FROST & SULLIVAN

Secure Access Service Edge Growth Opportunities

Accelerated Cloud Migration and Distributed Workforce Requirements Drive SASE Growth Potential

Global Security Research Team at Frost & Sullivan

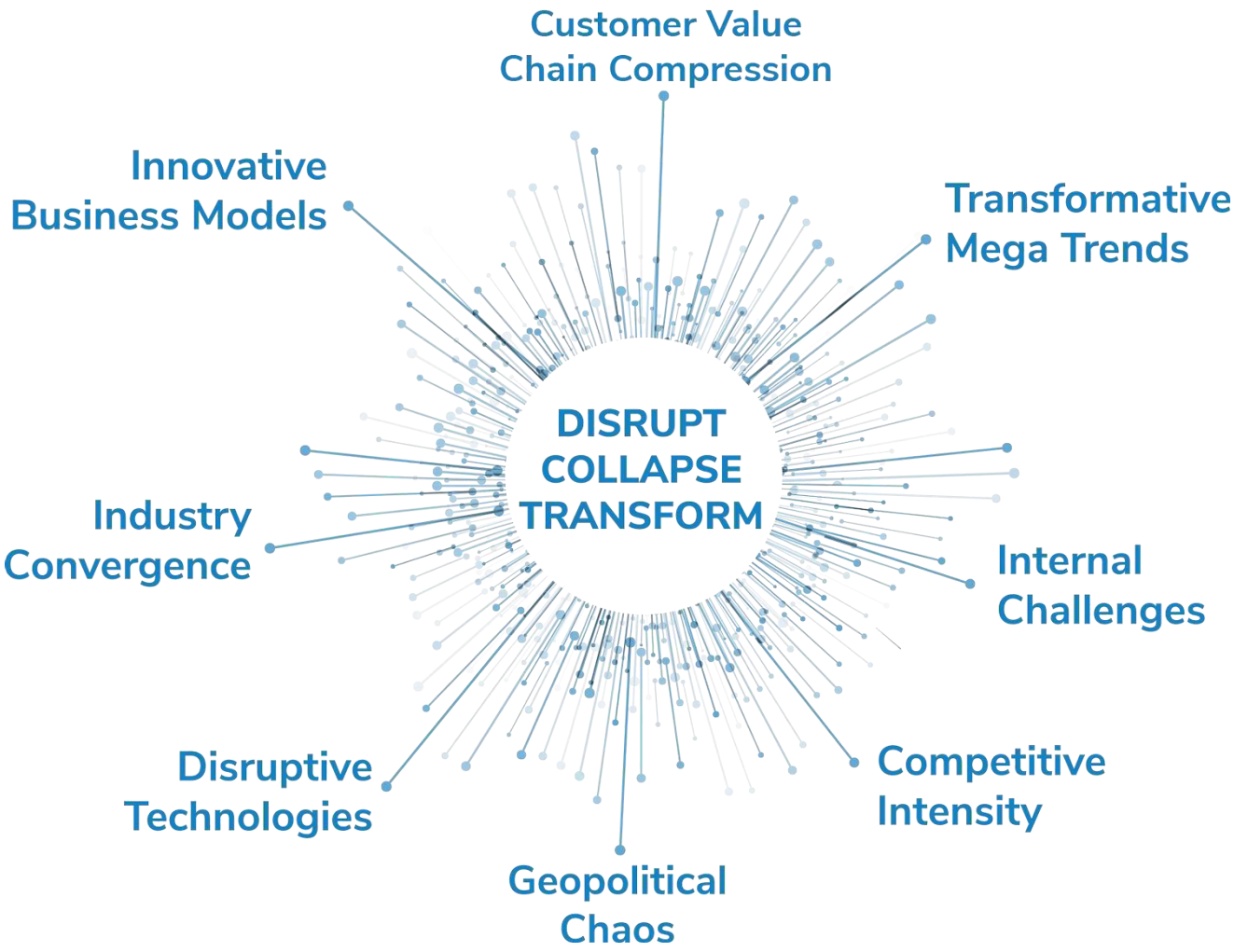
The Growth Pipeline™ Company
Powering clients towards a future shaped by growth

PF02-74
December 2023

Strategic Imperatives

Why is it Increasingly Difficult to Grow?

The Strategic Imperative 8™: Factors Creating Pressure on Growth



Source: Frost & Sullivan

The Strategic Imperative 8™

Innovative Business Models	Customer Value Chain Compression	Transformative Mega Trends	Internal Challenges
A new revenue model that defines how a company creates and capitalizes economic value, typically impacting its value proposition, product offering, operational strategies, and brand positioning.	Customer value chain compression as a result of advanced technologies, internet platforms, and other direct-to-consumer models that enables reduction in friction and the number of steps in customer journeys.	Global forces that define the future world with their far-reaching impact on business, societies, economies, cultures, and personal lives.	The internal organizational behaviors that prevent a company from making required changes.

Competitive Intensity	Geopolitical Chaos	Disruptive Technologies	Industry Convergence
A new wave of competition from start-ups and digital business models that challenge the standing conventions of the past, compelling established industries to re-think their competitive stance.	Chaos and disorder arising from political discord, natural calamities, pandemics, and social unrest that impact global trade, collaboration, and business security.	New, disruptive technologies that are displacing the old, and significantly altering the way consumers, industries, or businesses operate.	Collaboration between previously disparate industries to deliver on whitespace cross-industry growth opportunities.

Source: Frost & Sullivan

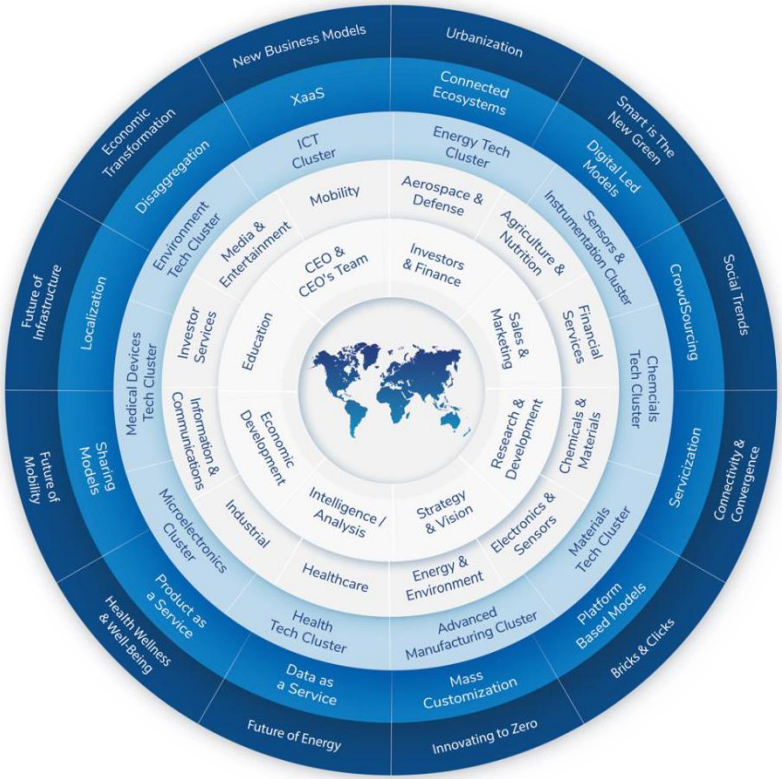
The Impact of the Top 3 Strategic Imperatives on the Secure Access Service Edge (SASE) Industry

SI8	Transformative Mega Trends	Internal Challenges	Competitive Intensity
Why	• In the face of a fast-paced business landscape, organizations have accelerated digital transformation to transform traditional business processes. • The adoption of hybrid and multi-cloud infrastructures across regions continues to accelerate digital initiatives. • A strong need exists to make networking and security architectures more agile and scalable to drive business outcomes.	• The lack of collaboration between networking and security teams remains the biggest challenge for organizations to roll out a SASE model. • These teams must work together to converge networking and security functions in SASE to reduce operational inefficiency and complexity.	• Network and security vendors aggressively expand their SASE portfolio to incorporate organically developed functions or acquire technology companies to strengthen SASE offerings. • With the rising demand for vendor consolidation and the shift to single-vendor SASE, SASE vendors continue to enhance the comprehensiveness of their SASE platforms.
Frost Perspective	• Siloed networking and security architectures are no longer adequate to support a highly distributed environment. • Investment in SASE has increased significantly among global organizations during the last 2 years owing to the need to modernize networking and security architecture. • The adoption of SASE will continue to increase in the next 5 years as organizations aim to achieve a converged SASE platform that is more cost-effective, flexible, and efficient.	• Chief information security officers (CISOs) in organizations increasingly take the initiative to drive SASE projects. The top-down approach makes it easier for networking and security teams to collaborate for SASE implementation. • The convergence of networking and security functions onto a single, unified SASE platform allows both teams to simplify their investment and management efforts. • SASE adoption will grow for the next 5 years as more customers demand a cloud-native SASE approach that converges networking and security functions.	• SASE vendors must provide comprehensive networking and security capabilities to securely connect applications, data, users, and Internet of Things (IoT) endpoints across different deployment locations, such as in physical data centers, hybrid environments, or multi-cloud environments. • The SASE adoption trend will continue to increase in the next 5 years, with more network or security vendors entering the market with a converged SASE offering.

Source: Frost & Sullivan

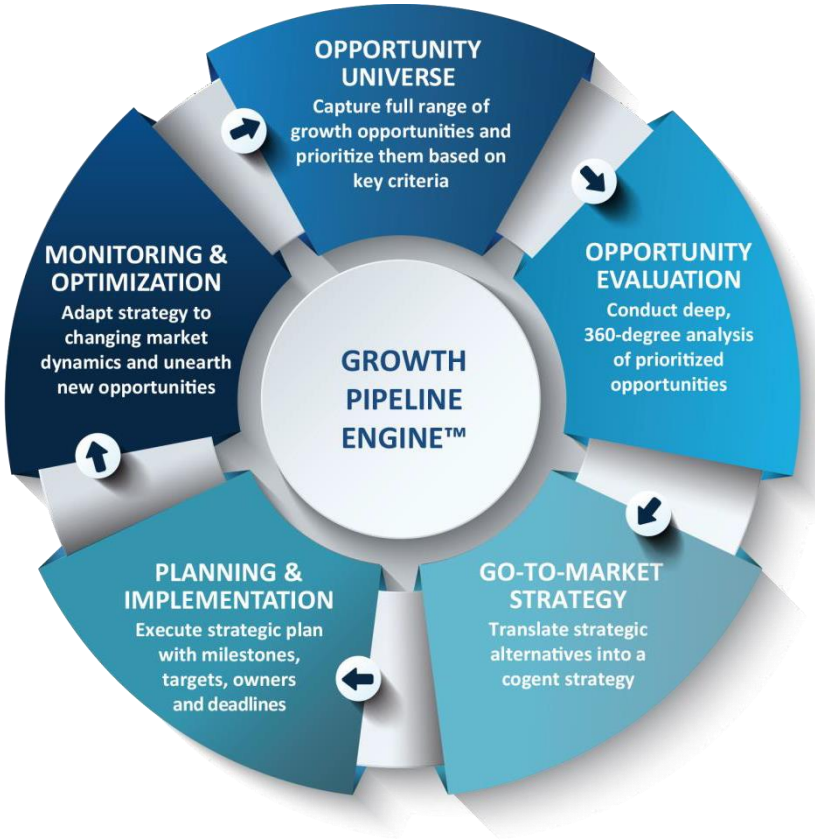
Growth Opportunities Fuel the Growth Pipeline Engine™

The Innovation Generator™



Analytical Perspectives

The Growth Pipeline Engine™



Source: Frost & Sullivan

Growth Opportunity Analysis

Market Definitions

SASE, a cloud-based solution, provides network and security services to protect users, applications, and data, regardless of location. Either globally distributed, interconnected, highly available, and scalable points of presence (PoPs) networks, which SASE vendors and their cloud service provider (CSP) partners manage, or thick edges in an organization's physical or cloud data centers deliver these network and security functions. SASE's purpose is to bring users closer to the origins of content quickly and securely.

A cloud management console manages SASE. This console provides zero-touch provisioning and consolidated and unified policy enforcement capabilities, enabling companies to secure and protect their access to services efficiently, no matter where they are, without sacrificing performance or user experience.

The inspection of traffic between the edges and from the edges to the internet (regardless of form factors such as physical and cloud data centers, branches, remote sites, users, and IoT) happens for threat prevention and access control using the least privilege principle and zero-trust model.

SASE is Achievable in 2 Ways, As Service Chaining or Converged Platforms/Service.

Service Chaining: Organizations build their SASE architecture by chaining several networking and security services from 1 or more vendors. These vendors provide application programming interfaces (APIs) that integrate the chained services.

Converged Platform/Service: A single platform (software stack/image) tightly converges and integrates both networking and security functions, and a single management console manages them. A single-pass processing architecture conducts the security and network inspection, enabling the optimal efficiency and performance of the converged services.

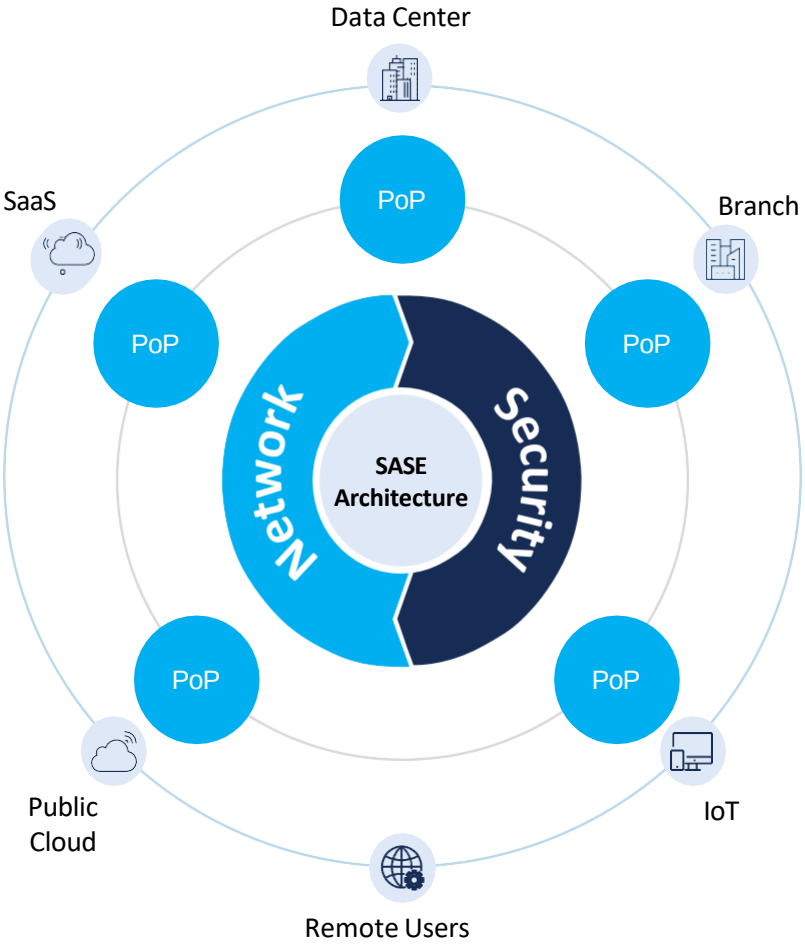
Source: Global SASE Growth Opportunities; Frost & Sullivan

Key SASE Services

A typical SASE architecture comprises different networking and security services, and SD-WAN is the core service for a networking function. Next-generation firewall (NGFW), cloud access security broker (CASB), secure web gateway (SWG), and zero-trust network access (ZTNA)/secure private access are crucial services for security functions. Depending on business needs, an organization may need more than these core services.

Networking 1

- SD-WAN
- Wide area network (WAN) optimization
- Software-as-as-Service (SaaS)/cloud optimization
- Multi-cloud connectivity
- Bandwidth aggregation
- Dynamic path selection
- Quality of service (QoS)
- Content delivery network



Security 2

- NGFW
- CASB
- SWG
- ZTNA
- DLP
- ATP
- IDS/IPS
- DNS protection
- RBI
- WAAP
- UEBA

Key: DLP: Data loss prevention; ATP: Advanced threat prevention; IDS/IPS: Intrusion detection systems/intrusion prevention systems; DNS: Domain name system; RBI: Remote browser isolation; WAAP: Web application and API protection; UEBA: User and entity behavior analytics; SD-WAN: Software-defined wide area network.

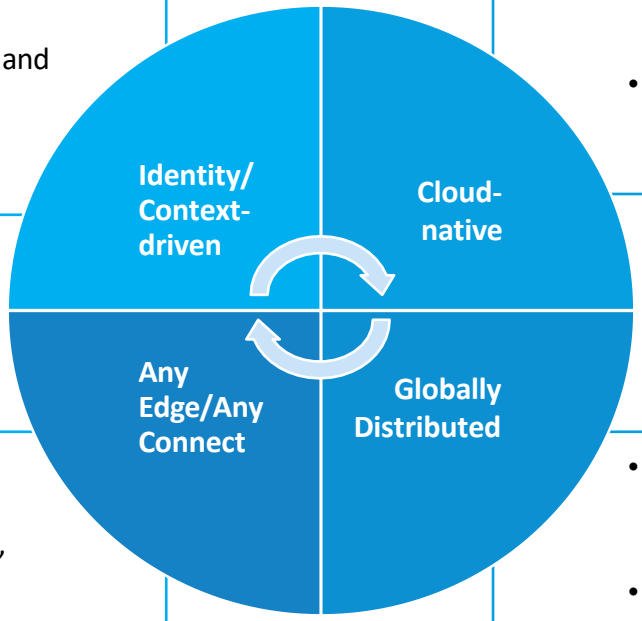
Source: Frost & Sullivan

Key SASE Attributes

Identity/context-driven, cloud-native, globally distributed, and supportive of all edge and connectivity types are the main attributes of a SASE architecture.

- The setting of policies is based on user and resource identity and context, not only on IP address.
- Policies are consistent across all edges and based on the zero-trust principle.

- SASE is a cloud-native architecture with all networking and security functions integrated into a cloud-delivered security platform.
- SASE is highly secure, available, and scalable.



- SASE supports all types of edges, including physical and cloud data centers, branch locations, remote sites, users, and IoT.
- In addition, SASE supports all kinds of connectivity, including MPLS, public internet, LTE broadband, 4G/5G, and DSL.

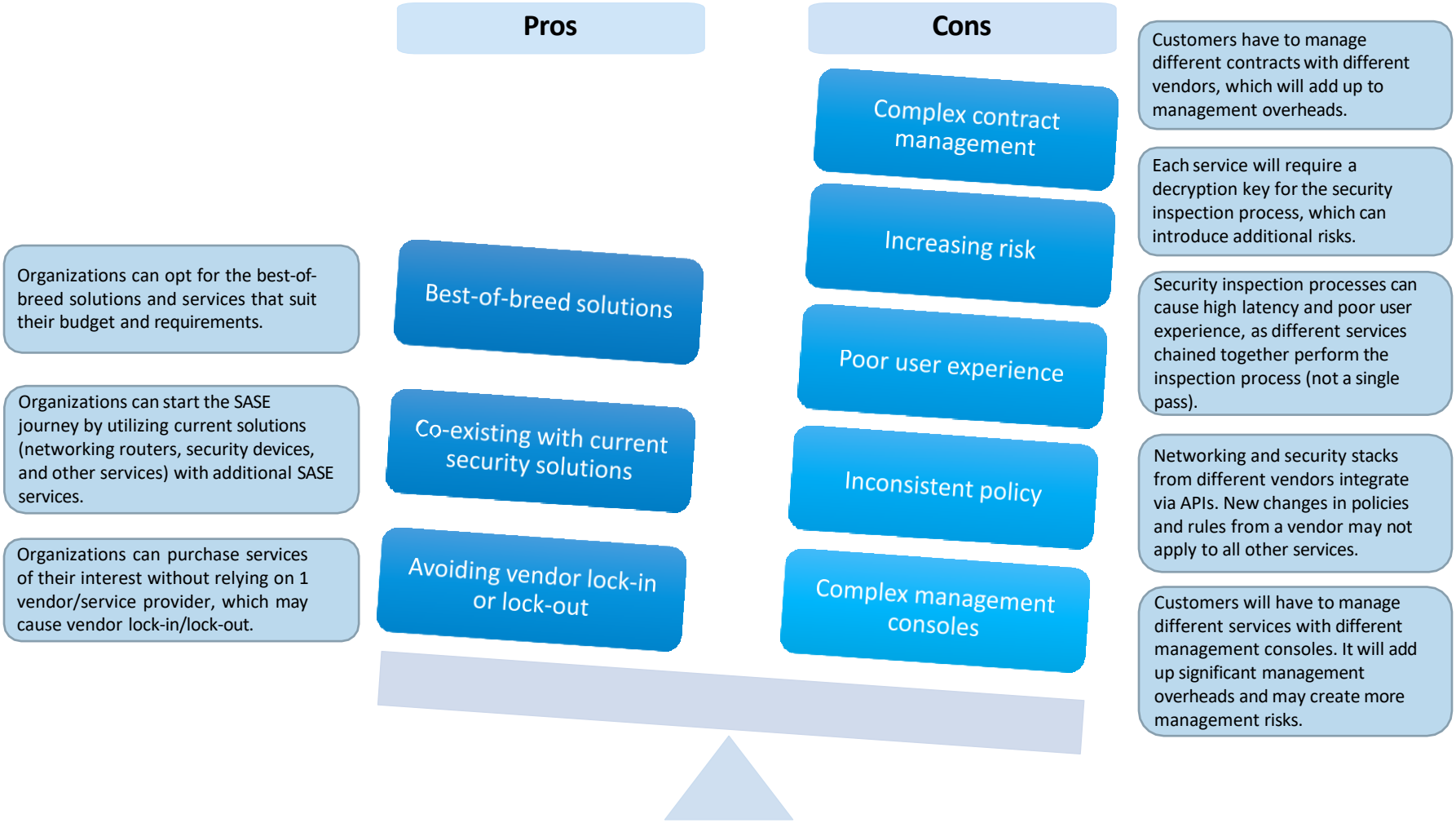
- SASE is a globally distributed cloud platform with dozens of PoPs that SASE vendors or partners manage.
- Contents, functions, and performance are consistent among these distributed PoPs.

Key: MPLS: Multiprotocol label switching; LTE: Long-term evolution; DSL: Digital subscriber line.

Source: Frost & Sullivan

Comparison of SASE Types—Service Chaining

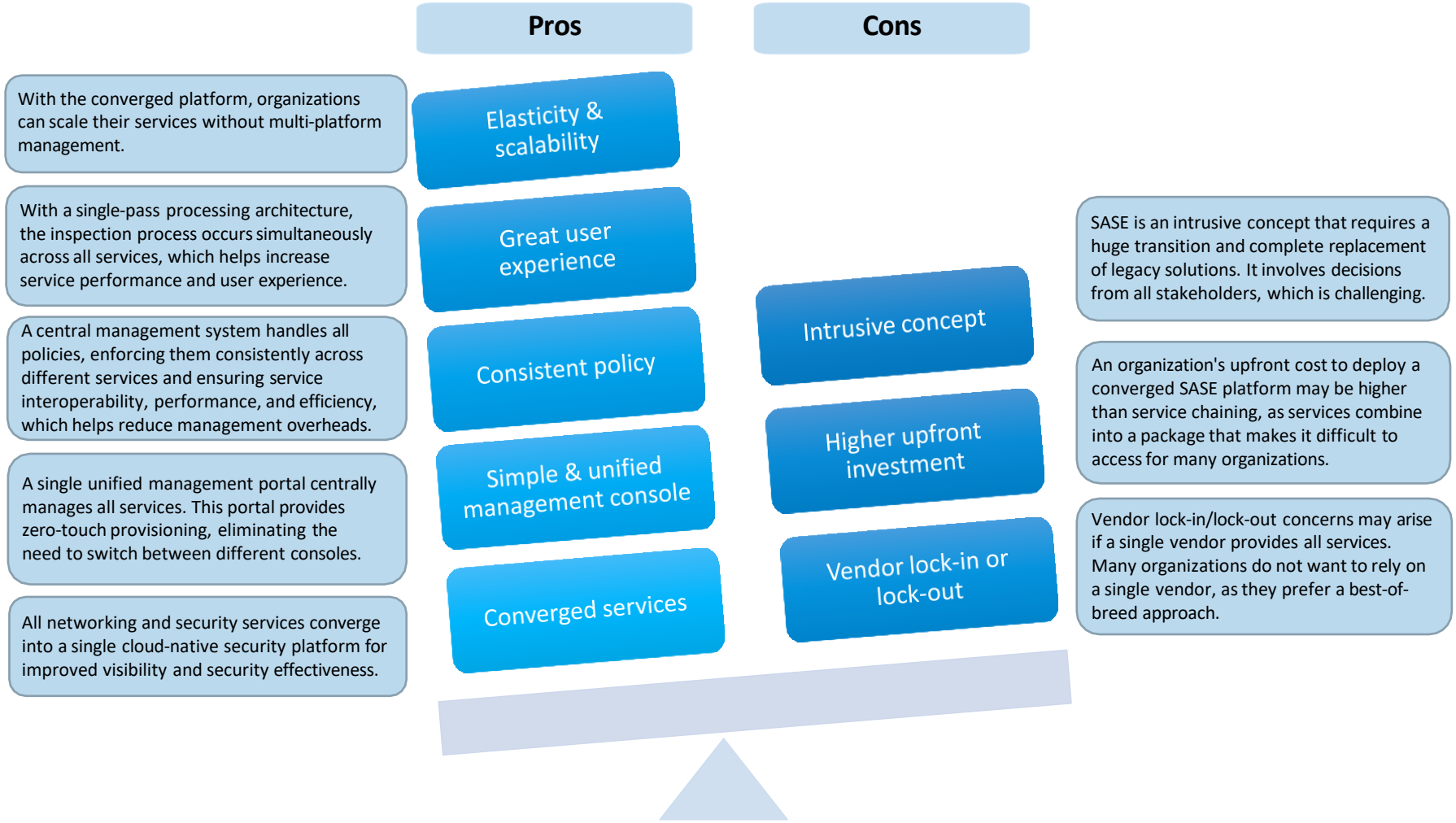
The service chaining type of SASE architecture enables organizations to embrace the SASE initiative more flexibly, as it is not intrusive. However, operationally, it may cause long-term issues, such as higher costs for management, inconsistent policy, poor experience, and higher security risks.



Source: Frost & Sullivan

Comparison of SASE Types—Converged Platform/Service

Though the converged SASE solution can be intrusive, as it involves different organizational stakeholders, it brings several benefits compared to the service chaining in the long run.



Source: Frost & Sullivan

Scope of Analysis

- The study covers vendors that provide a converged SASE platform and vendors offering SASE products/components that enable SASE architecture via service chaining.
- The platform and product portfolio must include the following services/capabilities:
  - **Networking Services:** SD-WAN and a global PoP system (running in public clouds or private data centers).
    - SD-WAN is a must-have capability for inclusion.
  - **Security Services:** FWaaS, ZTNA, and SWG.
- The study provides insights into the global market landscape with a regional breakdown of North America (NA); Europe, the Middle East, and Africa (EMEA); Asia-Pacific (APAC); and Latin America (LATAM).
- Revenue for SASE platforms and portfolios includes revenue from edge devices (routers, firewall platforms, and networking sockets) and cloud SASE service offerings under a managed service (by the vendor or local partners).
- This report recognizes license revenue for the SASE software stacks/images that end users deploy and manage at their data centers or their local service providers' physical or cloud data centers. However, this report does not recommend this model because it may not scale well and does not effectively support remote users.
- The study excludes revenue from the partnership model. However, it features vendors that provide core components of SASE and those with a SASE roadmap.

Scope	
Geographic Coverage	Global
Study Period	2021–2027
Base Year	2022
Forecast Period	2023–2027
Monetary Unit	US Dollars

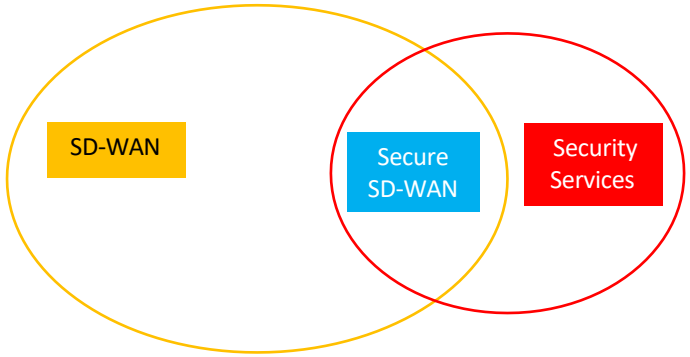
Key: FWaaS: Firewall-as-a-service.

Source: Frost & Sullivan

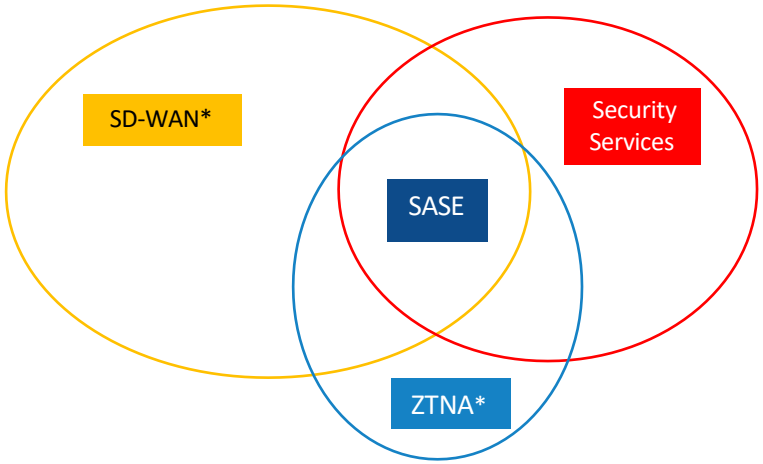
Revenue Calculation Methodology—SASE–2022

- Different vendors approach SASE differently and have different ways to recognize their SASE revenue. Many security vendors that only provide cloud-delivered security services without SD-WAN claim they are SASE vendors. However, per this study's definition, they do not qualify as a SASE vendor; hence, this study will not recognize their SASE revenue.
- **This Report Recognizes SASE Revenue Only when a Customer Uses SD-WAN, ZTNA, and Security Services Such as FWaaS or SWG from a Single SASE Vendor During the Base Year (2022).**
- Nevertheless, though a vendor qualifies as a SASE vendor under this study's definition, if it sells its security services to customers using other vendors' networking services (SD-WAN) or vice versa, this study will not recognize the revenue generated from the sales of these services, as it falls under the partnership model. This research service cannot verify the total revenue generated from customers using SD-WAN, security services, and ZTNA from multiple vendors.
- When a SASE vendor's customers use other security services from the same SASE platform, such as CASB, DLP, ATP, or RBI, the study will recognize the revenue if the same vendor provides all the services.
- The diagram on the right explains how this study recognizes secure SD-WAN and SASE revenues.

Secure SD-WAN Formation



SASE Formation



Key: *All components must be from a single SASE vendor.

Source: Frost & Sullivan

Revenue Calculation Methodology—SASE–2022 (continued)

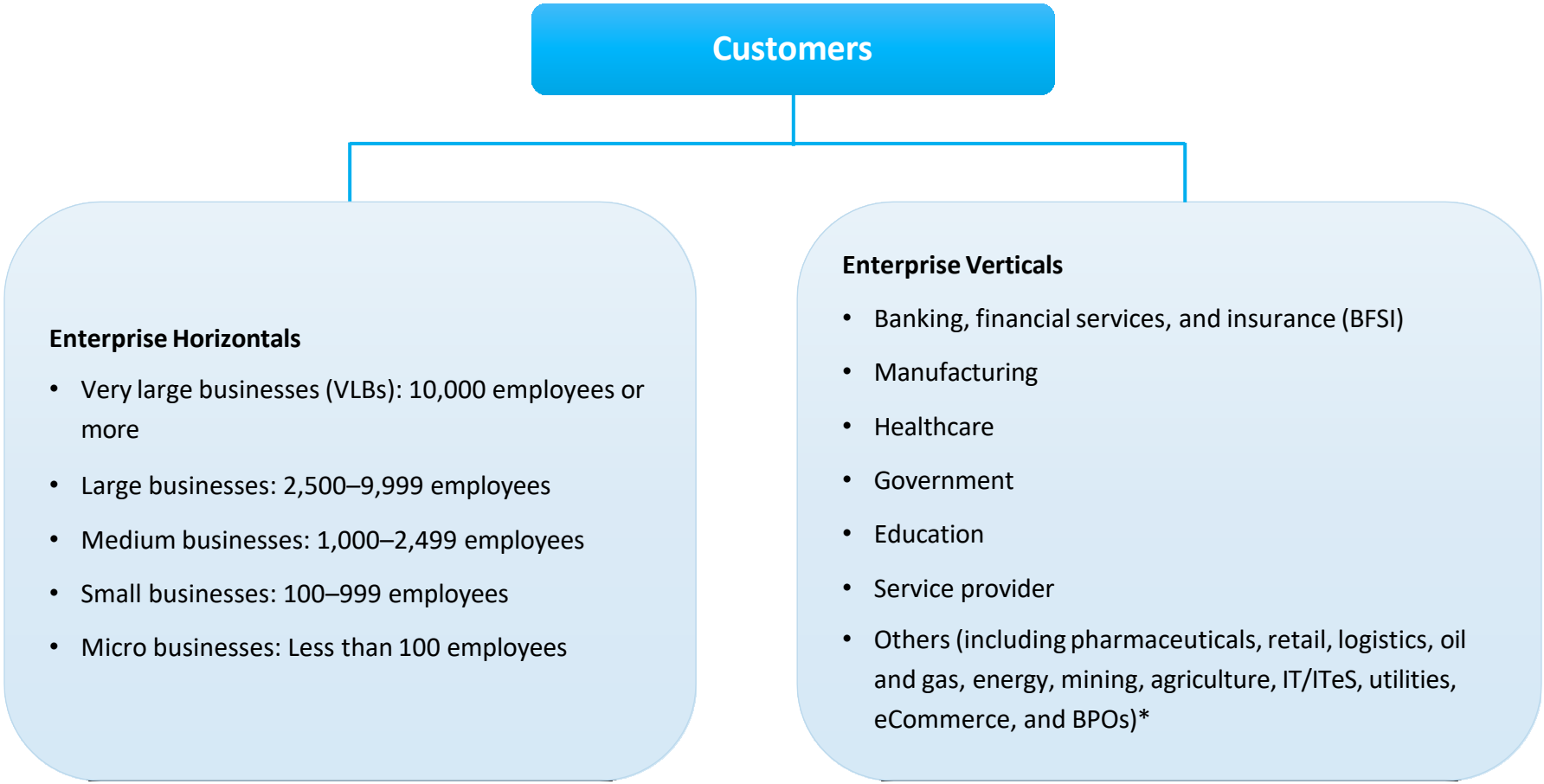
This report recognizes SASE revenue only when a customer uses SD-WAN, ZTNA, and security services such as FWaaS or SWG from a single SASE vendor during the base year (2022).

Scenario	Networking Services	Security Services	Revenue Recognition
Customer 1	Using SD-WAN from vendor A	Using ZTNA, FWaaS, SWG, and other security services from vendor B	This report does not recognize the revenue generated. The customer is not using both networking and security services from the same vendor. The customer achieves SASE through a partnership model.
Customer 2	Not using SD-WAN	Using ZTNA, FWaaS, SWG, and other security services from vendor A	This report does not recognize the revenue generated. This model does not fit into Frost & Sullivan's SASE definition, as the customer is not using SD-WAN to achieve SASE.
Customer 3	Using SD-WAN from vendor A	Using ZTNA, FWaaS, SWG, and other security services from vendor A	This report recognizes the revenue generated from this SASE deal. The customer is using both networking and security services from the same vendor to achieve SASE.

Source: Frost & Sullivan

Customer Segmentation

SASE: Customer Segmentation, Global, 2022

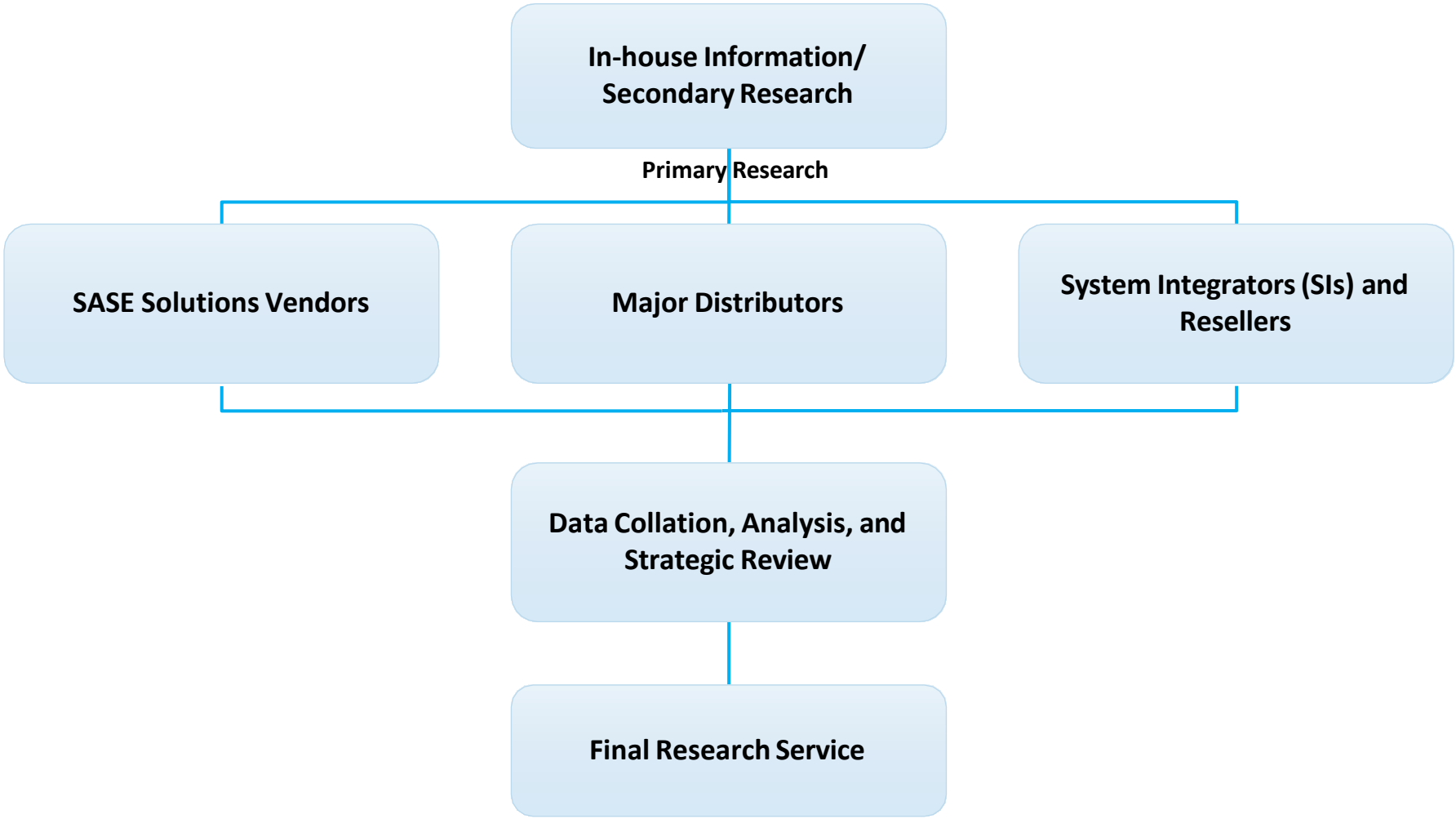


Note: *IT/ITeS: Information technology/information technology-enabled service; BPO: Business process outsourcing.
Key: This study discusses revenue shares for customer segmentation only. It does not provide a forecast.

Source: Frost & Sullivan

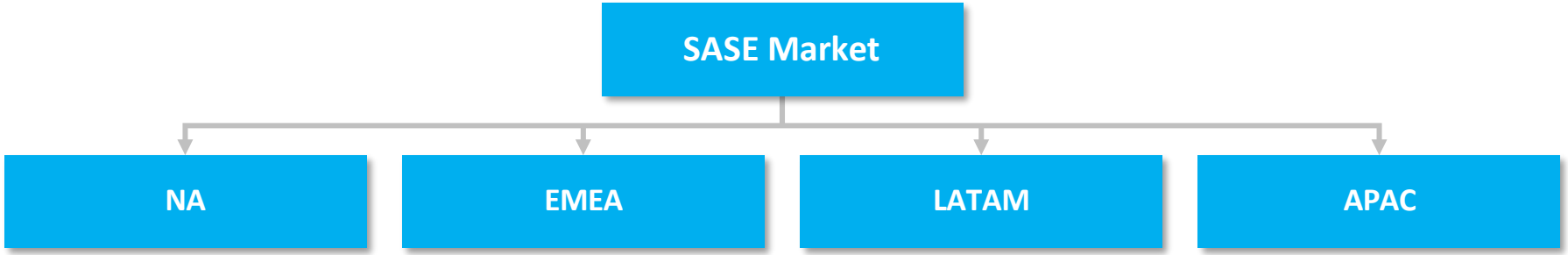
Research Methodology

SASE: Research Methodology, Global, 2022



Source: Frost & Sullivan

Market Segmentation



- NA has higher maturity and readiness to adopt the cloud, SaaS applications, and cloud-native initiatives compared to other regions.
- The strong cloud adoption, the wide acceptance of cloud-delivered services, and the rising need to support a distributed workforce drive the need to transform IT infrastructure among organizations. These trends have accelerated the adoption of SASE to converge networking and security infrastructure.
- The region has the highest adoption of SASE. It dominated the global SASE market with a market share of 58.4% in 2022.

- Data privacy regulations, such as GDPR, impact the preference of organizations in choosing the deployment options for SASE. Most of the organizations in this region opt for a local presence regarding SASE deployments.
- The increased adoption of remote and hybrid work models among EMEA organizations drives the need to enable secure access for a distributed workforce.
- Although EMEA continues to lead in technology adoption after NA, EMEA is the second-largest SASE market, with a market share of 23.8% in 2022.

- The low maturity level and cloud readiness in LATAM have impacted the adoption of SASE in the region.
- Many organizations in the region still rely on legacy infrastructure, and they have low awareness of the need to transform their networking and security architecture to a cloud-native SASE model.
- As a result, organizations show low investment and awareness regarding the SASE concept.
- The adoption of SASE remains low in the region. LATAM is the smallest SASE market globally, with a market share of only 2.5% in 2022.

- The adoption of SASE has increased significantly as organizations look for a cost-effective approach to streamline and simplify their network and security infrastructure.
- Organizations tend to opt for a combination of on-premises deployment and cloud-delivered services to kickstart their SASE projects.
- Data privacy laws in some countries have impacted the deployment model for SASE, as organizations need to comply with data localization requirements. These organizations prefer to adopt thick edges on their premises for networking and security functions.

Key: GDPR: General Data Protection Regulation.

Source: Frost & Sullivan

Key Competitors for SASE

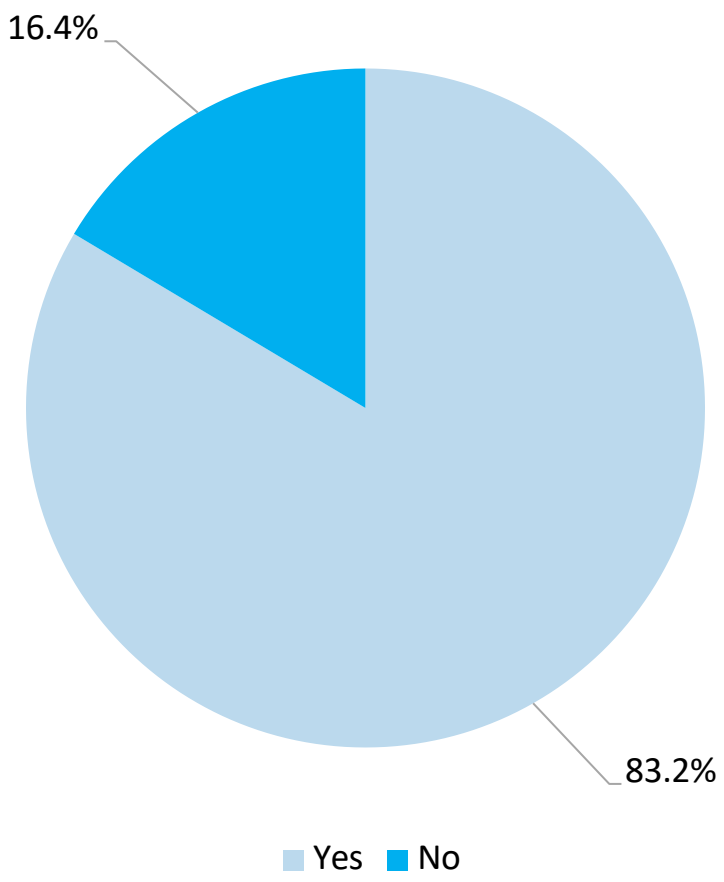
Global	North America	Europe, The Middle East, and Africa	Asia-Pacific	Latin America
• Barracuda Networks	• Barracuda Networks	• Barracuda Networks	• Barracuda Networks	• Cato Networks
• Cato Networks	• Cato Networks	• Cato Networks	• Cato Networks	• Cisco
• Cisco	• Cisco	• Cisco	• Cisco	• Forcepoint
• Forcepoint	• Forcepoint	• Forcepoint	• Forcepoint	• Fortinet
• Fortinet	• Fortinet	• Fortinet	• Fortinet	• Palo Alto Networks
• Palo Alto Networks	• Palo Alto Networks	• Palo Alto Networks	• Palo Alto Networks	• Versa Networks
• Sangfor	• Versa Networks	• Versa Networks	• Sangfor	• VMware
• Versa Networks	• VMware	• VMware	• Versa Networks	
• VMware			• VMware	

Source: Frost & Sullivan

Key Findings—Rising Cloud Adoption Drives SASE Adoption

Distributed Workforce—The New Norm

Organizations' Current Remote Workforce, Global, 2023



- The pandemic has accelerated the remote working trend, and the survey result indicates that organizations have embraced a flexible work arrangement with remote workers working from home offices at least once a week.
- The shift to a hybrid work environment has transformed today's technology consumption to enable people to work from anywhere. Users can access corporate applications and cloud services from any location and device.
- As a result, the traditional network architecture is no longer sufficient to secure the expanded network perimeter beyond the physical boundaries. Organizations' network perimeters are exploding with the rapid growth of remote users, cloud-based applications, and IoT devices. The perimeter will continue to evolve, exposing organizations to security risks with the expanded attack surface.
- To enable a secure and seamless connection for the distributed workforce, organizations must rethink their architectural approach to network and security requirements.

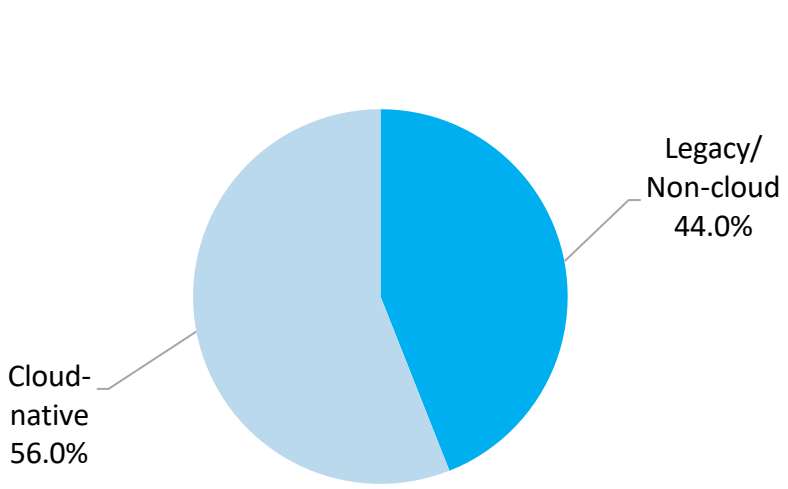
Base, n = 1624
Q: Does your organization have remote workers working from home offices at least once a week?
2023 ICT Network Services Survey, May 2023.

Source: Frost & Sullivan

Legacy Applications Continuing to Migrate to the Cloud

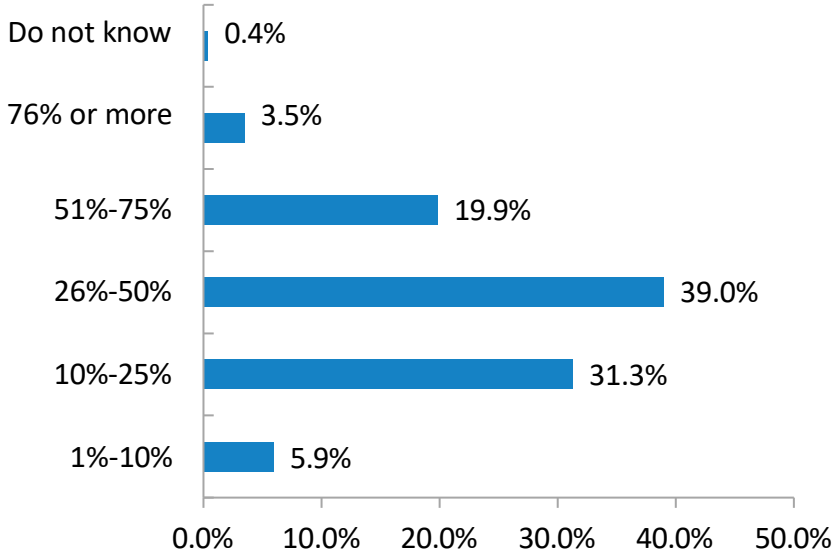
- Today, businesses house more than half of their applications in cloud environments; the rest remain in legacy infrastructures. Some applications remain hosted in the legacy environment, as it could be too difficult, heavy, or sensitive to migrate to cloud environments.
- Businesses will continue to move their applications to a cloud-native environment. By 2025, 37% of businesses will move more than half of their remaining legacy workloads to a cloud environment.

Organizations' Share of Cloud-native and Legacy Applications, Global, 2023



Base, n = 701
Q. What share of your applications are cloud-native versus non-cloud/legacy?

Percentage of Organizations' Applications That will Migrate to the Cloud in the Next 24 Months, Global, 2023



Base, n = 690
Q. What share of your legacy/non-cloud applications are you planning to migrate to a cloud environment in the next 24 months?

Key: 2023 Frost & Sullivan Global Cloud Survey, November 2023.

Source: Frost & Sullivan

The Rise of the New Network Perimeter

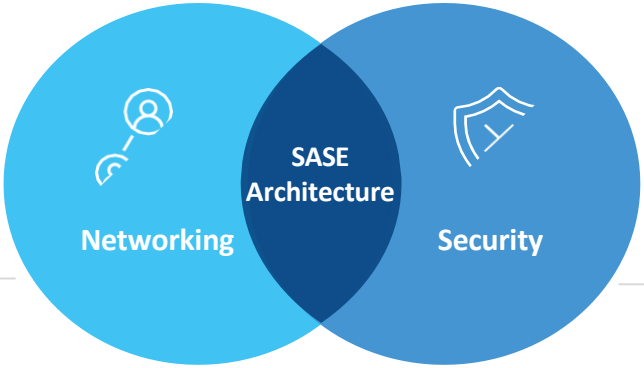
The drastically changing business environment is pushing for a new networking and security solution to help organizations address challenges that the legacy architecture fails to handle. SASE is the solution that combines networking and security functions into 1 platform or architecture to enable businesses to achieve this goal.

The New Network Perimeters

Source: Global SASE Growth Opportunities; Frost & Sullivan

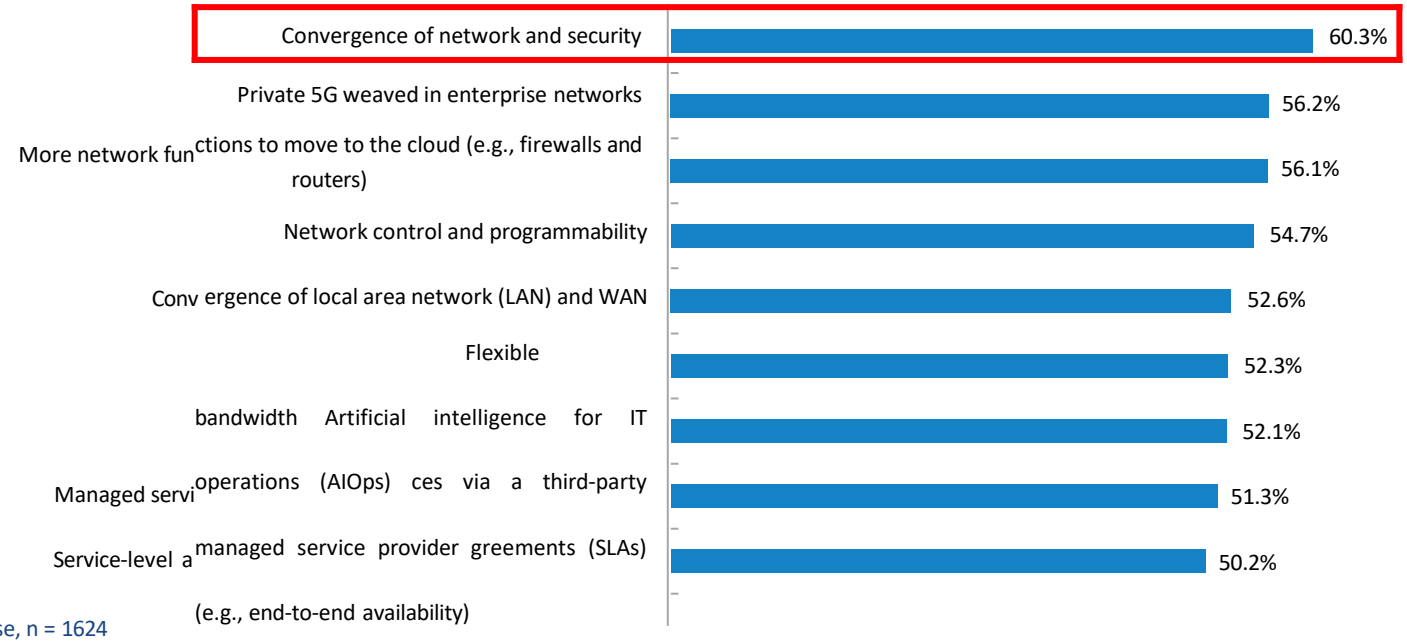
Strong Needs to Converge Networking and Security

Technology tools that integrate well with a defined process and informed people



Integrated procedures and processes designed to achieve the desired outcomes

Organizations' Network Strategy in the Next 2 Years, Global, 2023



Sixty percent of organizations indicate that they will prioritize the convergence of network and security functions as part of their network strategy in the next 2 years. This trend shows a rising need for organizations to streamline their IT operations for greater efficiency and better business outcomes.

Base, n = 1624

Q: How important will be the following factors for your organization's network strategy in the next 2 years? Top 2 Box Summary (crucial, very important).

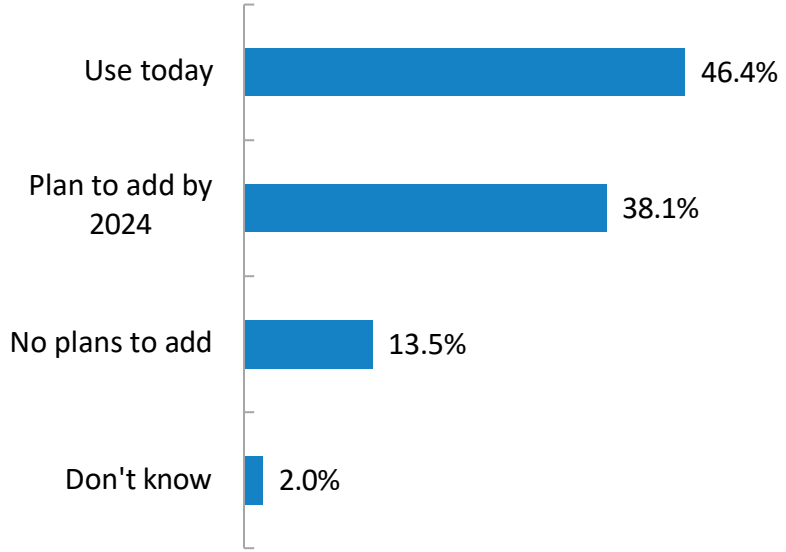
2023 ICT Network Services Survey, May 2023.

Source: Frost & Sullivan

Increasing SASE Adoption to Manage the Expanded Network Perimeter

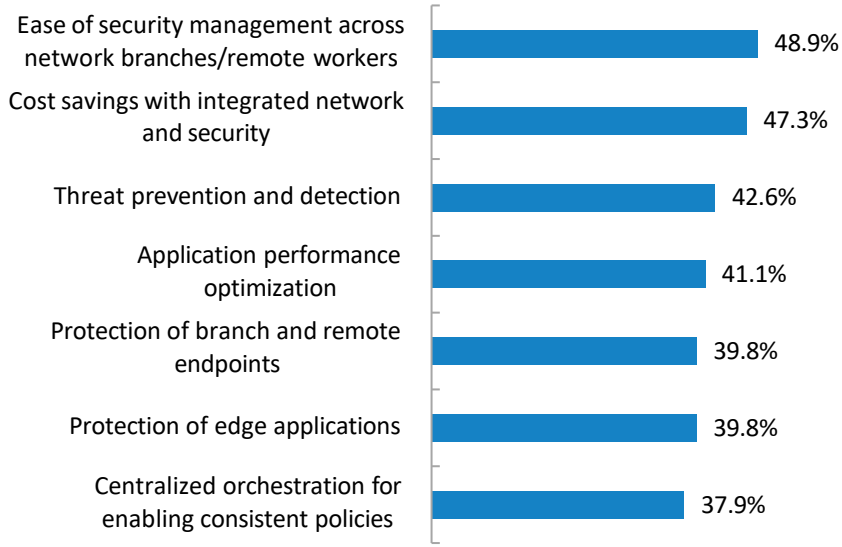
- SASE, which converges networking and security, has become a vital tool to manage an increasingly distributed network. Most organizations have embraced the SASE model, which provides high-performance networking services and comprehensive protection and security for applications, data, and users.
- Many organizations are replacing their MPLS services with SD-WAN and cloud-delivered security services to simplify security management across branches and support their remote workers. At the same time, organizations look at reducing costs through an integrated network and security approach.

Organizations' Current and Planned Use of SASE, Global, 2023



Base, n = 1,771
Q: Which of the following security services solutions does your organization use: - Secure Access Service Edge (SASE)?
2023 Voice of the Enterprise Security Customer Survey, September 2023.

Reasons for Deploying SASE, Global, 2023



Base, n = 947
Q: What are the key reasons your organization has deployed SASE or is planning to deploy it within the next 2 years?
2023 ICT Network Services Survey, May 2023.

Source: Frost & Sullivan

Key Findings—SASE

Key Findings

Organizations face challenges from increasing operational complexity due to the discrete networking and security tools in their environment. The heightened concerns about operational inefficiencies resulting from infrastructure silos drive a strong need to consolidate tools. Organizations seek to consolidate multiple solutions under a single SASE platform instead of deploying and managing networking and security tools individually.

Most SASE platforms in the market allow customers to gradually embrace a full SASE solution from a single vendor. During the initial deployment process, these SASE solutions can co-exist with legacy networking and security solutions. Customers can shift to SASE in phases and replace the existing legacy hardware when the contract expires. This SASE platform architecture provides greater flexibility to customers, especially large businesses that rely heavily on legacy networking or security hardware appliances.

One of the biggest challenges for organizations implementing SASE is having the networking and security teams work together toward a common goal when deploying the converged networking and security solution. Most SASE deployments are now top-down projects. The chief information officer or CISO drives these projects to ensure the unification of 2 teams as organizations continue to transform and modernize their architecture.

Major CSPs are increasingly offering cloud-native security features and may introduce their SASE offerings in the future. With the rising adoption of a multi-cloud strategy, organizations should consider a cloud-agnostic SASE solution that can provide networking and security services to multiple public cloud platforms and avoid the risk of vendor lock-in.

Regulatory compliance across countries and industries will continue to significantly impact customer requirements for SASE adoption. Highly regulated industries will still face limitations in adopting a cloud-native SASE model; these sectors will look for private or on-premises SASE deployment to meet compliance needs. Local PoP is critical in addressing data localization requirements in most countries.

Source: Frost & Sullivan

Customer Expectations and Top Features

Key Customer Expectations from SASE Implementation Include the Following:

- Vendor consolidation
- A zero-trust approach
- Unified protection for remote users and branch offices
- Centralized networking and security management to balance security needs and network performance
- Operational efficiency
- Cost reduction
- Ease of use and simplicity of deployment
- Optimized application performance and secure remote access to those applications

Features that Customers Prioritize when Evaluating a Single SASE Solution Include the Following:

- ZTNA is a crucial component of a zero-trust model, providing granular access controls, supporting users based on zero-trust principles, and offering continuous monitoring to enforce strict security policies.
- Scalable architecture is a cloud infrastructure that allows customers to easily scale their network and security capabilities as business requirements evolve.
- Centralized management and orchestration is a unified management tool that provides simplified network and security administration and policy enforcement, easy configuration, zero-touch provisioning, and monitoring across multiple locations.
- Single-pass processing architecture consolidates all networking and security functions into a single element or packet to perform process requirements only once, allowing improved efficiency and performance, reduced processing overhead, and decreased risk of misconfiguration.
- Extensive PoP coverage ensures PoPs have the capacity to deliver integrated networking and security capabilities and process requests from different edges (physical data centers, remote users' devices, IoT devices, and public cloud data centers). These PoPs should be highly available and elastic to meet customers' requirements at different levels.

Source: Frost & Sullivan

Key Growth Metrics for SASE

SASE: Key Growth Metrics, Global, 2022

Life Cycle Stage	Revenue	Revenue for Last Year of Study Period
Nascent	$1,358.2 M (2022)	$6,162.9 M (2027)

Base Year Growth Rate	Compound Annual Growth Rate	Number of Competitors	Market Concentration
60.1% (2022)	35.3% (2022–2027)	9 (active competitors in 2022)	68.2% (Revenue share held by top 3 companies)

Note: All figures are rounded. The base year is 2022. Source: Frost & Sullivan

Growth Drivers

SASE: Growth Drivers, Global, 2023–2027

Driver	1–2 Years	3–4 Years	5th Year
The rise of a distributed and dynamic workforce drives the need for secure, low-latency connectivity in remote and hybrid office environments.	High	High	High
The surge in cloud migration among enterprises drives stronger demand to transform legacy networking and security architecture for lower network latency, greater user experience, and improved security posture.	High	High	High
Enterprises increasingly require the consolidation of networking and security functions to achieve operational efficiency, simplify operations, and optimize user experiences.	High	High	Medium
The rise of IoT devices and edge computing drives the need for robust network operations to optimize application performance.	Medium	High	High

Source: Frost & Sullivan

Growth Driver Analysis

The Rise of a Distributed and Dynamic Workforce Drives the Need for Secure, Low-latency Connectivity in Remote and Hybrid Office Environments

- In the wake of the COVID-19 pandemic, though offices are reopening, most organizations continue to implement flexible work arrangements, and remote work is here to stay. Most employees will continue to work from anywhere, between corporate offices, home offices, branch offices, and on the road.
- The shift to a distributed and dynamic workforce expands the potential attack surface. The new operational model has created challenges for organizations to secure various types of devices and endpoints with traditional remote work mechanisms, such as virtual private networks (VPNs). The dramatic increase in remote access owing to increased remote work and hybrid cloud adoption has caused a spike in network traffic and an overload of legacy VPN tunnels. This has resulted in poor network performance and user experience. VPNs are no longer adequate to secure remote access to corporate assets, as they can create a huge attack surface owing to poor patching.
- Organizations recognize the architectural and technological limitations they face with the rise of the work-from-anywhere model and cloud adoption, and a new approach is necessary to support the norm of workforce flexibility. As a result, they increasingly shift to a zero-trust security model to better manage users, applications, devices, or networks in a highly distributed environment. This also drives the adoption of SASE, as it is a core component of a zero-trust strategy.
- The converged networking and security capabilities under a SASE platform provide secure, reliable, and low-latency network connectivity for users to access corporate systems, applications, and services across multi-cloud environments from any location globally. In addition, organizations can maintain and enforce consistent security policies for all devices and users regardless of their hosting locations, such as physical data centers or in the cloud.

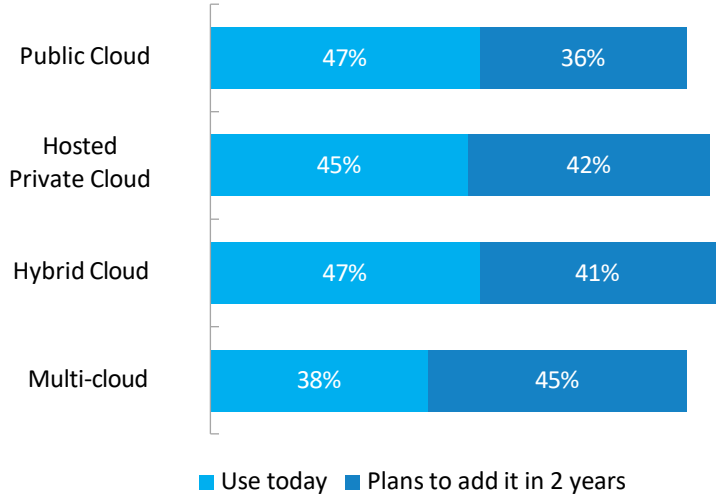
Source: Frost & Sullivan

Growth Driver Analysis (continued)

The Surge in Cloud Migration Among Enterprises Drives Stronger Demand to Transform Legacy Networking and Security Architecture for Lower Network Latency, Greater User Experience, and Improved Security Posture

- In Frost & Sullivan's latest global cloud end-user survey, 47% of organizations use public cloud and hybrid cloud, and 45% indicated that they will move to a multi-cloud model in the next 2 years.
- Organizations have accelerated their cloud adoption journey to leverage public and private SaaS and other cloud services for their applications or collaboration services. The multi-cloud strategy enables businesses to be more agile, scalable, and efficient, indicative of the high adoption of public cloud and multi-cloud and the future investment in these service models.
- Traditional data center-centric approaches and MPLS-based legacy architectures cannot scale and support access to these cloud service models. As organizations' computing, storage, and applications do not reside in a fixed data center location, perimeter security solutions that protect physical data centers are no longer adequate to secure distributed resources in multiple locations, such as on-premises or cloud environments across SaaS, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and private clouds.

Rising Cloud Adoption Across Service Models, Global, 2023



Base, n = 757

Q: Which of the following infrastructure options does your organization use today or plan to use in the future to run your applications? Multiple answers allowed; 2023 Frost & Sullivan Global Cloud Survey, November 2023.

- Organizations seek to adopt security services and shift to the SASE platform, which enables lower network latency, greater user experience, and improved security posture while managing secure access to data and applications from any location and device. The SASE approach, which converges networking and security capabilities into 1 cloud-based service, provides a more flexible way to build a secure network.

Source: Frost & Sullivan

Growth Driver Analysis (continued)

Enterprises Increasingly Require the Consolidation of Networking and Security Functions to Achieve Operational Efficiency, Simplify Operations, and Optimize User Experiences

- Organizations have increasing requirements to consolidate networking and security functions because of heightened concerns about operational efficiency with disjointed networking and security products. The traditional approach of deploying fragmented products from multiple network and security vendors has resulted in overcomplexity, operational inefficiencies, inconsistent user experiences, and a lack of visibility resulting from separate management systems.
- In addition, the integration process of the products from different vendors is time-consuming and highly complex and can create cybersecurity gaps that lead to high security risks. The increasing complexity of network and security infrastructure, along with the expanded network perimeter owing to the shift to hybrid work and rising cloud adoption, has accelerated the adoption of SASE solutions.
- Organizations need to shift from siloed network and security architectures to converge networking and security functions into a cloud service platform that allows for lower latency and greater user experience. The SASE solution connects edge users or endpoints to nearby PoPs instead of routing them back to the data center, delivering a more secure and faster connection than traditional networking solutions.
- The integration of networking and security capabilities, including SD-WAN, SWG, ZTNA, CASB, FWaaS, DLP, RBI, and other capabilities, offers higher efficiencies, enhanced agility and flexibility, simplified operations, and optimized user experiences. SASE's single management console allows unified configuration, policy enforcement, and reporting, which improves visibility and facilitates centralized management across applications, data, and users.

Source: Frost & Sullivan

Growth Driver Analysis (continued)

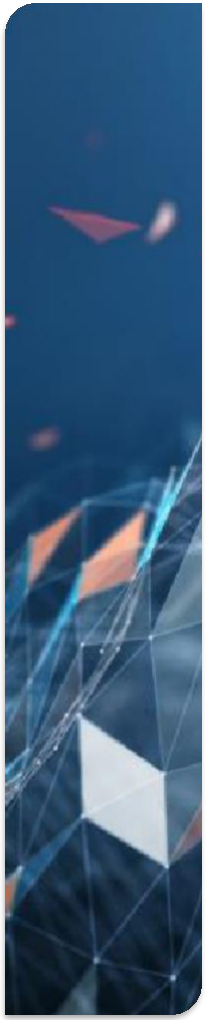
The Rise of IoT Devices and Edge Computing Drives the Need for Robust Network Operations to Optimize Application Performance

- The surge of IoT devices and the vast amount of data that these devices generate have caused the rapid rise of edge computing. Edge computing is highly required for real-time decision-making, as data processing can occur closer to the source without sending a large amount of data back to the data center.
- The decentralized approach to data processing enables reduced latency and improved performance as required in use cases such as industrial automation and autonomous vehicles. The use cases will continue to expand owing to the implementation of 5G or 6G infrastructure, which generates a higher volume of data with the increasing number of sensors and IoT devices at the edge locations.
- With the growing volume of data and network traffic in the modern decentralized edge computing model, organizations realize that perimeter-based defense has become irrelevant, as most applications and data do not reside within the data center. A rising need exists to redesign organizations' security strategies to support globally distributed users and devices.
- The cloud-native SASE architecture is a breakthrough to support modern IT infrastructure in the era of edge computing, as it delivers networking and security capabilities to multiple edge computing devices and locations closer to the resources. It provides secure access to distributed resources from any location with end-to-end visibility and consistent policy control. The ability to provision computing resources, networking, and security functions at the network's edge allows the SASE solution to deliver improved application performance, reduce latency, and enhance the overall user experience. To better address edge computing scenarios, especially in highly regulated industries such as government, BFSI, or healthcare, which have requirements to keep data in a localized network, more SASE vendors will offer local computing options.

Source: Frost & Sullivan

Growth Restraints

SASE: Growth Restraints, Global, 2023–2027



Restraint	1–2 Years	3–4 Years	5th Year
Organizations tend to take a more cautious approach to the SASE model because of its intrusive concept, which requires different stakeholders in an organization to align their requirements.	High	High	High
Market confusion around SASE and a lack of technical expertise among channel partners and service providers cause hesitation among organizations to adopt the SASE architecture.	High	Medium	Medium
Organizations, especially those in highly regulated industries, are more cautious about embracing the cloud-native SASE model because of the stringent data regulations and localization requirements in some regions.	High	Medium	Medium
Macroeconomic uncertainty may lead to organizations' budget constraints and concerns about the cost of implementing SASE solutions.	High	Medium	Medium

Source: Frost & Sullivan

Growth Restraint Analysis

Organizations Tend to Take a More Cautious Approach to the SASE Model Because of its Intrusive Concept, Which Requires Different Stakeholders in an Organization to Align their Requirements

- Though the SASE concept provides organizations with improved agility, flexibility, and operational efficiency, the intrusive concept of a converged SASE model requires organizations to introduce significant changes to their existing legacy networking and security architecture. SASE is more than just a solution; it is a change of process that will disrupt the traditional siloed network and security infrastructure.
- Implementing a SASE solution often involves different stakeholders across networking, security, and operation teams within an organization to transition to the new SASE architecture fully. These teams typically have separate functions and operate fully independent of each other. Security and networking are traditionally 2 siloed departments, as both cover different areas of expertise. In many cases, both teams do not actively collaborate and work together to implement a unified IT management and security strategy.
- As a result, different stakeholders will have their own purchasing cycles and preferences for adopting technologies. Adopting a complete set of SASE solutions from a single vendor also means that networking and security teams cannot choose the best-of-breed products based on their preferences, which might lead to dissatisfaction among the teams. Internal friction between these siloed teams may also be present regarding budget and project ownership, especially in larger companies that commonly have distinct networking and security teams.
- Coming to a mutual agreement with all these stakeholders to transition to a new SASE architecture is challenging. Also, the decision-making process will take longer, as it involves different stakeholders, who will have to consider their priorities and requirements carefully.
- This results in the slow adoption of SASE, particularly cloud-native and converged single SASE platforms that require organizations to look at networking and security functions holistically. Large organizations will see a stronger impact owing to the lengthy evaluation process across multiple teams, whereas small and mid-sized businesses (SMBs) with no distinct teams to liaise with have a simple decision-making process when adopting SASE.

Source: Frost & Sullivan

Growth Restraint Analysis (continued)

Market Confusion Around SASE and a Lack of Technical Expertise Among Channel Partners and Service Providers Cause Hesitation Among Organizations to Adopt the SASE Architecture

- The SASE market is still evolving, and vendors from different backgrounds are trying to fill the gaps to offer single SASE solutions to the market. Vendors with a point solution or patchwork of SASE components also claim to be SASE vendors. The inconsistent SASE offerings across vendors cause confusion in the market and hamper the adoption of SASE among organizations.
- As a result, organizations face challenges in identifying the appropriate SASE solutions to address their business needs. The SASE vendors from either networking or security backgrounds approach SASE differently with their definition, setup, and infrastructure. Legacy security vendors may have strong security capabilities but are weak in cloud-native technologies. Networking vendors are strong in their networking solutions but lack comprehensive security capabilities. Some vendors offer component-based SASE solutions instead of a unified approach, resulting in loose integration and complex management that goes against SASE's principle of operational simplicity.
- In addition, the market is relatively new, and channel partners, including managed security service providers (MSSPs), SIs, and resellers, may not have the right knowledge, technical expertise, and experience to support a seamless SASE implementation and configuration. Organizations are hesitant to embrace the entire SASE framework because of the lack of experts to help with the migration and day-to-day operations and management of the SASE architecture.
- This has impacted the adoption of SASE, as organizations now need more time for due diligence. They must sift through various SASE solutions from vendors and partners, ensuring they choose credible partners who can address their networking and security challenges. These partners should also have the technical knowledge and support to help organizations unlock the benefits of SASE.

Source: Frost & Sullivan

Growth Restraint Analysis (continued)

Organizations, Especially those in Highly Regulated Industries, are More Cautious About Embracing the Cloud-native SASE Model Because of the Stringent Data Regulations and Localization Requirements in Some Regions

- Most countries or regions have introduced data privacy regulations, such as the EU GDPR, data protection acts, cybersecurity laws, and data privacy laws. The evolving data privacy laws will become stricter across regions to limit cross-border data transfers.
- Organizations in highly regulated industries, such as banking, financial services, healthcare, government, and other critical information infrastructure sectors that process sensitive data, must comply with data privacy regulations to avoid severe penalties.
- Concerns over data sovereignty present a significant challenge for organizations considering adopting cloud-delivered services under the SASE offering. These concerns could impact organizations' approach to SASE, potentially leading them to choose on-premises deployment through a service-chaining approach, which is against SASE's cloud-native architectural philosophy.

Macroeconomic Uncertainty May Lead to Organizations' Budget Constraints and Concerns About the Cost of Implementing SASE Solutions

- The impact of macroeconomic uncertainty causes companies to be more careful with their cybersecurity spending, especially on new projects such as SASE that need to replace or re-architect their existing legacy networking and security infrastructure.
- According to Frost & Sullivan's 2023 ICT Network Services Survey, 24% of organizations highlighted that high cost or lack of budget is the second-biggest challenge to adopting SASE in their organizations. High rates of inflation have eroded organizations' spending power, resulting in a delayed transition to the cloud-native SASE model to reduce costs during uncertain times.

Source: Frost & Sullivan

Forecast Assumptions

- The COVID-19 pandemic has accelerated the digital transformation process. The shift to remote work and the increased usage of cloud applications have fundamentally changed how businesses consume technologies. As more businesses move their workloads to the cloud, including private, public, or multi-cloud, their physical data center is no longer the focal point of access for remote users and applications.
- To facilitate the acceleration of digital initiatives, organizations are looking to transform their networking and security architecture to better support the work-from-home requirement and secure the highly distributed environment. This trend drives a stronger demand to shift from traditional WAN connectivity, such as MPLS, to secure SD-WAN or embrace SASE.
- Organizations, especially those that still heavily rely on legacy technology stacks, will find it challenging to shift to the new SASE architecture that cuts across networking and security stakeholders. These organizations will take a component-based approach to SASE in the next 3 years to adopt services such as SD-WAN, FWaaS, SWG, CASB, or ZTNA as they kickstart their SASE project.
- Nevertheless, today's CISOs have a stronger need to modernize the network and security architecture through simplifying technology stacks and converging networking and security functions for improved operational efficiency and a better user experience. As a result, the adoption of SASE services from a single vendor will gain popularity in the next 3 to 5 years.
- Mid-sized businesses, or SMBs, will have a faster decision-making process and a relatively shorter implementation process when adopting the converged SASE platform from a single vendor compared to large enterprises. Owing to the complex infrastructure and longer purchase process with the involvement of multiple stakeholders, large enterprises may opt for a component-based SASE model or a combination of on-premises SASE and SASE service deployment to support their legacy infrastructure and address specific use cases.

Source: Frost & Sullivan

Revenue Forecast Analysis

- The adoption of SASE will maintain strong growth momentum in the next 5 years, mainly because of several factors, including the shift to remote and hybrid work models, the rapid adoption of cloud and cloud-delivered services, increasing requirements toward integrating disjointed networking and security solutions, and the rising need to support edge computing use cases.
- A stronger need exists for organizations to modernize their IT infrastructure to accelerate digital initiatives by embracing the SASE model. By converging networking and security functions under a unified cloud-based platform, SASE allows organizations to offload the operational burden of managing and maintaining various network and security hardware appliances. SASE's cloud-native architecture also enables enhanced scalability, flexibility, and secure access for a distributed environment while optimizing network performance regardless of user or branch location.
- In addition, the single-vendor SASE approach is gaining popularity, and organizations will increasingly shift from a multiple-vendor SASE to a single-vendor SASE offering in the next 3 years. Organizations will continue to consolidate vendors and value the benefits of having unified SASE solutions over best-of-breed SASE components from multiple vendors. The convergence approach allows organizations to overcome challenges resulting from tool sprawl, such as operational complexity, limited visibility, and potential security gaps, and prioritize enhanced interoperability between security and networking functions for a better outcome and user experience.
- Organizations that have embraced the SASE concept will request the integration of more security capabilities with the broader SASE portfolio. Vendors will continue to enhance their security capabilities by integrating more proactive security measures, including endpoint protection, extended detection and response (XDR), and IoT security, to offer comprehensive protection to customers.

Source: Frost & Sullivan

Revenue Forecast Analysis by Region

- The global SASE market will maintain its rapid growth momentum with a compound annual growth rate (CAGR) of 35.3% from 2022 to 2027 to generate a total market size of $6,162.9 million by 2027.
- NA will remain the largest revenue contributor in the next 5 years, generating a total revenue of $3,213.8 million in 2027, which makes up more than half of the global market share throughout the forecast period. The region has a high adoption rate regarding cloud or cloud-native technologies. As early cloud adopters, organizations in the region have a higher acceptance of the cloud-native SASE concept and are more open to adopting cloud-delivered networking and security services. The extensive coverage of cloud regions and SASE vendors' PoPs will continue to drive the adoption of SASE while adhering to data privacy compliance.
- EMEA will be the second-largest SASE adopter from 2022 to 2027, with 24.6% of the market share by 2027. Organizations in EMEA are more concerned about data privacy regulations owing to the stringent data privacy and residency (GDPR) requirements. Highly regulated industries in the region will have a stronger preference to adopt on-premises SASE or a hybrid SASE deployment. The political and economic uncertainties may impact the investment strategies of EMEA organizations in the short term, but the growth momentum remains strong in the next 5 years, with a CAGR of 36.2%.
- APAC will be the third-largest SASE adopter from 2022 to 2027, generating 18.7% of the market share by 2027. Organizations in the region are increasingly migrating their workloads to the cloud, resulting in the rising adoption of SASE among APAC organizations. Several countries in the region increasingly require data localization and data sovereignty, and SASE vendors and CSPs are investing in expanding their cloud regions and PoPs coverage to support the rapid adoption of SASE services. As a result, APAC has emerged as the 2nd fastest-growing region, with a strong CAGR of 40.8% from 2022 to 2027.
- LATAM is the fastest-growing region, with a projected CAGR of 52.7% from 2022 to 2027. However, the region generates low absolute revenue and will only account for 4.6% of the market share by 2027. The adoption of SASE remains relatively low in the region, primarily because of budget constraints and low awareness and adoption of cloud-delivered services.

Source: Frost & Sullivan

Pricing Trends and Forecast Analysis

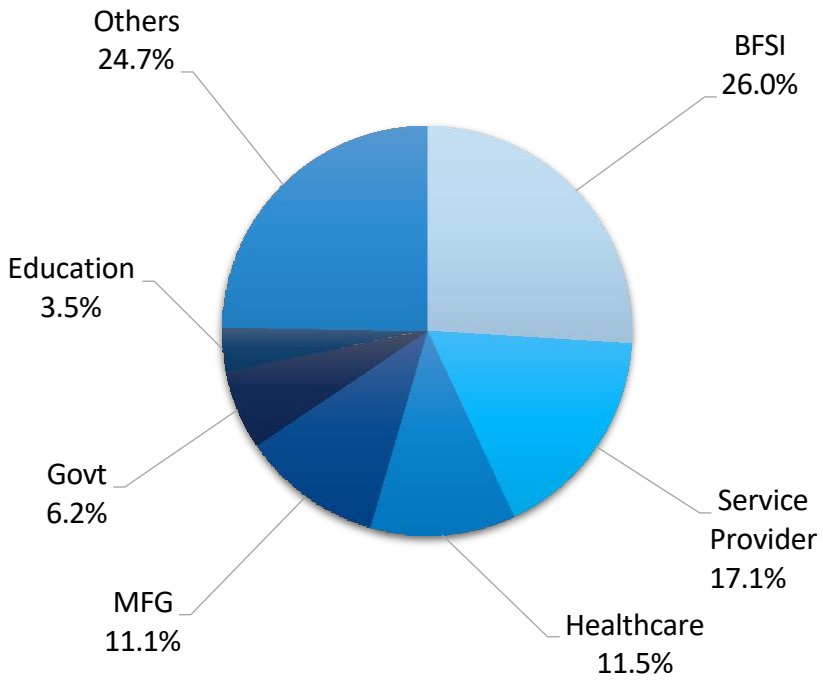
- Most vendors offer SASE services in bundled packages that include different services on a subscription basis with flexible subscription terms (1, 3, or 5 years). Some vendors also offer SD-WAN, or next-generation firewall, as a hardware appliance or virtual edge.
- Most SASE vendors offer user-based or bandwidth-based pricing models:
  - Per bandwidth: The sites connected to the SASE service determine billing based on their bandwidth. Vendors typically apply the bandwidth model to vital services such as firewalls, anti-virus, IPS/IDS, DNS security, SWG, CASB, DLP, anti-distributed denial-of-service (DDoS), and malware detection when pricing security services delivered through the security service edge (SSE) model.
  - Per user: The user or account determines the billing. This model applies to the ZTNA or private internet access services that support remote users.
- Customers can choose various licensing options (e.g., essential, enterprise, and premium) with tiered pricing and service levels depending on their budget and performance requirements. These bundled SASE packages typically include core SASE services, such as SD-WAN, WAN optimization, NGFW, SWG, and ZTNA. Customers can add advanced services such as DLP, CASB, and RBI.
- For hardware appliances, such as SD-WAN routers, network sockets, or security gateways, the pricing depends on the function of the feature tier, bandwidth support, and software license term (usually with multiple years, such as 1, 3, or 5). Most SASE vendors also offer professional services, including onboarding, technical support, training, and optimization to support the implementation and ongoing management of the SASE service.
- The pricing and sales model can differ for larger enterprises, depending on the level of customization needed. SASE vendors must design a more holistic and transparent pricing model to ease customers' decision-making processes.

Source: Frost & Sullivan

Revenue Share by Vertical

- BFSI remained the largest revenue contributor in the global SASE market in 2022, with 26% of the total market share. It is one of the highly regulated industries that leads cloud adoption and other digital initiatives. The compliance requirements drive these organizations to take a more proactive approach to secure their modern networking and security architecture. In some cases, these organizations will opt for private SASE deployment to address the stringent requirements for data privacy and localization compliance.
- Service providers were the second-largest adopters of SASE globally in 2022, making up 17.1% of the market share. Most of these organizations took the service-chaining approach to SASE by adopting on-premises solutions and security services that they needed to achieve the SASE model.
- The healthcare sector emerged as the third-largest adopter of SASE owing to its strong preference for adopting the converged platform that consolidates both network and security tools into a single platform.
- The increased usage of cloud-delivered services, rising requirements to allow end-to-end visibility across sites (data centers, cloud, remote users, or branches), and the strong need to improve operational efficiency continue to drive investments in SASE across verticals. The adoption of a converged SASE platform will maintain its strong growth momentum across verticals such as the tech industry, retail/e-commerce, and other digital companies, as most of these organizations have embraced a cloud-first approach to introducing digital initiatives at a rapid pace.

SASE: Percent Revenue by Vertical, Global, 2022



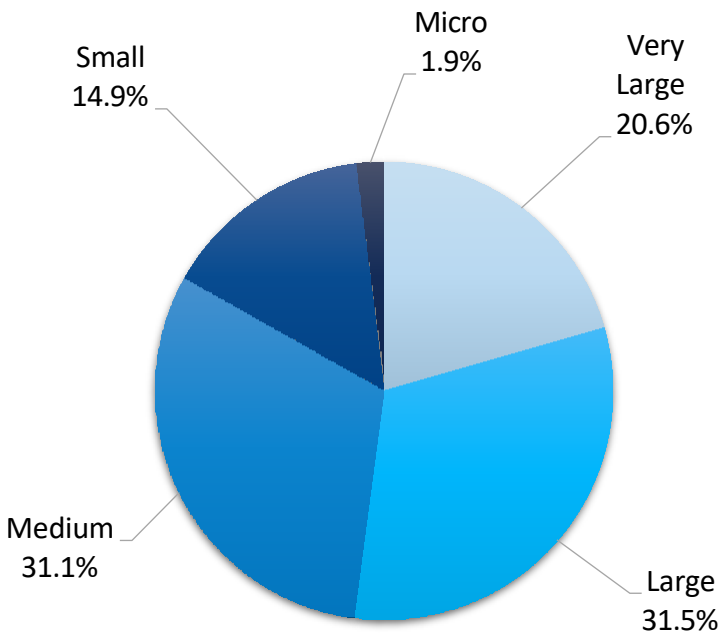
Key: Others*: Pharmaceuticals, retail, logistics, oil and gas, energy, mining, agriculture, IT/ITeS, utilities, eCommerce, and BPOs; Govt: Government; MFG: Manufacturing.

Note: All figures are rounded. The base year is 2022. Source: Frost & Sullivan

Revenue Share by Horizontal

- Medium and large enterprises were the leading adopters in the global SASE market in 2022, accounting for 62.6% of the total market share. These sectors are leading the SASE adoption across regions, as they have a stronger priority to modernize their IT architecture in today's fast-paced business landscape.
- Medium enterprises typically do not have separate security and networking teams, and they can easily shift to the SASE architecture with a simple decision-making process. These organizations are more flexible in adopting all-in-one networking and security solutions such as SASE, which allows them to adopt cloud-delivered services through a pay-as-you-go model without the need to invest in hardware or multiple standalone solutions. The flexible and agile SASE model brings enterprise-grade security services to smaller enterprises, such as SMBs. Most of these smaller enterprises tend to adopt converged SASE from scratch, as the SASE model allows them to address challenges such as limited resources, high upfront and management costs, and a lack of skilled IT and security personnel.
- Larger enterprises with more complex networking and security infrastructure typically adopt a component-based SASE approach as a start and gradually shift to the converged SASE platform by phasing out the legacy hardware as contracts expire. Most of these large organizations require a longer implementation process than smaller enterprises, as they cannot rip and replace their legacy infrastructure. Highly regulated industries that still store their data and applications in a hybrid environment will prefer a combination of on-premises SASE and cloud-delivered SASE service deployment.
- These large organizations have higher requirements for SASE components to address their specific use cases, such as providing secure access to the data and applications in the data center and the cloud, enabling stable connectivity across multiple branches, stores, or offices, or supporting an increased number of remote or roaming users.

SASE: Percent Revenue by Horizontal, Global, 2022



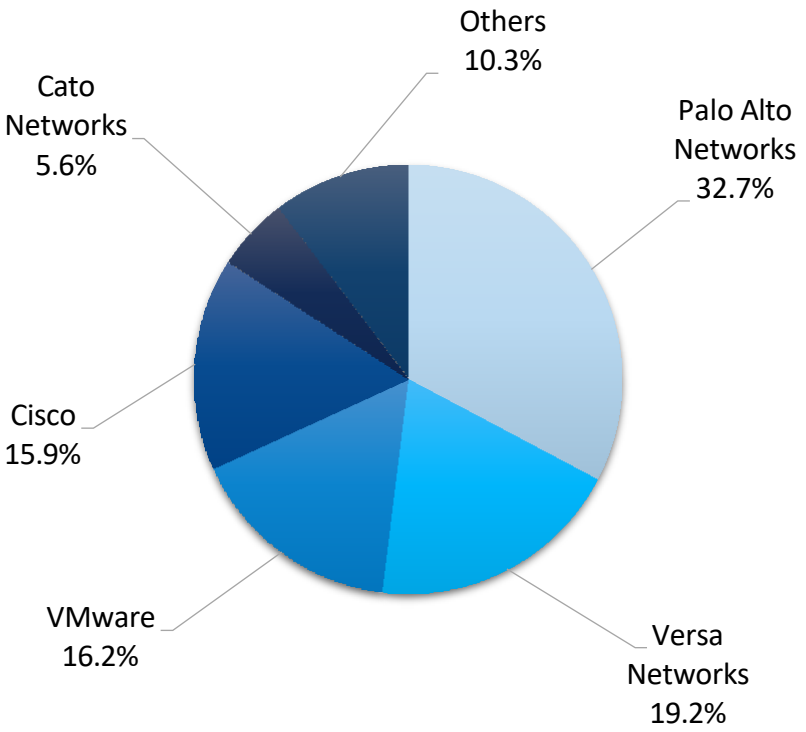
Key: Very large businesses: 10,000 employees or more; Large businesses: 2,500–9,999 employees ; Medium businesses: 1,000–2,499 employees; Small businesses: 100–999 employees; Micro businesses: Less than 100 employees.

Note: All figures are rounded. The base year is 2022. Source: Frost & Sullivan

Revenue Share

- Based on Frost & Sullivan's definition, this report only recognizes SASE revenue when vendors offer in-house SD-WAN and security solutions in the SASE deal.
- Palo Alto Networks remained the largest SASE vendor, with 32.7% of the market share in the global SASE market. The company has expanded its SASE business aggressively across regions. In 2022, its Prisma SASE business experienced tremendous triple-digit year-over-year (YoY) growth in EMEA, APAC, and LATAM. Its core market, NA, made up 66.9% of its overall global SASE business, and the NA market maintained a strong growth momentum of 91.8% on a YoY basis in 2022. The company has a strong footprint in large businesses globally through its established brand name in the security industry.
- Versa Networks maintained its leadership position as the second-largest SASE vendor, with 19.2% of the market share. The company offers comprehensive networking and security functions under its converged SASE platform. It also provides flexible deployment options, including on-premises, public cloud, or cloud-native services, to support all types of enterprises, including highly regulated industries.
- VMware has emerged as the third-largest SASE vendor, with 16.2% of the market share. Its SASE offering combines its strong SD-WAN capabilities and cloud-delivered security services to address specific use cases across different verticals. Most of VMware's SASE business came from NA, and the company is increasingly gaining greater preference among businesses from other regions, including EMEA and APAC.

SASE: Revenue Share of Top Participants, Global, 2022



Key: Others* include Fortinet, Forcepoint, Sangfor, and Barracuda Networks.
Note: All figures are rounded. The base year is 2022. Source: Frost & Sullivan

Competitive Environment

SASE: Competitive Environment, Global, 2022

Number of Competitors	9 companies
Competitive Factors	Cost, performance, PoP, support, technology, reliability, contractor relationships, and channel partners
Key End-user Industry Verticals	BFSI, service provider, healthcare, manufacturing, government, education, tech (IT/IT-enabled services, software development), and eCommerce/retail
Leading Competitors	Palo Alto Networks, Versa Networks, and Vmware
Revenue Share of Top 5 Competitors	89.7%
Other Notable Competitors	Cisco, Cato Networks, and Fortinet
Distribution Structure	Direct sales, channel partners (distributors, telcos, MSSPs, SIs, resellers), and cloud marketplaces
Notable Acquisitions and Mergers	Checkpoint acquired Perimeter 81; Netskope acquired Infiot

Source: Frost & Sullivan

Service Provider Analysis

SASE Landscape—Service Provider Analysis

- Many organizations face challenges in moving to a new SASE architecture. SASE solutions can be complex to deploy, especially among larger organizations, because of their legacy infrastructure and disjointed networking and security functions. Organizations' internal IT or security teams may not have enough knowledge to create the strategy and roadmap for SASE implementation that addresses their business needs.
- As a result, organizations increasingly turn to service providers such as MSSPs for managed SASE services or consulting services. They look for third-party experts to support their SASE project in terms of planning, architecture design, vendor selection, road mapping, implementation, fine-tuning, and ongoing management and monitoring services.
- Below are the objectives that organizations look to achieve using the managed SASE service:
  - Expertise: Access a team of experts who specialize in implementing and managing SASE solutions to ensure the proper configuration, maintenance, and optimization of the system.
  - Integration support: Support integrations between SASE and other service areas with MSSPs' own platforms to enable unified management across SASE and other SOC services.
  - Simplified management: Reduce the complexity of implementing and maintaining SASE solutions, allowing the internal IT/security team to focus on their core business functions.
  - Flexibility: Adapt to changing business requirements with better scalability and flexibility by leveraging MSSPs' infrastructure and resources.
- MSSPs were the 1st to offer managed SASE services and have been leading the adoption of SASE globally. They work closely with SASE, SD-WAN, and SSE vendors to provide managed SASE services. Customers can leverage their extensive networking and security expertise to deploy and manage SASE projects.

Source: Frost & Sullivan

Service Provider Profile—LevelBlue

SASE Infrastructure	SASE Capabilities	SASE Partnerships
• **Number of PoPs:** Utilize PoPs from SASE partners • **Network Backbone:** Global private backbone	• **Security:** NGFW, SWG, ZTNA, CASB, and DLP • **Networking:** SD-WAN	• Palo Alto Networks, Cisco, VMware, Fortinet, Silver Peak, Versa Networks, Zscaler, and Checkpoint

Company Overview

- LevelBlue, previously known as the cybersecurity division of AT&T Business, has transitioned into an independent entity following a joint venture between WillJam Ventures and AT&T. Now operating under the name LevelBlue, the company has been delivering cybersecurity services for over 25 years and AT&T Business has been delivering network services for over 100 years, providing it with the unique position to deliver managed SASE services. LevelBlue has ownership of the managed network security, MDR, and cybersecurity consulting services, making it one of the largest security services providers globally. LevelBlue is also one of the 1st to introduce managed SASE services.

Managed SASE Service Overview

- LevelBlue combines its comprehensive security capabilities with AT&T's networking solutions, managed SD-WAN services, and 5G connectivity services to deliver SASE solutions to businesses. The company aims to provide businesses with improved network performance, lower cost and complexity, enhanced user experience, and higher security efficacy through the combination of SD-WAN, ZTNA, SWG, FWaaS, CASB, and LevelBlue.
- LevelBlue offers a try-before-you-buy SASE service to demonstrate multiple core technologies under the SASE offering using a proof-of-concept (POC) environment. The zero-cost POC offer will showcase how the solution can address customers' business challenges. The dedicated SASE workshops also showcase how the SASE platform can address customers' specific use cases, delivering a mini-managed services experience through a structured engagement and delivery process.
- The company also pairs the SASE offering with its cybersecurity consulting services to support customers along their SASE implementation journey. This includes gap analysis, strategy, roadmap and planning, implementation, and service delivery with support from dedicated SASE consultants, helping customers to plan and shift to SASE or SSE solutions. As a trusted cybersecurity partner for businesses, LevelBlue continues to expand its engineers' expertise by establishing an Expert Engineer role in the United States, Europe, and Asia, providing customers with in-depth expertise in the configuration and detailed design of IT projects. The company has also introduced mini-labs into these engineering teams to make sure they have the knowledge in practice when new software-defined and SASE capabilities become available in the market.
- LevelBlue continued partnership with AT&T and extensive experience in delivering both networking and security services differentiates LevelBlue from other close competitors, making it a trusted partner to support organizations' transition to SASE. The company integrate its security capabilities, including SASE and other security services, with AT&Ts LAN and WAN solutions to automate and orchestrate network and security operations. The company continues to invest in improving automation, correlation, diagnostics, self-servicing, and zero-touch ticker solutions under its Service Assurance.

Recent Development & Future Roadmaps

- In 2022, LevelBlue continued to work with its principal SASE vendors to add new service capabilities as they expand their SASE platform features.
- The company is also developing an overlay customer service and operations management platform built atop the LevelBlue USM Anywhere platform. This platform will focus on centralizing data sharing and integration across all service offerings via a unified dashboard, improving operations and the customer experience.

Note: www.levelblue.com.

Source: LevelBlue; Frost & Sullivan

Growth Opportunity Analysis—North America

Growth Metrics

SASE: Key Growth Metrics, North America, 2022

Life Cycle Stage	Revenue	Revenue for Last Year of Study Period
Nascent	$793.0 M (2022)	$3,213.8 M (2027)

Base Year Growth Rate	Compound Annual Growth Rate	Number of Competitors	Market Concentration
57.3% (2022)	32.3% (2022–2027)	8 (active competitors in 2022)	73.2% (Revenue share held by top 3 companies)

Note: All figures are rounded. The base year is 2022. Source: Frost & Sullivan

Forecast Analysis

- NA was the largest market and will continue to lead the overall adoption of SASE in the next 5 years, making up more than half of the total market share from 2022 to 2027. The market will maintain a strong CAGR of 32.3% from 2022 to 2027, generating a total revenue of $3,213.8 million by 2027.
- Organizations in NA often lead the rest of the world in technology adoption. The region is also leading the adoption of cloud computing technology globally. Organizations are confident about shifting to the cloud and adopting cloud-delivered services, as all the main CSPs have extensive cloud infrastructure in the region. As a result, NA organizations widely leverage cloud-native technology for improved flexibility, agility, scalability, resiliency, and cost-effectiveness. They are more open to using the cloud-native SASE architecture to support the post-pandemic hybrid working model. Strong cloud adoption, wide acceptance of cloud-delivered services, and the rising need to support distributed workforces will drive SASE adoption among businesses in the region.
- In addition, many organizations have their global headquarters in the region, and facilitating site-to-site connectivity across locations, including branch offices and retail locations, is crucial. This necessity propels businesses to consider secure remote access solutions, such as ZTNA, which provides reliable and secure connectivity for remote users and distributed sites across diverse environments, including the cloud, physical data centers, branch offices, and a hybrid environment.
- Most SASE vendors have extensive coverage of their PoPs in the region, showcasing their strong commitment to boosting SASE businesses. The robust network of SASE PoPs and the strong coverage of cloud regions by CSPs lead to more investment in cloud-native and integrated SASE platforms, as customers can easily comply with data privacy regulations.
- The converged SASE services will continue to gain popularity, as organizations in NA have stronger needs than other regions to transform networking and security architecture to keep pace with digital transformation in today's fast-evolving business landscape. As a result, the adoption of SASE will maintain a strong double-digit growth momentum in the next 5 years.

Source: Frost & Sullivan

Growth Opportunity Analysis—EMEA

Growth Metrics

SASE: Key Growth Metrics, EMEA, 2022

Life Cycle Stage	Revenue	Revenue for Last Year of Study Period
Nascent	$323.6 M (2022)	$1,516.8 M (2027)

Base Year Growth Rate	Compound Annual Growth Rate	Number of Competitors	Market Concentration
61.5% (2022)	36.2% (2022–2027)	8 (active competitors in 2022)	63.4% (Revenue share held by top 3 companies)

Note: All figures are rounded. The base year is 2022. Source: Frost & Sullivan

Forecast Analysis

- EMEA was the second-largest market, and the region will increase its market share to 24.6% in 2027. This region has more stringent requirements for data privacy and residency owing to GDPR enforcement. Organizations, especially those in highly regulated industries or those that store sensitive customer data, are more cautious about cloud-native SASE services. Some of these organizations prefer to adopt the hybrid model, which consists of on-premises hardware appliances and other cloud-delivered services, to better control and manage their data.
- Recognizing the compliance challenges facing EMEA organizations, SASE vendors have put in more effort to increase their PoP coverage in the region to support customers in addressing data governance requirements and provide better service availability and user experience. Major CSPs have also expanded their cloud infrastructure, which will drive stronger cloud adoption and cloud-native SASE services.
- In addition, the acceleration of digital transformation initiatives and the rising requirements to support remote and hybrid work models are also driving the need for ZTNA and broader SASE services. Larger organizations that are more concerned about compliance will prefer to adopt a hybrid deployment of SASE, whereas businesses in the private sector or smaller businesses will be more open to adopting the converged and cloud-native SASE model to modernize their networking and security architecture and support their journey to cloud and digital transformation.
- While EMEA continues to lead in cloud adoption after NA, the investment in SASE will help it to maintain its second-largest position in the next 5 years with a strong CAGR of 36.2% from 2022 to 2027, generating a total revenue of $1,516.8 million by 2027.

Source: Frost & Sullivan

Insights for CISOs

SASE—CISOs' Concerns

Cross-functional Conflicts: How do I encourage communication and collaboration between network and security teams throughout the solution decision-making process?

User Experience: How do I maintain a consistent user experience with the rising volume of remote workers and flexible working arrangements?

Consistency and Seamless Interoperability in the Multi-cloud Environment: Will the SASE adopted in my organization support my cloud migration journey and enforce consistent security and networking policies across different cloud platforms?

Stringent Compliances: How can I comply with data security regulations when I adopt a cloud-native SASE service? Do I have visibility or control over where the data and traffic will be transferred, processed, and stored?

Complexity and Effectiveness: How can the SASE strategy help to reduce operational complexity? Should I opt for a multi-vendor or single-vendor SASE approach?

Lack of Visibility: The complexity of a combination of legacy and modern architecture running in different environments posed greater challenges for CISOs to have visibility into users, devices, and applications in their environment.

Fragmented Products: Networking and security products are disjointed in the legacy data center architecture. The proliferation of cloud computing and mobility drives the need to converge both functions to support a highly distributed workforce and IT environment.

Lack of Expertise: The SASE model is challenging to deploy as it cuts across both networking and security systems. CISOs are concerned about the shortage of in-house security expertise that can help with SASE implementation and ongoing management.

Source: Frost & Sullivan

SASE—Key Trends

- The rise of the distributed workforce has expanded the potential attack surface area.
- Organizations increasingly adopt SASE to provide their work-from-anywhere workforce with secure and seamless access to cloud services, applications, and critical corporate infrastructure.

- Organizations have significantly accelerated their cloud adoption, including hybrid and multi-cloud deployments.
- As a result, they are looking for services that leverage cloud-native infrastructure, such as SASE, that can provide the flexibility to scale their network and security capabilities depending on their evolving business needs.

- Organizations with SASE deployment in place increasingly request further convergence in areas such as endpoint protection, XDR, and IoT security.
- SASE vendors will integrate more comprehensive security measures into their SASE infrastructure.

- The adoption of single-vendor SASE is increasing as it is more operationally efficient.
- This approach helps to reduce the costs and complexity of managing an excessive number of vendors and point solutions.

- Centralized management and orchestration capabilities are 2 vital requirements for SASE deployment.
- Organizations emphasize simplified network administration, easy configuration, centralized monitoring, and consistent policy enforcement across multiple locations.

- Organizations increasingly seek to consolidate their security and networking architectures into 1 converged cloud-native platform.
- The integration of both capabilities helps to improve an organization's operational efficiency, network performance, and overall security posture by enabling a secure network.

Source: Frost & Sullivan

SASE—Insights and Recommendations

CISOs should determine their requirements before selecting a SASE vendor. They need to understand the benefits of different SASE models and select a model that, based on their actual needs, can effectively integrate with their existing network and security architecture investments without re-architecting the whole system.

CISOs should evaluate the SASE architecture that vendors offer to avoid deploying complex and loosely integrated SASE components that do not provide optimized performance and user experience. It is crucial for a SASE solution to provide a single management capability that leverages a single dashboard, a single data lake, and a single control plane.

CISOs should consider a SASE solution with a global presence to support a highly distributed workforce and environment in different locations. SASE vendors must have extensive PoP coverage across regions to support customers regardless of their locations with low latency and high availability.

CISOs should evaluate the SASE vendor's vision, strategy, and roadmap during the decision-making process. This can help ensure the SASE solution can support future services such as 5G, ultra-fast connectivity, and bandwidth-intensive applications when organizations deploy applications at the edge or across multi-cloud platforms.

Source: Frost & Sullivan

Why Frost, Why Now?

Our Expertise

EXPERIENCE	• 60 years of proven global experience • Trusted partner of investors, corporates, and governments
COVERAGE	• Industry convergence through comprehensive coverage • Global footprint to match client needs
ANALYTICS	• Innovation Generator™ driving 6 analytical perspectives • Proprietary growth tools and frameworks
BEST PRACTICES	• Growth Pipeline Engine™ and Companies to Action™ • 10 Growth Processes: Best practices foundation

Client Impact

- **FUTURE GROWTH POTENTIAL:** Maximized through collaboration
- **GROWTH PIPELINE™:** Continuous flow of growth opportunities
- **GROWTH STRATEGIES:** Proven best practices
- **INNOVATION CULTURE:** Optimized customer experience
- **ROI & MARGIN:** Implementation excellence
- **TRANSFORMATIONAL GROWTH:** Industry leadership

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, write to: permission@frost.com