Product Brochure

Singtel Unified Secure Access Service Edge (SASE) Convergence

Delivering secure next-gen connectivity to the enterprise

Singtel Unified Secure Access Service Edge (SASE) Convergence powered by Palo Alto Networks Prisma Access, enables enterprises to harness the power of next-generation connectivity with a cutting-edge solution designed for speed, security, and simplicity.

It integrates key security services necessary for implementing a zero-trust model, along with a management overlay that provides a unified view across the different security components. The solution is delivered over the Singtel backbone, ensuring optimal performance and robust regional coverage.

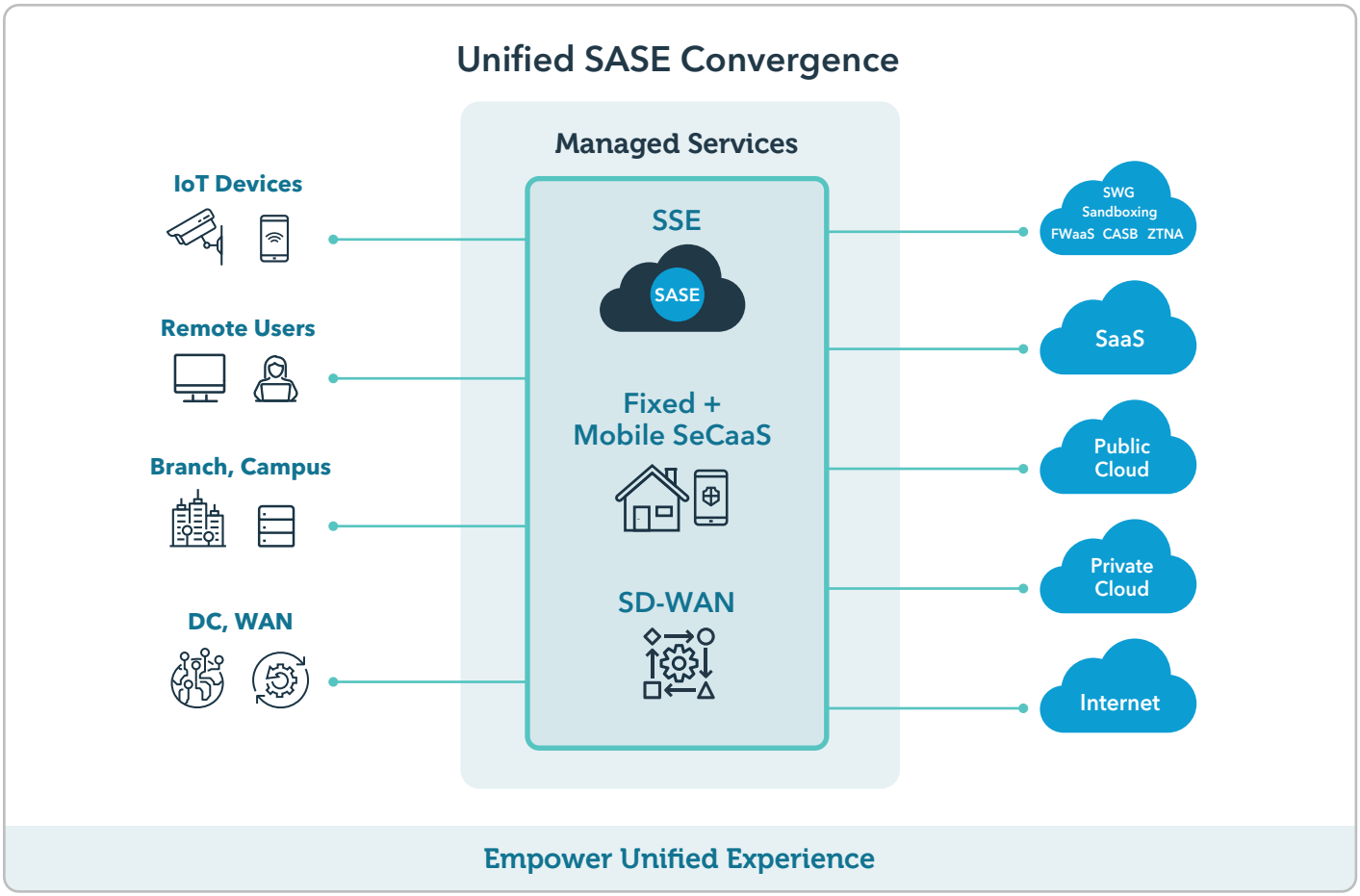
Singtel Unified Secure Access Service Edge (SASE) Convergence

The enterprise challenge

With an increasing number of users, devices and resources now operating outside the traditional network perimeter, securing the modern enterprise requires a zero-trust model to govern access control, browser and cloud security, and data protection. However, adopting a zero-trust approach with point products from multiple vendors not only incurs high setup costs but also complicates scaling and optimising the architecture to deliver high performance across diverse locations.

Singtel Interconnect Secure Service Edge, powered by Palo Alto Networks Prisma Access, addresses this challenge by integrating multiple security capabilities into a single cloud-native Secure Service Edge (SSE) solution, with a managed services overlay to simplify security for enterprises.

Underpinned by direct connectivity to the Singtel network for enhanced performance and comprehensive regional coverage, the solution enables enterprises to purchase SSE services that meet their security needs, which are provisioned and managed through a single portal. This enhances visibility and ensures secure connectivity for a hybrid workforce and cloud-centric workloads, all based on the zero-trust principle.



Features

The Singtel Interconnect Secure Service Edge comprises the Secure Service Edge with its different components, and a Managed Security Services overlay.

Secure Service Edge

Zero Trust Network Access (ZTNA)

- True least-privileged access with precise controls at the app and sub-app levels.
- Continuous security inspection and continuous trust verification to protect all data and secure all apps.

Firewall-as-a-Service (FWaaS)

- Includes next-generation firewall capabilities including threat prevention, URL filtering, sandboxing and more.
- Serves as a single, scalable firewall with unified security policies across globally distributed branches and users.

Cloud Secure Web Gateway

- Maintains visibility into all types of traffic and filters online hazards such as malware from web/Internet traffic.
- Ensures policy compliance according to corporate guidelines.

Data Loss Prevention

- Detects and prevents potential breaches/exfiltration of sensitive data in use, in motion and at rest across the web, cloud, private access and endpoints.
- Ensures customer data integrity and security with unique egress IPs and dedicated data planes.

Cloud Access Security Broker

- Ensures that security controls are integrated and applied to all cloud application policies.
- Locates and tracks data across different enironments and controls access to sensitive information.

IoT Security

- IoT Security to profile all devices for discovery, risk assessment, vulnerability analysis, anomaly detection, and trust-based policy recommendations to prevent known and unknown IoT threats.

Managed Security Services

Unified digital platform (CUBΣ)

- Single, consistent 360-degree view across different best-in-class network and cyber security solutions for effective threat monitoring.

Seamless service orchestration

- Streamlined provisioning of end-to-end services from virtual network functions to security sevices.

Managed threat detection

- Continuous real-time threat monitoring to detect security exploits, carry out event triage and prioritise threat alerts and response.
- Provides detailed reports on threat activities.

24/7 support

- Full 24/7 technical support
- Includes change management, user account management and policy management services, troubleshooting, guidance and fault escalation.

Consulting and professional services

- Provides expertise for integrating Interconnect SSE into the enterprise's existing IT environment.
- Fine-tunes policies to optimise security services for greater accuracy.

Benefits

Simplifies network and security management
- Minimises adminstrative burden for IT teams with a centralised platform to monitor performance and detect threats.
- Provides comprehensive visibility with end-to-end network and cyber management tools powered by advanced analytics.

Enhances the user experience
- Reduces latency with optimised routes and direct connectivity with the Singtel network for quicker access to resources.
- Service level agreements (SLAs) ensure reliable, high-speed connectivity, high availability and low latency.

Strengthens the security posture
- Isolated data paths and dedicated IPs ensure client data integrity and security through isolation.
- Limits exposure to the Internet and enables the use of private connections for secure application connectivity.

Use cases: Leveraging Singtel Interconnect SSE and CUBΣ

1) Achieving unified connectivity

Problem: Enterprises have siloed services and operations for SSE, Internet access and wide area networks, hindering network and security visibility and management.

Solution:
- Provision SSE components on demand and orchestrate services easily over the Singtel network.
- Enable unified network and security visibility and management with CUBΣ through API integration.

2) Securing enterprise IoT

Problem: Enterprises lack visibility and effective control over the SaaS IoT sensors and controllers implemented for intelligent building management, exposing risks from unmanaged or rogue devices.

Solution:
- Integrate IoT security with SSE using branch SD-WAN CPE.
- Leverage Singtel CUBΣ for auto-discovery of IoT assets, network segmentation, security policy enforcement and threat monitoring.

Why Singtel?

Network and Security Convergence
- Unified solution combining SSE and SD-WAN for securing users and IoT devices on both fixed and mobile networks.

Unified experience
- Single dashboard provides unified view of secure Internet access, secure private access, and IoT security.
- Clients can tailor SSE services to fit their environment and dive into detailed insights on each use case.

Comprehensive portfolio of security services
- Accredited managed security service provider with an extensive service portfolio.
- AI-powered Managed Threat Detection and Remediation delivers continuous security monitoring and threat mitigation to identify and block threats.

Access to specialised skills
- Provides access to security specialists and experts from Singtel's Security Operations Centres.

About Singtel

Singtel is a leading Asian communications technology group, operating next-generation connectivity, digital infrastructure and digital businesses including regional data centre arm Nxera and regional IT services arm NCS. The Group has presence in Asia, Australia and Africa and reaches over 780 million mobile customers in 21 countries.

For consumers, Singtel delivers a complete and integrated suite of services, including mobile, broadband and TV. For enterprises, Singtel offers a complementary array of workforce mobility solutions, data hosting, cloud, network infrastructure, analytics and cyber security capabilities.

Singtel is dedicated to continuous innovation, harnessing technology to create new and exciting customer experiences, support enterprises in their digital transformation and shape a more sustainable, digital future.

For more information, visit **www.singtel.com**.

March 2025

Copyright © 2025 Singapore Telecommunications Ltd (CRN:199201624D). All rights reserved.