TIEVA

FULCRUM IT PARTNERS

SASE is a Journey, Not a Product

How to Start Without Buying Everything at Once

By Andy Jukes

About the Author

Andy Jukes is the Secure Networks Team Leader at TIEVA and has been a key part of the business for over five years. He brings deep technical expertise in the design, implementation, and support of secure networking solutions.

Andy specialises in SASE, SD-WAN, and next-generation firewalls - helping organisations modernise their network security to enable secure distributed workforces, reduce operational complexity, and support long-term cloud strategies. With a practical, hands-on approach, he works closely with IT teams to align technical decisions with real business outcomes.

Andy Jukes

Executive Summary

SASE (Secure Access Service Edge) represents a major evolution in network and security architecture. But for many IT leaders, the hype has outpaced the practical guidance. This guide offers a grounded, outcome-focused approach to SASE adoption. It outlines a clear five-stage journey, showing how to evolve your architecture step by step - avoiding overbuying, managing change effectively, and building a future-proof foundation.

Whether you've already invested in key technologies or are just beginning to think about zero trust, this guide will help you make confident, context-aware decisions. It's designed to cut through the noise, emphasise flexibility, and help you unlock real business value from SASE.

TIEVA

FULCRUM IT PARTNERS

Contents

Introduction

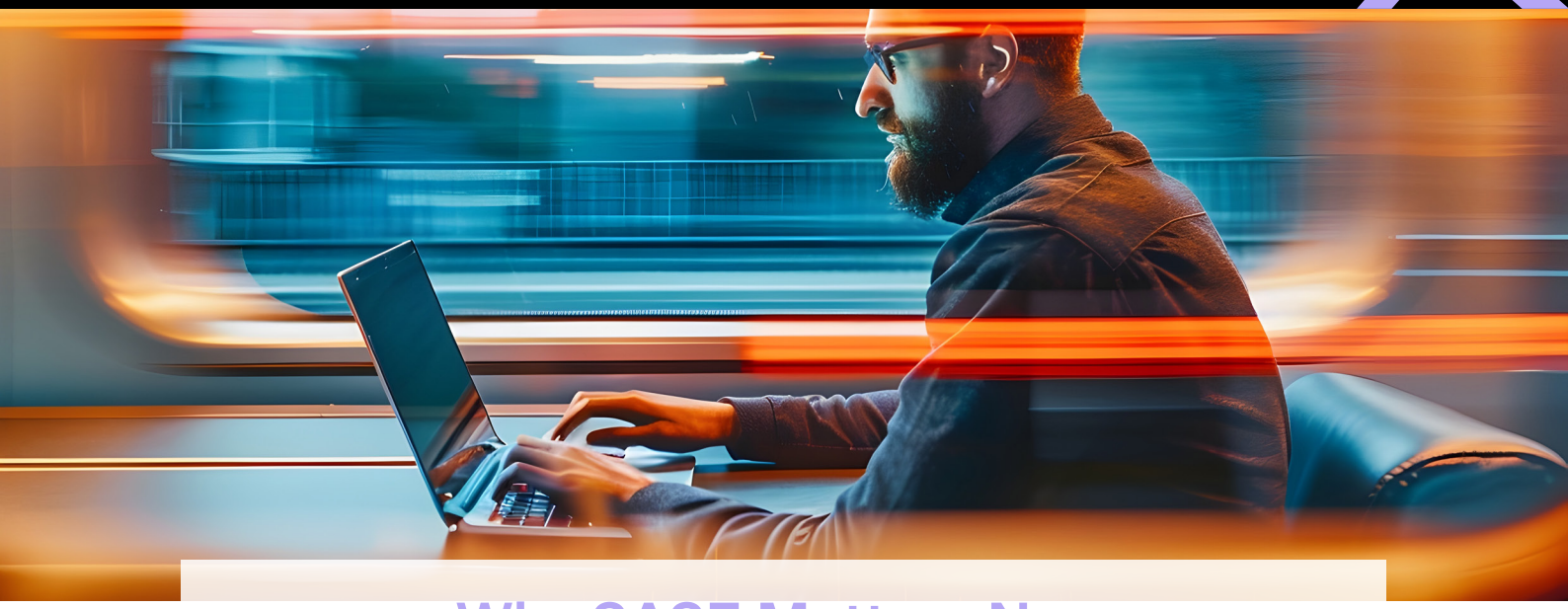
Secure Access Service Edge (SASE) has quickly become one of the most talked-about buzzwords in network and security. Organisations are often told they need it, but without enough context or clarity as to why. This can lead to misunderstandings about what SASE truly is and can sometimes be framed as a one-stop product something you can simply buy and deploy, rather than a broader journey.

In reality, SASE is not a fixed product, it's an evolving architectural approach. As a relatively new and still maturing framework, it continues to develop rapidly with vendors innovating and standards changing in real time. When I first began exploring SASE in 2023, it was early in its journey. By mid-2025, it has made significant progress particularly in areas like: ZTNA, Digital Experience Monitoring and unified management yet there's still a long way to go. SASE isn't about buying a single tool; it's about strategically rethinking how networking and security come together in a cloud-first world.

SASE has emerged from a legacy of disparate network and security tools, all operated in silos. It represents the convergence of these once disconnected technologies into a single unified, cloud-native framework. One that delivers security and connectivity as integrated services.

At its core, SASE is about unifying networking and security under a single pane of glass, enabling organisations to securely and efficiently connect users to both public SaaS platforms (like Microsoft 365, Salesforce, or Dropbox) and private applications hosted in data centres or cloud environments. It ensures seamless, identity-driven access across all environments without sacrificing performance, visibility, or control.

This guide is for IT leaders navigating that evolution. It's designed to give you clarity - not just on what SASE is, but on how to approach it strategically, incrementally, and in a way that delivers real outcomes.



Why SASE Matters Now

The traditional network perimeter is gone. Remote work, SaaS adoption, and cloud-native infrastructures have made it obsolete. The way people connect has changed - and the architecture supporting them must evolve too.

Organisations need a scalable, identity-driven approach to network and security that aligns with modern workflows and supports users wherever they are, whenever they are.

SASE meets this challenge head-on. It enables identity-driven access, consistent policy enforcement, and seamless user experiences across environments. This is not just a trend, it's a fundamental overhaul in how businesses operate. According to Gartner,

> **By 2027, 65% of new software-defined wide-area network (SD-WAN) purchases will be part of a single-vendor SASE offering, an increase from 20% in 2024.**

For many organisations, this change won't start from scratch. Having already invested in SD-WAN, or other technologies, they're now looking to "sweat those assets" and build on that foundation - extending its value while gradually layering in SASE capabilities as the technology matures. It's a pragmatic approach: using existing infrastructure as a launchpad toward a more modern, scalable, and secure architecture.

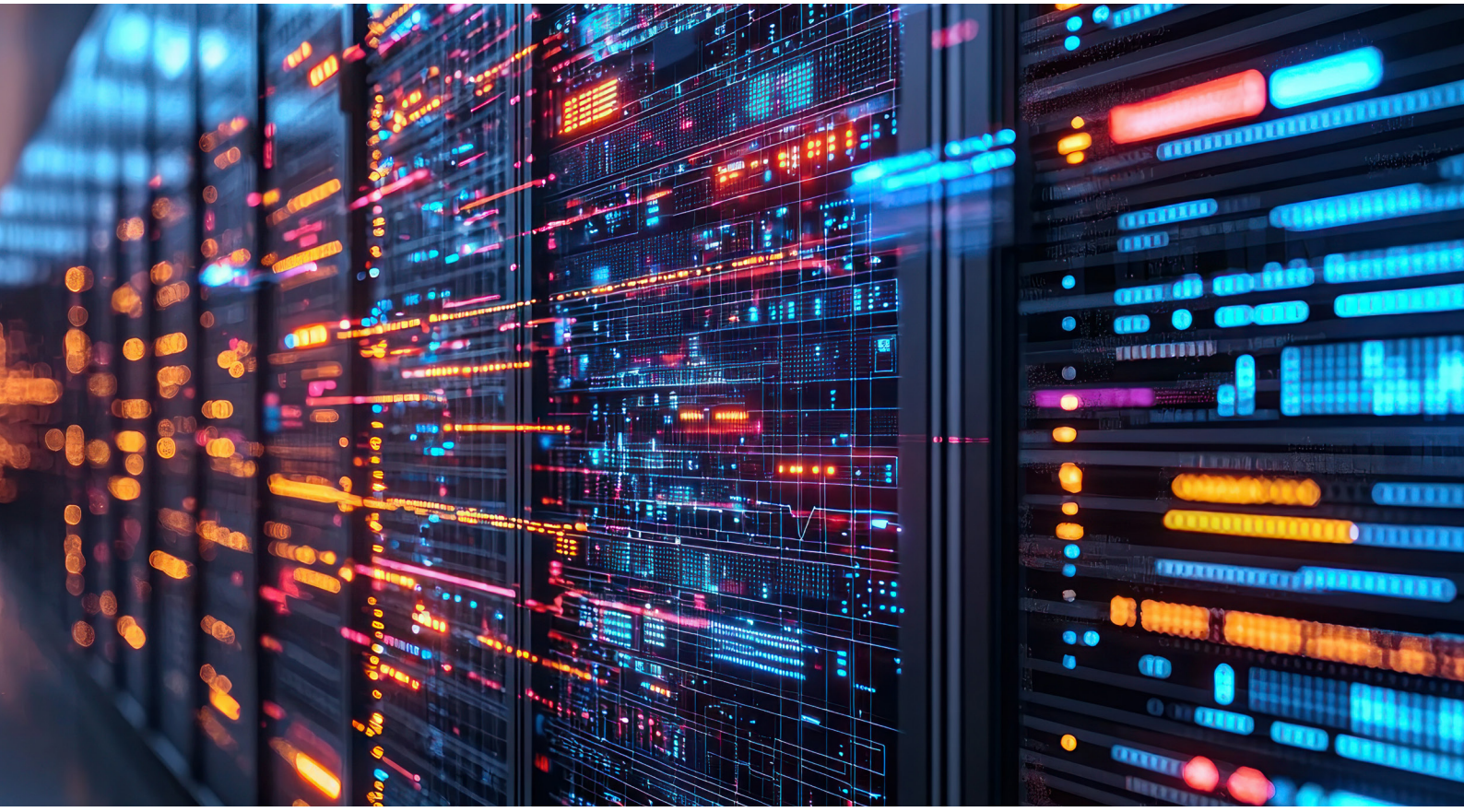
This strategy not only aligns with Gartner's prediction but also reflects a wider industry trend. Just as businesses once transitioned from MPLS to SD-WAN in phases, the move to SASE is unfolding as an evolution, not a rip-and-replace revolution.

Ultimately, SASE adoption is being driven by a combination of technical necessity and strategic business goals.

Organisations are looking to:

- **Support secure hybrid and remote workforces** without the limitations of legacy VPNs.
- **Reduce exposure risk** by enforcing identity-aware access to both private and public applications.
- **Enhance user experience and performance** by ensuring fast, reliable, and secure access to cloud and SaaS applications regardless of user location.
- **Optimise investments** by reducing hardware dependencies and overlapping point solutions.
- **Simplify IT operations** using consolidated tools with centralized policy management and unified visibility.
- **Accelerate digital transformation** by aligning network and security architectures with multi-cloud and SaaS strategies.

The message is clear: the convergence of networking and security is no longer optional. SASE is not just a technology decision it's a business imperative.



Breaking Down the SASE Framework

To understand the journey, you need to know where you're going and the foundational components that make up the architecture. Each element plays a distinct role in delivering a converged, cloud-native approach to networking and security. Aligning these capabilities with business objectives ensures that every phase of adoption delivers measurable value.

The core components of SASE are:

- **Software-Defined Wide Area Networking (SD-WAN):** Application-aware intelligent routing that optimises performance.
- **Secure Web Gateway (SWG):** Secures internet access with web traffic filtering, threat protection and policy enforcement.
- **Cloud Access Security Broker (CASB):** Governs SaaS use with visibility and data control over cloud application usage.
- **Zero Trust Network Access (ZTNA):** Replaces legacy VPNs with identity-based, least-privilege access by verifying user identity and device posture.
- **Firewall as a Service (FWaaS):** Cloud-delivered firewalls for consistent protection and user experience and reducing the need for traditional hardware**.**

Together, these services form the foundation of a secure, agile, cloud-native network.

The 5-Stage SASE Adoption Journey

It's important to understand that adopting the core components of SASE isn't a single event. As the title of this guide suggests, it's a journey - a phased transformation. And, as SASE is still emerging, adoption plans must be dynamic. Standards evolve, vendors are iterating, and feature maturity varies across the market.

A structured, flexible roadmap that balances short-term wins with long-term strategic alignment is essential. The following five-stage journey will help you evolve from a legacy network and security architecture to a secure, cloud-delivered SASE architecture that can adapt as SASE matures.

1. Assess Your Current Environment

Evaluate your network and security architecture. Identify technical debt, performance issues, and visibility gaps. Understand how users access apps and where the friction lies.

Key focus areas:

- **WAN architecture:** MPLS, internet breakout, VPNs, remote access methods.
- **Security stack:** Firewalls, proxies, endpoint protection, identity providers, CASB solutions.
- **Visibility gaps:** Shadow IT, unmanaged devices, unsanctioned cloud apps.
- **Monitoring capabilities:** Existing tools for logging, performance, and threat detection.

2. Map Risks and Dependencies

With your current environment assessed, pinpoint areas of highest risk or strategic value. Map out dependencies - highlighting fragile points, latency issues, or security concerns.

Key focus areas:

- High-risk locations, user groups, and applications.
- Flat networks or over-reliance on VPNs.
- User-to-app, app-to-app, and branch-to-cloud traffic flows.
- Latency-sensitive workflows and bandwidth-heavy services.
- Network telemetry, performance statistics and incident data.
- Inconsistent policy enforcement and monitoring gaps.

3. Prioritise High-Impact Use Cases

Focus on the pain points that offer clear business value with minimal risk. This enables you to demonstrate early wins while building momentum for broader transformation.

Key focus areas:

- **Secure Remote Access:** Replace legacy VPNs with ZTNA to enable identity-based access, reduce attack surfaces, and improve user experience for remote workers.
- **Cloud Application Visibility and Control:** Use CASB and SWG to monitor SaaS usage, enforce data protection policies, and secure cloud access.
- **Branch Network Modernisation:** Shadow IT, unmanaged devices, unsanctioned cloud apps.
- **Zero Trust for Internal Environments:** Existing tools for logging, performance, and threat detection.
- **Tool Consolidation:** Eliminate redundant solutions and simplify policy management through a single pane of glass. Eliminate solutions with overlapping functionalities.
- **Low-Risk Pilots:** Identify non-critical departments or regions where controlled pilots can validate integration with identity providers, logging systems, and performance baselines.

With your initial use cases defined, the next step is selecting a vendor that meets today's priorities while supporting long-term growth. In a rapidly evolving market, a single-vendor strategy offers clear benefits: simplified integration, unified policy enforcement, and streamlined management through one pane of glass.

Consolidating core SASE capabilities like ZTNA, SWG, SD-WAN, and CASB with one provider reduces complexity, accelerates deployment, and lowers operational overhead. While multi-vendor setups may promise best-of-breed tools, they often lead to fragmentation, inconsistent policies, and increased admin burden.

Look for a vendor offering a fully integrated platform, seamless compatibility with your existing identity, endpoint, and logging infrastructure, and a strong innovation roadmap. Validate their offering with a hands-on proof of concept - not just feature checks, but real-world tests of performance, reliability, and policy enforcement. A vendor that supports this level of testing signals both platform maturity and a commitment to long-term partnership.

4. Pilot Key Components

Deploy targeted pilots for your selected SASE capabilities. This is your opportunity to validate interoperability, user experience, and policy consistency in a real-world environment.

Key focus areas:

- ZTNA and/or SWG deployment for specific user groups.
- Integration with identity and endpoint solutions.
- Logging and analytics setup for monitoring.
- Performance baselining: latency, reliability, and failover testing.
- End-user feedback collection and policy refinement.

5. Phase In Additional Capabilities

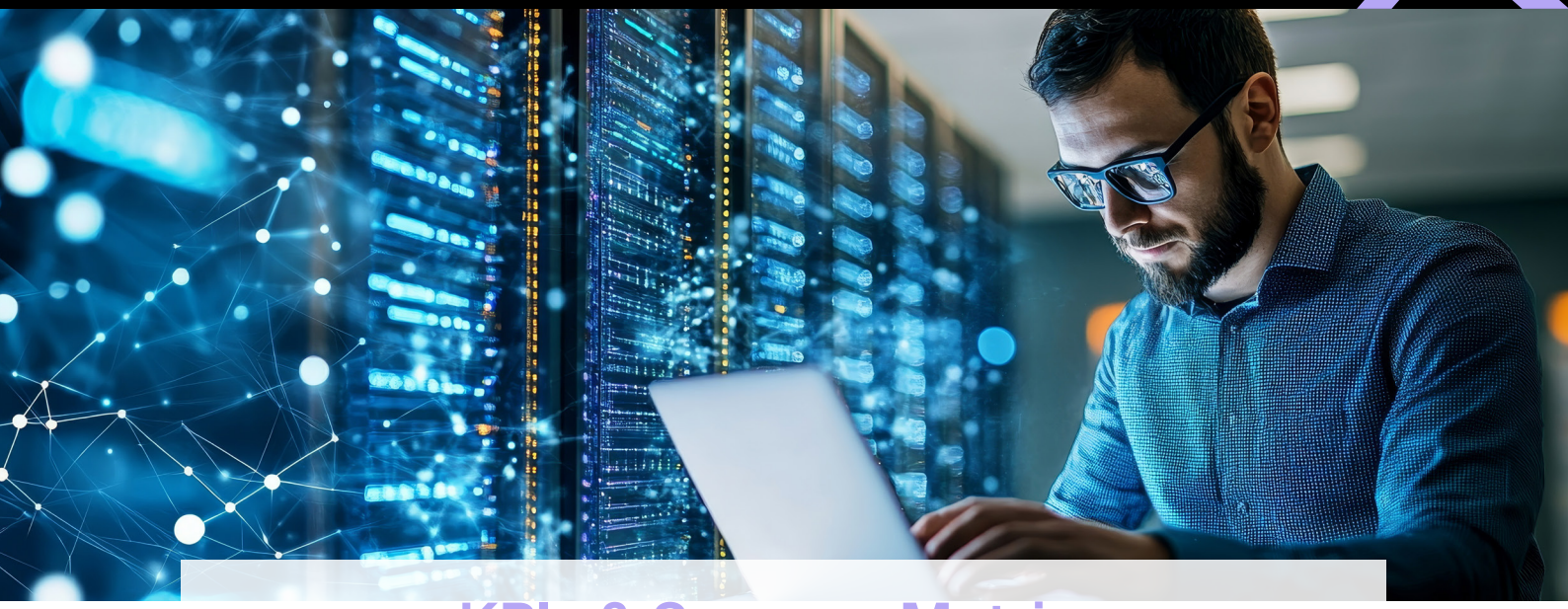
With pilots validated, expand SASE coverage in line with business needs and vendor roadmaps. Layer services progressively while ensuring each step builds toward your target architecture.

Key focus areas:

- **SD-WAN:** Traffic prioritisation, dynamic path selection, failover.
- **CASB:** SaaS usage visibility, data loss prevention (DPL) policies.
- **FWaaS:** Cloud-delivered security replacing legacy firewalls.
- **Policy unification:** Enforcing identity-aware rules across services.
- **User and performance analytics:** Informing continuous rollout.

This phased expansion approach ensures you can scale securely and sustainably without overburdening IT teams or disrupting business operations while staying agile as SASE technologies continue to mature.

Finally, fine-tune your architecture. Consolidate vendors, reduce redundancy, and build a unified policy framework that simplifies management and enhances control.



KPIs & Success Metrics

How do you know you're on the right path? Track measurable outcomes throughout your SASE journey to validate business value, and guide continuous improvement.

Track these indicators:

- **Deployment Efficiency:** Time to implement each SASE component (e.g. ZTNA, SWG, SD-WAN) to assess rollout speed and team agility.
- **Operational Impact:** Reduction in tickets and manual interventions, particularly related to VPN, firewall access and connectivity issues, indicating improved stability and user experience.
- **User Experience Improvements:** Track latency, connection speeds, and session reliability for remote and branch users to ensure performance gains across the network.
- **Security Effectiveness:** Evaluate policy enforcement accuracy, threat detection rates, and compliance with internal and regulatory requirements.
- **Cost Optimisation:** Quantify the decrease in total cost of ownership (TCO) by consolidating vendors, retiring legacy hardware, and reducing licensing overlap.

Managing Change for Long-Term Success

SASE adoption isn't just about the tech stack - it's about people, too. A strong change management strategy helps reduce friction, build trust, and ensure long-term adoption across the organisation.

- **Engage cross-functional teams early** by involving both security and networking stakeholders from the outset. Their collaboration is essential for aligning architecture, policy, and operational workflows.
- **Communicate clearly with end users** during pilot phases to gather feedback, address concerns, and build awareness around how access and experience may change.
- **Present ROI-focused insights to leadership** by highlighting measurable business outcomes such as reduced support overhead, faster incident response, and improved user productivity.
- **Develop targeted training plans** for IT and security teams to ensure they are equipped to operate, monitor, and optimise the new platform effectively.
- **Cost Optimisation:** Quantify the decrease in total cost of ownership (TCO) by consolidating vendors, retiring legacy hardware, and reducing licensing overlap.

Change managed proactively is change that sticks, setting the stage for a successful long-term SASE deployment.

Example SASE Roadmap

This high-level roadmap outlines a phased, outcome-driven approach to implementing SASE over 12 months balancing quick wins with long-term strategic value.

Quarter	Key Actions	Expected Outcomes
Q1	Assess current environment and define strategic needs	Clear priorities established, key use cases identified, vendor shortlist created
Q2	Launch pilot with core components (e.g. ZTNA or SWG)	Early validation of architecture, improved user experience, enhanced security posture
Q3	Expand deployment to include SD-WAN and/or CASB	Improved application performance, broader policy coverage, better visibility into cloud usage
Q4	Consolidate platforms, optimize policies, train teams	Reduced complexity and cost, unified policy enforcement, operational readiness for scale

Final Thoughts

SASE isn't a one-size-fits-all solution or a product you can buy off the shelf. It's a strategic journey that, when executed with intent and planning, aligns your organisation's security architecture with the demands of today's hybrid, cloud-first world.

Start small.
Learn fast.
Scale smart.

With the right approach, you'll not only modernise your architecture - you'll empower your business to move faster, safer, and with greater confidence into the future.

About TIEVA

TIEVA helps organisations navigate the evolving demands of modern IT, from secure networking to cloud transformation, with a focus on simplifying complexity and delivering measurable business outcomes.

As SASE continues to redefine the way businesses approach connectivity and security, we support our customers on that journey. Our team works closely with IT leaders to design and implement secure, scalable architectures that align with real-world challenges, from enabling hybrid workforces to consolidating tools and improving visibility.

With deep expertise in SASE technologies and a practical, consultative approach, we help you move at the right pace — starting small, learning fast, and scaling smart.

To learn more about how we can support your SASE journey, from assessing your current environment to building a long-term roadmap.
Visit: tieva.co.uk/sase

TIEVA

BY FULCRUM IT PARTNERS

Contact us

Email TIEVA
hello@tieva.co.uk

Call TIEVA
+44(0)333 0430 333

tieva.co.uk