Market Guide for Single-Vendor SASE

Published 28 September 2022 - ID G00768660 - 25 min read

By Neil MacDonald, John Watts, **and 2 more**

Single-vendor SASE delivers converged network and security capabilities to connect and secure distributed users, devices and locations to resources in the cloud, edge and on-premises. Infrastructure and operations leaders should use this research to analyze the emerging single-vendor SASE market.

Overview

Key Findings

- The market for well-architected single-vendor SASE offerings is immature but developing quickly, and SASE interest among our clients has been growing rapidly.
- Multiple providers now have a single-vendor SASE offering; but few offer the required breadth and depth of functionality with integration across all components, a single management plane, and unified data model and data lake.
- Most leading SD-WAN vendors have added a cloud-based security stack to build out a single-vendor SASE, and a few security service edge (SSE) vendors have acquired SD-WAN to deliver single-vendor SASE.
- There are three primary options for SASE adoption — a single-vendor offering, explicit pairing of two vendors (one for network services, one for security services), and managed SASE.
- Demand for single-vendor SASE tends to come from: smaller enterprises that don't have

strongly siloed network and security teams and don't require best of breed across all capabilities, and from architecture teams in large global multinationals.

Recommendations

Infrastructure and operations leaders responsible for cloud and edge connectivity strategies should:

- Engage the security organization and establish a cross-functional SASE strategy team to speed the time to value and increase the chances of a successful implementation.
- Choose single-vendor SASE offerings that provide single-pass scanning, single unified console and data lake covering all functions to improve user experience and staff efficacy.
- Evaluate a single-vendor SASE offering, along with two explicitly partnered vendors and managed SASE offerings to provide the most flexibility in selection and timing.
- Have the SASE team rank RFI/RFP requirements based on what is mandatory versus preferred or optional to understand the trade-offs when a single-vendor SASE offering is used; the offering may not be best of breed in all areas.
- Run a functional pilot with real-world users and locations, before selecting a single-vendor SASE offering, to ensure functionality and performance meet requirements.

Strategic Planning Assumptions

By 2025, one-third of new SASE deployments will be based on a single-vendor SASE offering, up from 10% in 2022.

By 2025, 80% of enterprises will have adopted a strategy to unify web, cloud services and private application access using a SASE/SSE architecture, up from 20% in 2021.

By 2025, 65% of enterprises will have consolidated individual SASE components into one or two explicitly partnered SASE vendors, up from 15% in 2021.

By 2025, 50% of new SD-WAN purchases will be part of a single-vendor SASE offering, up from

10% in 2022.

Market Definition

Single-vendor SASE offerings deliver multiple converged network and security as-a-service capabilities, — such as software-defined WAN (SD-WAN), secure web gateway (SWG), cloud access security broker (CASB), network firewalling and zero trust network access (ZTNA) — using a cloud-centric architecture.

SASE supports branch office, remote worker and on-premises general internet security, private application access and cloud service consumption use cases. It is delivered primarily as a service and enables zero trust access based on the identity of the user, device or entity, combined with real-time context (such as device security posture) to enforce and govern security and compliance policies. Single-vendor SASE offerings should have a common management plane and data lake across all capabilities.

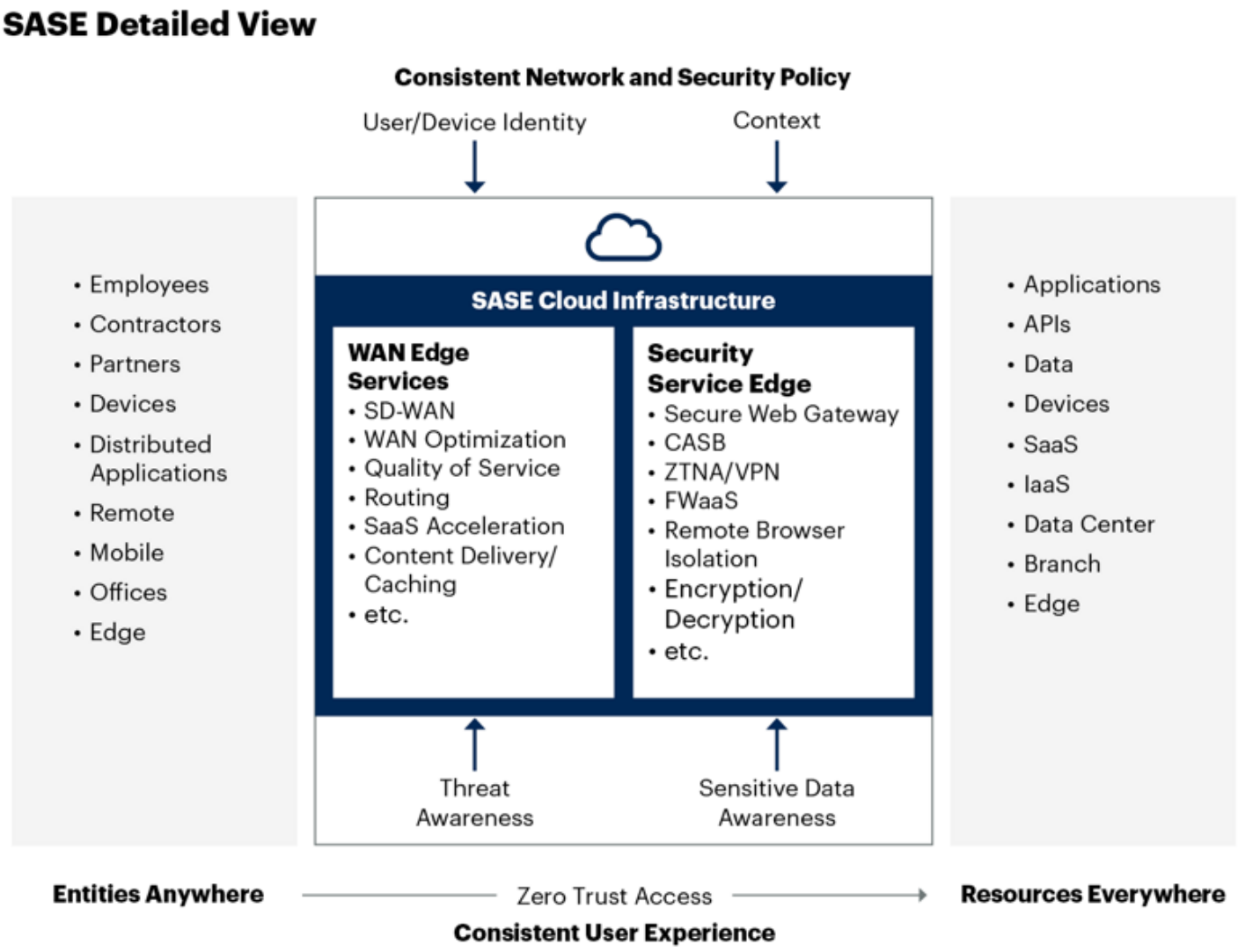
Market Description

The adoption of cloud and edge computing and work-from-anywhere initiatives has radically shifted access requirements. For most organizations, there are now more users, devices, applications, services and data located outside of an enterprise than inside. Attempts to use traditional perimeter-based approaches to securing anywhere, anytime access have resulted in a patchwork of vendors, policies, consoles and complex traffic routing, creating complexity for security administrators and users.

What is needed is an identity-aware and context-aware network and security access fabric that connects users, devices and locations everywhere (see the left side of Figure 1) to the enterprise's digital resources anywhere (see the right side of Figure 1).

Delivering this anywhere, anytime access to any user, device or location requires a cloud-centric SASE capability. A complete SASE offering (see the blue box at the center in Figure 1) combines network edge capabilities, most notably SD-WAN, and a set of cloud-centric security service edge (SSE) capabilities, most notably SWG, CASB and ZTNA.

Figure 1: Secure Access Service Edge — Detailed View



Source: Gartner
768660_C

Gartner

SASE provides hybrid workers, devices and locations anywhere secure access to digital resources everywhere — in private applications (on-premises or cloud-based), SaaS and the internet. To adopt a SASE architecture, we see enterprises in one of three primary planning and buying motions:

- Some customers prefer a self-managed, single-vendor SASE, with a single purchase order for both networking and security components and support services. This is the focus of this

Market Guide.

- Some customers — those with separate networking and network security teams, or that have already deployed an SD-WAN (or managed SD-WAN) and/or SSE provider — may select different vendors for the other components and look to purchase a separate offering, ideally integrated through an explicit partnership.
- Some customers prefer a single vendor to deliver SASE capabilities as a managed service — typically organizations with resource constraints that prefer dealing with a single managed service provider.

Sponsorship for SASE typically comes from the CIO, with the ability to tear down organizational silos to enable the vision of a SASE architecture. Many SASE projects are driven by the objective to simplify policy management and enforcement and improve the organization's security posture. Some projects are led by networking and branch office transformation, some are led by security and the need to support a hybrid workforce. Because SASE offerings target both network and network security capabilities, the recommended approach is to form a joint team across networking and security to develop a strategic roadmap for the enterprise adoption of SASE.

Market Direction

Since defining the emerging SASE market in 2019, industry and client interest in SASE has exploded, primarily driven by enterprise needs not being met by existing vendors. End-user client inquiries on SASE grew 89% in 2021, as compared to 2020. Strong end-user interest in SASE and the related market for SSE continues into the first half of 2022 (up 15% as compared to 1H21).

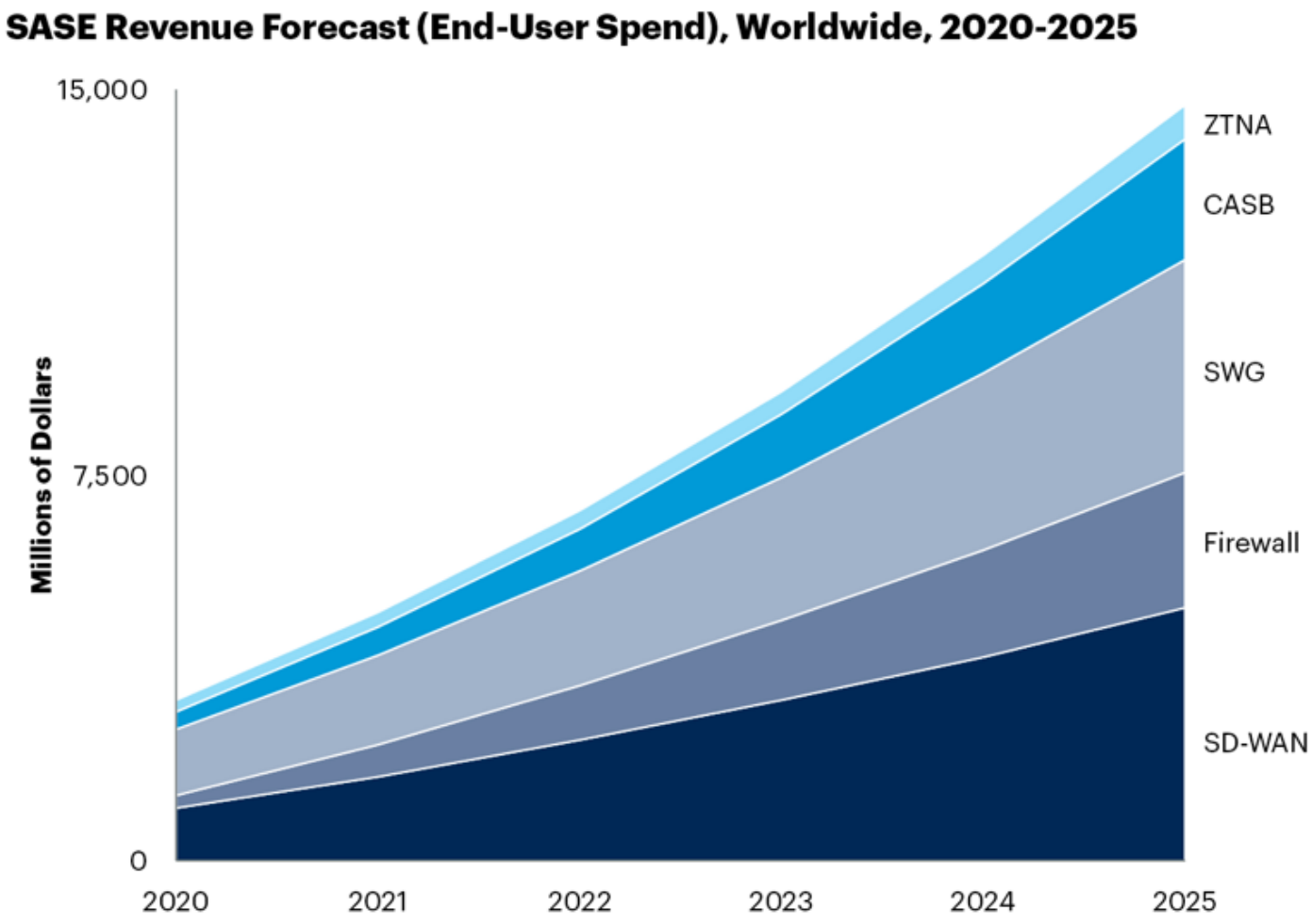
In the 2022 Gartner CIO and Technology Executive Survey, SASE was the third most commonly cited technology investment (deployed or planning to deploy within 12 months) after AI/ML and distributed cloud, respectively, providing further evidence that momentum around SASE is growing among enterprise buyers. [1]

The desire to reduce complexity by consolidating the number of security vendors (see Infographic: Top Trends in Cybersecurity 2022 — Vendor Consolidation) is also driving interest in SASE. The 2022 Gartner Security Vendor Consolidation: XDR and SASE Trends Survey data indicates a clear customer preference to consolidate vendors in the security space, with 92% of enterprises

indicating they will be actively pursuing a vendor consolidation strategy by year-end 2022. [2] In the same survey, over one-third of respondents indicated they will have SASE implemented by the end of 2022, and 75% of respondents either have or will have SASE deployed by 2024 or later. [2]

All of this is expected to lead to significant growth in the SASE market over the next several years. Our Forecast Analysis: Secure Access Service Edge, Worldwide indicates that over the next four years, the SASE market will grow at a CAGR of 32%, reaching almost $15 billion by 2025 (see Figure 2).

Figure 2: SASE Revenue Forecast



Market Analysis

As with any technology category, SASE has been subject to an immense amount of marketing hype and abuse, where vendors market SASE but don't meet Gartner's minimum requirements. Gartner has been consistent in its core and recommended SASE capabilities since we first introduced the concept in 2019 (see Table 1).

Table 1: SASE Core and Recommended Capabilities

SASE Core Capabilities	SASE Recommended Capabilities
• Secure web gateway • Cloud access security broker • Zero trust network access • Software-defined WAN • Network firewalling services • Sensitive data and malware inspection • Line rate operation	• Remote browser isolation • Network sandbox • DNS protection • API-based access to SaaS for data context and configuration information • Support for managed and unmanaged devices • Web application and API protection • Enhanced internet and/or private backbone transport • Content delivery network • External DNS services • Cloud onramp (simplified and automated integration with public cloud networking services)

Source: Gartner (September 2022)

The capabilities in Table 1 should be cohesive. A well-architected single-vendor SASE offering should have the following characteristics:

- **Integrated**

- All services fully integrated, not loosely coupled independent modules (typically resulting from a vendor's internal silos, poorly integrated OEM'd component or one added during an acquisition)
- A single data lake and unified data model for storing relevant log and event information (the logs may be stored regionally for data residency and compliance reasons)
- Integrated advanced analytics across all channels to help with usage and risk identification capabilities

- **Unified management and policy**
  - A single unified management plane to reduce switching between multiple consoles, not disparate management systems loosely integrated via API
  - Single security policy for malware/sensitive data inspection across all channels
  - A multitenant cloud-based management control plane

- **Unified and scalable architecture**
  - An elastic architecture (dynamic scale up/down) built using small units of loosely coupled code (typically microservices)
  - Single-pass scanning for malware/sensitive data (may be parallelized)
  - A software-based, hardware-neutral architecture for flexibility in policy inspection placement
  - In-line encryption/decryption that scales, ideally without requiring hardware

- **Flexibility and ease of use**
  - Simplified consumption-based billing, based on user/device as a subscription service
  - Globally distributed points of presence (POPs) so policy enforcement can be as close as possible to remote workforce and branch locations
  - The option for single tenancy (for security-sensitive use cases)

- Options for customer-controlled inspection points for security-sensitive use cases (for example, performing inspection on-premises versus in the SASE provider's cloud)

A single-vendor SASE must own or directly control (OEM, not service chain with a partner) each of the capabilities in the core category (see Table 2).

Table 2: Single-Vendor SASE — Core Requirements for Various Functionalities

SWG Functionality Core Requirements	CASB Functionality Core Requirements	ZTNA Functionality Core Requirements	SD-WAN Functionality Core Requirements
• Integrated URL filtering and categorization • Integrated malicious URL protection from a continuously updated threat intelligence feed • The ability to scan for malware on content/attachments being handled	• In-line SaaS application discovery and categorization • Integrated SSO with third-party identity providers • Visibility and control based on policy for SaaS application access • Conditional access based on location and device security posture • In-line content inspection and control	• Contextual access control (identity- and context-based) • Integrated SSO with third-party identity providers • Policy-based access to specified applications (least privilege), not network-level access • Removal of enterprise application assets from visibility on the network, and access only allowed after a user and/or device is	• Dynamic path selection (traffic steering) based on business or application policy • Support for multiple active physical links simultaneously • Centralized policy and management of appliances and support for zero-touch configurations • Site-to-site VPN capabilities • Basic firewalling

	for sensitive data and malware	authenticated and explicitly authorized to access the application	functionality • Routing, including support for Border Gateway Protocol (BGP) • Native support for granular customer-managed configuration of SD-WAN, including traffic steering

Source: Gartner (September 2022)

Even in this adolescent phase of the SASE market, there are multiple single-vendor SASE offerings in the market that meet these core requirements. Vendors of these offerings are listed in Table 3. In addition, several vendors are quite close to delivering a single-vendor SASE offering, but did not meet all of our selection criteria at this time.

Since single-vendor SASE vendors have different starting points (some were SD-WAN vendors adding security, some were security vendors adding SD-WAN), no single vendor is best of breed in every capability. For this reason, it is critical that the joint network/network security teams agree on which capabilities they will consider to be required versus recommended in their evaluation in a single-vendor approach. For example, a highly regulated online finance company with thin branch requirements for pop-up locations might mark advanced SD-WAN features as optional, and FWaaS and robust sensitive data security controls as required.

Multivendor SASE Using Explicit, Functional Vendor Integration

Some organizations pursue the selection of SD-WAN and security services separately, so single-

vendor SASE offerings often can be purchased with SD-WAN only or SSE only and integrated with another vendor. With a multivendor SASE, the functional integration between these potentially two different vendor offerings becomes a critical differentiator. Even single-vendor SASE offerings may not be well-integrated, but the most benefit in multivendor SASE comes from tightly integrated and orchestrated networking and security offerings. A full discussion of multivendor SASE is outside the scope of this research, but examples of multivendor integrations to deliver SASE are listed in Note 3. We have also provided a framework to help enterprises evaluate the strength of integrations (see in Note 4).

Managed SASE

The demand for enterprise SASE capabilities, combined with resource constraints, has created an opportunity for managed SASE offerings. Managed SASE offerings provide a single source for SASE services with a single vendor buying and supporting experience for the enterprise. The managed SASE provider may use a single-vendor SASE or multivendor SASE approach to build their offering. A full discussion of managed SASE offerings is outside the scope of this research, but example providers are listed in Note 5.

Benefits of Single-Vendor SASE Offerings

Adoption of a SASE architecture — whether single-vendor, multivendor or managed — has many benefits (see Note 6). Specific reasons an organization may favor single-vendor SASE are:

- **Improved security posture**
  - Reduces attack surface and shortens remediation times
  - Reduces operational complexity through consolidation of vendors, consoles, policies and contracts, thereby reducing chances of misconfiguration or mistakes
  - Consistently enforces security policy across all access channels: web, cloud services and private applications; the policy can be applied whether the user is on-premises in a branch or working remotely
- **Improved network and security staff efficacy**

  - Reduces deployment time for new users, locations, applications and devices
  - Requires less skills and resources to manage than if using separate vendors for SD-WAN and SSE
  - Eliminates overlapping policies and standardizes application policies and policy objects across SD-WAN as well as security policy enforcement points such as SWG, CASB and firewalls
  - Eliminates redundant capabilities (for example, most SD-WAN vendors also offer firewalling services and a ZTNA agent for remote users)

- **Improved user and administrator experience**
  - Avoids potential latency and performance issues due to traffic routing, forwarding and tunneling between different vendors' SD-WAN POPs and SSE vendor security POPs
  - Implements a single data lake, data model and unified graph database for all event logging, reporting, alerting and relationship mappings
  - Provides a single SLA commitment with reduced opportunity to blame the partner
  - Easier to provide complete end-to-end user experience monitoring from user to resource, regardless of whether the user is in the branch or working remotely

Challenges to Single-Vendor SASE Adoption

- **Organizational silos:** A single-vendor SASE implementation requires a coordinated and cohesive approach across network security and networking teams. Traditionally, these teams have operated separately with different vendor allegiances.
- **Existing investments:** Enterprise transition to a single-vendor SASE architecture will take time, as enterprises have investments in hardware and software with time and value remaining. Hardware refresh cycles at branch offices average four to seven years.
- **Skills gaps:** Relationships and staff expertise with incumbent vendor offerings introduce a learning curve for migration when a single vendor is used and an incumbent network or network security vendor is replaced. Organizations must cross-train and upskill existing team members

from traditional, low-level policies/controls based on IP address, to implementing and troubleshooting more abstract policy definitions enforced by the SASE technology stack.

- **Global coverage:** SASE depends upon cloud-delivery, and a single vendor's POP footprint may prevent deployments in certain geographies — such as China, Russia and the Middle East, where a vendor may have limited cloud presence. Further, customers are increasingly demanding more control of how and where the traffic and data are handled.

- **Maturity:** For the next several years, single-vendor SASE capabilities will vary widely. For example, sensitive-data visibility and control is often a priority capability, but it is difficult for many SASE vendors to address. Another example is API-based CASB capabilities to augment in-line inspection. This is needed for full visibility and control of sensitive data, but several single-vendor SASE vendors don't yet offer this. Your preferred single-vendor SASE may lack the capabilities you require in the short term, leaving two-vendor explicit partnerships as the most viable approach.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Introduction

Network operations and network security leaders looking to support the anywhere, anytime access requirements of a distributed, hybrid workforce (including branch offices and edge locations) should consider SASE as an integrated, cloud-centric solution. SASE can improve the end-user experience by enabling the same access to digital capabilities, regardless of their location or the location of the application they are accessing.

SASE can help organizations adopt a zero trust security posture by applying consistent identity- and context-based policies, regardless of the type of resource the user is accessing (internet, cloud services, private applications). Security policy management can be simplified by applying the same inspection mechanisms for sensitive data and malware across all access mechanisms and by shifting toward identity-centric policies rather than network location.

Table 3 lists representative vendors selected based on the requirements stated in Note 1.

Table 3: Representative Vendors in the Single-Vendor SASE Market

Vendor	Headquarters	Offering
Cato Networks	Tel Aviv, Israel	Cato SASE Cloud
Cisco	San Jose, California, U.S.	Cisco+ Secure Connect
Citrix	Fort Lauderdale, Florida, U.S.	Citrix Secure Internet Access with Citrix SD-WAN
Forcepoint	Austin, Texas, U.S.	Forcepoint ONE with FlexEdge Secure SD-WAN
Fortinet	Sunnyvale, California, U.S.	FortiSASE
Netskope (Infiot)	Santa Clara, California, U.S.	Netskope SASE
Palo Alto Networks	San Jose, California, U.S.	Prisma SASE
Versa Networks	Santa Clara, California, U.S.	Versa SASE
VMware*	Palo Alto, California, U.S.	VMware SASE

> * In May 2022, Broadcom announced its intent to acquire VMware. The deal has not yet closed (for details, see Note 7).

Source: Gartner (September 2022)

Market Recommendations

Strategy and Planning

- Invest in SASE to support the secure anywhere, anytime access requirements of a modern hybrid digital workforce and workplace.
- Create a unified SASE project team consisting of networking and network security to develop the enterprise strategic roadmap for SASE adoption.
  - Establish a vision for the “branch of the future” that includes thin branch and heavy cloud SASE architecture.
  - Leverage branch office transformation, hybrid WAN and MPLS offload projects to adopt SASE for security services.
- Leverage WAN, firewall or SD-WAN refresh cycles to update network and network security architectures to SASE.
- Consolidate vendors to cut complexity, simplify security policy enforcement, move to a zero trust security posture and improve the end-user hybrid work experience. There is also the potential to reduce duplicative costs of point solutions as contracts renew for SWG, CASB and ZTNA offerings.
- Plan strategically and act tactically, even a use case at a time. Enterprises can start their SASE journey today by adopting SD-WAN and SSE (even just starting with ZTNA) independently without requiring the same vendor for both. At a future point, when functionality gaps have been addressed and new use cases emerge, consolidation to a single-vendor SASE may be considered.
- Prepare for continued market technology changes and acquisitions by choosing offerings that have broad market potential and maintaining a fallback strategy in the event of a

merger/acquisition.

Evaluation

- Have the joint network/security team identify and rank the enterprise functionality requirements into required, preferred and optional before sending out requests for information/purchase, as no single vendor is best of breed in all SASE capabilities as yet.
- Be open to single-vendor SASE, explicitly partnered vendors or managed SASE offerings during the evaluation process to provide the most flexibility.
- Prefer SASE offerings that use a unified management plane, unified security plane with a single data lake, and support single-pass decryption and inspection for malware and sensitive data.
- Strive for not more than two vendors for all core services to minimize complexity and improve performance.
- Run a functional pilot with real users and remote locations before selecting a single-vendor SASE offering to ensure functionality and performance meet your requirements.
- Focus pricing negotiations using the same priority ranking, as single-vendor SASE offerings often have individual licenses to negotiate.

Deployment

- Deploy ZTNA to augment or replace legacy VPN to limit investment in legacy technology. Prioritize the shift of contractor and third-party access to a zero trust access security posture.
- Adopt universal ZTNA by applying zero trust access principles for all types of access whether or not the user is remote.
- Extend a zero trust security posture using ZTNA to support inbound and outbound communications for headless devices (without a user) such as IoT/OT, industrial control system (ICS) and cyber-physical systems (CPS), where agents typically cannot be deployed and no traditional user context is available to enforce access policies.
- Combine branch office and remote access in a single implementation to ensure consistent

policies and minimize the number of vendors required.

- For enterprises where mergers and acquisitions are common or planned, quickly onboard or migrate new entities to the SASE platform to reduce redundancies and retire legacy approaches to security.

Evidence

[1] **2022 Gartner CIO and Technology Executive Survey.** This survey was conducted to help CIOs and technology executives adopt business composability as a means to thrive during periods of volatility and uncertainty. It was conducted online from 3 May through 19 July 2021 among Gartner Executive Programs members and other technology executives. Qualified respondents were each the most senior IT leader (CIO) for their overall organization or a part of their organization (for example, a business unit or region). The total sample was 2,387, with representation from all geographies and industry sectors (public and private). Disclaimer: Results do not represent global findings or the market as a whole, but reflect sentiment of the respondents and companies surveyed.

[2] **2022 Gartner Security Vendor Consolidation XDR & SASE Trends Survey.** This study was conducted to determine how many organizations are pursuing vendor consolidation efforts, what the primary drivers are for consolidation, expected or realized benefits of vendor consolidation, and how those who are consolidating are prioritizing their consolidation efforts. A primary purpose of this survey was to collect objective data on extended detection and response (XDR) and secure access service edge (SASE) for consolidation of megatrend analysis.

The research was conducted online during March and April 2022 among 418 respondents from North America (U.S., Canada), Asia/Pacific (Australia, Singapore) and EMEA (France, Germany, U.K.). Results were gathered from respondents with $50 million or more in 2021 enterprisewide annual revenue. Industries surveyed included manufacturing, communications and media, information technology, government, education, retail, wholesale trade, banking and financial services, insurance, healthcare providers, services, transportation, utilities, natural resources, and pharmaceuticals, biotechnology and life sciences. Respondents were screened for job title, company size, job responsibilities to include information security/cybersecurity and IT roles, and primary involvement in information security.

Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[3] Zscaler + Network and UCaaS Partners, Zscaler.

[4] Zscaler + Aruba, Zscaler.

[5] Zscaler + Cisco SD-WAN, Zscaler.

[6] Zscaler and VMware, Zscaler.

[7] VMware SD-WAN With Zscaler Cloud Security, VMware.

[8] Partner Finder, HPE (Aruba).

[9] Technology Alliances, iboss.

[10] Technology Partners & Integrations, Netskope.

[11] Integrate Third-Party SD-WANs with Prisma Access, Palo Alto Networks.

[12] SSE SD-WAN Integrations, Skyhigh Security.

Note 1: Representative Vendor Selection

To develop the list of representative vendors, we used the core and recommended capabilities and characteristics described in the Market Analysis section of this research, along with the following guidelines:

- The vendor must have a generally available single-vendor SASE offering as of 1 September 2022, with active, paying enterprise customers.
- The vendor must sell and actively market SASE directly to enterprise customers to set up, maintain and configure themselves (not as a service) as evidenced by public materials such as a vendor website, blog or official social media account.

- The SD-WAN capabilities must be technology directly owned or controlled by the single vendor and must meet Gartner's definition of SD-WAN (see Magic Quadrant for SD-WAN).
- The security services capabilities must be technology owned or controlled by the single vendor and must include at least ZTNA, SWG and a basic CASB capability. Malware-scanning signatures, URL categorization and threat intelligence feeds may be licensed from a third party.
- At a minimum, the network and network security services must be integrated from an auto-provisioning and tunnel creation perspective.

Note 2: Gartner's Initial Market Coverage

This Market Guide provides Gartner's initial coverage of the market and focuses on the market's definition, rationale and dynamics.

Note 3: Examples of Partnerships and Integrations Between SD-WAN and SSE Providers to Deliver SASE

Zscaler is an excellent example of an SSE provider with multiple partnerships, offering different levels of integration. For example, Zscaler's integrations include: Arista Networks; Aryaka; Citrix; Cradlepoint; FatPipe Networks; Fortinet; Infovista; Juniper; Lancom; ngena; Nokia (Nuage Networks); Oracle; Palo Alto Networks Prisma SD-WAN (formerly CloudGenix); Riverbed [3]

Zscaler provides greater details on integrations with some partners:

- HPE (Silver Peak) [4]
- Cisco SD-WAN (Viptela) [5]
- VMware SD-WAN (VeloCloud) [6]

Moreover, even though VMware has its own single-vendor SASE offering, VMware SD-WAN tightly integrates with Zscaler Cloud Security. [7] This shows bidirectional commitment to integration from both vendors (from Zscaler to VMware, and from VMware to Zscaler).

Other examples of SD-WAN and SSE providers with partnerships are:

- HPE (Aruba) [8]
- iboss [9]
- Netskope [10] — although it now has its own SD-WAN offering, it also lists SD-WAN partners for its SSE offering
- Palo Alto Networks [11] — although it has its own single-vendor SASE offering, its SSE offering, Prisma Access, lists partners
- Skyhigh Security [12] — provides specific partner integration configuration guidance

We recommend organizations use the framework in Note 4 to evaluate the integration strength of partnerships.

Note 4: Evaluating Strength of Multivendor SASE Integrations

Our six-level framework helps you evaluate the strength of multivendor SASE offerings:

- **Basic/Limited**

The two vendors interoperate with each other through the creation of a tunnel or route between the two offerings using standard protocols such as IPsec. This is commonly supported by most vendors and is a baseline capability for any SASE implementation.

- **Validated or Co-certified**

Validated: The existence of a documented standard design and implementation guide (validated design guide [VDG]) that includes reference configurations. If deployed according to the VDG, the solution will be supported by the vendor providing the validation guide.

Co-certified: The existence of a VDG that is co-certified and supported by both vendors.

- **Installation and Console Automation**

Turnkey automation of validated or certified configurations. This automation must be natively included in the vendor's management console, fully GA and commercially supported by the vendor (not reliant on "community") plug-ins. For example, the automatic provisioning of services and creation of tunnels from the management consoles of different vendors.

- **Management Plane Integration**

The vendors pull relevant information about each other's management plane such as telemetry, up/down status and performance; this aids in troubleshooting. This integration must be natively included in the vendor's management plane and commercially supported. This capability must allow a reasonable portion of Vendor 1's solution to be managed via Vendor 2, including common management tasks. Manual configuration of basic Simple Network Management Protocol (SNMP), or DIY API-level integration that is available to any external party, is not part of this.

- **Basic Data Plane Integration**

The two vendors have integrated their networks and POPs for optimized connectivity and routing between their joint customers.

- **Data Plane Intelligence**

The two vendors share information that can alter or steer traffic routing in an automated fashion. For example, if Vendor 1's POPs are overloaded, it can redirect Vendor 2 to send to another POP. This is the most advanced level of integration and well beyond basic failover/fallback.

Note 5: Example Providers of Managed SASE

- Aryaka
- AT&T
- BT

- Comcast
- Deutsche Telekom
- Expereo
- Horizon Telecom
- KDDI
- Lumen
- MetTel
- NTT Group
- Open Systems
- Orange Business Services
- Telefónica
- Telstra
- Verizon
- Windstream Communications

Note 6: General Benefits of All SASE Offerings — Single-Vendor, Multivendor and Managed

- Increases visibility, agility, resilience and security, particularly for distributed organizations with hybrid workforce and strong cloud services adoption.
- Simplifies delivery and operation of critical network and network security services through primarily a cloud-delivered model.
- Enables the “branch office of one,” anywhere hybrid worker.
- Helps to move toward a zero trust security posture where access is continuously assessed

using identity and other elements of critical context, not just physical location.

- Improves and ensures consistent application and security access policy user experience, regardless of users' location and device.
- Provides support for granting access to protected resources by managed and unmanaged devices used by the internal and extended workforce.
- Shifts network and security skills from managing boxes to policies supporting the digital workforce.

Note 7: VMware Acquisition by Broadcom

The VMware SASE security stack is OEM'd from Menlo Security, run and controlled by VMware and hosted in the VMware SD-WAN (previously VeloCloud) POPs. In May 2022, Broadcom announced its intent to acquire VMware. The deal has not yet closed. Symantec (previously acquired by Broadcom) also has an SSE security stack. The overlap in security stacks and implications for VMware's single-vendor SASE offering are discussed in more detail in Quick Answer: How Will the Broadcom Acquisition of VMware Affect Existing SASE Customers?