Principle Networks

SSE vs SASE:

WHY LESS CAN BE MORE

A GUIDE TO MODERN NETWORK SECURITY ARCHITECTURE

The network security landscape has undergone a fundamental shift.

As organisations embrace cloud-first strategies and remote working becomes the norm, traditional network architectures are being challenged by two competing paradigms: Secure Service Edge (SSE) and Secure Access Service Edge (SASE).

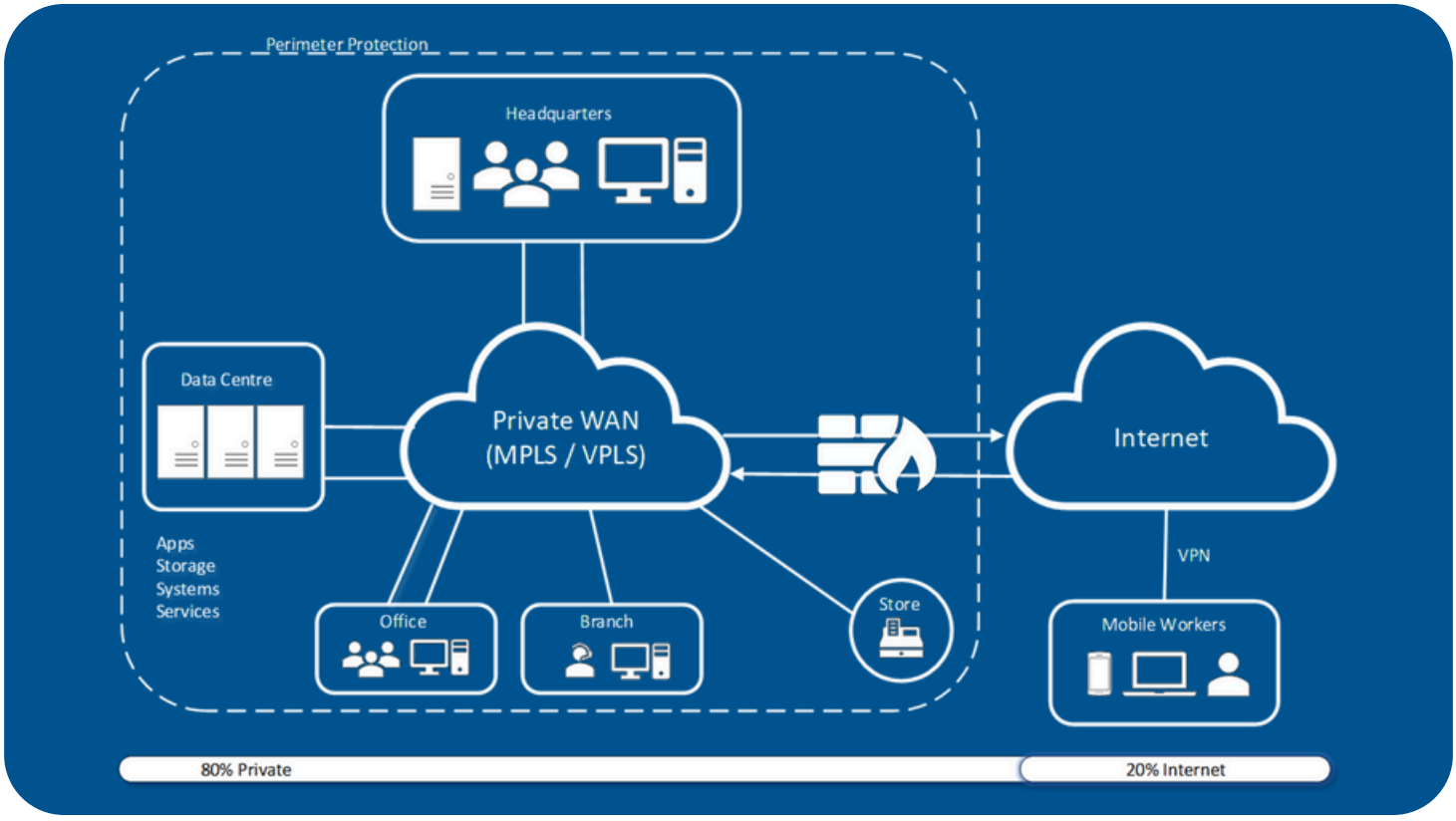
Whilst SASE has garnered significant attention from vendors and analysts alike, we argue that for many organisations, SSE represents a more pragmatic, cost-effective, and operationally sound approach to modern network security. This whitepaper examines **why SSE may be the end goal** for your organisation, rather than merely a stepping stone to SASE.

The Evolution of Network Security: From Castle Walls to Cloud-First

The Traditional Network Paradigm

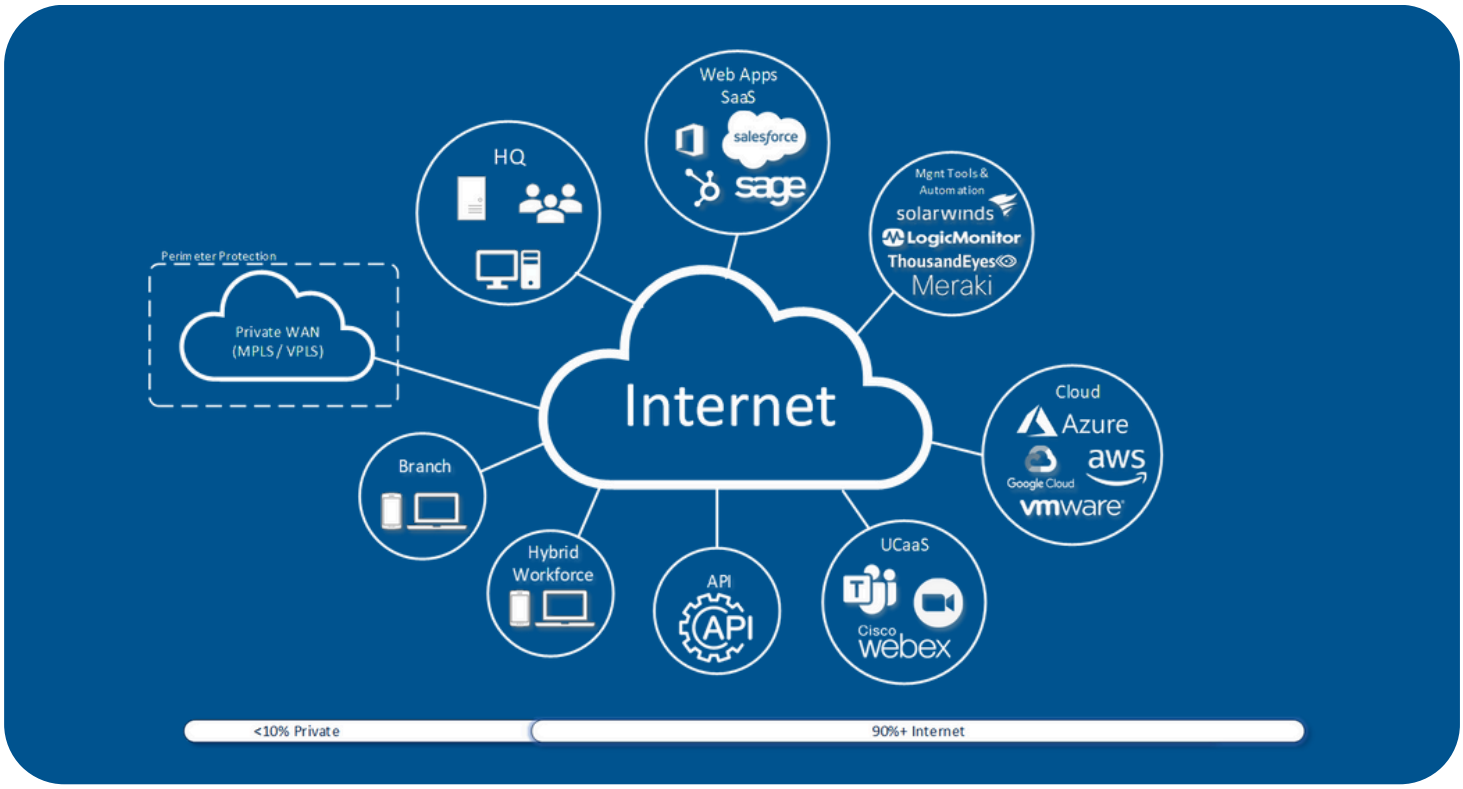
For decades, enterprise networks operated on a simple premise: users worked in offices, applications ran in data centres, and everything was connected via private networks. MPLS circuits formed the backbone of corporate connectivity, creating secure but rigid pathways between locations. This model worked well when the perimeter was clearly defined and controllable.

The corporate network was essentially a digital castle, with high walls protecting valuable assets inside and carefully controlled gates managing who could enter and leave. IT departments invested heavily in building and maintaining these fortifications, with substantial budgets allocated to circuit costs, network hardware, and specialist staff to manage increasingly complex infrastructures.



The Great Disruption

Three seismic shifts have fundamentally altered this landscape. **Cloud migration** has seen applications move from carefully controlled on-premises data centres to public cloud platforms where they're accessible via the internet. The **rise of remote work** has transformed users from office-bound employees to a distributed workforce operating from home offices, co-working spaces, coffee shops, and client sites. Perhaps most significantly, **the internet itself** has evolved into a reliable, ubiquitous network infrastructure, particularly in developed markets like the UK and Europe.



These changes have rendered traditional network architectures not just obsolete, but counterproductive. The question becomes stark:

> **Why invest in expensive MPLS circuits to connect offices when your applications are in AWS or Azure?**

Why force remote users through corporate network choke points when they can access cloud services directly with better performance and user experience?

Understanding the Gartner Magic Quadrants

The Birth of SASE

Gartner coined the term SASE (Secure Access Service Edge) in 2019, defining it as a network security architecture that combines wide area networking (WAN) and network security services into a single, cloud-delivered service model. **The promise was compelling**: converged networking and security, delivered from the cloud, optimised for the modern enterprise.

The concept emerged from the recognition that traditional network architectures were struggling to cope with digital transformation. Rather than separate WAN and security infrastructures, SASE promised to unify these functions in a single platform that could adapt to modern working patterns and cloud-first application architectures.

SSE: The Security-First Approach

In 2021, Gartner refined their thinking and introduced SSE (Secure Service Edge) as a subset of SASE, focusing purely on the security services without the networking components. This distinction is crucial and represents more than just semantic differences. It reflects a fundamental philosophical divide about what modern enterprises need.

SSE acknowledges that for many organisations, the networking problem

> **has already been solved by the internet itself.**

Rather than building overlay networks on top of internet connectivity, SSE focuses on making that existing connectivity secure and manageable for enterprise use.

The 2025 Magic Quadrant Split

Gartner's decision to publish **separate Magic Quadrants for SSE and single-vendor SASE** in 2025 validates what many practitioners have observed: these are distinct approaches suited to different organisational needs and maturity levels. The separation recognises that not every organisation needs or wants the full complexity of SASE when SSE can deliver the security outcomes they require.

The Case for SSE:
Security Without the Baggage

Internet as Infrastructure

The modern internet, particularly in developed markets like the UK and Europe, has achieved remarkable reliability and performance. Consider the transformation that has occurred over the past decade. **Fibre broadband** has become ubiquitous in urban and suburban areas, delivering symmetrical bandwidth that often exceeds what organisations were paying premium prices for via private circuits. **5G networks** provide mobile connectivity that rivals fixed-line performance, whilst satellite services like **Starlink** are eliminating the last connectivity dead zones.

> **This isn't the unreliable, best-effort internet of the 1990s. Modern internet infrastructure provides availability that rivals or exceeds traditional private circuits, often with multiple redundant paths and competitive pricing that makes private networking look expensive and inflexible by comparison.**

The SSE Advantage

By leveraging the internet as the underlying transport and overlaying security services, SSE provides a fundamentally different value proposition. Users receive **consistent security posture** whether they connect from the office, home, or a coffee shop, with identical security controls and policies applied regardless of access method.

> **The operational simplicity is transformative.**

There's no need to manage complex WAN architectures, worry about circuit provisioning, or maintain expensive networking hardware. When a new office opens, **it needs internet connectivity and nothing more**. When users travel, they maintain full access to applications and services without VPN complexity, and the inherent capability for users to "work around" it when not strictly driven to use it or performance degradation.

Cost effectiveness extends beyond simple circuit savings. The reduction in networking complexity translates to lower management overhead, reduced specialist staffing requirements, and elimination of the procurement and vendor management complexity associated with private networking.

Scalability becomes trivial. Adding new users or locations requires no additional networking infrastructure, no capacity planning for WAN links, and no complex traffic engineering. Growth is limited only by internet availability, which in most developed markets is ubiquitous.

The SASE Trap:
When More Isn't Better

The Single-Vendor Seduction

The "**single vendor**" promise of SASE platforms sounds appealing in boardrooms and procurement meetings. The idea of one throat to choke, one contract to manage, and one platform to rule them all has obvious administrative appeal. This apparent simplicity often masks underlying complexity and compromises that become apparent only during implementation and operation.

The challenge is that networking excellence doesn't automatically translate to security expertise, and vice versa. We've witnessed network appliance manufacturers struggling to build credible security solutions that match the depth and sophistication of dedicated security vendors. Similarly, security specialists venturing into networking often underestimate the operational complexities of WAN management and optimisation.

Master of None

The single-vendor SASE platforms emerging in the market often feel like collections of acquired technologies rather than purpose-built, integrated solutions. Network giants have acquired security divisions, creating platforms that excel in connectivity but **struggle with advanced threat detection**. Security specialists have bought networking companies, resulting in solutions with robust security capabilities but **questionable networking performance** and reliability.

The hybrid approaches through acquisition frequently result in **platforms that feel bolted together** rather than architected as cohesive systems. Users experience inconsistent interfaces, duplicated functionality, and gaps where different acquired technologies don't integrate seamlessly.

The Vendor Lock-In Risk

Single-vendor SASE platforms create significant **dependency risks** that extend well beyond technical considerations. Organisations find themselves with limited negotiating power at renewal time, facing **substantial switching costs** that vendors use to justify premium pricing. The difficulty of adapting to changing requirements becomes apparent when the single platform doesn't evolve in directions that align with business needs.

Perhaps most concerning is the **reduced ability to adopt best-of-breed solutions** as they emerge. In rapidly evolving markets like cybersecurity, being locked into a single vendor's roadmap can mean missing out on breakthrough technologies or approaches that could provide competitive advantage.

Best-of-Breed vs Single Platform:
A Strategic Choice

The Power of Partnership

Rather than seeking a single vendor to provide everything, organisations should consider partnering with specialists who can **architect integrated solutions** using best-of-breed components. This approach combines connectivity from multiple internet providers using diverse access technologies, ensuring resilience and competitive pricing. Security services come from leading ZTNA, SWG, CASB, and DLP providers who **specialise** in their respective domains and invest heavily in **staying ahead of evolving threats**.

Identity management leverages robust IAM platforms with advanced authentication capabilities developed by companies whose entire focus is on solving identity challenges. **Monitoring and response** utilise comprehensive SIEM and SOC capabilities from security specialists who understand the threat landscape and have the scale to provide effective response services.

Endpoint protection comes from advanced EDR and device management specialists who focus exclusively on endpoint security and understand the nuances of different operating systems, device types, and deployment scenarios. Governance integrates **risk management and compliance** tools from providers who specialise in regulatory requirements and understand the complexities of different industry frameworks.

Single Partner, Multiple Solutions

The **optimal approach** combines the benefits of unified management and accountability with the flexibility of specialised solutions. A trusted partner can design integrated architectures using best-in-class components whilst providing unified support and troubleshooting capabilities. They manage vendor relationships and contract negotiations, leveraging their scale and expertise to achieve better terms than individual organisations could obtain.

Such partners ensure **solutions work together seamlessly** through proper integration design and ongoing management. They adapt the architecture as requirements evolve, adding new capabilities or replacing components as better solutions emerge.

> **Most importantly, they provide the single point of accountability that organisations need without forcing them into the compromises inherent in single-vendor platforms.**

Implementation Strategy:
Making the Transition

Assessment and Planning

Before embarking on any transformation, organisations must honestly assess their requirements through comprehensive analysis of their application portfolio, user behaviour patterns, and existing network dependencies. This assessment often reveals surprising insights about what connectivity is required versus what has been assumed to be necessary.

Application portfolio analysis examines where applications are hosted, how users currently access them, and what the genuine performance and security requirements are. Many organisations discover that applications they assumed required private network access perform better when accessed directly via the internet, without the latency and complexity introduced by WAN routing.

User behaviour mapping reveals the reality of how and where people work, what devices they use, and their connectivity patterns throughout typical working days and weeks. This analysis frequently shows that traditional office-centric assumptions about user location and connectivity are outdated.

Network dependency reviews challenge assumptions about what site-to-site connectivity is required, which legacy systems truly need private network access, and what the real costs and benefits of current WAN infrastructure are. Often, expensive private circuits are maintained for edge cases that could be handled more cost-effectively through alternative approaches.

The SSE-First Approach

For organisations with **cloud-first strategies** and flexible working models, the implementation sequence becomes clear. Identity and access management provides the foundation, becoming the new control plane that replaces network-based security controls. Zero trust network access replaces VPN infrastructure with application-specific access that works regardless of user location or network connectivity.

Secure web gateway deployment ensures consistent web security policies regardless of access method, providing advanced threat protection that adapts to emerging risks without requiring user intervention or technical expertise. **Cloud access security brokers** extend this protection to cloud applications, providing visibility and control over both sanctioned SaaS and shadow IT usage.

Data loss prevention capabilities protect sensitive information as it moves between users and cloud services, maintaining security even when traditional network-based controls are absent. The entire architecture builds upon the assumption that the internet provides the underlying connectivity, with security services creating the controlled, enterprise-grade environment on top of commodity internet access.

Avoiding the SDWAN Detour

Many organisations face pressure to implement SD-WAN as a stepping stone to SASE, often from vendors with significant investments in networking hardware and software. However, if analysis reveals that applications are primarily cloud-hosted, users work flexibly across multiple locations, and site-to-site connectivity requirements are minimal, then SD-WAN represents **unnecessary complexity and cost**.

The decision to **skip SD-WAN** and move directly to SSE can be controversial, particularly within IT departments that have invested heavily in networking expertise and infrastructure. However, the benefits of **avoiding this complexity** often outweigh the political challenges, delivering immediate improvements in user experience, cost reduction, and operational simplicity.

Real-World Considerations

Regulatory and Compliance Requirements

Some organisations face regulatory requirements that **influence** their architecture choices, but these constraints are often less restrictive than initially assumed. **Data sovereignty** requirements may favour certain cloud regions or providers, but don't necessarily mandate private networking. **Industry regulations** may mandate specific security controls, but these can often be implemented more effectively through specialised security solutions than through integrated SASE platforms.

Audit requirements may influence logging and monitoring approaches, but modern cloud-based security solutions often provide superior audit capabilities compared to traditional network-based approaches.

> **SSE architectures can accommodate these requirements more flexibly than rigid SASE platforms, allowing for specialised compliance tools and region-specific deployments that evolve with regulatory changes.**

Legacy System Integration

Organisations with significant legacy systems often cite this as a **barrier to SSE adoption**, but the challenges are frequently overstated. On-premises applications that can't be cloud-migrated may indeed require private network access, but this **doesn't necessarily justify maintaining expensive WAN infrastructure** for the entire organisation.

Industrial systems requiring local network access and legacy protocols that don't work well over internet connections represent genuine technical constraints, but these can often be addressed through targeted solutions rather than enterprise-wide private networking. **Hybrid approaches** that combine SSE for modern workloads with specific private connectivity for legacy systems often prove more cost-effective than full SASE deployment.

The Economic Reality

Total Cost of Ownership

When evaluating **SSE versus SASE**, organisations must consider the **full economic picture** beyond simple platform licensing costs. SASE deployments typically involve platform licensing that includes networking components many organisations don't **fully utilise**, professional services for complex implementation projects that can take months or years, ongoing management of WAN infrastructure that requires **specialist skills**, and vendor lock-in which results in premium pricing at renewal time.

SSE approaches involve security platform licensing that can be right-sized to **actual needs**, internet connectivity that benefits from **competitive commodity pricing** with multiple provider options, and partner services in a competitive market with multiple options for support and management. The operational model is fundamentally **simpler**, requiring less specialist expertise and enabling **faster** deployment and scaling.

Return on Investment

SSE typically delivers **faster return on investment** through immediate elimination of MPLS and WAN costs, which can represent significant monthly operational expenses. The **reduced complexity** in network management translates to lower operational costs and reduced dependency on specialist networking skills that are expensive and hard to find.

Improved user productivity through **consistent access** regardless of location can deliver substantial **business benefits** that are often underestimated in traditional IT cost-benefit calculations. Enhanced security posture across all access methods **reduces risk and potential costs** associated with security incidents, whilst the flexibility to rapidly adapt to changing business requirements provides **strategic value** that's difficult to quantify but increasingly important in volatile business environments.

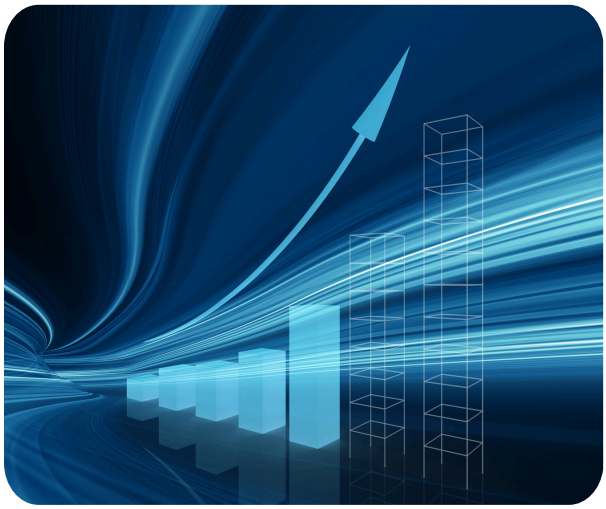
Future-Proofing Your Investment

Technology Evolution

The **pace of change** in both networking and security technologies continues to accelerate, with **new threats emerging constantly** and new capabilities being developed to address them. SSE architectures, with their emphasis on best-of-breed components and flexible integration, are better positioned to **adapt** to emerging security threats and response technologies.

New connectivity options including 5G, satellite, and edge computing can be incorporated into SSE architectures without fundamental redesign, whilst **evolving compliance and regulatory** requirements can be addressed through specific solutions rather than platform replacements. Changing business models and working patterns can be accommodated through configuration changes rather than infrastructure overhauls.

Scalability and Growth



As organisations **grow and evolve**, SSE provides superior **flexibility** for adding new users regardless of location, simple integration of acquired companies without network integration projects, and rapid deployment in new markets or regions without infrastructure prerequisites. **Cost-effective** scaling based on actual needs rather than infrastructure capacity becomes possible, enabling organisations to **grow** efficiently without over-provisioning network capacity.

Conclusion: Choosing Your Path

The choice between **SSE and SASE** is not merely technical but fundamentally strategic. It reflects your organisation's vision of the **future**, your appetite for complexity, and your commitment to flexibility and innovation. For organisations that have embraced cloud-first strategies, flexible working models, and modern security paradigms, SSE represents the destination, not a waypoint.

The internet has evolved to become reliable, ubiquitous infrastructure that connects users to applications more effectively than private networks ever could. SSE makes this connectivity secure, manageable, and enterprise-ready without the cost and complexity of unnecessary networking infrastructure.

> **Our key recommendations centre on honest assessment of actual connectivity requirements rather than historical assumptions, thinking cloud-first about both applications and security, choosing partners over platforms to gain expertise and integration rather than single-vendor convenience, and starting with SSE for most modern organisations that need security without unnecessary complexity.**

Planning for **flexibility** becomes crucial in rapidly changing business environments. Choose architectures that can adapt as your **business evolves**, technologies emerge, and user expectations change. The **future of enterprise networking** is not about building bigger, more complex networks but about making the internet secure, manageable, and enterprise-ready.

Principle Networks

Don't Navigate Network Security Transformation Alone

Understanding whether SSE or SASE is right for your organisation is the first step. Making the transition effectively requires expertise, experience, and the right approach.

Whether you're questioning your expensive MPLS circuits or already planning your cloud-first security strategy, we can help you assess your actual requirements, identify the architecture that fits your needs, and design a best-of-breed solution that delivers security without unnecessary complexity.

Ready to assess your network security architecture?

03330 124 003

enquiries@principle-networks.com