2021

SASE

The New Frontier in SD-WAN

UNDERSTANDING SECURE ACCESS SERVICE EDGE

VITG

MANAGING EXPERIENCES NOT JUST DEVICES

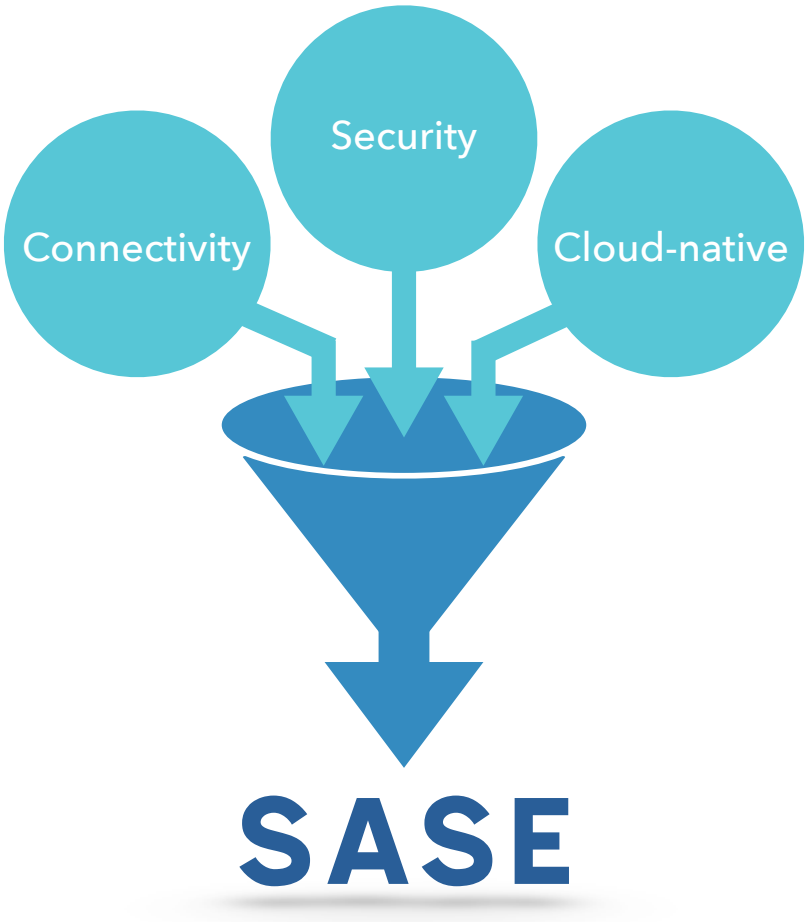
As connectivity technologies have evolved to tackle new demands and challenges around security, remote working, infrastructure management and maintenance, Secure Access Service Edge SASE is the most recent culmination of a single technology which addresses all needs.

Contents

What is SASE and What Does It Really Mean?

Perhaps the way SASE is pronounced is not the most confusing aspect of it. Even when decompressing the acronym, Secure Access Service Edge is not particularly intuitive either.

To understand what SASE really stands for, let's first define it: SASE is a connectivity technology that converges smart networking and security into a single, cloud-native offering. It provides secure and consistent connectivity across global points of presence that extend to the edge of the network, therefore including branches, users, Clouds, and applications.



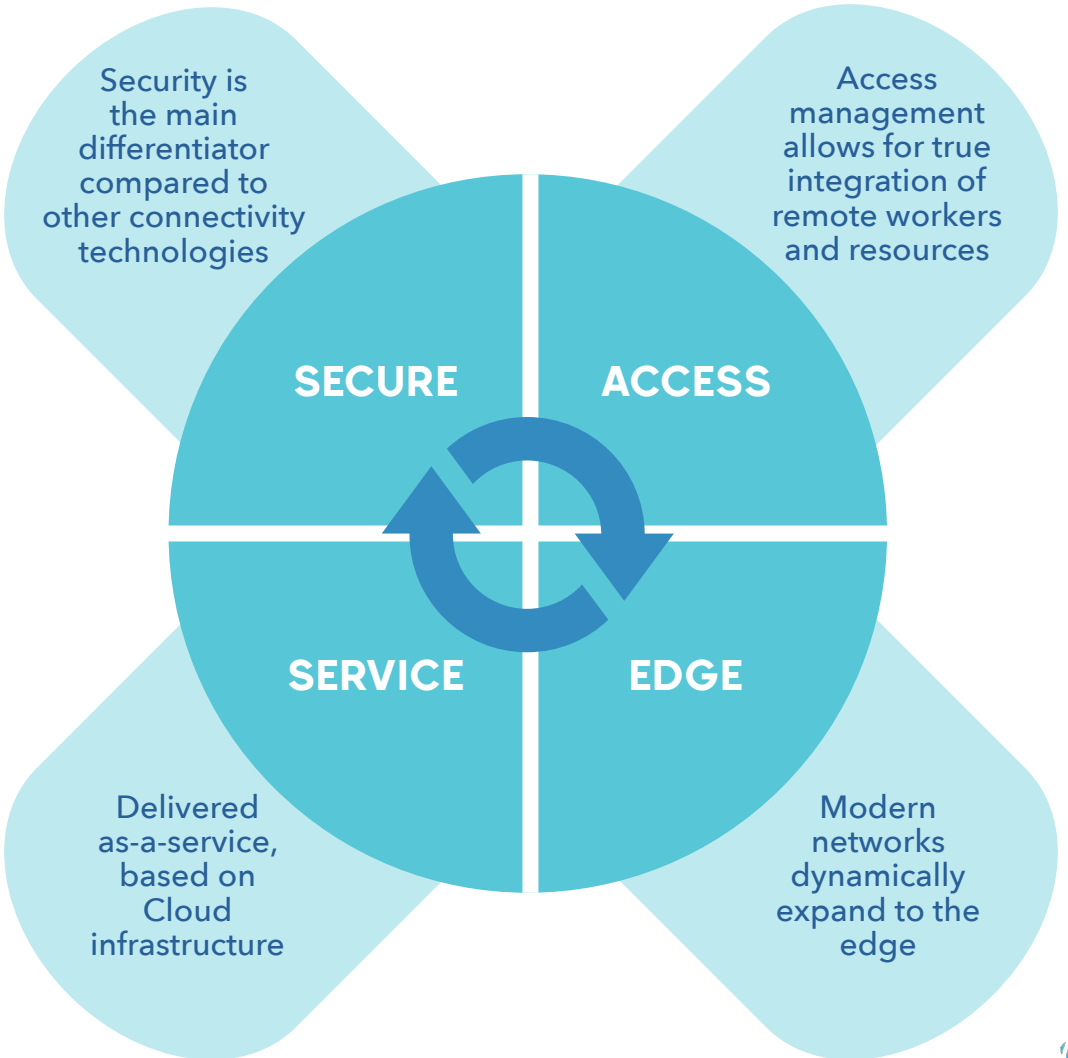
With this in mind, let's also develop an intuition for why SASE is named the way it is:

1 **SECURE**: security is the main differentiator compared to other connectivity technologies

2 **ACCESS**: access management allows for true integration of remote workers and off-premise

3 **SERVICE**: the whole technology is delivered as-a-service, using a Cloud model

4 **EDGE**: the network is no longer a defined box, but rather it dynamically expands to include end-user devices and applications

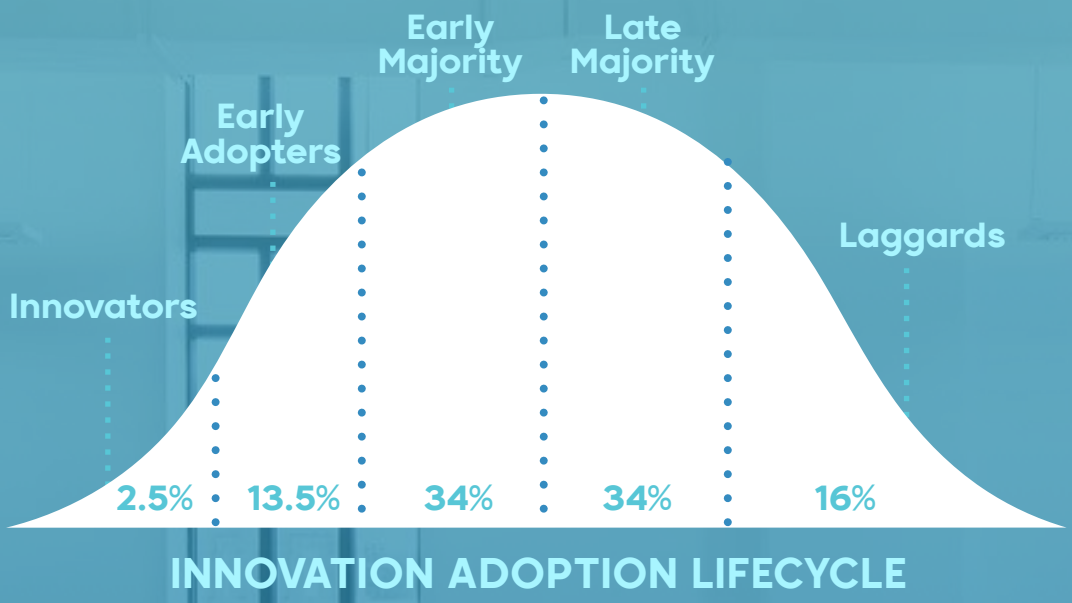


We can already achieve fairly efficient and secure networking by implementing SD-WAN and deploying security appliances such as firewalls and other security modules. Why do we need a single solution which converges the two? There are specific use cases where employing SD-WAN and Security as separate solutions will not address the challenges that enterprises are facing today. Some of those include:

- **High security without compromising on performance:** in an SD-WAN solution, traffic is inspected as it passes through each security module, adding latency. With SASE, traffic only needs to be inspected once.
- **Remote workforces:** Users require the same standard of performance and security regardless of their physical location. Traditional technologies such as VPN achieve a minimum amount of security and offer limited control compared to Zero Trust Network Access.
- **Increased reliance on Cloud:** as enterprises have been outsourcing their infrastructure and applications, SASE embraces this and puts the Cloud at the centre of the network.

With SASE, we also have the massive benefit of simplifying the whole network architecture. This could reduce overheads, operations costs and the in-house skills required to manage the network.

Why SASE Penetrates the Market Quickly



INNOVATION ADOPTION LIFECYCLE

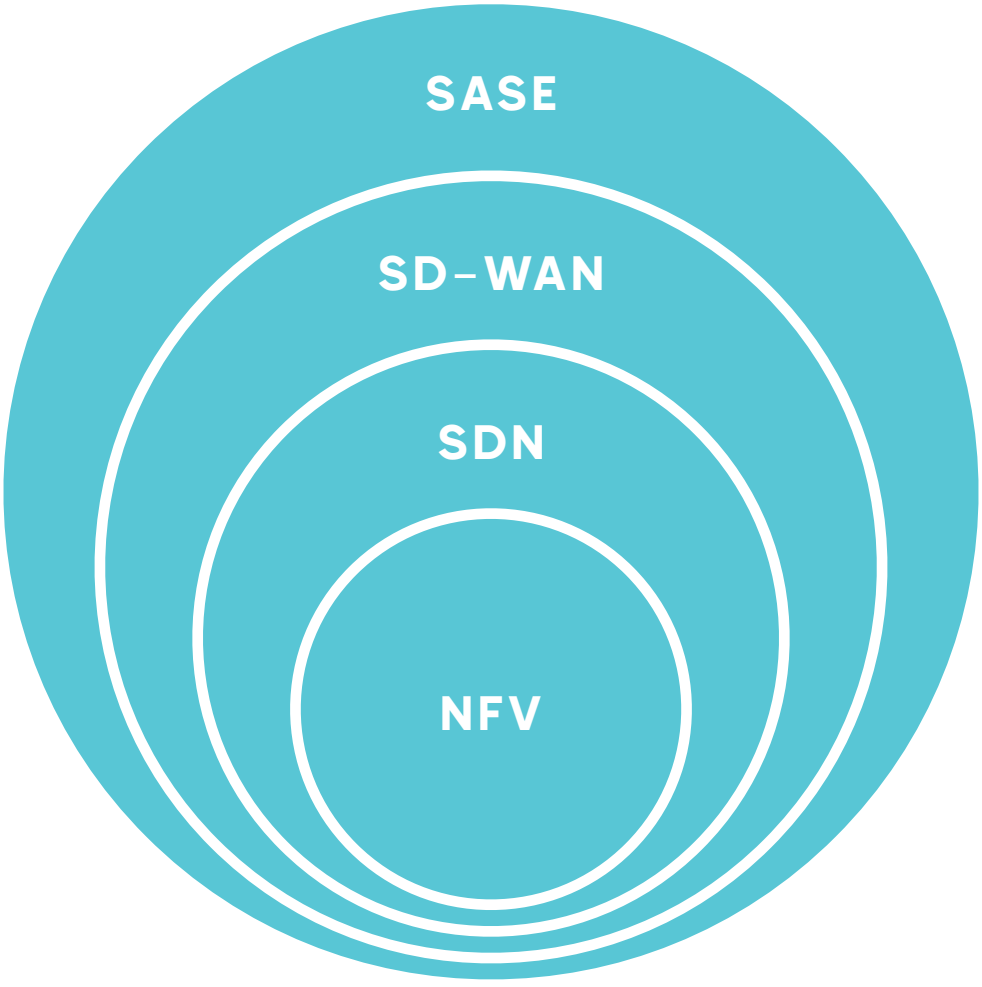
It feels like SASE's precursor, SD-WAN, was only starting to gain traction with the Early Majority. So why would we be looking at adopting yet another technology when most businesses have already created their financial projects for the next year or so?

The short answer has to do with COVID. Even after a year of headlines, we'll quickly recap how COVID impacted the technology sector:

- Cyberattacks up 400% compared to pre-COVID-19 levels
- 64% of cybersecurity teams understaffed in Australia
- Only 40% of Australian CIOs confident protecting against cyberattack
- Network downtime can cost over US$300k per hour

The longer answer is that SASE was due to come around at some point. Granted, it would have been later without the COVID ordeal, but it was coming nonetheless. We can better understand this by looking at a timeline of the latest networking technologies.

1. **Software-Defined Networking (SDN):** the concept was defined in the late 2000s as engineers were looking at improving network performance and monitoring by decoupling the control and the data plane
2. **Network Function Virtualisation (NFV):** created in the early 2010s to complement SDN by abstracting network appliances into virtual instances
3. **Software-Defined Wide Area Network (SD-WAN):** an application of SDN which started gaining traction in the networking world in the second half of the 2010s
4. **Secure Access Service Edge (SASE):** first introduced in 2019, SASE is becoming increasingly important due to the immediate security challenges of 2020 and 2021.



The COVID pandemic has marked 2020 as a 'digital leap year'. McKinsey have found that we have vaulted five years forward in consumer and business digital adoption in a matter of around eight weeks. Such is the case for the adoption of SASE. If widespread SD-WAN deployment has naturally happened over the course of five years or more, SASE is already penetrating the market one or two years after it was first introduced.

SASE Characteristics

There's clearly a market need today for security and connectivity baked together into a single solution, but how does SASE achieve this? SASE leverages a Cloud-based architecture to connect and secure any enterprise resource through a single network. SASE was developed with four market-driven characteristics in mind:

- **Cloud-native Architecture:** leveraging Cloud-based architecture allows enterprises to inherit key cloud capabilities such as flexibility, scalability and self-maintenance.
- **Identity-driven:** Shifting from IP addresses to resource and user identities will allow companies to develop one set of networking and security policies regardless of device or location.
- **Supports All Edges:** SASE can help expand the enterprise networks to include all marginal elements, such as data centres, branches, cloud resources, and mobile users.
- **Globally Distributed:** to achieve truly global secure connectivity, SASE makes use of Cloud providers' geographical presence through their distributed points of presence.

These characteristics are what make SASE solution a suitable offering for companies that are doing business across multiple regions or countries and require a modular network and low latency routing.

Core SASE Components

As we've discussed so far, SASE is a comprehensive solution which converges connectivity and security into a single offering. To further break down how SASE is delivering on both of these aspects, we'll describe below the core components which make up the solution:

- Software-Defined Connectivity: Using SDN technology, SASE delivers easy-to-manage, resilient and low-latency connectivity over any type of network transport. It provides dynamic path selection based on quality assessments, self-healing WAN capabilities, support for demanding high-performance applications, and consistent user experience.
- Secure Web Gateway (SWG): An SWG is a cybersecurity solution used to protect users and devices from online security threats by enforcing internet security, compliance policies and filtering out malicious internet traffic. A SWG sits between users and the web, inspecting and acting upon configurations. It can also enforce acceptable use policies for web access, ensure compliance, and prevent data leakage.

- Cloud Access Security Broker (CASB): A CASB manages access control for all approved and unapproved SaaS apps, including securing application access to eliminate Shadow IT challenges. CASB security solutions provide improved application visibility, data security through access management, user behavioural analysis to detect threats, and simplified proof of compliance.
- Data Loss Protection (DLP): A data loss protection engine offers visibility over data in use, in motion and at rest. It can quarantine risky data or activity, enforce encryption and send network security alerts to lower the overall risk of a data breach. Combining CASB with on-premises DLP further as an integrated system will also further ensure the protection of critical data.
- Zero Trust Network Access (ZTNA): is a framework which enforces the principle of least privilege for authorised users accessing sanctioned applications. It authenticates users to applications using context and role-based identity combined with multi-factor authentication. This allows for a better user experience, tighter security controls and reduced complexity compared with traditional VPN solutions.
- Firewall as a Service (FWaaS): Using next-generation FWaaS solutions will integrate anomaly-based (signature-less) threat detection, network sandboxing, geolocation, anti-malware software and IDS/IPS solutions. FWaaS is often integrated with analytics solutions for comprehensive protection for data centres, cloud instances and branch offices.
- Content Encryption: Leveraging SASE's single-pass architecture enables encrypted traffic to be opened and inspected just once. This reduces the latency of traditional security stacks with service-chained inspection engines.

Each SASE provider can add more functionalities, typically in the security space, which could tackle industry-specific requirements.

Differences Between SASE and SD-WAN

The first point to understand when considering both technologies is that SASE has SD-WAN at the core of its networking technologies. From a connectivity perspective, SASE is a software-defined network applied to wide area networks, with enhanced capabilities around Cloud-based delivery and expansion of networks to the Edge to include remote devices.

From a more business-oriented perspective, the critical differentiator between the two is that SASE is a truly next-generation technology which addresses burning challenges and enables new use cases, whereas SD-WAN has typically been a step improvement in achieving more efficient connectivity, most likely acting as an MPLS replacement.

Does this mean that we can skip deploying SD-WAN altogether? In short, yes. When deploying SASE, you will also get a baked-in SD-WAN service, which could mean that you could save further investments from a few years down the line. Depending on your priorities, complexity of networks and available CAPEX & OPEX, “skipping” SD-WAN and going straight for SASE can make business sense and help position you as a leader in your area.

There’s a high chance - with SASE coming out of left field - that IT decision makers have already put together an SD-WAN RFP. If you decide to opt for SASE rather than SD-WAN at this point, you can convert your SD-WAN RFP into a SASE RFP and expand your number of questions to include Cloud-nativity, security and flexibility at the edge.

SASE Benefits

SASE is a sure-fire way of future proofing your network from a number of perspectives:

1

End-to-end security: As enterprises have historically had to deploy multiple security solutions depending on requirements, budget and expertise, IT departments had to deal with patchy security coverage, lack of true visibility, difficult configurations and management. Rather than trying to secure each network segment and endpoint separately, SASE can deliver security features such as URL filtering, anti-malware, IPS, and fire walling into the underlying network infrastructure, permeating full stack security to all edges, from sites to mobile devices and the Cloud.

2

Reduced and simplified costs: traditional connectivity and security solutions have many moving parts that must be managed and paid for individually. These usually include rack space, power, internet connectivity, MPLS connectivity, hardware costs, in-house maintenance, operational costs, license costs, upgrades and refreshes. This entails both high CAPEX and OPEX spending. SASE consolidates the costs and management into a single point, eliminating not only the cost of the appliances, but also reducing network complexity through abstraction of upgrades, patches, and network maintenance.

3

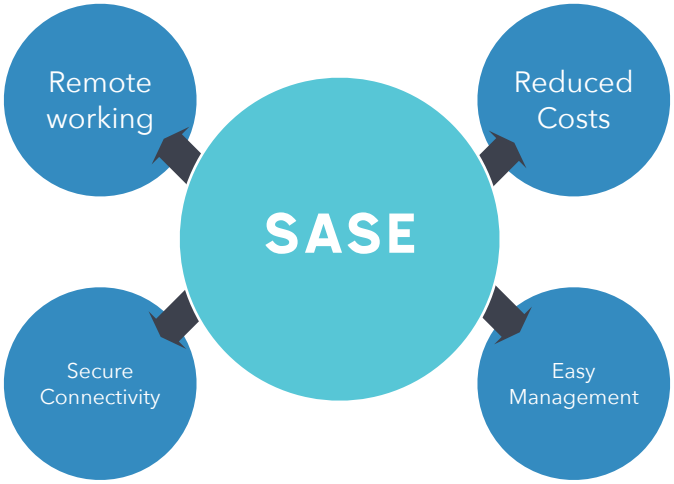
Limitless scalability: Using a Cloud-based architecture, SASE can deliver secure connectivity as a service just as containers and virtual machines have delivered computing power. Using hyperscalers such as AWS, Azure or others, enterprises can have an all-you-can-eat approach to network expansion. New sites may have taken weeks to spin up can now be configured within a couple of hours. This is due to SASE's characteristic of global distribution which leverages existing infrastructure delivered as a service.

4

Simplified management: SASE is easy to deploy and operate when delivered as a managed service by a single provider. This means that there is one contract, one point of contact and one bill at the end of the month for everything connectivity or security-related. Rather than spending time on technology scouting, immediate security patching or dealing with complexities of setting up a new site, enterprises who work with a managed service provider can free up many resources and focus on other value-adding activities.

5

Airtight network and security convergence: even though we stated this as the main proposition of SASE, we can further dissect this to truly understand what this means. So far, both connectivity and security solutions were created by patching together individual elements. This works, but may lead to inefficiencies or gaps in capabilities. A reputable SASE vendor has well-crafted and pre-packaged capabilities ready to be deployed, resulting in fully efficient solutions. Some features can include: 99.999% uptime, worldwide points of presence, Network and Security Operations Centres, 24x7x365 support, end-to-end monitoring, WAN optimisations and full network security stack.



Keep in mind that as with all technologies, SASE is not a silver bullet for guaranteed performance and security, and depends on your existing infrastructure and network strategy.

SASE's Impact on Existing Connectivity and Security Elements

When considering SASE, it's worthwhile asking the following:
What would deploying SASE mean to the already existing connectivity and security elements? Because SASE offers a 2-in-1 connectivity and security solution, deploying it into your network without a comprehensive migration and decommissioning strategy may result in duplicating functionalities and inefficiencies. In a similar fashion to how SD-WAN is deployed, SASE implementations must support gradual migration. This will ensure that in the transition periods, SASE can coexist with both the current network services (including SD-WAN) and security services.

With regard to security services, keep in mind that some SASE vendors can support heterogeneous vendor deployments, but it will be unlikely to swap out any of the vendor's security components for existing third-party offerings. Enterprises have the possibility of running only the connectivity component of SASE on some sites without the vendor's security services.

If your organisation has a requirement to maintain legacy appliances (such as contractual commitments or compliance purposes) you can consider an approach called firewall bursting where your existing firewall appliance function as usual, and any excess traffic is sent to the SASE cloud for processing.

Being mindful of your existing commitments when deploying SASE, make sure that any migration and implementation process takes into consideration the following:

- **Asset lifecycles –** it's worth timing the rollout of SASE to match up with the end-of-life date of various appliances in your network
- **Contractual support –** be aware of existing support contracts, their exit and renewal clauses to ensure that when implementing SASE, you will not pay a vendor for supporting decommissioned infrastructure
- **Customer commitments –** make note of the impact the rollout of SASE will have on your customers. This would be particularly important with highly regulated industries which have specific security requirements. Any change in security infrastructure that would impact customers need to be highlighted
- **Compliance and certifications –** ensure that your existing certifications will not be impacted by deploying new technologies
- **Bids and roadmaps –** any in-flight or won customer bids must also have a smooth transition between your previous solutions and SASE.

Creating a roadmap for gradually migrating to SASE will require combined efforts from the customer and SASE provider alike.

SASE as a Managed Service

Due to the Cloud-native architecture, SASE is delivered as an end-to-end managed service, shifting the design, deployment and operational activities from the customer's IT department to the SASE provider. While the in-house IT department needs to have high-level knowledge of the SASE technologies and how it works, low-level configurations and troubleshooting are fully managed by the SASE providers, who are experts in the area.

As such, one of the most important decisions required when deploying a SASE solution is selecting a managed services provider which understands your challenges and requirements.

SASE in the Australian environment

Australia is in a prime position for deploying Secure Access Service Edge solutions. The market has demonstrated network maturity with an uptick in SD-WAN adoption in 2020, at the height of the pandemic. Partly supported by the migration of last-mile access to the National Broadband Network (NBN), nearly 60% of Australian enterprises with more than 200 employees have already adopted SD-WAN and one in three are considering implementing it in the next 12 months

We've also observed a lower appetite for traditional hardware, with a 23.9% CAGR decline when spending on traditional branch office routers. The budget is being reallocated towards modern technologies, specifically SD-WAN hardware and software, which saw a 23.4% CAGR growth.

As Australian businesses are demonstrating maturity in the IT sector, enterprises have the opportunity of future-proofing both their connectivity and security solutions by adopting SASE over SD-WAN. There is no prerequisite to SASE, so investing in a next-generation solution may help you reallocate future budgets to other value-adding services rather than working through an SD-WAN to SASE migration.

Planning Your SASE Journey

Secure Access Service Edge is a promising technology which can enable the enterprises of the future. Its development comes at a much needed time in the wider technology industry, which explains why it sees such an early adoption compared to previous generation technologies.

The key to successfully rolling out SASE as a core element of your network is collaborating with your vendor of choice to create a solution which tackles your business' specific needs. The expert teams at VITG can leverage decades of combined experience to help you consolidate your position as a leader in your market.

VITG's managed services also provide flexible and tailored solutions that meet the demand of network infrastructure, applications, security and day-to-day 24/7 IT support. Reach out to our team to discuss the best solution to help your business achieve its goals.

Contact the VITG team today info@vitg.com.au or find us on LinkedIn