Telstra SASE

Confused about where SSE fits into the SASE approach?

For enterprises worried about relinquishing their existing networking infrastructure and security investments to adopt Secure Access Service Edge (SASE) right now, SSE (Security Service Edge) could be the answer.

The SASE approach combines networking and security capabilities, including SD-WAN, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Next Generation Firewall (NGFW) and Zero Trust Network Access (ZTNA), primarily delivered as a service. SASE, however, is an ongoing process that does not happen at the flick of a switch.

As a result, enterprises who want to put their toe in the water with SASE are opting for SSE, which incorporates the security part of SASE - CASB, SWG, and ZTNA - in a single cloud-centric platform as a stepping stone to SASE. SSE secures access to the web, cloud services, and private applications. The platform capabilities number access control, threat protection, data security, security monitoring, and acceptable-use control enforced by network-based and API-based integration.

By 2025, 80% of organisations looking to procure SSE-related security services will purchase a consolidated SSE solution rather than a standalone cloud access security broker, secure web gateway, and ZTNA offerings, up from 15% in 2021, according to Gartner.[1]

The traditional security perimeter is breaking up

With the trend for hybrid working, anytime access, and cloud applications, security functions must evolve to keep one step ahead of malevolent actors.

SSE is the simple answer, providing consistent security across multiple clouds, data centers, and software-as-a-service applications. At the same time, when combined with SASE, it enhances the user experience. SSE really is a no-brainer.

A step in the journey to SASE

With SSE, enterprises gain access to an overarching security approach independent of their existing networking infrastructure. They will not, however, get access to all the benefits of SASE, such as bandwidth control and intelligent network optimisation. This is why some enterprises choose to approach SSE before completing a full SASE adoption.

SSE provides a set of controls that enterprises need today to protect their remote workforce from malicious actors by deploying zero-trust, data protection, and browser and cloud services security solutions. The zero-trust security model demands strict, continuous verification of every user and every device to access internal resources.

Enterprises that find adopting SSE overwhelming can first deploy a Secure Web Gateway (SWG) before moving to a complete SSE. An SWG is a security solution that stops unsecured internet traffic from entering or leaving the network. They perform two essential functions; filtering out untrustworthy content from web traffic and blocking unauthorised user behaviour.

Once an enterprise has deployed SSE successfully, it can look at adding additional SSE services, such as ZTNA and CASB, as required.

[1] Gartner Magic Quadrant for SSE 2022
https://www.gartner.com/doc/reprints?id=1-29P0URMJ&ct=220412&st=sb&submissionGuid=1bbb52bf-ab92-4b44-b175-5b02180f7612

Understanding an enterprise's SSE requirements

By deploying SSE, enterprises achieve many security benefits of SASE without the initial heavy lifting. But it isn't a switch-on-and-go scenario. SSE still requires careful planning and migration efforts to be a success. This includes the right vendor and solution to fit in with business outcomes.

Getting to complete SSE requires having SWG, CASB, and ZTNA, each of which requires a target state technical and service design, along with a migration strategy.

Enterprises should look at precisely what they need to secure and evaluate their top cybersecurity priorities. This should be matched with interim requirements in line with the budget available.

Choosing an SSE solution that offers complete visibility to enforce one set of security policies across the entire enterprise is paramount. At the same time, it must synch with your business roadmap and budget.

SSE provides early value, enhances security, and reduces complexity. However, some enterprises are unsure what to look for in a unified platform like SSE to get the required end-to-end data protection. This is where Telstra's Quickstart SASE assessment can help.

Telstra's team of consultants can provide an overarching view of your enterprise's suitability for adopting SASE building blocks such as SD-WAN - while helping you take the first steps on the SASE journey with SSE.

This includes assessing an enterprise's existing network and security infrastructure, people, and processes to put together a long-term SASE strategy that is flexible, secure, and cost-effective.

To learn more about how Telstra Purple's SASE QuickStart Assessment can deliver high-performance connectivity and security wherever you are on your SASE journey, **click here**.

Telstra Purple

Telstra Purple brings together Telstra Enterprise's business technology services capabilities, and several recently acquired companies, focused on outcome-based, transformative tech solutions.

Learn more about Telstra Purple and our Security, Network, Cloud and Modern Workspace solutions by visiting **telstrapurple.co.uk**