



Secure Access Service Edge

A Practical Guide

What SASE is, how to tell if you are ready, and how to roll it out without disrupting the business. For IT leaders, operations directors and CEOs of UK organisations.

Contents

Introduction	3
SASE at a Glance	4
Part 1: Understanding SASE	5
What SASE Is	6
Core Components	7
SASE, SSE and Traditional Security Compared	8
Business Benefits	9
Part 2: Adopting SASE	10
Market and Regulatory Context	11
Is Your Organisation Ready?	12
Implementation Roadmap	13
Choosing a Provider	14
Common Pitfalls and Key Takeaways	15
Glossary and Sources	16
How Cybergen Helps	17
About Cybergen	18

Introduction

The way we work has changed faster than the way we secure it. Most business applications now live in the cloud, most teams work at least part of the week away from the office, and attackers have learned that a stolen login is often easier to use than a software flaw. Security built around a single office firewall was never designed for this.

Secure Access Service Edge, or SASE, is the industry's answer. It brings networking and security together into one cloud service, so every user, device and site is protected by the same policy, wherever they connect from.

This guide is written for IT leaders, operations directors and CEOs of UK organisations who want a clear, vendor-neutral view of SASE before they commit budget or time to it.

Read on and you will gain:

- 1 A Clear Picture of What SASE Is and Is Not**
How SASE differs from SSE and traditional perimeter security, the six core components, and the business problems each one solves.
- 2 A Practical Readiness Check**
The signs that SASE is worth a serious look now, and the foundations to put in place first so your project is faster and cheaper.
- 3 A Roadmap and a Buying Checklist**
A phased rollout plan with clear gates, the questions to ask every provider, and the pitfalls that catch most projects out.

The UK's regulatory direction is clear: stronger identity controls, better visibility and faster incident reporting. SASE helps with all three. Our aim is to help you decide how and when to adopt it, on your terms.

SASE at a Glance

Four forces shaping how UK organisations secure access in 2026

2019

Year Gartner defined SASE

SASE Has Gone Mainstream

Since Gartner defined SASE in 2019, it has moved from concept to mainstream, and Gartner forecasts **strong double-digit growth** through to 2030. Organisations are consolidating separate security tools onto unified platforms, and single-vendor SASE is winning share in the SME and mid-market segments.

Identity Is the New Perimeter

Under **Cyber Essentials v3.3**, published by the NCSC in April 2026, authentication to cloud services must always use MFA. Access is now decided by who the user is and the health of their device, not by which network they sit on.



MFA

Required for cloud services

24h / 72h

Incident reporting windows

Reporting Deadlines Are Tightening

The Cyber Security and Resilience Bill has passed the Commons and is now in the House of Lords. It brings managed service providers and data centres into scope, with an initial incident notice within **24 hours** and a full report within **72 hours**. Centralised logging and access control make those deadlines achievable.

One Policy, Everywhere

SASE replaces a patchwork of VPNs, web proxies, branch firewalls and separate consoles with **six core capabilities** delivered as one cloud service. One set of rules follows every user and site, which closes the gap between office and remote protection.

6 in 1

Core capabilities, one service

Sources: Gartner; NCSC; GOV.UK; UK Parliament. Full list on page 16.

UNDERSTANDING SASE

What SASE is, what it is made of, how it compares with SSE and traditional security, and the business problems it solves.

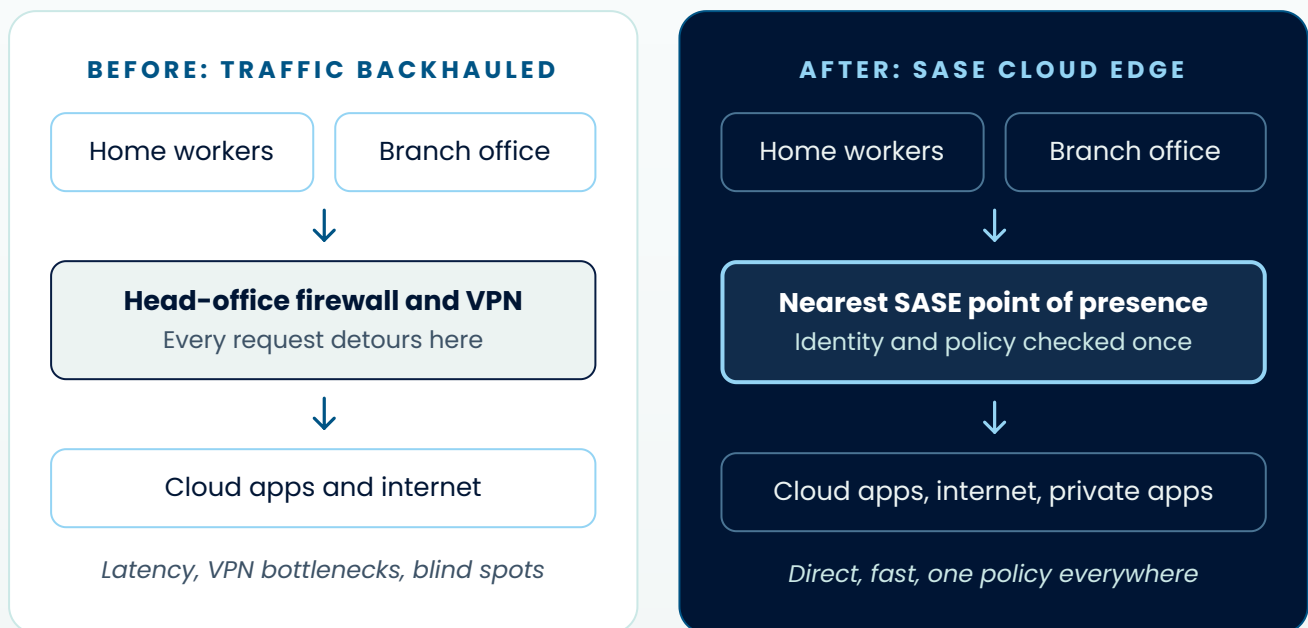


What SASE Is

SASE is a cloud-delivered architecture that combines wide-area networking with a full stack of security controls, enforced close to the user rather than in a central data centre. Gartner coined the term in 2019 to describe the convergence of the two.

Traditionally, branch and remote traffic is backhauled to head office, inspected by on-premises firewalls, then sent on. That made sense when apps lived in your server room. Today most apps are SaaS and most users are hybrid, so backhauling adds cost, latency and blind spots.

SASE flips the model. Users and sites connect to the nearest point of presence in the provider's cloud, where identity, device health and context are checked and one policy is applied before traffic goes straight to its destination.



Three Principles at the Heart of SASE



Identity-Driven

Access is decided by who the user is and the state of their device, not by which network they sit on.



Cloud-Native

Security is delivered as a service from a global network, so it scales with the business and needs little hardware.



Zero Trust

Nothing is trusted by default. Every request is verified, and users reach only the specific apps they need.

Core Components

SASE is not one product but a set of capabilities delivered as one service. Six are core; several others are increasingly expected.



SD-WAN

Connects sites over any link (broadband, 4G/5G, fibre) and steers traffic over the best path.

Replaces: MPLS circuits, branch routers



SWG Secure web gateway

Filters web traffic, blocks malicious sites and downloads, and enforces acceptable use.

Replaces: on-premises web proxies



CASB Cloud access security broker

Gives visibility and control over SaaS use, including shadow IT.

Replaces: manual SaaS audits, point CASB tools



ZTNA Zero trust network access

Grants users access to specific private apps after verifying identity and device.

Replaces: traditional VPNs



FWaaS Firewall as a service

Cloud firewall with intrusion prevention for all traffic, not just web.

Replaces: branch firewall appliances



DLP Data loss prevention

Finds and protects sensitive data in motion across web, SaaS and email.

Replaces: standalone DLP tools

Often Included or Offered as Add-Ons

Remote browser isolation: runs risky web pages in the cloud so malicious code never reaches the device.

DNS security: blocks malicious domains before a connection is even made.

AI security controls: governs generative AI use, including stopping sensitive data being pasted into AI tools.

Digital experience monitoring: measures app performance per user, so IT spots problems before tickets arrive.

Threat intelligence and sandboxing: inspects unknown files safely before they are delivered.

SASE, SSE and Traditional Security Compared

SSE (Security Service Edge) is the security half of SASE: SWG, CASB, ZTNA and usually FWaaS and DLP, without the SD-WAN networking. Many organisations start with SSE and add SD-WAN later, or keep an existing SD-WAN.

	Traditional perimeter	SSE	Full SASE
Where security is enforced	Head-office firewall	Provider cloud	Provider cloud
Remote access	VPN to the network	ZTNA to specific apps	ZTNA to specific apps
Branch connectivity	MPLS or VPN tunnels	Unchanged	SD-WAN, integrated
Hardware at each site	Firewall, router, proxy	Existing kit	Small edge device or none
Policy management	Several consoles	One console for security	One console for network and security
Best fit	Few sites, office-based staff	Remote-heavy, few branches	Multi-site, hybrid workforce

Single-Vendor or Multi-Vendor?

Single-Vendor SASE

Networking and security from one provider, with one console and one policy engine. Simpler to run and usually faster to deploy, which suits most SMEs and mid-market firms.

Multi-Vendor SASE

Best-of-breed SD-WAN from one provider with SSE from another. Suits large existing investments or specialist needs, but needs more integration work and in-house skill.

Key Takeaways

- SSE is a valid first step.** You can secure users and apps now and bring networking into the same platform later.
- The real difference is where policy lives.** SASE moves enforcement from your building to the cloud edge, close to every user.
- Vendor model follows capacity.** Choose single-vendor for simplicity, multi-vendor only where existing investment or specialist needs justify the extra effort.

Business Benefits

SASE pays back through stronger security, lower running costs and a better experience for staff. How much weight each carries depends on your starting point.

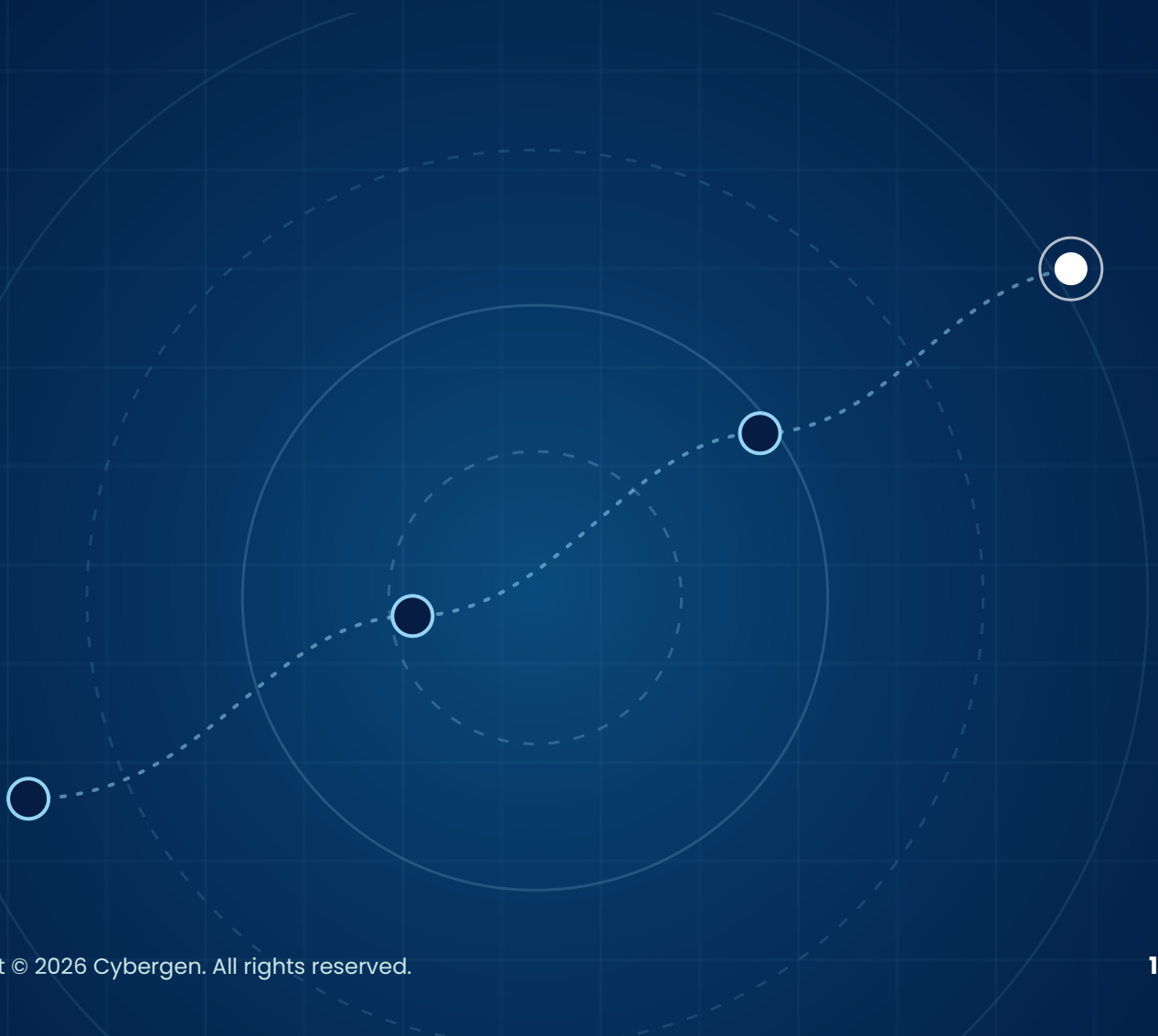
PROBLEM TODAY	HOW SASE HELPS	WHO NOTICES
VPNs are slow, overloaded and a common attack route	ZTNA connects users directly to the apps they need, never the whole network	Staff, IT, the board
Home and travelling users are less protected than office users	The same policy follows every user, on any network	Security team
Too many security tools and consoles	One platform, one policy, one place to investigate	IT team
MPLS and hardware refreshes are expensive	SD-WAN uses lower-cost links, with less kit to buy, patch and replace	Finance
Little visibility of SaaS and AI tool use	CASB and DLP show what is used and where data goes	Compliance, DPO
New sites and acquisitions take weeks to connect	New sites and users connect to the cloud service in days	Operations
Ransomware spreads sideways once inside	Users never sit on the network, which limits lateral movement	Everyone



A stronger position with auditors, insurers and customers. One service that enforces MFA, logs every access decision and protects data makes evidence far easier to produce.

ADOPTING SASE

The market and regulatory picture, how to tell if you are ready, a phased roadmap, how to choose a provider, and the pitfalls to avoid.



Market and Regulatory Context

SASE is now mainstream, and UK regulation is pushing the same way: stronger identity controls, better visibility and faster incident reporting.

Market Trends

- **Growth.** Gartner forecasts strong double-digit growth in the SASE market from 2025 to 2030.
- **Single-vendor momentum.** Unified platforms are winning share, especially among SMEs and the mid-market.
- **AI.** Providers are adding controls for generative AI use and machine-learning threat detection.
- **Consolidation.** Organisations are cutting the number of security vendors they manage and favouring platforms.
- **Identity-first.** Access decisions are tied to identity providers such as Microsoft Entra ID and Okta.

UK Regulation and Standards

Cyber Essentials v3.3

Current, April 2026

Authentication to cloud services must always use MFA, and cloud services and home working are firmly in scope. SASE enforces MFA, device checks and web filtering consistently.

Cyber Security and Resilience Bill

In the House of Lords

Has passed the Commons; duties take effect through secondary legislation after Royal Assent. Extends NIS rules to managed service providers and data centres, with a 24-hour initial notice and a 72-hour full report.

EU NIS2 and DORA

In force

Relevant for UK firms that operate in or supply the EU, especially in financial services.

NCSC zero trust principles

Guidance

SASE is a practical way to adopt zero trust: verify every user, device and request.

UK GDPR and the Data (Use and Access) Act 2025

In force

DLP and CASB help show where personal data goes and who can reach it.

Regulation alone rarely justifies SASE, but it changes the risk calculation. Customers in government, critical infrastructure and regulated sectors will increasingly ask for this level of control.

Is Your Organisation Ready?

Count how many of these signs apply to you. If three or more do, SASE is worth a serious look now.

01 A third or more of your staff work remotely or hybrid.

02 Your VPN is slow, often overloaded or due for renewal.

03 Your main apps are SaaS, such as Microsoft 365, Salesforce or HubSpot.

04 You run several sites on MPLS or ageing branch firewalls.

05 Firewall, proxy or VPN hardware is due for refresh within 18 months.

06 You manage four or more security tools, each with its own console.

07 You cannot easily see who uses which SaaS or AI tools.

08 You must meet Cyber Essentials, ISO 27001, NIS2 or customer requirements.

09 You are growing, opening sites or integrating acquisitions.

1 to 2

Keep watching the market

3 to 5

Start planning now

6 or more

Make it a priority

Readiness Checklist

Work through these before you talk to providers. Each one makes the project faster and cheaper.

☐ Identity provider in place, with MFA enforced for all users

☐ Business applications listed, with where they are hosted and who needs them

☐ Current contracts mapped (MPLS, firewalls, VPN, proxy) with renewal dates

☐ Executive sponsor and project owner named

☐ Up-to-date inventory of users, devices, sites and internet links

☐ Device management (MDM) in place, so device health can be checked

☐ Data classification agreed: what is sensitive and where it lives

☐ Budget range and success measures agreed

Implementation Roadmap

Roll SASE out in phases, moving on only when each gate is met. A phased approach keeps the business running and lets you prove value early.

1

Discover and Plan

Inventory users, devices, apps, sites and current contracts. Agree goals, success measures, budget and an executive sponsor.

◆ **Gate: business case and scope signed off**

2

Build the Foundations

Enforce MFA through your identity provider and enrol devices in MDM. Classify data and design access policy around users and apps.

◆ **Gate: MFA enforced, devices managed, apps mapped**

3

Prove It

Run a proof of concept with a pilot group, one site and your key apps. Measure user experience and security results against agreed targets.

◆ **Gate: pilot meets experience and security targets**

4

Roll Out in Waves

Remote users first: replace VPN with ZTNA and add web and SaaS security. Then sites: move branches to SD-WAN as MPLS and firewall contracts end.

◆ **Gate: all users and sites migrated**

5

Retire and Optimise

Decommission VPN, MPLS and legacy appliances on a fixed date. Tune policy, feed logs to a 24/7 SOC, then add DLP and AI controls.

Why remote users go first: VPN pain is usually the quickest win. Sites follow as MPLS and firewall contracts come up for renewal. Run old and new side by side during each wave, with a tested rollback.

Choosing a Provider

Every major platform now claims the same headline capabilities. Judge providers on how well they fit your estate and how they perform in a real pilot, not on feature lists.

Criterion	What good looks like	Question to ask
Network reach	Points of presence in the UK and wherever your staff and customers are	Where are your nearest PoPs, and what latency do UK users see?
Single-pass architecture	Traffic inspected once, by one engine, with one policy	Is every security function run in one pass, or chained between services?
Integration	Works with your identity provider, MDM, SIEM and SOC	Which integrations are native, and which need custom work?
Management	One console for network and security, with clear reporting	Can I see one user's full activity in one place?
Data residency	Logs and inspected data kept in the UK or EU on request	Where is our data processed and stored?
Resilience	Published uptime SLA and automatic failover between PoPs	What happens to users if a PoP fails?
Migration support	Tools and services to move from VPN and MPLS in phases	Can we run alongside our current setup during migration?
Commercials	Clear per-user or per-site pricing, no surprise add-ons	Which features in the demo cost extra?
Certifications	ISO 27001, SOC 2, Cyber Essentials Plus and relevant UK public sector routes	Can you share your latest audit reports?



Always Run a Proof of Concept

Test with a real group of users, a real site and your most important apps. Measure user experience before and after, not just whether the policies work.

Common Pitfalls

Most SASE projects that disappoint fail on planning and people, not technology.

Pitfall	How to avoid it
Treating SASE as a firewall swap	Start from business outcomes and access policy, then choose technology
Weak identity foundations	Fix MFA, user lifecycle and device management before migration
Big-bang cutover	Migrate in phases by user group or site, with a rollback plan
Copying old firewall rules across	Rebuild policy around users and apps; retire rules no one can explain
Ignoring user experience	Measure app performance before and after; brief staff on what changes
Leaving the VPN running indefinitely	Set a decommission date and track progress towards it
No one watching the alerts	Feed SASE logs into a 24/7 SOC or managed detection service
Underestimating TLS inspection	Plan certificate rollout and exceptions (banking, health sites) early
Buying features you will not use	Licence what the roadmap needs in year one; add modules later

Key Takeaways

- 1 Get identity right first.** MFA, device management and a clean user directory make every later phase faster and every policy more effective.
- 2 Phase it, and prove it.** Move in waves with clear gates, starting with the remote users who feel VPN pain most, and let a real pilot pick the provider.
- 3 Finish the job.** Value comes from retiring VPN, MPLS and legacy kit on a fixed date, and from someone watching the alerts around the clock.

Glossary

CASB Cloud access security broker: visibility and control over SaaS use

DEM Digital experience monitoring: measures app performance per user

DLP Data loss prevention: stops sensitive data leaving where it should not

FWaaS Firewall as a service: a firewall delivered from the cloud

IdP Identity provider, such as Microsoft Entra ID or Okta

MDM Mobile device management: controls and checks device health

MPLS Private WAN circuits traditionally used to link offices

PoP Point of presence: a provider data centre where traffic is inspected

RBI Remote browser isolation: runs web pages away from the device

SASE Secure access service edge: networking and security as one cloud service

SD-WAN Software-defined WAN: smart routing across any internet link

SOC Security operations centre: the team that monitors and responds to threats

SSE Security service edge: the security part of SASE, without SD-WAN

SWG Secure web gateway: filters and protects web traffic

TLS inspection Decrypting encrypted traffic so it can be checked for threats

ZTNA Zero trust network access: per-app access that replaces VPN

Sources

Forecast Analysis: Secure Access Service Edge, Worldwide, 2025–2030, Gartner, May 2026
gartner.com/en/documents/7865781

Cyber Essentials: Requirements for IT Infrastructure v3.3, NCSC, April 2026
ncsc.gov.uk

Cyber Security and Resilience (Network and Information Systems) Bill: factsheets, GOV.UK
gov.uk

Cyber Security and Resilience (Network and Information Systems) Bill, UK Parliament
bills.parliament.uk/bills/4035

Regulatory status is correct as of October 2026 and may change. This guide is general information, not legal advice.

How Cybergen Helps

Cybergen helps UK organisations design, deploy and run SASE using leading vendor tooling, matched to your estate rather than to a single product. Our consultants are recognised leaders in cyber security, with deep experience across networking, identity and security operations.



Assess

A readiness review of your identity, devices, apps, sites and contracts, with a clear business case.



Design

An architecture and policy model built around your users and data, single- or multi-vendor as fits.



Prove

A structured proof of concept with real users and measurable success criteria.



Deploy

Phased migration from VPN and MPLS, with minimal disruption and a rollback plan at every stage.



Operate

Ongoing management, tuning and 24/7 monitoring through our managed SOC service.

Available on G-Cloud 15

Direct contracts for private sector clients

Book a SASE Readiness Conversation

Find out where you stand and what to do first.

cybergensecurity.com

About Cybergen

Cybergen is a UK cyber security specialist helping organisations protect what matters most. We combine expert consultancy, managed security services and leading vendor technology to help clients reduce risk, meet regulatory requirements and stay resilient as threats evolve. From readiness reviews to round-the-clock monitoring, we work as an extension of your team.

Get in Touch

cybergensecurity.com

Read More Insights

cybergensecurity.com/blog

