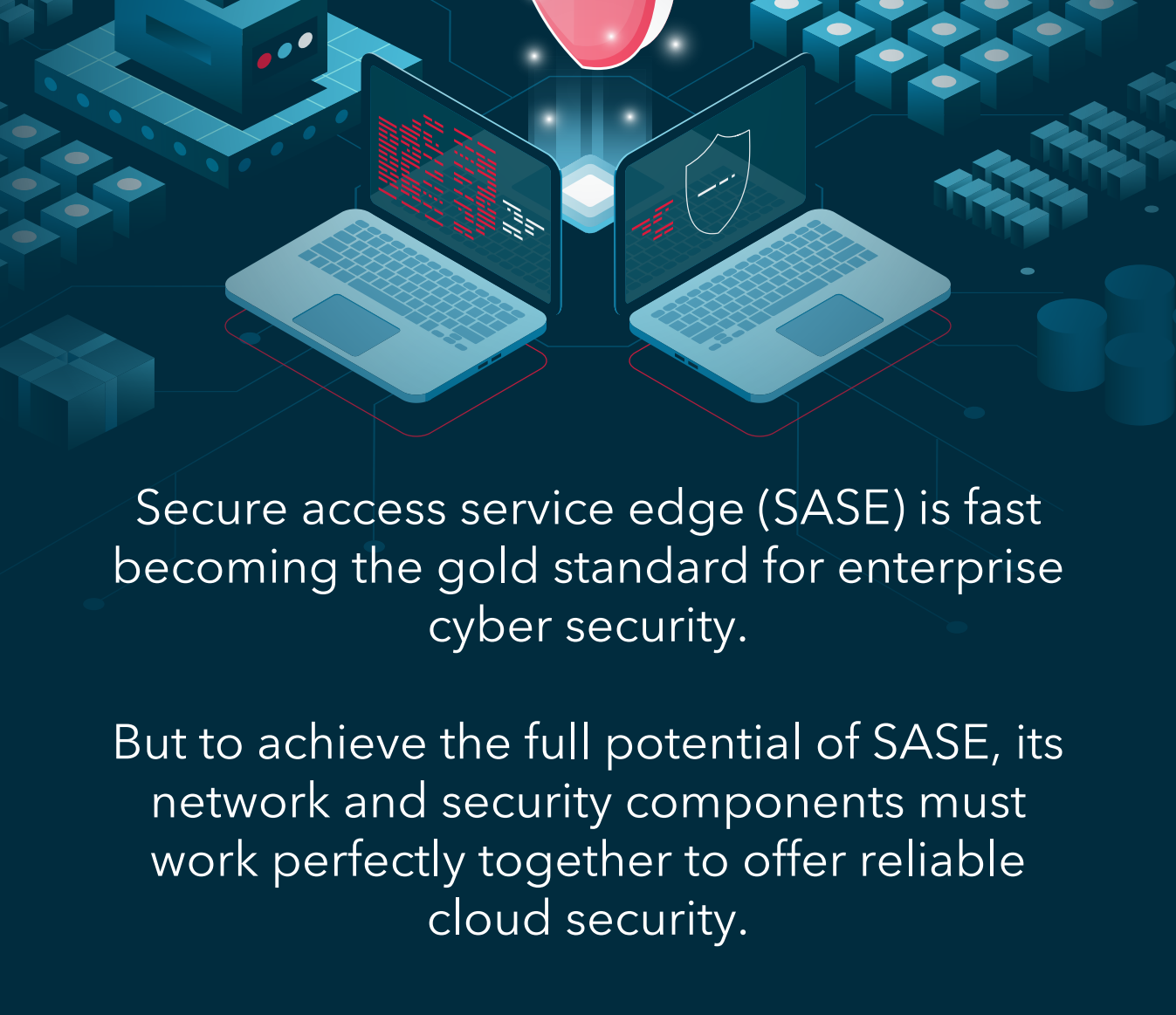


Singtel Managed SASE

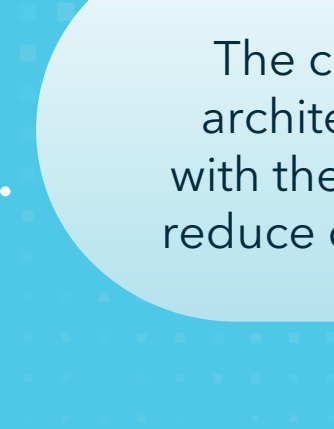


Secure access service edge (SASE) is fast becoming the gold standard for enterprise cyber security.

But to achieve the full potential of SASE, its network and security components must work perfectly together to offer reliable cloud security.

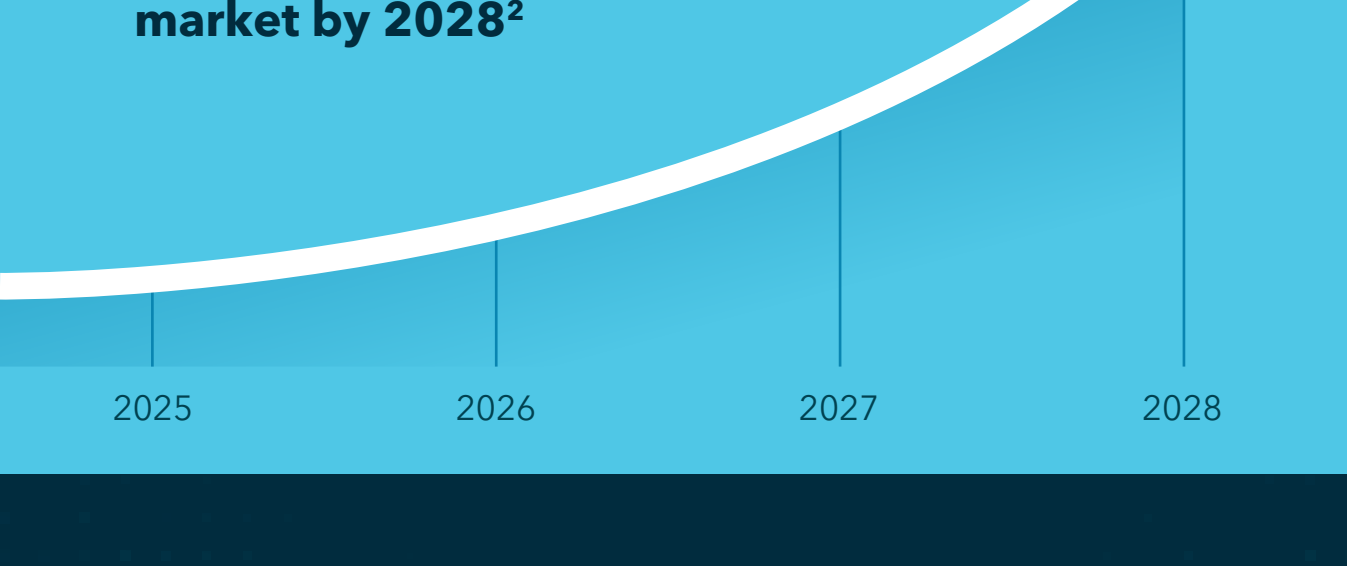
What goes into a SASE solution?

SASE integrates software-defined wide area networking (SD-WAN) and advanced secure service edge (SSE) components for efficient networking and secure remote access



80% of enterprises will have adopted a SASE/SSE architecture to unify web, cloud services and private application access by 2025¹

The critical role of resilient SD-WAN in SASE



Single-vendor SASE solutions will represent over 85% of the market by 2028²



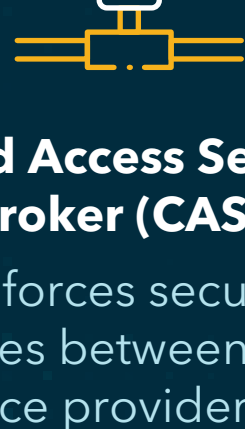
2025

2026

2027

2028

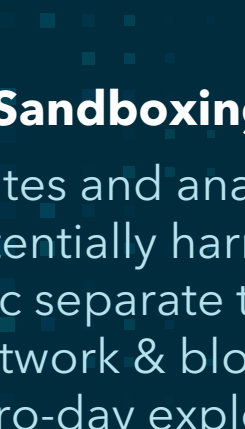
The security components of a robust SASE solution



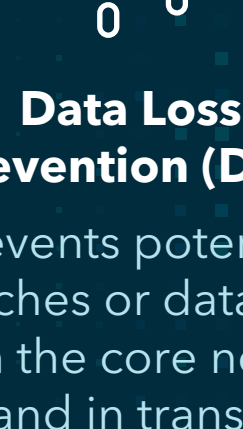
Firewall as a Service (FWaaS)
A virtualised firewall providing access controls, URL filtering, intrusion prevention and DNS security



Secure Web Gateway (SWG)
Filters malware and enforces policy compliance - also enables secure remote connection



Cloud Access Security Broker (CASB)
Enforces security policies between cloud service providers and the enterprise



Zero Trust Network Access (ZTNA)
Only grants permission to relevant, verified users within an organisation



Sandboxing
Isolates and analyses potentially harmful traffic separate to the network & blocks zero-day exploits



Data Loss Prevention (DLP)
Prevents potential breaches or data theft within the core network and in transit



FUNCTION

SD-WAN Network connectivity

FWaaS Network security

SWG Web security

CASB Cloud security

ZTNA Secure access

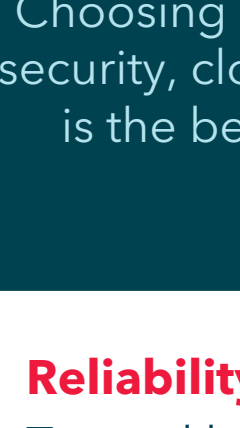
Why choose a managed SASE solution?

A managed solution provides true peace of mind to a global enterprise - with network management and optimisation taken care of and future-proof cyber security built into the network.

Key benefits:



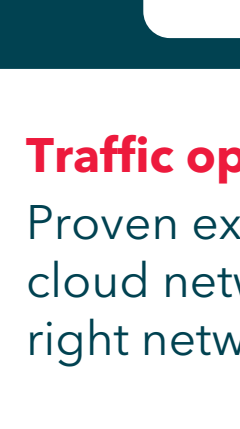
Cutting-edge networking
Access the latest technologies without increasing your in-house resource burden



Consolidated control
Control network services, cloud connections and security protocols through a single platform



Intrinsic cyber security
Future-proof network security to protect your enterprise from new and existing threats



Simplified SLAs
Save costs and compatibility issues by implementing all services under a single agreement

What should I look for in a SASE partner?

Choosing a SASE provider with expertise in cyber security, cloud networking and as-a-service models is the best place to start, along with these key considerations.³

Reliability and trustworthiness

Trusted by both international telco organisations and cyber security authorities



Global consistency

Cohesive local, regional and global policy configurations to provide global flexibility



Traffic optimisation expertise

Proven expertise in optimising cloud networks and offering the right network services



Scalable cost-savings

An integrated SD-WAN and SSE provider protects your bottom line as your network grows

Vendor-agnostic

Partner with Singtel to augment organisation's existing SASE with delivery of SSE and network on demand via a unified digital portal

Supercharge your cyber security strategy

Embarking on your SASE journey with the guidance of a global managed services provider removes the complexity of a multivendor approach. A comprehensive integration between SD-WAN and SSE paves the way for cost-effective, secure and reliable digital transformation.

Contact Singtel today to find out how to streamline your SASE journey

References

¹ Gartner, 2022, 2022 Strategic Roadmap for SASE Convergence

² Dell'Oro Group, Securing Cloud- and Mobile-First Enterprises to Drive SSE to \$10 Billion by 2028, Aug 2024

³ Gartner, 2022, Market Guide for Single-Vendor SASE