BUYER'S GUIDE

SASE

SAEPIO.CO.UK

SAEPIO

Assured Service Provider

in association with National Cyber Security Centre

TABLE OF

Contents

WHAT IS

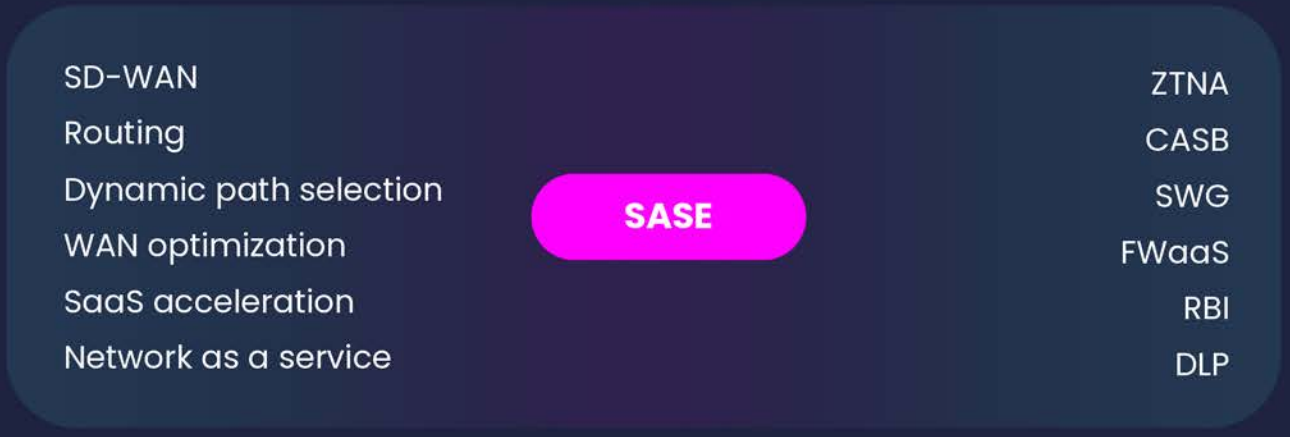
SASE / SSE

1

SASE (Secure Access Surface Edge) / SSE (Secure Surface Edge) is a critical component of a business's security stack and represents the evolution of traditional, hardware defined Network Security. Coined in 2019 SASE articulated the convergence of Networking infrastructure and Security capabilities. In 2021 this thinking was extended to focus on a security-only converged architecture in SSE.

SASE fundamentally describes an integrated and converged set of security and networking capabilities. Traditionally discreet capabilities these controls are integrated via proxy based deployments.

The relevance and adoption of SASE have been accelerated by the increased use of cloud. Both hyperscaler-based application hosting and the use of SaaS platforms are well suited to the Zero-Trust principles and content awareness of a SASE architecture.



THE EVOLUTION OF

SASE / SSE

2

Having launched SASE as an approach analysts (Gartner, Forrester et al) soon split out the security-only components due to slower than anticipated adoption of SD-WAN as a replacement for MPLS networks. SSE was launched as an approach focussed, in-part, on the need to secure the post-covid boom in remote working.

Return-to-office Policies and copper-switch-off has since refocussed attention on “full-stack” SASE.

SSE as an approach has fundamentally seen the convergence of the several key security control capabilities.

- Secure Web Gateway (SWG)
- Zero Trust Network Access (ZTNA)
- Cloud Application Security Broker (CASB)
- Next Generation Firewall (NGFW)
- Remote Browser Isolation (RBI)
- Enterprise Browser
- Data Loss Prevention (DLP)

In addition to these solutions falling into the SSE architecture we have seen the merging of capabilities across technology controls.

- Capability consolidation.
- DLP delivered by a CASB control plain
- NGFW being deployed as a service via a proxy (FWaaS)
- Inline CASB functionality being including in “next generation” SWG
- VPNs being replaced by ZTNA solutions in line with Zero Trust principles of least privilege/access.

Any User | Any Device | Any App | Any Location

A unified cloud architecture to protect users, workloads and IoT/OT devices.

CHOOSING THE RIGHT

SASE / SSE

3

In today's cyber security landscape, it can be challenging to distinguish between the numerous SASE / SSE vendors. The aim of this guide is to simplify your decision-making process and guide your review of the market.

KEY

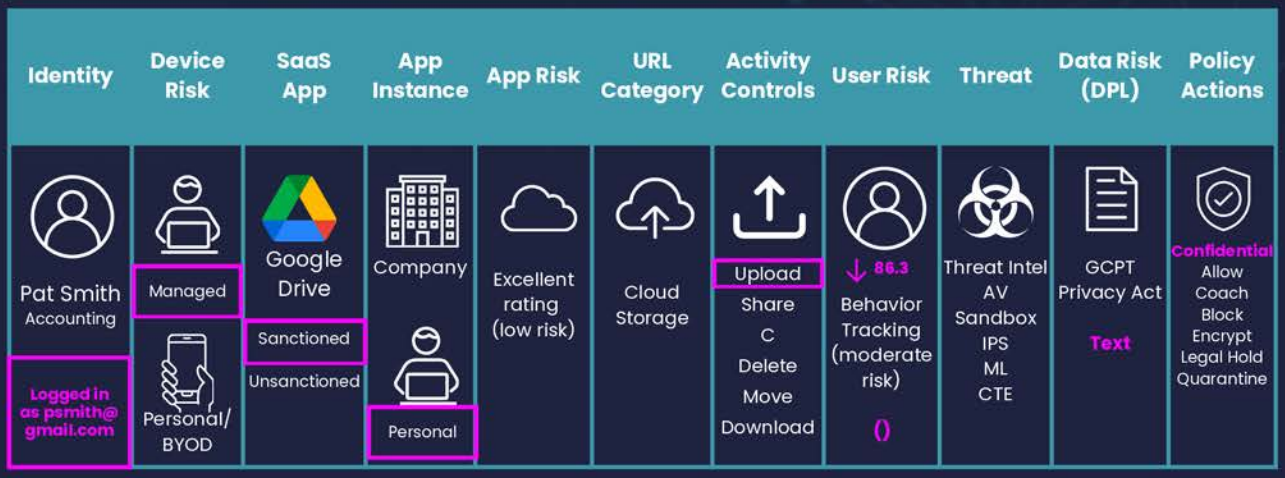
Considerations

4

Requirements and Objectives

- **Current Security Tools:** Many organisations will have existing technology controls and networking capability. It is crucial to align a strategy with commercial and operational priorities as well as cyber risk management objectives.
- **Full Platform vs. Phased:** Aligning a S(A)SE adoption strategy inline with these various priorities allows organisations to maximise the existing investment, whilst dealing with prioritised usecases. What cyber risk management objectives exist? What deadlines are being faced? What rate of adoption can you accommodate?
- **Maturity Objectives:** Don't rush to niche use case capability, identify core capabilities and grow into the architecture.
- **Consolidation:** Identify parts of the architecture that can be deprecated following S(A)SE adoption; branch UTMs are often a good candidate.
- **Rule-base:** Consolidate and review your network and web security rules to ensure continuity in a simplified, centralised management UI.
- **IDAM:** S(A)SE relies on well governed identities to apply appropriate rules (RBAC etc)

Zero-Trust Data Protection: Dynamic & Adaptive Policies



Selection

- **Ease of setup: The solution should clearly demonstrate a degree of simplicity in implementation, operationalisation and BAU when compared with a traditional network security architecture.**
- **Adoption Roadmap: How are the capabilities which meet your objectives licensed? What are the options for phased adoption that matches desired outcomes?**
- **Ease of Use:** as above, the solution should have an intuitive, simple UI. Focus on two areas: delivery of key statistics and events, together with ease of threat hunting and investigation of network security traffic when needed.
- **End User Experience:** SSE often presents an opportunity to improve UX via the removable of clunky solutions. Test performance in POV to ensure that not only the EUC experience is improved, but application performance is maintained or improved.
- **Customisation:** some customers choose to leave the solutions in 'out of the box mode' while others may wish to customise rules. This is dependent on the needs of users and your organisation. If you do require customisation, it is important to review how this is done. It is also important to understand the baseline configuration requirements and "standard" policies which are default.
- **Integration:** How easily can the solution integrate with your existing SecOps tack, notably SIEM or MDR tooling. What impact will this network log ingestion have on SecOps costs and processes? How does the tool support optimising your SecOps objectives.

COMPARISON

Criteria

5

- **Commercials:** what are the pricing metrics? What is the annual purchase cost? How expensive would it be to add additional end users if the organisation grows?
- **Roadmap:** does the vendor have a clear roadmap for the development of their solution, both in terms of new features, but also to quickly respond to new threats?
- **Customer Service:** how would the contract be managed, is support available when it is required?
- **Resilience:** application and web access are critical requirements for the business, does the solution guarantee a sufficient level of resilience and availability?
- **User feedback:** what do existing customers, especially within your industry say about the vendors?

NEXT

Steps

Choosing the right SASE / SSE provider is a strategic decision, and Saepio is here to guide you every step of the way. Here's how we help customers move from evaluation to a confident selection:

Step 1. Define your requirements

Understand your environment, current challenges and goals and organisational specific requirements.

Step 2. Build a shortlist of providers

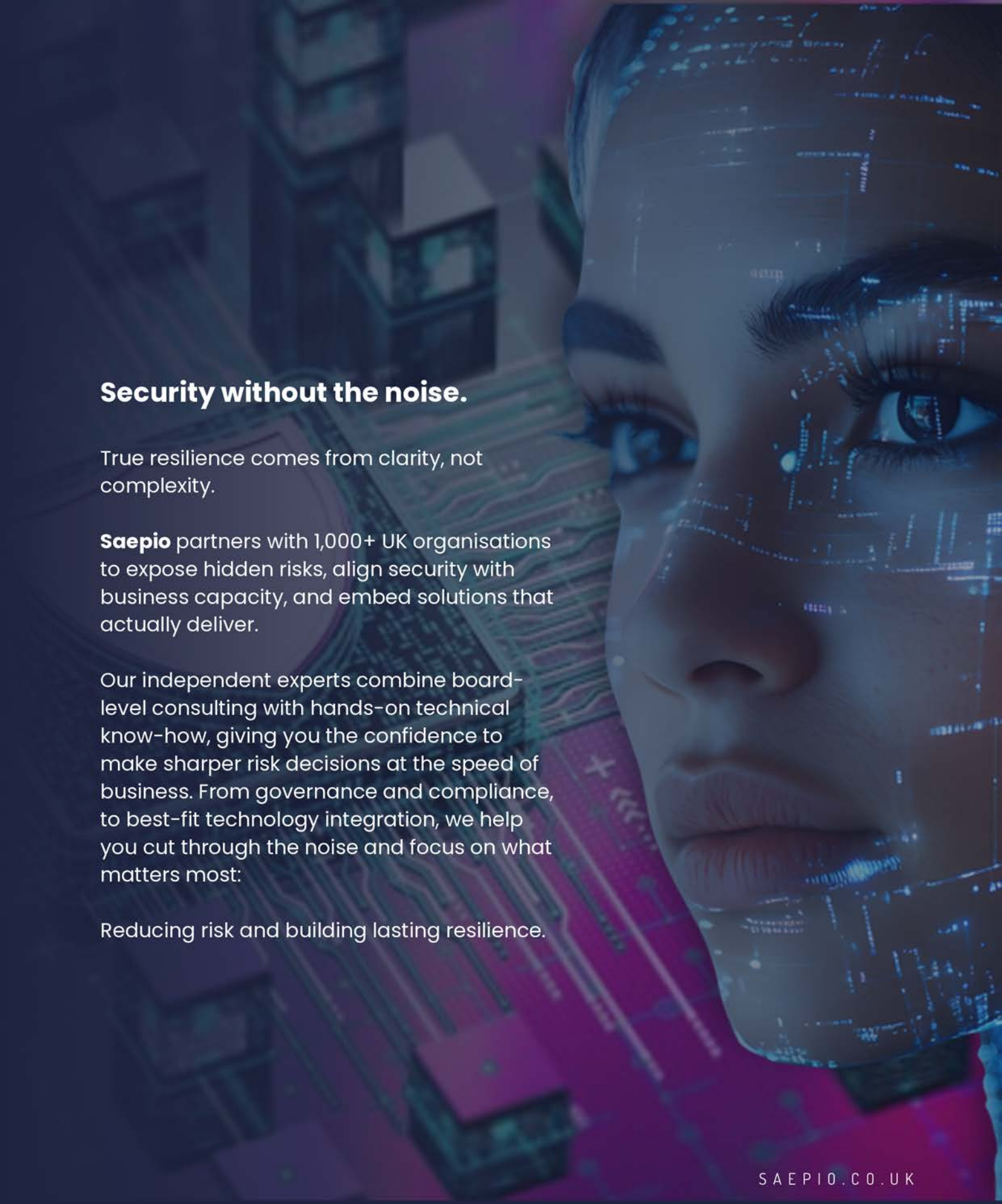
Using our vendor-neutral approach to shortlist providers based on your requirements.

Step 3. Facilitate demos and proof of concepts

A key stage to see how the solution performs in your environment and where possible provide hands on access to the platforms so that you and the team can validate the tool.

Step 4. Procurement and onboarding support

We can assist with contract negotiation and commercial alignment, as well as ensuring that onboarding plans are realistic and aligned with your internal timelines.



Security without the noise.

True resilience comes from clarity, not complexity.

Saepio partners with 1,000+ UK organisations to expose hidden risks, align security with business capacity, and embed solutions that actually deliver.

Our independent experts combine board-level consulting with hands-on technical know-how, giving you the confidence to make sharper risk decisions at the speed of business. From governance and compliance, to best-fit technology integration, we help you cut through the noise and focus on what matters most:

Reducing risk and building lasting resilience.

SAEPIO.CO.UK

SAEPIO

Assured Service Provider

in association with National Cyber Security Centre