Magic Quadrant for Single-Vendor SASE

3 July 2024 - ID G00800940 - 27 min read

By Andrew Lerner, Neil MacDonald, **and 2 more**

The single-vendor SASE market remains dynamic, with more viable vendors and offerings now available. I&O leaders responsible for networking should work with their security colleagues and use this research to cut through marketing hype when selecting vendors.

Strategic Planning Assumption

- By 2027, 65% of new software-defined wide-area network (SD-WAN) purchases will be part of a single-vendor SASE offering, an increase from 20% in 2024.

Market Definition/Description

This document was revised on 17 July 2024. The document you are viewing is the corrected version. For more information, see the ***Corrections*** page on gartner.com

Gartner defines single-vendor secure access service edge (SASE) offerings as those that deliver multiple converged-network and security-as-a-service capabilities, such as software-defined wide-area network (SD-WAN), secure web gateway (SWG), cloud access security broker (CASB), network firewalling and zero trust network access (ZTNA). These offerings use a cloud-centric architecture and are delivered by one vendor.

SASE securely connects users and devices with applications. It supports branch office, remote worker and on-premises general internet security, private application access and cloud service consumption use cases.

Must-Have Capabilities

The must-have capabilities for this market include the following functionalities, primarily delivered as a cloud service:

- Secure web access via proxy
- In-line SaaS visibility and access controls
- Identity-, context- and policy-based secure remote access to private applications
- A branch appliance that supports dynamic traffic steering out of multiple physical, locally attached WAN interfaces, with steering based on applications (not just IPs/ports)
- Firewalling to secure traffic bidirectionally across networks
- Centralized management that covers all of the above capabilities of the offering (with both GUI and API) enabling visibility, troubleshooting, reporting and enables granular configuration and policy changes

Standard Capabilities

The standard capabilities for this market include:

- Unified management delivered by a single console covering all capabilities of the offering (with GUI and API) enabling visibility, troubleshooting, reporting, and enabling granular configuration and policy changes
- The ability to secure end-user browsing via RBI or a secure enterprise browser
- Sensitive data visibility and control

Optional Capabilities

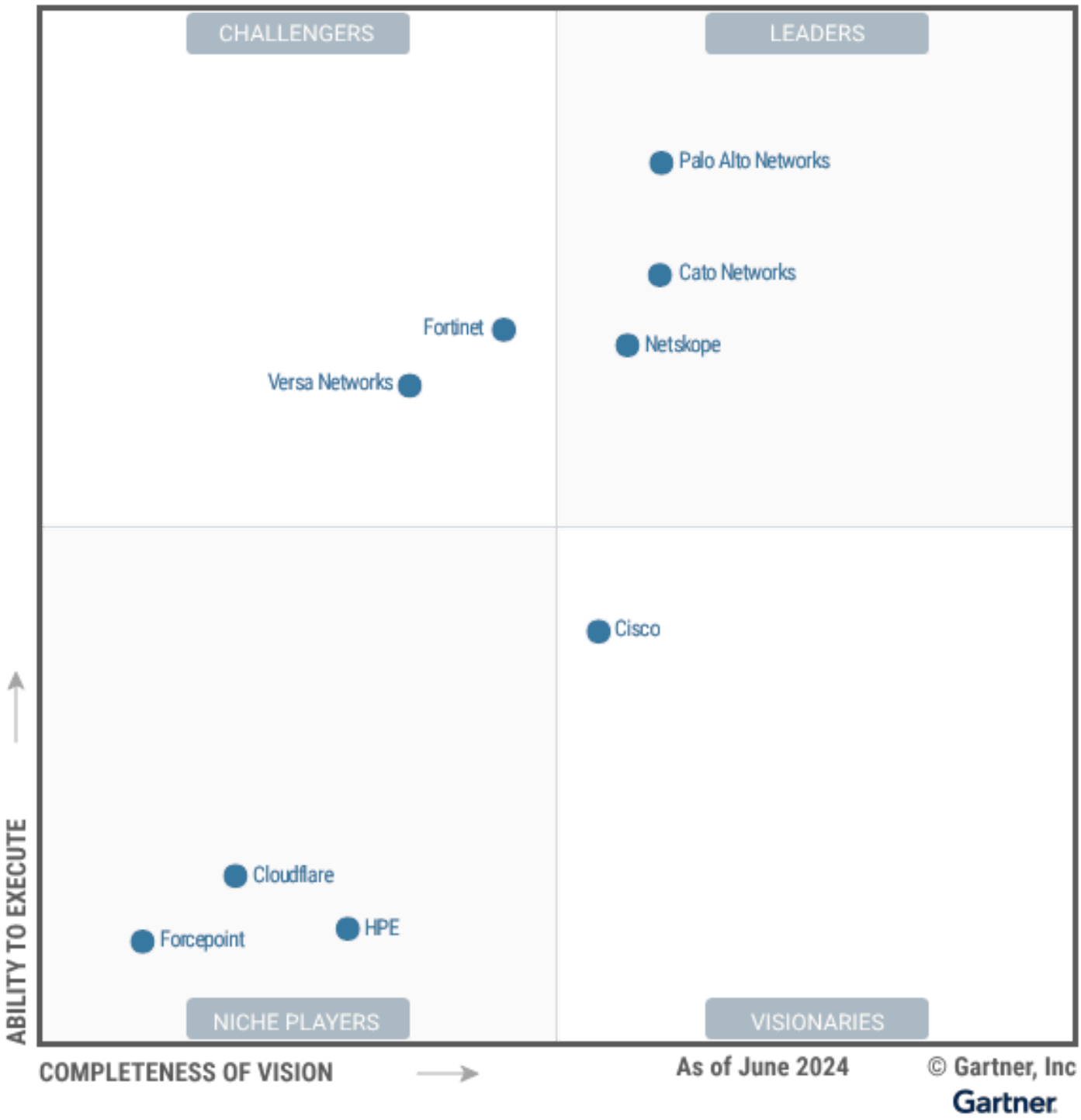
The optional capabilities for this market include:

- Security capabilities, such as network sandboxing, DNS protection, SaaS security posture management (SSPM), API-based access to SaaS for data context and configuration information, application layer visibility and protection, and continuous adaptive risk scoring.
- Advanced network functionality, including enhanced internet, private backbone transport, content delivery networks, external DNS services, cloud onramps (simplified

and automated integration with public cloud networking services), or advanced branch networking features

Magic Quadrant

Figure 1: Magic Quadrant for Single-Vendor SASE



Vendor Strengths and Cautions

Cato Networks

Cato Networks is a Leader in this Magic Quadrant. Its primary offering in this market is Cato SASE Cloud, which is a unified SASE platform. Its operations are primarily in North America, Europe and Asia. Its SASE customers tend to be all sizes but with a concentration in midsize enterprises. We expect the vendor to make future investments in this market, focused on simplifying security policy management, leveraging AI and enhancing its on-premises security.

Strengths

- The vendor provides a single, straightforward UI that is delivered via a unified platform.
- Cato was an early pioneer that helped drive the market, and its planned innovations are likely to continue to shape the market.
- The vendor delivers above-average customer experience compared to other vendors in this research.

Cautions

- Gartner clients report frustration with the vendor's pricing model, as sales proposals can be high and/or difficult to understand. Costs are related to site bandwidth, which can lead to large increases when site bandwidth upgrades are required.
- The vendor's geographic strategy lags competitors, due to limited localization of documentation and technical support, and its sovereign processing approach.
- Some of Cato's security capabilities are limited, including SaaS control and visibility, and on-premises firewalling.

Cisco

Cisco is a Visionary in this Magic Quadrant. Its primary offering in this market is Cisco Secure Connect, which includes the Meraki dashboard to manage cloud-based security services and Meraki SD-WAN appliances. ThousandEyes is optional for advanced digital experience monitoring. Cisco's operations are on a global basis and its Secure Connect customers tend to be midmarket and enterprises. We expect the vendor's future investments in this market to focus on extending SASE functionality further into campus and branch network infrastructure, and using AI to simplify operations.

Strengths

- The Meraki dashboard is straightforward and intuitive to use, and familiar to existing Meraki customers.
- Cisco has a solid product roadmap for Secure Connect that is aligned with emerging customer requirements.
- Cisco has robust channels to market and a large existing installed base of customers, which helps it serve a range of customers on a global basis.

Cautions

- At the time of evaluation, Cisco Secure Connect had product limitations compared to other offerings, most notably in the ability to secure private applications, secure SaaS, and enable adaptive access.
- For many customers, Cisco leads with other offerings besides Secure Connect. This can confuse customers and/or drive suboptimal investments.
- The vendor's footprint of points of presence (POPs) for Secure Connect lags most competitors in this research.

Cloudflare

Cloudflare is a Niche Player in this Magic Quadrant. This is the first year the vendor met our inclusion criteria. Its primary offering in this market is Cloudflare One, which is a unified SASE platform. Its operations are on a global basis and its SASE customers tend to be all sizes but with a concentration in SMBs and midsize enterprises. We expect the vendor's future investments in this market to focus on enhancing the automation of its data security and extending its SASE functionality into public cloud environments.

Strengths

- Cloudflare has the most robust geographic distribution of POPs of any vendor in this research, which helps to address current and future customer needs on a global basis.
- Cloudflare has a simple and intuitive UI underpinned by a single unified platform.
- Cloudflare has strong experience with smaller customers, including SMBs and midsize enterprises.

Cautions

- Cloudflare's local SD-WAN and firewall capabilities within a branch are very limited compared to other vendors in the research.
- Cloudflare was late to enter the market with its branch appliance, and consequently has less experience in full SASE implementations than others in this research.
- The vendor's enterprise SASE pricing is much higher than other vendors assessed in this research.

Forcepoint

Forcepoint is a Niche Player in this Magic Quadrant. Its primary offering in this market is Forcepoint ONE SASE, which includes Forcepoint ONE for security services integrated with FlexEdge Secure SD-WAN appliances. Its operations are primarily in Asia, North America, South America and Europe, and its SASE customers tend to be enterprises and large enterprises. We expect the vendor's future investments in this market to focus on data security and improving its agent.

Strengths

- Forcepoint ONE offers strong security functionality.
- Forcepoint's roadmap is well-aligned with customers who prioritize data security.
- Forcepoint offers flexibility to deliver security either on-premises or cloud-delivered.

Cautions

- The vendor's customer experience lags other vendors in this research.
- The vendor has low customer adoption and limited visibility among Gartner clients, which could hinder its ability to grow in the market.
- Forcepoint's sales and marketing strategies lag most competitors in this research, which could limit its ability to grow in the market.

Fortinet

Fortinet is a Challenger in this Magic Quadrant. Its primary offering in this market is FortiSASE integrated with FortiGate Secure SD-WAN appliances. Its operations are on a global basis and its SASE customers tend to be all sizes. We expect the vendor's future

investments in this market to include using AI to improve operations and bringing additional Fortinet products into the FortiSASE offering.

Strengths

- Fortinet provides excellent value in terms of features versus cost, and its BOMs are the simplest of any vendor in this research.
- Fortinet has a solid product roadmap that is aligned with the emerging requirements of customers.
- Fortinet provides strong SD-WAN and firewall functionality.

Cautions

- POP selection can create confusion and/or lead to suboptimal investment because Fortinet has two types (Fortinet-owned or Google-based) that are not interchangeable, have different price points and different geographic footprints.
- The vendor's planned innovations are unlikely to disrupt the market and reshape customer expectations.
- Fortinet's customer experience lags most competitors in this research.

HPE

HPE is a Niche Player in this Magic Quadrant. This is the first year HPE met the inclusion criteria for this Magic Quadrant. Its primary offering in this market is HPE Aruba Networking Unified SASE, which includes HPE Aruba Networking SSE cloud security integrated with EdgeConnect SD-WAN appliances. The vendor also offers EdgeConnect SD-Branch to address specific customer use cases. Its operations are on a global basis (although limited in Africa) and its SASE customers tend to be all sizes. We expect the vendor's future investments in this market to focus on filling out the portfolio, simplifying product operations, and extending SASE further into branch network infrastructure and network access control (NAC) use cases.

Strengths

- The vendor has strong SD-WAN and ZTNA capabilities.
- The vendor has planned innovations that could drive the market, including extending SASE to address customers' campus and NAC needs.

- The vendor delivers a good customer experience, compared to other vendors in this research.

Cautions

- The vendors' security functionality — including SaaS control/visibility, data security, threat protection and web proxy — lag most vendors in this research.
- Because HPE was late to enter the market, it lacks experience and is behind in terms of POP coverage and security features.
- HPE's geographic strategy lags other vendors in this research based on limitations in localization, regional certifications and sovereign processing approach.

Netskope

Netskope is a Leader in this Magic Quadrant. This is the first year the vendor met the inclusion criteria for this Magic Quadrant. Its primary offering in this market is Netskope One SASE, which includes Netskope's cloud security services, Borderless SD-WAN appliances, Netskope One Client and NewEdge POPs. Its operations are global (although limited in Africa) and its SASE customers tend to be enterprises or large enterprises. We expect the vendor's future investments in this market to focus on edge computing use cases.

Strengths

- The vendor has strong customer experience as expressed by Gartner clients during inquiries.
- Netskope has a strong geographic strategy compared to other vendors based on its geographic coverage, localization, regional certifications and sovereign processing approach.
- The vendor has strong feature breadth and depth for both networking and security.

Cautions

- Administrators must use multiple consoles to access the full functionality of the platform.
- Netskope was late to enter the market with a generally available (GA) product, and thus lacks experience compared to some other vendors assessed.

- There is limited financial information available about the vendor, which creates uncertainty over its long-term viability.

Palo Alto Networks

Palo Alto Networks is a Leader in this Magic Quadrant. Its primary offering in this market is Prisma SASE, which is a unified SASE platform. Its operations are on a global basis and its SASE customers tend to be enterprises and large enterprises. We expect the vendor's future investments in this market to focus on browser security and security policy automation.

Strengths

- The vendor has strong security and networking features, delivered via a unified platform.
- The vendor has a proven track record in this market, and a sizable installed base of customers.
- The vendor has strong financial viability and customer awareness, which should help it grow in the market.

Cautions

- Based on customer feedback and Gartner's analysis, Palo Alto's offering is expensive compared with most of the other vendors in this research.
- The vendor has limited support for non-English UIs, documentation, and technical support compared to most vendors in this research.
- The vendor's new Strata Cloud Manager is less intuitive than its previous user interface.

Versa Networks

Versa Networks is a Challenger in this Magic Quadrant. Its primary offering in this market is Versa Secure Access Fabric (VSAF), which is a unified SASE platform. The vendor also has a secondary offering, Titan, which addresses specific use cases. Its operations are primarily in Asia, North America and Europe, and its SASE customers tend to be enterprises and large enterprises. We expect the vendor's future investments in this market to focus on improved security policy automation and extending SASE to the LAN, cloud and data center.

Strengths

- Versa has strong feature depth across networking and most security.

- VSAF is a unified SASE platform with a single management console.
- The vendor offers strong price/feature value for customers.

Cautions

- The quality of the vendor's technical product documentation is poor.
- Gartner assesses that Versa's planned product enhancements lag competitors in terms of mainstream enterprise customer value, and is more aligned with service providers and very large global enterprises.
- Versa's marketing lags its competitors, which can impact its ability to attract new customers and grow in the market.

Inclusion and Exclusion Criteria

General

- Provide a generally available (GA) single-vendor SASE offering as of 1 March 2024. All components must be publicly available, shipping and be included on the vendors' published price list as of this date. Products shipping after this date only may influence the Completeness of Vision axis.
- Provide commercial support and maintenance for its enterprise SASE offering (24/7) to support deployments on multiple continents. This includes hardware/software support, access to software upgrades, security patches, troubleshooting and technical assistance.
- Participate in the enterprise SASE market, including actively selling and publicly marketing SASE to enterprises.

Gartner defines "general availability" as the release of a product to all customers. When a product reaches GA, it becomes available through the company's general sales channel — as opposed to a limited or controlled release, pre-GA, or beta version.

Product

Vendors must have a SASE offering that includes all the following functionality, generally available as of 1 March 2024.

- The ability to secure web access via proxy.
- The ability to enforce SaaS access controls in-line. This requires support for in-line malware scanning and data security to cover at least three SaaS enterprise suites (for example, Microsoft 365, Salesforce and Google Workspace).
- The ability to provide identity- and context-based secure remote policy-based access to private applications (not just network-level access), often referred to as zero-trust network access (ZTNA).
- All of the above functionalities must be operated “as a service” and primarily delivered as a cloud service to customers.
- Firewall capability to secure traffic bidirectionally across networks.
- A branch appliance that supports:
  - Dynamic traffic steering across multiple physical locally attached WAN interfaces.
  - Traffic steering based on well-known applications (not IPs/ports).
  - An appliance that is deployable at a customer’s physical branch location to directly terminate connectivity.
- The ability for customers to define sensitive data inspection policies and apply them via in-line network data inspection.
- An endpoint software agent for connecting users to the SASE offering.
- Centralized management covering all of the above capabilities of the offering (with both GUI and API) enabling provisioning, visibility, troubleshooting, reporting and that enables granular configuration and policy changes.
- The ability for customers to directly manage and administer the full offering themselves, including granular configuration and policy of all SASE functions (commonly referred to as do it yourself [DIY]).
- Single-pass scanning for malware/sensitive data (may be parallelized).
- Support for single sign-on (SSO) integration with third-party identity providers.
- Maintain POP infrastructure meeting all of the following requirements.

1. Located in 15 distinct geographic metropolitan cities, including at least three metropolitan cities each on two separate continents.

1. POPs are in a highly secure facility; and offer the following services locally (intra-POP): firewall, web proxy, private access, and in-line SaaS control in a highly available fashion; and be generally available to all enterprise customers.

1. Vendors must provide a publicly available POP monitoring/status capability and a documented POP SLA.

Global customer relevance and adoption

Vendors must show high relevance to Gartner clients via achieving at least one of the following as of 1 March 2024:

- **Overall Adoption:** At least 250 unique enterprise customers that have purchased and deployed the vendor's primary single-vendor SASE offering in a production environment and are under an active commercial support license.

- **Recent Adoption:** At least 75 **new** unique enterprise customers that have purchased and deployed the vendor's primary single-vendor SASE offering in a production environment and are under an active commercial support license. These are customers who purchased the vendor's single-vendor SASE offering for the first time after 1 March 2023.

- **Large Enterprise Adoption:** At least 75 **large** unique enterprise customers that have all purchased and deployed the vendor's primary single-vendor SASE offering in a production environment and are under an active commercial support license.

Gartner defines "Enterprise" as an organization with at least $50 million in annual revenues and/or 100 to 1,000 employees. Gartner defines "Large Enterprise" as an organization with at least $1 billion in annual revenues and/or over 1,000 employees. Enterprises can be a private for-profit organization or not-for-profit entities such as charitable organizations, government, and education institutions.

Vendors must also show high relevance to Gartner clients via achieving all the following as of 1 March 2024:

- The vendor's primary offering must address at least two use cases (as defined by Gartner) for single-vendor SASE.

- At least 25 unique SASE customers, headquartered in two continents, under active support contracts; for example, 25 customers in Asia and 25 separate customers in North America.

Magic Quadrant exclusion criteria

Vendors will be excluded from this research for any of the following reasons:

- The vendor is exiting the market or ceasing sales of the product.
- The vendor is ceasing development of new features of the product.
- The vendor's offering is a collection of individual products that don't have native integration between them.
- The vendor requires a customer to use three or more management consoles to operate its enterprise SASE offering for the foundational use case.
- The vendor is unable to provide a single-support experience to customers, meaning customers must engage multiple parties for support.
- The vendor relies on other product vendor(s) to deliver the majority of its SASE functionality.
- The vendor only delivers its offering as a managed service.

Honorable Mentions

- Aryaka has relevant technology and is investing in this market, but did not meet product inclusion criteria as of the research cutoff date.
- Barracuda has relevant technology and is investing in this market, but did not meet product inclusion criteria as of the research cutoff date.
- Broadcom (VMware) has relevant technology and is investing in this market, but did not meet product inclusion criteria this year. Specifically, the vendor is undergoing a product transition resulting from the Broadcom acquisition (to leverage Symantec for security), which has created a transient requirement for more than two consoles.
- Check Point Software Technologies has relevant technology and is investing in this market, but did not meet product inclusion criteria as of the research cutoff date.

- Ericsson (Cradlepoint) has relevant technology and is investing in this market, but did not meet customer adoption criteria as of the research cutoff date.
- iboss has relevant technology and is investing in this market, but did not meet product inclusion criteria as of the research cutoff date.
- Juniper has relevant technology but did not meet product inclusion criteria as of the research cutoff date.
- SonicWall has relevant technology and is investing in this market, but did not meet product inclusion criteria as of the research cutoff date.
- Sophos has relevant technology and is investing in this market, but did not meet product inclusion criteria as of the research cutoff date.
- Zscaler has relevant technology and is investing in this market, but did not meet product inclusion criteria as of the research cutoff date.

Evaluation Criteria

Ability to Execute

Ability to Execute Evaluation Criteria

Evaluation Criteria	*Weighting*
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	Medium
Marketing Execution	Medium

Evaluation Criteria	*Weighting*
Customer Experience	High
Operations	NotRated

Source: Gartner (July 2024)

Completeness of Vision

Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	Medium
Marketing Strategy	Low
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	NotRated
Vertical/Industry Strategy	NotRated
Innovation	High
Geographic Strategy	Low

Source: Gartner (July 2024)

Quadrant Descriptions

Leaders

A Leader has the ability to address both current and future end-user requirements in the market. Leaders have strong offerings that address multiple use cases, typically via a unified platform that provides a single, straightforward and easy-to-use administrative interface. Further, a Leader's strategy is well-aligned with emerging user needs, and has the potential to drive, shape and transform the market going forward. A Leader typically has strong visibility in the market, solid networking and security features, a large installed base of customers, and maintains positive relationships with its customers and partners on a global basis. A Leader typically is increasing its investments in the single-vendor SASE market.

Challengers

A Challenger has a proven ability to address current end-user requirements in the market. A Challenger typically has good visibility, a sizable installed base of customers, and products that are more than good-enough for most enterprises across multiple use cases. However, a Challenger's strategy and roadmap are less likely to transform the enterprise market going forward.

Visionaries

Visionaries often help transform the market — from driving new ideas/innovations, including new business models, to solving enterprise challenges. While Visionaries often have a solid strategy going forward, they often lack a consistent, proven ability to address customer challenges in a scalable manner to date. For example, a visionary may have a limited installed base of customers, lack visibility to prospects, offer only partial geographic coverage, or lack comprehensive product capabilities across all enterprise use-case requirements today.

Niche Players

Niche Players are often focused on specific portion(s) of the market, such as a specific use case, geography, vertical or technological specialty. They have a viable technology, but have not shown the ability to drive the broader market or sustain execution in the broad enterprise market. A Niche Player typically has a near-complete single-vendor SASE offering, with some limitations that manifest outside of their core focus areas. These limitations often include feature depth, usability, geographic reach, market visibility and installed base. For example, Niche Players may be focused on only certain use cases, geographies or evolving

their existing installed base. This focus can create limitations in the broader market, including reducing their ability to address emerging customer needs.

Context

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, applications 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 complicated and/or inefficient traffic routing, creating complexity for security administrators and users. At the same time, enterprises are increasingly pursuing zero-trust strategies, but finding meaningful implementations of zero-trust principles can be challenging.

The need to support digital business combined with a desire for a zero-trust security posture while keeping things manageable is the major driver of the single-vendor SASE market.

The reason is that 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. Further, 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 (whether they be internet, cloud services or private applications).

Market Overview

The market for well-architected single-vendor SASE offerings is dynamic and maturing, and SASE interest among our clients has been growing rapidly. Client interest in single-vendor SASE has more than doubled year over year. We estimate there are over 10,000 organizations using a vendor's primary single-vendor SASE offering. However, many customer implementations have not yet fully enabled all core features of the vendor's SASE offering. For example, it is common to see enterprises using SD-WAN, firewall and SWG from a SASE vendor but not CASB or ZTNA.

Multiple vendors now have a single-vendor SASE offering (nine qualify for this research); 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.

SASE Adoption Patterns

There are three primary options for SASE adoption:

1. Single-vendor offering
2. A dual-vendor offering that is an explicit pairing of two vendors (typically one for network services and one for security services)
3. Managed SASE

Single-vendor SASE is the exclusive focus of this research.

Market Shifts

From the demand side, end-user priorities are maturing:

- There is still confusion in the market over the term SASE, as it is sometimes used synonymously with cloud-delivered security or SSE.
- Buyers are increasingly preferring unified offerings. This includes a single management console, agent, policy engine underpinned by a single data lake. Further, they desire simplified and unified pricing for the offering.
- Buyers expect worldwide POP coverage that matches their enterprise requirements. Further, buyers are increasingly demanding more options for data and cloud sovereignty, including where traffic is routed, where it is inspected and where logs are stored. In some use cases, buyers are asking for local SASE delivery options, where inspection and logs can be kept local to the customer under their control.
- Digital experience monitoring has moved from an optional feature in 2023 to an expected capability in 2024, to improve troubleshooting and reduce mean time to detect/resolve issues.
- ZTNA is in the early stages of transitioning from being only for remote and mobile users, to an expected capability for users regardless of location (referred to as Universal ZTNA) — even when the user is located in campus or branch locations.
- Coffee shop networking — With hybrid work and the increasing mobile workforce, we see the increasing desire for coffee shop networking use cases where a user can plug in

regardless of location and have the “same” experience.

From the supply side, vendors are investing heavily including:

- The multibillion-dollar market opportunity of SASE has attracted new vendors to the market including Cloudflare, HPE, Netskope, Zscaler and others.
- Most SSE vendors now have developed or acquired SD-WAN capabilities. For example, Cloudflare, iBoss and Zscaler all announced SD-WAN capabilities in the last 12 months.
- Most SD-WAN vendors now offer their own security stack. The past 18 months have seen continued acquisitions: HPE acquired Axis, CradlePoint acquired Ericom, and Sonicwall acquired Banyan Security.
- GenAI enhancement within vendor consoles has been a rapid area of innovation over the past 12 months. Initial use cases were around simplified operations (documentation and conversational troubleshooting) but are evolving to broader functionality, including security policy automation and recommended actions.
- Most SASE vendors made strides in unification including reducing the number of consoles or agents required by their customers.
- Vendors are providing customers with a choice of where SASE policies are enforced and are enabling their customers to mix and match enforcement locations across on-premises hardware appliances, on-premises virtual appliances, the vendor’s own POPS and hyperscale-based POPs.
- Some vendors are converging their SD-Branch with SASE offerings to address broader universal ZTNA (consistent zero-trust experience for remote, mobile and on-campus users) requirements with increasingly disparate location types.

Market Direction

In the next six to 18 months, we expect the following changes in the single-vendor SASE market:

- **More vendors:** We expect several additional vendors to enter the market with a single-vendor SASE offering over the next 12 months.
- **GenAI assistants become mandatory:** Although GenAI only recently emerged in 2023, GenAI assistants that are integrated natively into a SASE management console will become a mandatory requirement from buyers.

- **Price differences stemming from POP strategy:** Clients will see notably higher pricing of 25% up to 250% more from vendors that rely exclusively on hyperscaler infrastructure to deliver services, and in different regions. SASE vendors that build solely on hyperscale providers will be at a competitive pricing disadvantage compared to those that own their own infrastructure (or utilize a hybrid approach). This is especially true for hyperscaler-based SWG services where the network egress costs can become significant.

- **SASE vendors expand to adjacent markets:** There are several security markets immediately adjacent to SASE. For example, addressing endpoint security, endpoint DLP, DSPM, SSPM, microsegmentation, NDR, and network access control use cases. Some vendors are now looking to expand from the integrated SD-WAN capabilities to include wired and wireless networking at branch offices and edge locations.
- **Sensitive data discovery and control** becomes as important as threat intelligence as buyers evaluate offerings.

- **Expanded support for unmanaged devices:** Rather than a one-size-fits-all approach, support for unmanaged devices will expand into a spectrum of options including reverse proxies, dissolvable agents, browser plugins, remote browser isolation and local browser isolation (either through separate secure enterprise browser or tighter integration with browser security capabilities exposed by Google and Microsoft).

⊕ Evidence

⊕ Evaluation Criteria Definitions

objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.