SECURE ACCESS ANYTIME, ANYWHERE

with StarHub Managed SASE

Provide complete security for your remote users via the cloud

With an increasingly mobile workforce and the widespread adoption of cloud-based applications, the traditional network-based security model is no longer effective. Additionally, the implementation of 5G also presents increased exposure to attacks due to the addition of new network entry points. Organisations now demand immediate, consistent and secure access to its remote users without taking on more complexity and resources.

StarHub Managed Secure Access Service Edge (SASE) consolidates networking and security point solutions into a single, cloud-delivered service model, allowing organisations to apply secure access no matter where their users, applications or devices are located.

STARHUB BUSINESS

Challenges faced with today's network and security model

Broken security perimeters

Employees who are working remotely and accessing work applications via the unprotected Public Internet fall outside of the traditional security perimeter and are therefore not secured.

Inefficient network design

The traditional way of backhauling traffic from branch offices causes congestion and latency concerns which affect the performance within an organisation.

Complicated stacks of security solutions

The old model of stacking multiple security appliances to protect different security concerns is not only costly, complex and operationally intensive to manage, it could potentially create more network entry points for hackers to exploit during the transition to 5G.

Evolving organisational network needs

With the move of corporate data and applications to the cloud and the surge in usage of mobile devices, traditional WAN architectures are no longer effective and cost-efficient in supporting the significant increase in bandwidth.

Ineffective packet-based routing

Legacy SD-WAN's Layer 3 packet-based policies have limited app visibility and ability to configure application-based networking policies, making it difficult to deliver on-app SLAs.

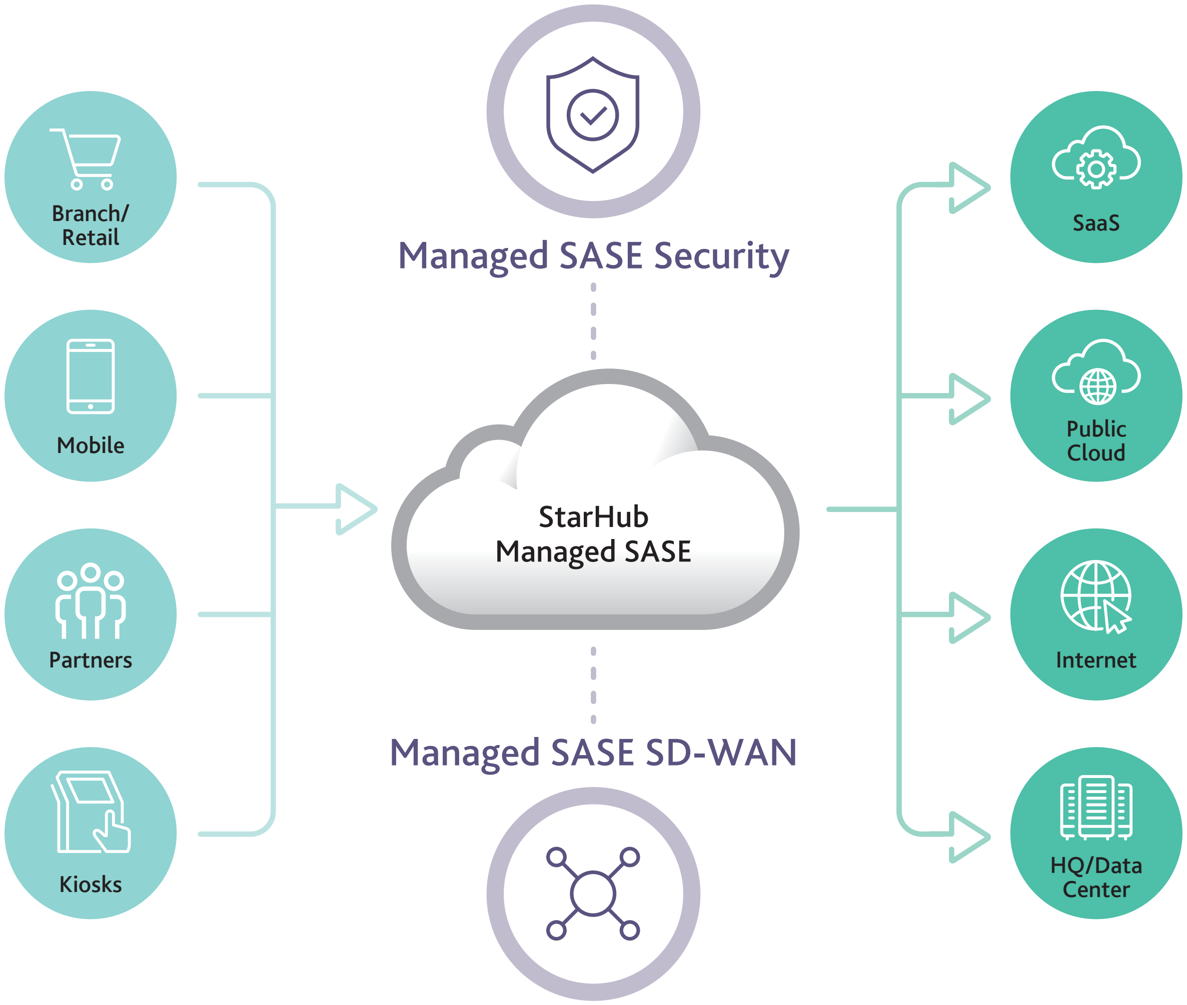
What is StarHub Managed SASE

StarHub Managed SASE is a modern approach to the traditional data center-oriented security, with a new type of cloud-based architecture that brings together networking and security services into one unified solution. This converged network and security solution places network controls on the cloud edge — not the corporate data center. This allows enterprises to expand their network perimeter to provide secure access to any remote user, branch office, device, or application.

By consolidating a variety of network and security functions in one service that can be deployed anywhere from the cloud, StarHub Managed SASE can provide enhanced protection and optimised performance, while reducing the cost and complexity it takes to secure the network.

StarHub Managed SASE consists of two main product components – **Managed SASE Security** and **Managed SASE SD-WAN**.

How StarHub Managed SASE works



Managed SASE Security

What is Managed SASE Security

In a traditional office setup, the perimeter-based security model enables the organisation to protect users and applications within the on-premise network architecture. However, with the modern office adopting a direct-to-cloud architecture over the Internet, organisations can no longer control its network, hence putting its users at risk.

StarHub's Managed SASE Security provides a full suite of cloud-based security-as-a-service built on four key security layers. It coordinates intelligence and provides protection across all attack vectors, effectively eliminating the coverage gaps created by disparate network security tools.

By moving security to a globally distributed cloud, it protects users, applications and data regardless of device, location or network. This also effectively eliminates the cost and complexity of network and appliance infrastructure. The fully managed security service is also easily scalable depending on your security needs.

Key security layers

Firewall as a Service

Firewall-as-a-service (FWaaS) provides full inbound and outbound protection, native user authentication and access control, and Layer 3–7 single-pass inspection to secure branch offices against threats.

Cloud Secure Web Gateway

Secure Web Gateway (SWG) protects remote users across all web traffic protocols and applications. URL and content filtering is enabled for users based on dynamic group monitoring, allowing you to implement granular behavior-based policies. Advanced DNS security prevents command-and-control (C2) callback and DNS tunneling attacks.

Zero Trust Network Access

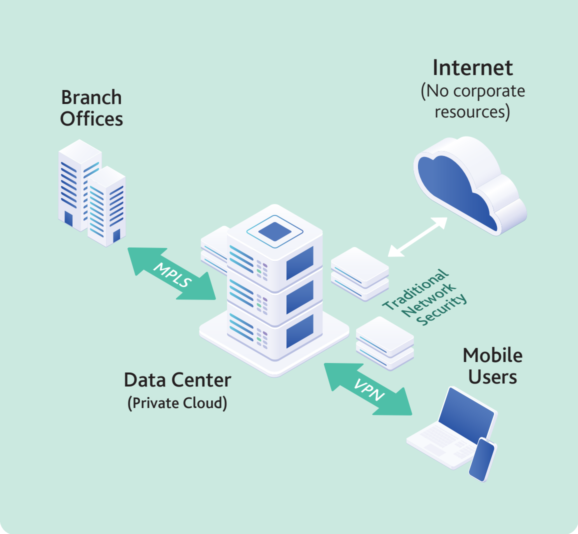
Zero Trust Network Access (ZTNA) incorporates identity-based authentication and granular access control capabilities. Our ZTNA supports both agent-based and agentless connection methods to provide secure remote access regardless of the user's location. Unlike standalone VPN or proxy solutions, it conducts post-connect single-pass traffic monitoring for signs of malware, data loss and compromised credentials.

Cloud Access Security Broker

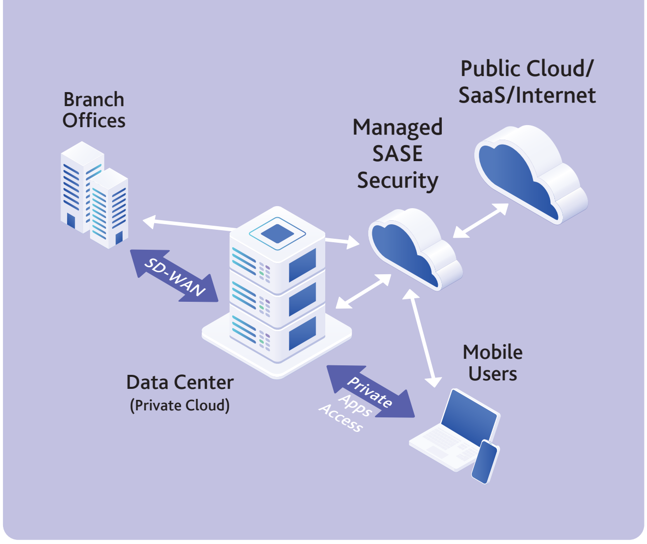
Cloud Access Security Broker (CASB) is a security policy enforcement software that ensures policy compliance between users and cloud service providers. A combination of inline API security and contextual controls are used to determine access to sensitive information. These security controls are integrated and applied throughout all cloud application policies.

How it works

TRADITIONAL SETUP



MODERN SETUP



Key features

Internet Security

Deliver full threat protection from malicious web content with full SSL/TLS traffic inspection.

Threat Prevention

Go beyond Traditional Intrusion System (IPS) solutions to automatically prevent all known threats across all traffic
in a single pass (AV, Anti-Spyware, Vulnerability).

URL Filtering

Enable safe use of the Internet by preventing access to known and new malicious websites before users can access them.

DNS Security

Prevent command-and-control attacks and data theft that use DNS without having to change your infrastructure.

Sandbox Detection

Keep files safe by automatically detecting and preventing unknown malware with industry-leading cloud-based analysis.

Cloud Access Security Broker

Control user access to known and unknown cloud applications.

Additional Security Features with Customisable Options

Enterprise Data Loss Prevention (DLP), Private App Access, Net Interconnect for Site-to-Site and User-to-Site Access, Autonomous Digital Experience Management (ADEM) and IoT Security.

Physical NGFW (Optional)

Complement your cloud-delivered security solutions by securing your east-west traffic with on-premise ML-based NGFW appliances.

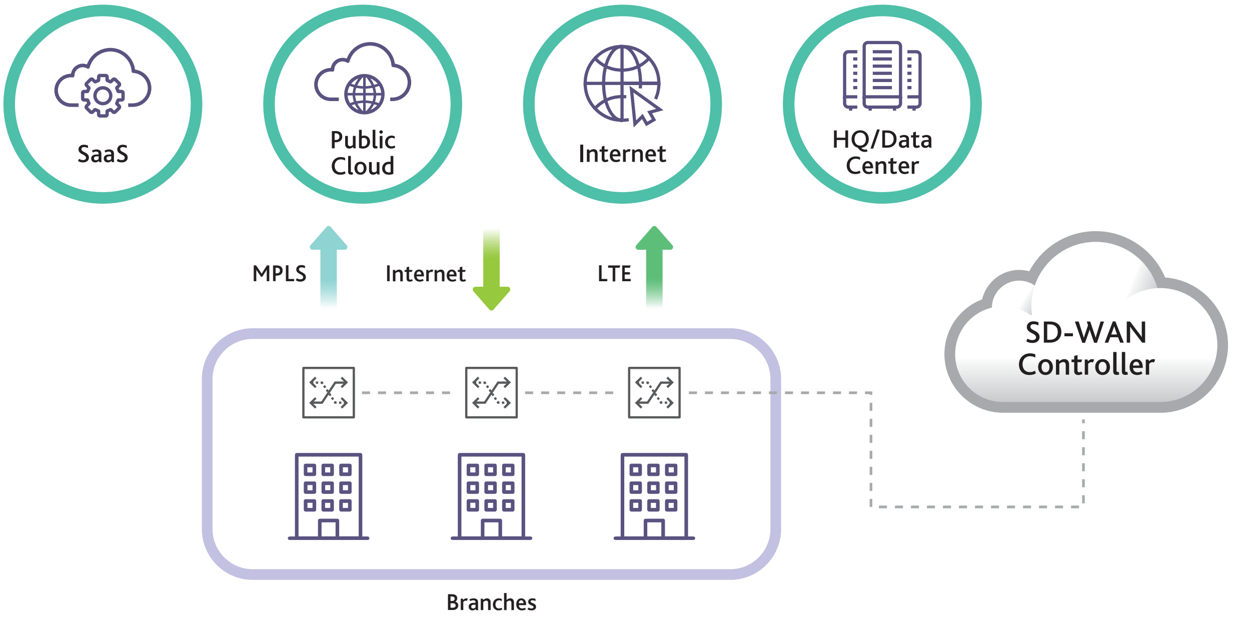
Managed SASE SD-WAN

What is Managed SASE SD-WAN

Organisations have traditionally deployed multiprotocol label switching (MPLS) networks, using conventional routers to connect branch offices to centralised data centers. Unlike this traditional router-centric WAN architecture, the SD-WAN model is designed to fully support applications hosted in on-premise data centers, public or private clouds and SaaS services, while delivering the highest levels of application performance.

StarHub's Managed SASE SD-WAN is a next-generation cloud-delivered SD-WAN solution that delivers a rich set of security and network services at optimal speeds. It provides a fully autonomous application-defined networking to support organisations' migration to cloud. This cloud-delivered SD-WAN offers infinite scalability and performance at a reduced cost.

How it works



Key features

Application-defined

Gain deep application visibility with Layer 7 intelligence for network policy creation and traffic engineering. This significantly improves user experience while enabling network teams to deliver SLAs for all applications.

Autonomous

Automate operations and problem avoidance using machine learning and data science methodologies. This enables agile deployment by leveraging APIs to simplify network operations.

Cloud-delivered

Enable delivery of all branch services to and from the cloud, including networking and security. This simplifies WAN management while increasing ROI.

Why leading enterprises choose StarHub Managed SASE

Reap cost savings

Instead of managing and paying for a variety of point security solutions, utilising a single cloud-based platform can significantly reduce your costs and IT resources.

Reduce complexity

Simplify your security infrastructure with a unified cloud-delivered solution that provides built-in integration, eliminating the need to install, maintain and upgrade any hardware.

Optimise performance and reliability

Leveraging cloud availability, your users can access apps, the internet and corporate resources securely and consistently from anywhere they are, whether on or off the network.

Enhance user experience

Ensure optimal bandwidth and low latency by securing user connections directly at the Internet exchanges.

Gain better control and visibility

Centralised management allows you to easily control and monitor activities within hybrid environments and generate consolidated reports for quicker analysis.

Lessen administrative resources

Ease your administrative workload with a fully managed solution supported by a 24x7 helpdesk and technical team.

Enjoy greater scalability

Pay for only what you need with subscription options that allow you to scale according to your security needs.

High security standards

Enjoy peace of mind with ISO27001-certification and 99.999% availability SLA.

Protect your organisation in a mobile and cloud-first world with StarHub Managed SASE.

STARHUB BUSINESS

☎ 1800 888 8888 starhub.com/managedsase business@starhub.com

All information stated is correct at time of printing and subject to change without notice.

May 2021