

Secure Access Service Edge (SASE) - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License \$4750.00
- Team License (1-7 Users) \$5250.00
- Site License \$6500.00
- Corporate License \$8750.00

Report description:

The Secure Access Service Edge Market size is estimated at USD 12.94 billion in 2025, and is expected to reach USD 32.60 billion by 2030, at a CAGR of 20.29% during the forecast period (2025-2030).

SASE signifies a paradigm shift in network access security. It combines network and security features, like Firewall-as-a-service (FWaaS) and SD-WAN, further combining network-as-a-service (NaaS) into a single cloud-native service. With this convergence, distributed workforces and cloud-based applications will be protected and connected in a scalable, flexible, and secure manner.

Key Highlights

- SASE improves security in SDN environments, thereby completing software-defined networking (SDN) systems. Dynamic network configuration is made possible by SDN, and SASE guarantees that these networks are secure as they change in order to meet the changing requirements. SASE protects IoT devices and the data they generate as the Internet of Things (IoT) develops. In the context of the IoT, secure communications and data protection are essential.
- Furthermore, cloud-based SASE may witness a surge in adoption. For instance, in February 2024, Huawei announced the new HiSec SASE Solution launch at the IP Club Carnival. This newly launched solution comes with cloud-network-edge-endpoint integrated intelligent protection, providing consistent security assurance for the enterprise headquarters and branches.
- The increasing usage of the public cloud is boosting cloud spending for businesses of all kinds. Cloud spending is already a significant aspect of IT budgets, wherein about 77% of companies stated that their annual cloud spending value surpasses USD 12 million, and 80% of them stated that the value exceeds USD 1.2 million. As SMBs have fewer and smaller workloads, their overall cloud costs are cheaper.
- The market players are concerned about maintaining proper regulatory compliance while offering clients SASE services and executing expenses. Sometimes, vendors find it difficult to safeguard their technology, keep running smoothly, and comply with

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

all applicable laws and regulations. Vendors' non-compliance with rules and standards can adversely affect their services and jeopardize clients' business operations. By adhering to the accepted standards and best service-delivery practices, they offer programs and services to prioritize them. Vendors need help keeping up with evolving technologies and government regulations.

- The growth in investment strategies in a larger share of businesses globally will accelerate the adoption of secure access service edge in supporting business growth. In the post-COVID-19 era, there will be a significant increase in the number of vendors with single-vendor SASE offerings. New SD-WAN purchases in the post-COVID-19 era will be part of a single-vendor SASE offering.

Secure Access Service Edge (SASE) Market Trends

Large Enterprises will Hold Major Market Shares

- Increased adoption of edge computing, the shift to cloud infrastructure, and a surge in remote work have challenged many traditional network architectures and security models. Large enterprises with access to larger IT budgets and skilled employees are rapidly adapting to this market reality.
- Large enterprises with a distributed workforce model find the traditional WAN architectures with rigidly limited VPN aggregation capacity inadequate for most work-from-anywhere (WFA) workflows. Existing security models and fixed digital transformation investments have slowed down the adoption of SASE among large enterprises over the last few years.
- The global market is witnessing an expansion in new IT infrastructure. Large enterprises that combine security and networks into a single cloud platform are proliferating. As a result, Malware-as-a-service has moved to large-scale operations against exposed IoT and OT in hospitals, oil and gas fields, electrical grids, transportation services, and corporate networks. Threat actors require significant research efforts to uncover and exploit the configuration of operating environments and embedded IoT and OT devices.
- According to the Microsoft Digital Defense Report 2023, Microsoft said that globally, there has been a growing number of attacks, of which identity attacks are the most common, and 42% of the total attacks are only identity attacks. Also, every year, there has been an increasing number of cyberattacks, and the cost of ransomware-related damage increases globally. As per the report published by Microsoft in 2024, attempted password attacks have soared to over 30 billion from around 3 billion per month.
- In a connected digital world, devices communicate online with larger systems, collecting voluminous data and creating visibility to bring business opportunities to large enterprises. This situation also opens the doors for cyber threats, making the cybercrime business worth multi-billion dollars. IoT devices such as computers, routers, printers, web cameras, and remote management devices are at a security risk. These devices are critical to many organizations' operations; hence, they can quickly become a liability and security risk. The rapid adoption of IoT solutions close to every industry has increased the number of attack vectors and organizations' risk exposure. Attacks against remote management devices, attacks via the web, and attacks on databases are most prevalent among large enterprises.
- The aforementioned incidents are likely to boost the adoption of the network-as-a-service (NaaS) in large enterprises due to its ability to stand out from other secure networking strategies. Rather than relying on data center security, SASE has a direct approach as the overall traffic from the users' devices is inspected at a nearby point of presence before being sent to its final destination. This makes it an ideal option for protecting distributed workforces and data in the cloud. In modern cloud-centric large enterprises, users, devices, and applications require secure access while working from anywhere. Legacy systems cannot tolerate the bandwidth needed to provide this flexibility. However, SASE can do so while maintaining enterprise-level security for users and devices at any location, which bolsters this segment's demand.

North America will Hold a Significant Share

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

- The United States is a developed economy with a significant inclination toward implementing and accepting advanced technology, development in network automation, and surge in cloud-based services, thereby contributing to the secure access service edge market. The growing digitization among end-user industries and the presence of prominent market vendors, like Cisco Systems Inc., VMware Inc., Palo Alto Networks, Versa Networks Inc., and Akamai Technologies, are contributing to the market's growth.
- Security is moving toward cloud computation due to the fast acceleration of the digital transformation of businesses. The significant adoption of cloud services in several end-user industries necessitates securing the network infrastructure and reducing complexity to improve speed and agility. This is anticipated to create substantial growth opportunities for market vendors in the coming years.
- The United States is home to three major cloud service providers: Amazon Web Services, Microsoft's Azure, and Google Cloud. It is also considered to be the hub for major technological innovations such as 5G, autonomous driving, IoT, Blockchain, artificial intelligence, and gaming. Integrating SASE capabilities converges zero trust security capabilities into enterprise architectures, which is paramount in achieving a trusted network security posture. Thus, SASE solutions are analyzed to transform the end-users networks and security architectures to reduce cyber risks, costs, and complexities.
- Orange Business, Palo Alto Networks, and Orange Cyberdefense partnered in August 2023 to deliver a cloud-native managed security access service edge (SASE) solution to enterprises globally. The digital attack surface has expanded as organizations expedite cloud adoption to accommodate hybrid work and deliver the latest products and services to their customers. The partnership provides the industry's most complete AI-powered SASE solutions, advisory and consultant services, and global managed network, security, and digital services. Organizations using this offering can maximize their SASE transformation's return on investments (ROI).
- Canada is at the forefront of cloud adoption. Many organizations are deploying a mix of public, private, and edge clouds. With the rise of hybrid work and cloud transformation, the demand for security services to expand beyond the network perimeter is increasing, positively impacting the growth of the country's market. In addition, stringent data protection and regulatory legislation in the country further drive the demand for SASE solutions in end-user industries.
- The market demand is anticipated to rise significantly due to increasing automation and deploying connected devices. The network-as-a-service (NaaS) model benefits small businesses by offloading day-to-day equipment maintenance and focusing on tasks such as customer service. With a large base of small businesses in Canada, NaaS is expected to become a significant trend in the coming years.

Secure Access Service Edge (SASE) Market Overview

The secure access service edge market vendors are moderately consolidated with an array of services. However, major vendors like VMware, Palo Alto Networks, Versa Networks Inc., and Cisco Systems Inc. are highly preferred network service providers for various end users in various regions.

- January 2024 - Kyndryl announced that the company partnered with Cisco to launch two of its new security edge services in order to help customers improvise their security controls and address and respond to cyber incidents proactively. The newly launched security edge services along with Kyndryl and Cisco's available SD-WAN services, enable organizations to build a solid foundation to transition into a secure access service edge (SASE) architecture.
- January 2024-Versa Networks, a leading provider of AI/ML-powered Unified Secure Access Service Edge (SASE) solutions, has announced the launch of a new series of Unified SASE gateways. These gateways offer an impressive throughput exceeding 100 Gbps, designed to address the rising demand for enhanced computing capabilities. This demand is driven by the industry's increasing integration of networking and security functions. Versa's new gateways integrate high-performance hardware with the Versa Operating System (VOS), the company's unified SASE software stack, which features a single-pass architecture. This

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

improved performance allows organizations to consolidate security functions and multiple networking into a single gateway for the first time.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

1 INTRODUCTION

- 1.1 Study Assumptions and Market Definition
- 1.2 Scope of the Study

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET INSIGHTS

- 4.1 Market Overview
- 4.2 Industry Attractiveness - Porter's Five Forces Analysis
 - 4.2.1 Bargaining Power of Suppliers
 - 4.2.2 Bargaining Power of Consumers
 - 4.2.3 Threat of New Entrants
 - 4.2.4 Intensity of Competitive Rivalry
 - 4.2.5 Threat of Substitute Products and Services
- 4.3 Assessment of Macro Economic Factors Impact on the Market

5 MARKET DYNAMICS

- 5.1 Market Drivers
 - 5.1.1 Growing Need for a Single Network Architecture that Combines SD-WAN, FWaaS, SWG, CASB, and ZTNA Capabilities
 - 5.1.2 Lack of Security Procedures and Tools
 - 5.1.3 Mandatory Compliance with Data Protection and Regulatory Legislation
- 5.2 Market Restraints
 - 5.2.1 Lack of Knowledge of Cloud Resources, Cloud Security Architecture, and SD-WAN Strategy
 - 5.2.2 High Upfront Implementation Costs and Lack of Standardization Around SASE Architecture and Its Components

6 MARKET SEGMENTATION

- 6.1 By Offering Type
 - 6.1.1 Network as a Service
 - 6.1.2 Security as a Service
- 6.2 By Organization Size
 - 6.2.1 Large Enterprises
 - 6.2.2 Small and Medium Enterprises
- 6.3 By End-user Vertical
 - 6.3.1 BFSI
 - 6.3.2 IT and Telecom

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

- 6.3.3 Retail
- 6.3.4 Healthcare
- 6.3.5 Government
- 6.3.6 Manufacturing
- 6.3.7 Other End-user Verticals
- 6.4 By Geography***
 - 6.4.1 North America
 - 6.4.1.1 United States
 - 6.4.1.2 Canada
 - 6.4.2 Europe
 - 6.4.2.1 Germany
 - 6.4.2.2 United Kingdom
 - 6.4.2.3 France
 - 6.4.2.4 Spain
 - 6.4.2.5 Italy
 - 6.4.2.6 Belgium
 - 6.4.2.7 Netherlands
 - 6.4.2.8 Luxembourg
 - 6.4.2.9 Denmark
 - 6.4.2.10 Finland
 - 6.4.2.11 Norway
 - 6.4.2.12 Sweden
 - 6.4.2.13 Iceland
 - 6.4.3 Asia
 - 6.4.3.1 India
 - 6.4.3.2 China
 - 6.4.3.3 Japan
 - 6.4.3.4 Taiwan
 - 6.4.3.5 South Korea
 - 6.4.3.6 Malaysia
 - 6.4.3.7 Hong Kong
 - 6.4.3.8 Australia and New Zealand
 - 6.4.4 Latin America
 - 6.4.5 Middle East and Africa

7 COMPETITIVE LANDSCAPE

- 7.1 Company Profiles*
 - 7.1.1 Cisco Systems Inc.
 - 7.1.2 VMWare Inc.
 - 7.1.3 Palo Alto Networks.
 - 7.1.4 Versa Networks Inc.
 - 7.1.5 Akamai Technologies Inc.
 - 7.1.6 Cato Networks
 - 7.1.7 Fortinet Inc.
 - 7.1.8 Check Point Software Technologies Ltd
 - 7.1.9 Cloudflare Inc.
 - 7.1.10 Forcepoint

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

8 INVESTMENT ANALYSIS

9 FUTURE OUTLOOK OF THE MARKET

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

Secure Access Service Edge (SASE) - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:

- Print this form
- Complete the relevant blank fields and sign
- Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	\$4750.00
	Team License (1-7 Users)	\$5250.00
	Site License	\$6500.00
	Corporate License	\$8750.00
		VAT
		Total

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*	<input type="text"/>	Phone*	<input type="text"/>
First Name*	<input type="text"/>	Last Name*	<input type="text"/>
Job title*	<input type="text"/>		
Company Name*	<input type="text"/>	EU Vat / Tax ID / NIP number*	<input type="text"/>
Address*	<input type="text"/>	City*	<input type="text"/>
Zip Code*	<input type="text"/>	Country*	<input type="text"/>
		Date	<input type="text" value="2026-02-28"/>
		Signature	

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

