead of relying on siloed tools and physical appliances, SASE consolidates core capabilities at the edge. This model not only simplifies IT operations but also ensures that security and performance can scale seamlessly together as a distributed workforce grows.

By converging these technologies in the cloud, SASE eliminates the trade-off between productivity and protection. Users connect securely to the applications they need – no matter where in the world they are - without being slowed down by backhauling traffic through traditional private data centres.

SASE combines two core components, interconnected in a centralised cloud solution:

1. SD-WAN

SD-WAN (Software-Defined Wide Area Networking) provides optimized, resilient connectivity across multiple sites and cloud services, intelligently managing traffic to ensure high-performance application delivery. Traditional WANs rely on fixed, often costly circuits between locations, which can create bottlenecks and limit flexibility.

SD-WAN abstracts the network control from the underlying hardware, enabling dynamic, policy-driven routing that adapts in real time to network conditions, improves reliability, and reduces latency. As a core component of SASE (Secure Access Service Edge), SD-WAN enhances connectivity and user experience while supporting secure, efficient access to cloud applications and services.

Optimised, resilient connectivity across sites and cloud services, with Policy driven routing that removes edge bottlenecks and improves application performance.

2. SSE

SSE delivers the cloud-native security layer of SASE, protecting users, devices, and data wherever they connect. By moving security functions to the cloud, SSE enforces policies consistently across all access points, whether on-premises, remote, or in the cloud.

It enables secure, seamless access to applications while reducing the complexity of managing traditional security appliances, ensuring threats are blocked at the edge, sensitive data is safeguarded, and access is granted based on identity and context.

SSE forms the security backbone that complements SD-WAN's connectivity, providing a unified approach to secure and optimize enterprise networks.
Some key bits of technology within SSE that you can utilise when adopting SASE include:

SWG (Secure Web Gateway)
Protects users from malicious websites, enforces compliance, and filters traffic at the edge so threats are stopped before they enter your network.

FWaaS (Firewall-as-a-Service)
Cloud-delivered, enterprise-grade firewall protection that provides consistent policies everywhere, without the complexity of managing physical appliances.

CASB (Cloud Access Security Broker)
Enforces security policies across SaaS applications, giving visibility and control over sensitive data in cloud environments.

ZTNA (Zero Trust Network Access)
Enhanced access to resources, replaces legacy VPNs with granular, identity-based access to private applications - ensuring least-privilege access for every user, device, and session.

How can the distributed workforce use SASE?

SASE has many applications and use cases, which can be tailored to the specific needs of your business. Here's a handful of ways SASE can be used to improve the network structure of your distributed network.

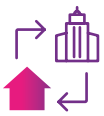
Migration of legacy VPN headend to the cloud

Traditional VPNs often force remote employees to tunnel all traffic through centralised data centres. This creates latency, slows access to SaaS and cloud applications, and exposes networks to unnecessary risk since VPNs grant overly broad access.

How SASE helps

With Zero Trust Network Access (ZTNA) as part of SASE, employees connect directly and securely to the applications they need, no matter where they are.
Every connection is verified based on user identity, device health, and context, providing least-privilege access instead of blanket network access.

The outcome here is that distributed teams enjoy faster, more seamless connectivity to business-critical apps without sacrificing security. IT teams reduce attack surfaces while eliminating the bottlenecks and frustration of legacy VPNs.



SASE can enable secure and productive hybrid work

Hybrid and remote work environments often rely on home networks, public Wi-Fi, or unmanaged personal devices. These create security blind spots and make it difficult for IT teams to enforce consistent protection. Traditional approaches that route traffic back to corporate data centres add latency, slowing access to cloud and SaaS applications.

How SASE helps

By delivering security services at the cloud edge - including Secure Web Gateways (SWG), Cloud Access Security Brokers (CASB), and Firewall-as-a-Service (FWaaS) - SASE applies consistent security policies no matter where employees connect from. Because traffic is inspected and secured closer to the user, latency is reduced compared with backhauling through central data centres.

The outcome is that employees get a smooth, high-performance experience whether they're at home, on the move, or in the office. IT gains better visibility and control across all connections, reducing risk while supporting productivity.

SASE can centralise security for a distributed workforce

Many organisations rely on a patchwork of point solutions, all operating in silos. This creates fragmented security, inconsistent policies, and significant operational overhead for IT teams managing multiple vendors and systems.

How SASE helps

SASE consolidates networking and security into a single, cloud-native platform. With integrated services such as SD-WAN, ZTNA, and FWaaS, IT teams can enforce access controls, manage policies, and detect threats centrally, all while routing traffic through the nearest SASE edge location for optimised performance.

The outcome is simpler IT management, with faster policy deployment, greater visibility, and reduced costs. At the same time, employees benefit from stronger security and faster application performance, no matter where they work.

What are the benefits of Secure Access Service Edge for a distributed workforce?

Secure Access Service Edge (SASE) does more than combine security and network solutions, it transforms how enterprises secure and connect their distributed workforces.

By converging networking and security into a single, cloud-native framework, SASE strengthens defences while delivering the speed, scalability, and simplicity that modern organisations need. The result is a model that keeps employees productive and businesses resilient, no matter where work happens.

Here are six key benefits SASE brings to today's enterprise:

- **Enhanced security at every connection**
  With Zero Trust principles, identity-based access, and integrated threat prevention, SASE ensures that only the right users and devices connect to the right applications. This minimises the risk of breaches and reduces the attack surface across remote and hybrid environments.

- **Consistent visibility and control**
  Centralised monitoring provides IT teams with real-time insight into users, devices, applications, and data flows. This unified view makes it easier to detect anomalies, respond to threats quickly, and maintain consistent policies across a distributed workforce.

- **Simplified compliance management**
  By applying security policies centrally across the entire network, SASE helps organisations more easily align with regulations such as GDPR, NCSC CAF and other data protection standards. Compliance becomes less about chasing gaps and more about maintaining ongoing assurance.

- **Faster, more reliable user experiences**
  Because security is delivered at the cloud edge, employees connect through the nearest SASE point of presence instead of being routed through a central data centre. This reduces latency and improves application performance, so people can work without slowdowns.

- **Effortless scalability**
  With its cloud-native design, SASE allows organisations to expand securely into new regions or scale with workforce growth without heavy infrastructure investments. Whether you're adding a new office or onboarding hundreds of remote employees, SASE adapts seamlessly.

- **Reduced complexity and cost**
  By consolidating multiple security and networking tools into one platform, SASE eliminates vendor sprawl and minimises the need for physical appliances. IT teams benefit from streamlined operations, lower overhead, and faster rollout of updates and policies.

The process of implementing SASE in the workplace

Adopting Secure Access Service Edge (SASE) is more than a simple upgrade of your technology; it's an entire digital transformation. Done right, it strengthens security, improves connectivity, and empowers your workforce without disruption. But you need to build a robust process to ensure it does go right.

At CAE, we've built a tried and tested implementation framework that reduces unnecessary downtime, prevents data loss during transition, boosts efficiency, and promotes adoption across your teams.

Our approach is structured yet flexible, tailored to your organisation's unique needs:

1. Assess and discover

We begin by analysing your current infrastructure, security posture, and business requirements. This step uncovers gaps in visibility, performance, and compliance while aligning the solution with your long-term goals.

2. Design and plan

Our experts design a tailored SASE architecture that integrates seamlessly with your existing systems. We create a roadmap that details the transition, ensuring that security, performance, and user experience remain central.

3. Deploy and integrate

We implement the core SASE components of SD-WAN and SSE, including, ZTNA, SWG, CASB, and FWaaS in a phased, low-risk manner. This approach limits downtime secures your data and ensures smooth integration with your current workflows.

4. Adopt and enable

Technology is only effective when people use it. We work closely with your teams to drive adoption, providing training, guidance, and change management support to embed SASE into daily operations.

5. Optimise and evolve

Once deployed, we continuously monitor and fine-tune your SASE environment. As your workforce, applications, and threats evolve, CAE ensures your solution adapts and keeps performance high and security strong.

CAE: Secure Access Service Edge experts

At CAE, we know that adopting SASE isn't just a technology decision; it's a business-critical transformation. As specialists in secure, scalable digital infrastructure, we help enterprises embrace SASE with confidence, ensuring your distributed workforce stays productive, secure, and future-ready.

Why CAE should be your SASE implementation partner

We've guided organisations across industries through complex networking and security transformations, combining deep technical knowledge with real-world experience to deliver successful SASE projects. As a long-standing Cisco Gold Partner - and Cisco Partner of the Year - we bring unrivalled access to the latest innovations, best practices, and roadmap insights, applying them directly to your environment.

Our approach is end-to-end. From initial assessment and design, through deployment and adoption, and into continuous optimisation, we stand by you every step of the way.
With co-managed services and a customer-first mindset, we tailor each solution to your goals, minimise disruption, and accelerate adoption across your teams.

Bring security and performance to every edge point, wherever your team works.

Deliver cost-effective connectivity to every site in your community

Take the next step towards complete digital transformation.
Contact one of our SASE experts to find out more

T: 0845 643 0033
E: Marketing@caeuk.com

thisiscae.com

A boxxe Group Company