Telstra SASE Security Fundamentals

SASE strengthens cybersecurity – but you still need a robust strategy

Secure Access Service Edge (SASE) brings excellent benefits, including enhanced network visibility, edge-to-edge security, easy scalability, simplicity, and secure application access. But it is important to remember that the foundations SASE is built on aren't new and still require a robust strategy to be a success.

This year, Gartner has identified SASE as a top trend impacting infrastructure and operations. It is little wonder that SASE adoption is on an upward curve. The analyst firm forecasts that total worldwide end-user spending on SASE will reach $9.2 billion in 2023, a 39% increase from 2022.[1] But it isn't quite as simple as it sounds. SASE requires careful planning and continuous commitment. Many proofs-of-concept (PoCs) fail because enterprises haven't outlined what they aim to achieve beforehand. They focus on technology and don't include their business objectives and expectations.

SASE is a framework converging network and security capabilities

Firstly, SASE is not a single product; it is a framework to unify parts to do precisely what it says on the tin – provide a Secure Access Service Edge. But, like any other security deployment, SASE requires a step-by-step migration plan and a roadmap. As suggested by Gartner, the first step is to run a complete inventory of equipment and contracts. Next, scheduling the phaseout of legacy on-premises perimeter and branch hardware is to be replaced with the cloud-centric delivery of SASE capabilities.

Enterprises can reduce SASE adoption time by looking at existing skill sets, vendors, and timing of hardware refresh cycles in their strategic roadmap for SASE adoption, advises Gartner.

[1] Gartner Trends infrastructure and operations 2023 https://www.gartner.com/en/newsroom/press-releases/2022-12-08-gartner-identifies-the-top-trends-impacting-infrastructure-and-operations-for-2023

Enterprises are advised to avoid point solution projects in the short term that deliver one single value proposition. Instead, they should go down the consolidation route by using the converged Security Service Edge (SSE) market at renewal time for cloud access security broker (CASB) or secure web gateway (SWG) to remove complexity. Long term, Gartner advises consolidating SASE to a single vendor, two explicitly partner networking and security vendors with deep integration, or a managed SASE service to reduce complexity. This is where an assessment such as Telstra Purple's SASE QuickStart Assessment comes in. A consultant team evaluates an enterprise's current network and security infrastructures and delivers a SASE strategy tailored to business requirements and timescales.

Many in-house teams need more resources or time to run SASE effectively. A managed service provider (MSP) provides a single source for deployment and management capabilities, providing skills that are scarce or non-existent internally. They also have experience integrating networking and security operations to provide a seamless migration process.

SSE: a stepping stone to SASE

SASE takes the labour-intensive strain of managing and securing networks from the data center to the cloud. Depending on how far you are through the SASE journey will command the benefits that can be unlocked. In addition, some enterprises are starting with SSE as a stepping stone to SASE. SSE provides the security components of an overarching SASE strategy. These include Zero Trust Network Access (ZTNA), CASB, and SWG.

Enterprises can first deploy SWG before moving to a complete SSE solution. An SWG protects enterprise data and enforces web-use security policies. With the expanding threat landscape on the internet, from malware-infected web pages, SWGs are an essential solution to protect the enterprise from web-based threats.

Take time to draw up a SASE strategy

The bedrock of any successful security strategy should be grounded in confidentiality, availability, and integrity. SASE helps enterprises further achieve these goals. However, it's important to remember the other fundamental principles it helps deliver upon, such as the principle of least privilege, minimising attack surface, and gaining security visibility across the environment. These must be considered when considering a strategy.

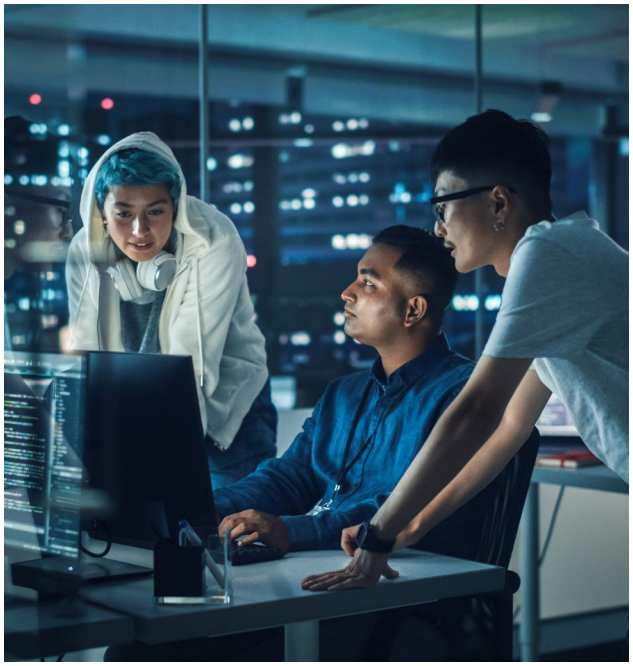
With many different SASE vendors, it is also important to validate which works best for the enterprise in terms of implementation, cost, and ongoing management.

Enterprises must also look at gaps that may slow down a SASE migration. The top three, according to Gartner, are organisational silos, existing investments, and a lack of in-house skills.

Increasing productivity and enhancing security through convergence

A robust security strategy should incorporate all aspects of people, processes, and technology – and SASE is no different. SASE should be one approach to ensure these fundamental goals and principles are applied to mitigating business risk and increasing operational efficiencies. It should also be regularly revisited as the market matures.

SASE is undoubtedly a game changer for businesses regarding performance and security. But, it doesn't come without its challenges. Enterprises must carefully evaluate their current infrastructures and security needs to ensure SASE delivers on its promises.



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**