Magic Quadrant for SASE Platforms

28 July 2026 - ID G00839446 - 44 min read

By Jonathan Forest, Andrew Lerner, and 1 more

The SASE platforms market is maturing, with vendors differentiating on securing AI, postquantum cryptography and sovereign controls. Still, core vendor capability differences remain. Heads of I&O and cybersecurity leaders should use these insights to help determine the right vendor for their needs.

Strategic Planning Assumptions

By 2029, 75% of SD-WAN purchases will be part of a single-vendor SASE platform offering, up from 35% in 2026.

By 2029, 60% of secure access requests will originate from nonhuman identity enforcement and collaborative access between identities, up from less than 5% in 2026.

Market Definition/Description

Gartner defines secure access service edge (SASE) platforms as offerings that deliver converged network and security capabilities.This includes software-defined WAN (SD-WAN) and secure access to the web, cloud services and private applications regardless of the user's location, the device used or where that application is hosted. These offerings primarily use a cloud-centric architecture delivered as a platform by one vendor.

SASE securely connects users and devices with applications, services and other users. It supports branch office and remote worker connectivity and on-premises general internet

security, private application access and public cloud service provider access use cases.

Mandatory Features

The mandatory features for this market include:

- Resilient global point-of-presence (POP) infrastructure providing functionality for secure access to the web, cloud services and private applications.
- Centralized management with no more than two consoles covering all the capabilities listed below, accessible via both GUI and API, enabling visibility, troubleshooting, reporting and granular configuration and policy changes:
  - Secure web access via proxy.
  - SaaS visibility and access controls.
  - Identity-, context- and policy-based secure remote access to private applications.
  - A branch appliance that supports performance-based dynamic traffic steering (such as packet loss, latency and jitter) across multiple physical WAN interfaces, based on applications (not just IPs/ports).
  - Layer 7 firewalling to secure traffic bidirectionally across networks.
- Sensitive data visibility and control.

Optional Features

The optional features 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 granular configuration and policy changes.
- The ability to securely connect end users to the SASE platform using a variety of techniques, including software agents, agentless portals, browser plug-ins, secure enterprise browsers and remote browser isolation.
- The ability to support next-generation firewall (NGFW) functionality as both a cloud service and as part of a branch appliance.

- Additional security capabilities, including network sandboxing, DNS protection, 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, cloud onramps (simplified and automated integration with public cloud networking services) and broader application optimization technologies.
- The ability to replace a branch router (such as support for Border Gateway Protocol [BGP]) and support meshed topologies.
- Integrated digital experience monitoring (DEM) capabilities.
- Support native capabilities or integration with third-party offerings to provide security controls for unmanaged operational technology (OT) and unmanaged Internet of Things (IoT).
- GenAI reporting and controls to restrict access and protect enterprise data.
- The ability to deliver SASE functionality in an environment controlled by the customer for sovereign use cases.
- Threat protection and intelligence.

Magic Quadrant

Figure 1: Magic Quadrant for SASE Platforms

Magic Quadrant for SASE Platforms

Gartner

Vendor Strengths and Cautions

Cato Networks

Cato Networks is a Leader in this Magic Quadrant. Its SASE platform offering is the Cato SASE Cloud Platform. Gartner estimates that the vendor has approximately 4,000 active SASE platform enterprise customers. The offering is delivered via the Cato Management Application (CMA), which manages all relevant security service edge (SSE) functionality, Cato Socket edge SD-WAN, Cato Client and Global Private Backbone. Its operations are primarily in North America, Europe and Asia/Pacific, with a focus on cloud-first enterprises across all verticals.

Gartner expects Cato to make future investments in integrating AI agents into its SASE platform, expanding data security to AI agents and introducing agentic threat protection.

Strengths

- **Customer experience:** Cato is above average in customer experience versus other vendors in this research, as demonstrated by Gartner client feedback and Peer Insights scores.
- **Planned feature enhancements:** The vendor's planned innovations around agentic threat prevention and FlowGuard, which detects and prevents exploitation of agentic AI vulnerabilities, have the potential to drive SASE platform buying decisions going forward.
- **Market responsiveness:** Cato was one of the early SASE platform vendors and has consistently responded to market trends in a timely manner for features such as universal ZTNA (UZTNA), DNS security for devices without agents and local network macrosegmentation.

Cautions

- **Modular adoption:** The vendor is expanding its focus to include modular SASE adoption. Cato is known as a unified platform offering, so customers consuming individual SASE components is inconsistent with its value proposition.
- **Financial profile:** Cato's financial score, calculated using Gartner's methodology, is lower than most vendors in this research. Customers should validate its financial health as part of a SASE platform evaluation.
- **Pricing:** Cato's pricing tends to be higher than other vendors in this research, based on feedback from Gartner Peer Insights and broader Gartner analysis.

Check Point Software Technologies

Check Point Software Technologies is a Niche Player in this Magic Quadrant. Its SASE platform is Check Point SASE. Gartner estimates that the vendor has approximately 1,000 active SASE platform enterprise customers. The offering requires two management consoles integrated into the Infinity Portal, with Check Point SASE providing the secure service edge (SSE) functionality and Check Point SD-WAN providing the SD-WAN functions. Its operations are primarily in North America, Europe and Asia/Pacific with a focus on hybrid cloud security-conscious organizations of all sizes and verticals. Gartner expects Check Point to make future

investments in AI security, unifying the SASE platform and autonomous digital experience monitoring (DEM).

Strengths

- **Financial profile:** Check Point's financial metrics are strong compared to most other vendors in this research, giving it flexibility to make longer-term SASE platform investments.
- **Firewall incumbency:** The vendor has incumbency in the firewall market, allowing it to easily upgrade customers to its SASE platform offering.
- **AI Defense Plane:** Check Point recently launched its AI Defense Plane, which provides discovery, posture and runtime control for AI applications and agentic systems.

Cautions

- **Management complexity:** Check Point requires two management consoles for SD-WAN and SSE and is complex to navigate.
- **Geographic strategy:** The vendor has a more limited geographic strategy around expanding its point of presence (POP) infrastructure, support for languages other than English and enabling sovereign controls.
- **Brand visibility:** Check Point's SASE platform market visibility is below average compared with other vendors in this research, primarily based on Gartner end-user client interactions.

Cisco

Cisco is a Challenger in this Magic Quadrant. Its primary SASE platform offering is Cisco SASE. Gartner estimates that the vendor has approximately 1,500 active SASE platform enterprise customers using this product. Cisco SASE integrates Cisco's Catalyst SD-WAN and Cisco Secure Access, requiring two management consoles to deliver the full SSE and SD-WAN functionality. While Cisco leads with Catalyst SD-WAN as part of the Cisco SASE offering, Meraki SD-WAN is also supported. Its operations are global, focusing on customers of all sizes and verticals and targeting more networking-led use cases. Gartner expects Cisco to make future investments in delivering its AI security platform, Cloud Control (which will offer a unified SASE management console), comprehensive browser security suite and unified data security.

Strengths

- **Sales execution:** Cisco has strong channels and a loyal customer base that it can leverage in the migration from stand-alone SD-WAN to its SASE platform offering.
- **POP infrastructure strategy:** The vendor is expanding its POP infrastructure to enhance its reach and improve service quality globally.
- **Market responsiveness:** Cisco has been responsive to recent market trends, such as GenAI prompt inspection for sensitive data, local network macrosegmentation and local network microsegmentation without requiring an agent.

Cautions

- **Customer experience:** Cisco's customer experience is below average compared with other vendors in this research, primarily based on Gartner end-user interactions that reflect concerns around product support and product complexity.
- **Planned feature enhancements:** The vendor's expected planned feature enhancements in unified data security and comprehensive browser security suite are late and adjacent capabilities and not expected to change buying decisions in the SASE platform market.
- **Management complexity:** Cisco's offering requires two management consoles to fully operate the SD-WAN and SSE functionality and can be complicated to navigate.

Cloudflare

Cloudflare is a Visionary in this Magic Quadrant. Its SASE platform offering is Cloudflare One. Gartner estimates that the vendor has approximately 4,500 active SASE platform enterprise customers. Cloudflare One is an integrated offering that provides all SSE functionality, with Cloudflare WAN, Cloudflare One Client and Cloudflare One Appliance managed via the Cloudflare dashboard. Its operations are global, focusing on cloud-first enterprises across all verticals. Gartner expects Cloudflare to make future investments in extending secure web gateway (SWG) policies using customer business logic, unified resource discovery across networking and security, expanding support for postquantum cryptography (PQC) and AI agent identity and governance.

Strengths

- **Planned feature enhancements:** Cloudflare's recent and planned investments in enhancing its PQC capabilities and AI agent full life cycle security have the potential to shape the SASE platform market going forward.

- **Pricing:** The vendor's new pricing strategy is simple and cost-effective, which benefits clients who prefer easier-to-consume offerings.
- **POP infrastructure:** Cloudflare has an extensive POP infrastructure, which provides reach to deliver high-performance service globally.

Cautions

- **On-premises product functionality:** Cloudflare's on-premises networking and security functionality is limited, which impacts its ability to address customers with more hybrid functionality needs.
- **Brand visibility:** The vendor has lower SASE platform market visibility compared with other vendors in this research based on Gartner end-user client interactions.
- **Sovereign controls:** Cloudflare has a narrow view of sovereignty, focusing more on encryption and decryption location rather than broader controls such as management plane ownership flexibility, routing path controls and partners offering the vendor's SASE platform service in their data centers.

Fortinet

Fortinet is a Challenger in this Magic Quadrant. Its SASE platform offering is Fortinet Unified SASE. Gartner estimates that the vendor has over 3,000 active SASE platform enterprise customers. Fortinet's Unified SASE offering includes FortiSASE (for the SSE functions) and FortiGate Secure SD-WAN integrated in the FortiSASE portal. Its operations are global, targeting all customers and verticals with a focus on organizations that have hybrid cloud networking and security needs. Gartner expects Fortinet to make future investments in universal zero trust network access (UZTNA) for nonhuman identities (NHI), securing agent-to-agent traffic, integrating quantum into FortiSASE (beyond existing SD-WAN support) and delivering managed SD-WAN hubs in SASE POPs.

Strengths

- **Product capabilities:** Fortinet has broad networking and security product features across both on-premises and the cloud with strengths in SD-WAN, in-line on-premises security controls, cloud-enforced in-line security controls and threat protection.
- **Financial profile:** The vendor's financial metrics are favorable compared to other vendors in this research, giving it flexibility to make longer-term SASE platform investments.

- **POP infrastructure:** Fortinet has invested in building out its company-owned POP infrastructure to reduce its reliance on hyperscalers and to provide better service globally.

Cautions

- **Planned feature enhancements:** Fortinet's future enhancements, such as intelligent managed SD-WAN hubs in SASE POPs and PQC support, are late and table-stakes functionality and not expected to change SASE platform buying decisions.
- **Customer experience:** The vendor's customer experience is below average compared with other vendors in this research, primarily based on Gartner end-user interactions that reflect concerns around cloud product maturity.
- **Security vulnerabilities:** Fortinet's large installed base makes its firewall platforms a target for attackers, exposing vulnerabilities. This has resulted in frequent patching and elevated customer concerns in production and when making buying decisions.

Hewlett Packard Enterprise

Hewlett Packard Enterprise (HPE) is a Niche Player in this Magic Quadrant. Its SASE platform offering is HPE Networking Unified SASE. Gartner estimates that the vendor has approximately 600 active SASE platform enterprise customers. The offering requires two management consoles, with HPE Networking EdgeConnect Cloud Orchestrator for SD-WAN and HPE Networking SSE. While the vendor has multiple SD-WAN products, it leads with HPE Networking EdgeConnect SD-WAN. Its operations are global, focusing on customers of all sizes and verticals with network-led use cases. Gartner expects HPE to make future investments in integrating the Juniper Networks SRX security stack, following its July 2025 acquisition, in its SASE platform; SSE into the EdgeConnect SD-WAN fabric; and Juniper Mist with HPE Networking Central for full stack (wired LAN, Wi-Fi and SD-WAN) agentic NetOps.

Strengths

- **Network incumbency:** HPE has incumbency in the SD-WAN market, allowing it to easily upgrade customers to its SASE platform offering.
- **SD-WAN:** The vendor continues to deliver a strong SD-WAN offering with integrated in-line on-premises security controls.
- **Customer experience:** HPE's customer experience is above average compared with other vendors in this research, based on Gartner end-user interactions.

Cautions

- **Planned feature enhancements:** HPE's planned feature enhancements are more tactical product integrations and unlikely to change SASE platform customer buying decisions.
- **Management complexity:** The vendor requires two management consoles for SD-WAN and SSE, and its offering is complex to navigate.
- **POP strategy:** HPE's POP count lags other vendors in this research, which limits its ability to serve global customers.

iboss

iboss is a Niche Player in this Magic Quadrant. Its SASE platform offering is iboss AI-Powered SASE Platform. Gartner estimates that the vendor has approximately 300 active SASE platform enterprise customers. The offering includes iboss unified management via the Cloud Management Console for both the SD-WAN and SSE components along with branch gateways and software licenses. Its operations are primarily in North America, Europe and Asia/Pacific, focusing on larger enterprises, government and education organizations prioritizing a simpler unified SASE experience. Gartner expects iboss to make future investments in its autonomous agentic SASE platform, AI-powered cloud access security broker (CASB) private AI models for data loss prevention (DLP) and unified AI traffic inspection.

Strengths

- **Pricing:** iboss' offering is competitively priced, which appeals to more cost-conscious buyers.
- **Planned feature enhancements:** The vendor's recent and future enhancements around AI-powered CASB, an AI agent for SASE operations, and in-line inspection of Model Context Protocol (MCP) and agent-to-agent API traffic are aligned with future enterprise needs.
- **In-line security controls:** iboss has solid on-premises and cloud-delivered, in-line security controls, including firewall, IPS and SWG functionality.

Cautions

- **Brand visibility:** iboss' SASE platform market visibility is below average compared with other vendors in this research, based on end-user client interactions, and searches on the Gartner website and via AskGartner.

- **Sales strategy:** The vendor's sales strategy includes targeting AI security teams, which may take the focus away from SASE buyer personas and ultimately limit its ability to grow.
- **Financial clarity:** iboss' financial position is less clear compared with other vendors in this research, and it offered limited financial information for inclusion in this analysis.

Netskope

Netskope is a Leader in this Magic Quadrant. Its SASE platform offering is Netskope One SASE. Gartner estimates that the vendor has approximately 2,000 active SASE platform enterprise customers. The fully integrated offering includes Netskope One Security Service Edge, Netskope One SD-WAN, Netskope One Client and NewEdge POP infrastructure managed via its Netskope One Orchestrator. Its operations are primarily in North America, Europe and Asia/Pacific targeting larger organizations across all verticals. Gartner expects Netskope to make future investments in its AI Command Center, AI agent sandbox, AgentSkope Marketplace and Netskope Customer Workspace, enabling partners to address the small and midsize business (SMB) market.

Strengths

- **Product functionality:** Netskope has broad and deep capabilities covering networking and security across on-premises and cloud with strengths in SD-WAN, cloud-enforced in-line security controls, SaaS app control and visibility, and adaptive access.
- **POP infrastructure strategy:** The vendor has a broad and comprehensive POP infrastructure with plans to expand in order to enhance its global service reach for end customers.
- **Customer experience:** Netskope's customer experience is above average compared with other vendors in this research, as demonstrated by Gartner end-user interactions.

Cautions

- **Market understanding:** Netskope's view of the market's evolution overly focuses on securing AI and goes beyond the scope of SASE platforms. This risks conflating with other markets and overlooking core SASE buyer needs.
- **Financial profile:** The vendor's corporate financial metrics are not as strong as most other vendors in this research, which may limit its ability to invest in the future.

- **Pricing:** Based on client interactions and Gartner analysis, Netskope's SASE platform bills of materials (BOMs) tend to be more complex, and pricing can vary when compared with other vendors in this research.

Palo Alto Networks

Palo Alto Networks is a Leader in this Magic Quadrant. Its SASE platform offering is Prisma SASE. Gartner estimates that the vendor has approximately 6,500 active SASE platform enterprise customers. The fully integrated offering includes Prisma Access (SSE) and Prisma SD-WAN with its ION appliances and corresponding software managed via Strata Cloud Manager. The traditional PAN-OS next-generation firewall (NGFW) is not part of its SASE offering and was not part of the product evaluation. The vendor operates globally and focuses on larger organizations and all verticals for networking and security use cases. Gartner expects Palo Alto Networks to make future investments in securing the agentic enterprise, proactive agentic Ops across networking and security, and sovereign SASE.

Strengths

- **Planned feature enhancements:** Palo Alto Networks' recent and future enhancements around PQC, securing agentic traffic flows and simplifying manageability with agentic SASE operations capabilities are aligned with future enterprise needs.
- **Financial profile:** The vendor's financial metrics are strong compared to most other vendors in this research, giving it flexibility to make longer-term SASE platform investments.
- **Market understanding:** Palo Alto Networks has a solid understanding of the current and future SASE market competition. It also has a strong understanding of unmet SASE platform market needs including simplification, reduced time from vulnerability discovery to exploitation driven by frontier AI defense models, sovereign controls, PQC and modern data security.

Cautions

- **Pricing:** Palo Alto Networks' offering is more expensive than most of the other vendors in this research, based on Gartner end-user client interactions and Gartner analysis.
- **Customer experience:** The vendor's customer experience is below average compared with other vendors in this research, as demonstrated by Gartner end-user interactions that reflect concerns around product support.

- **On-premises security:** Palo Alto Networks' on-premises security for ION appliances' intrusion prevention system (IPS) and content filtering are more constrained and cloud-reliant than most vendors in this research.

Sangfor Technologies

Sangfor Technologies is a Niche Player in this Magic Quadrant. Its SASE platform offering is Athena SASE. Gartner estimates that the vendor has approximately 1,000 active SASE platform enterprise customers. The platform includes two separate management consoles: Sangfor Access Secure for the unified agent and cloud security and NGAF Platform for the SD-WAN and firewall appliance. The vendor operates mainly in Asia/Pacific, Europe and South America, and focuses on organizations of all sizes and verticals for security-driven use cases. Gartner expects Sangfor to make future investments in its sovereign SASE fabric, enabling a multivendor ecosystem, AI-driven data security and DEM as well as agentic AI governance.

Strengths

- **Firewall incumbency:** Sangfor has incumbency in the firewall market, allowing it to easily upgrade its customers to the SASE platform offering.
- **Future investment:** The vendor plans increased future investment across product, sales, marketing and customer experience, which is more than most vendors in this research and demonstrates its commitment to the SASE platforms market.
- **In-line security controls:** Sangfor has solid in-line security controls delivered both on-premises and from the cloud.

Cautions

- **Geographic strategy:** Sangfor's minimal presence in North America limits its overall SASE platforms market opportunity.
- **Brand visibility:** The vendor has limited market visibility in the global SASE platforms market, restricting its ability to participate in customer procurements.
- **Management complexity:** Sangfor requires two management consoles to operate its offering, increasing operational complexity for end customers.

Versa Networks

Versa Networks is a Challenger in this Magic Quadrant. Its SASE platform offering is Versa Secure Access Fabric (VSAF). Gartner estimates that the vendor has approximately 5,000 active SASE platform enterprise customers. The fully integrated offering includes Versa SSE and Versa Secure SD-WAN on Versa CSG appliances managed via Versa Concerto. It also offers Titan for more streamlined SD-WAN use cases. It operates primarily in North America, Europe and Asia/Pacific, focusing on customers with network-centric use cases of all sizes and verticals. Gartner expects Versa to make future investments in model gateway foundation detection, scoring and enforcement, Model Context Protocol (MCP) gateway zero trust and large language model web application firewall (LLM WAF) prompt, context and response inspection.

Strengths

- **Product capabilities:** Versa has comprehensive networking and security functions across the cloud and on-premises with strengths in SD-WAN, in-line on-premises security controls and adaptive access.
- **POP infrastructure strategy:** The vendor plans to expand its POP infrastructure in several geographic regions in order to extend its reach and provide better global service quality.
- **Pricing:** Versa's offering is competitively priced for the functionality delivered compared with other vendors in this research.

Cautions

- **Planned feature enhancements:** Versa's planned feature enhancements, including XDR with AI-driven managed detection and response (MDR) and LLM WAF inspection, are adjacent to SASE and unlikely to drive the SASE platform market going forward.
- **Customer experience:** The vendor's customer experience is below average compared with other vendors in this research, as demonstrated by Gartner end-user interactions that reflect concerns around product complexity.
- **Brand visibility:** Versa's SASE platform market visibility is below average compared with other vendors in this research, based on end-user client interactions and searches on the Gartner website.

Zscaler

Zscaler is a Leader in this Magic Quadrant. Its SASE platform offering is Zero Trust SASE. Gartner estimates that the vendor has approximately 1,000 active SASE platform enterprise customers. The fully integrated offering provides the Zero Trust Exchange SSE platform and Zero Trust SD-WAN functionality via the Experience Center management console. The vendor operates globally, focusing on larger organizations across all verticals, targeting security-driven use cases. Gartner expects Zscaler to make future investments in a unified tunnel with Multiplexed Application Substrate over QUIC (Quick UDP Internet Connections) Encryption (MASQUE) to improve performance, agentic exchange to secure AI agents, agentic SASE operations to improve security and network operations, and Zero Trust SASE ZDX enhancements.

Strengths

- **Planned feature enhancements:** Zscaler's feature enhancements around improving its networking capabilities, delivering agentic SASE Ops, and launching its zero trust agent exchange are aligned with enterprise buyer needs.
- **Financial profile:** The vendor's financial metrics are favorable compared to other vendors in this research, giving it flexibility to make longer-term SASE platform investments.
- **POP infrastructure strategy:** Zscaler plans to expand its POP infrastructure to enhance its global footprint to deliver improved service quality as well as enhance its sovereign controls.

Cautions

- **Customer experience:** Zscaler's customer experience is below average compared with other vendors in this research, as demonstrated by Gartner end-user interactions that reflect product-related concerns.
- **On-premises capabilities:** The vendor has limited SD-WAN and on-premises security functionality and experience compared with other vendors in this research.
- **Market responsiveness:** Zscaler was comparatively late to enter the SASE platform market and tends to focus more on security driven with lightweight networking use cases.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A

vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

- iboss
- Sangfor Technologies

Dropped

- SonicWall

Inclusion and Exclusion Criteria

Magic Quadrants and Critical Capabilities reports identify and analyze the most relevant providers and their products in a market. The inclusion criteria are the specific attributes that a provider must have to be included in this research.

In addition to Gartner client relevance, as determined by analyst expertise and opinion, providers need to meet the following criteria to qualify for inclusion.

General

- Provide a generally available (GA) SASE platform offering as of 1 May 2026. The SASE platform offering must be publicly available, shipping and included on the vendor’s 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 platform 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 platforms market, including actively investing in, selling and publicly marketing its branded SASE platform to enterprises.
- Must be highly relevant to Gartner end-user clients.

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 platform offering that includes all the below functionality, generally available as of 1 May 2026:

- All of the following must be available as a shared service from the cloud to customers:
  - Secure web access via proxy.
  - Enforce SaaS access controls in-line. This requires support for in-line malware scanning and data security to cover at least two of the following three SaaS enterprise suites: Microsoft 365, Salesforce, Google Workspace.
  - Ensure least-privileged user access based on continuous identity- and context-based secure remote policy-based access to private applications (not just network-level access).
- Layer 7 firewall capability to secure traffic bidirectionally across networks.
- A branch appliance that supports performance-based dynamic traffic steering (supporting at least two of the following criteria: latency, packet loss or jitter) across multiple physical WAN interfaces; based on well-known applications (not IPs/ports). This appliance is deployable at a customer’s physical branch location to directly terminate connectivity.
- The ability to provide sensitive data visibility and for customers to define sensitive data protection policies and apply them via in-line network data inspection.
- An endpoint software agent (supporting Windows and Mac operating systems) for connecting users to the vendor’s SASE platform offering.
- Provide visibility, basic controls (e.g., block, warn, allow), and end users for at least three common generative AI applications (e.g., OpenAI ChatGPT, Perplexity AI, Microsoft Copilot, Google Gemini) initiated by an end user from the endpoint.
- Centralized management (with both GUI and API) enabling provisioning, visibility, troubleshooting, reporting, and granular configuration and policy changes.

- The vendor must have no more than two management consoles to operate its enterprise SASE platform offering for the foundational SASE use case.
- The ability for customers to directly manage and administer the full SASE platform offering themselves, including granular configuration and policy of all SASE functions (commonly referred to as do-it-yourself [DIY]).
- Single-pass scanning for malware and sensitive data (may be parallelized) for in-line security controls.
- Support single sign-on (SSO) integration with third-party identity providers.
- Leverage POP infrastructure meeting all the following requirements:
  - Presence in at least 15 distinct geographic metropolitan cities globally including with at least three distinct metropolitan cities each on three separate continents.
  - POPs are in a highly secure facility; and offer the following services locally (intra-POP): web proxy, private access and in-line SaaS control with high availability; and be generally available to all enterprise customers.
  - Vendors must provide a publicly available URL with POP metropolitan cities list, POP monitoring/status capability and a documented POP SLA.
- The vendor must be able to provide a single-support experience to customers, meaning customers must engage only with the vendor for support.
- The vendor must natively deliver all of the core SASE functionality (SD-WAN, firewall, ZTNA, CASB and SWG) as part of the SASE platform offering.

Global Customer Adoption

Vendors must achieve at least one of the following as of 1 March 2026 with the SSE functionality (ZTNA, CASB and SWG) of SASE delivered as a service from the cloud:

- **Overall adoption:** At least 300 unique enterprise customers using SD-WAN and, at a minimum, one of the SSE components (ZTNA, CASB or SWG) with the vendor's primary SASE platform offering in a production environment and under an active commercial support license.

- **Large enterprise adoption:** At least 100 unique large enterprise customers using SD-WAN and, at a minimum, one of the SSE components (ZTNA, CASB or SWG) with the vendor's primary SASE platform offering in a production environment and under an active commercial support license.

Vendors must achieve each of the following as of 1 March 2026:

- The vendor's primary offering must address at least three of the Critical Capabilities use cases for SASE platforms, with one of them being the foundational SASE use case.
- At least 50 unique SASE platform enterprise customers, each headquartered in two continents using SD-WAN and, at a minimum, one of the SSE components (ZTNA, CASB or SWG) in a production environment under active support contracts and under an active commercial support license; for example, 50 customers in Asia and 50 separate customers in North America.

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

Gartner defines "customer" as a paying end-user organization for the consumption of a service and under active support. This excludes trials, proofs of concept (POCs), paid pilots, "try and buys," lab trials, etc. Customers may include both DIY and those serviced through a managed SASE provider (i.e., any organization using a vendor's solution fully deployed, regardless how it is delivered).

Honorable Mentions

The providers that are most relevant to our clients were selected for evaluation in this Magic Quadrant. However, the decision not to evaluate a provider does not mean that the provider lacks viability. The following are noteworthy providers not included in the formal analysis. These providers have relevant technology and are investing in this market. They could be appropriate for clients, contingent on their requirements:

- Aryaka
- Barracuda

- Ericsson (Cradlepoint)
- SonicWall
- Huawei

Evaluation Criteria

Ability to Execute

Product/Service: We evaluate vendors by looking at their overall SASE offering, including both the networking and network security components. The majority of this assessment focuses on the existing capabilities of the vendor's primary SASE platform offering, as defined by what it sells to most enterprises. We also consider the breadth and depth of the SASE platform functionality provided by the vendor across all relevant offerings and the use cases they support. We consider the vendor's architecture, as well as product capabilities and quality. The functionality we primarily assess includes, but isn't limited to, SD-WAN, in-line on-premises security controls, securing private applications, in-line cloud-enforced security controls, SaaS app control and visibility, infrastructure delivery, ease of administration, lightweight networking, unified platform, data security, threat protection, adaptive access, AI security, sovereign controls, and coffee shop networking experience.

Overall Viability: We assess the vendor's overall financial health and the likelihood that they will continue to invest across multiple areas, such as marketing, sales, product development and support, in the business unit to expand their SASE platform offering.

Sales Execution/Pricing: We assess the vendor's pricing and direct/indirect sales structure and effectiveness. Approximately half of this assessment is based on sales effectiveness and go-to-market activities, along with depth and breadth of sales channels that are driving the business growth. The other half of the assessment evaluates the price versus value offered to customers. We also assess the hardware/support/licensing pricing model and simplicity/complexity of pricing.

Market Responsiveness and Track Record: This criterion evaluates the vendor's demonstrated history of responsiveness. It assesses the vendor's track record in delivering the right capabilities at the right time to address customer needs, compared with competitors. This criterion also evaluates the vendor's history of responsiveness in terms of changing market

demands and addressing limitations to remain competitive. This evaluation is not limited to SASE platform products as it also involves adjacent integrated capabilities that strengthen the overall SASE platform offering as well as responsiveness in integration, pricing, licensing models, go-to-market strategy and overall competitive dynamics.

Marketing Execution: This criterion assesses the efficacy of the vendor's marketing program. For SASE platforms, we evaluate the clarity, consistency and amplitude of messages, including, but not limited to, its website, social media channels, etc. We focus on whether the vendor's messaging resonates with enterprises, including key points of differentiation. We assess whether the vendor is making appropriate investments in marketing, and if it is delivering results. The evaluation focuses on how well the vendor is able to influence and shape perception in the market through marketing activities and thought leadership that drives awareness. An additional indicator for this criterion is how often Gartner clients inquire about a specific vendor in terms of capabilities/reputation or in a shortlist evaluation process.

Customer Experience: This criterion looks at all aspects of customers' experience inclusive of presales and postsales activities with the vendor's SASE platform offering. Additionally, we assess (1) how the vendor manages customer experience; (2) feedback on corporate employee engagement; and (3) customer satisfaction at a corporate level.

Operations: Not rated; by assigning a zero weight to this criterion, the assessment focuses the analysis more heavily on categories that are truly differentiating for current SASE platform customers.

Ability to Execute Evaluation Criteria

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

Evaluation Criteria	*Weighting*
Marketing Execution	Medium
Customer Experience	High
Operations	NotRated

Source: Gartner (July 2026)

Completeness of Vision

Innovation: We evaluate the future plans to bring differentiated capabilities to the market tha will enhance the vendor's ability to attract customers and drive business. We assess whether the vendor's most recent and planned innovations will add customer value, whether they're unique or differentiated, and whether they're true "game changers." The majority of the weighting for this category is applied to future innovations, not current in-market capability. Innovation is not simply a list of new features/functionality or product improvements: It can b created across multiple areas, including product, adjacent integrated capabilities, packaging pricing, licensing, sales, marketing, models and use cases. The most impactful innovations change the dynamics of a market in terms of customers. Hence, we assess whether the vendor's innovations will disrupt the market via shifting customer expectations and/or will force competitors to react.

Market Understanding: This criterion assesses the vendor's ability to understand the emerging networking and network security needs of customers of varying sizes, verticals and geographies. We also assess the vendor's self-awareness of key strengths/weaknesses in context of the competitive landscape in the market.

Marketing Strategy: This criterion evaluates the ability of the vendor to influence the market into the future through its messaging and marketing campaigns. This includes the extent to which the vendor articulates a forward-looking marketing message that is clear, relevant and differentiated, as well as aligned with future customer needs. We look for new and effective ways vendors reach customers, how they reach evolving customer buyer personas and how they plan to communicate their message to drive market demand.

Sales Strategy: This criterion evaluates the vendor's proposed use of direct and indirect sales and related investments to add new customers and/or extend sales within existing customers. Furthermore, evaluation includes the extent to which the vendor articulates a clear, relevant and differentiated sales strategy that resonates with customers and reaches new buyer personas. Additional factors include the development of effective go-to-market strategies, alliances and partnerships, leveraging value-added resellers (VARs), system integrators (SIs), ISP aggregators, master agents, network service providers (NSPs), managed network service providers and OEM resellers, as appropriate. The assessment further includes how the vendor leverages new pricing models that are emerging due to market and technology transition.

Offering (Product) Strategy: This criterion evaluates the vendor's SASE platform product around existing and future capabilities. This evaluation includes not just the raw features and services, but also the vendor's overall architecture across the portfolio, and how this architecture provides value to the end customer. We also assess whether the vendor closes key gaps in its existing offering. We evaluate product strategy across various capabilities, including, but not limited to, networking, network security, using AI to simplify management, securing AI and product integrations. This evaluation also may include multiple qualifying products that may exist within a vendor's portfolio.

Geographic Strategy: We assess whether the strategy is clear and will resonate with customers in order to grow adoption on a global basis. We assess aspects, including the vendor's plans to address specific needs within particular geographies, such as localized languages, sales and regional certifications. We also assess the vendor's ability to address any unique requirements (such as regional sovereignty) of particular geographies and to employ the associated messaging, partnerships and product features, as well as sales channels to build a sustainable business advantage.

Business Model and Vertical/Industry Strategy: Not rated; by assigning a zero weight to these criteria, the assessment focuses the analysis more heavily on other categories that are truly differentiating for current SASE platform customers.

Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	Medium

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

Source: Gartner (July 2026)

Quadrant Descriptions

Leaders

A Leader has the ability to address both current and future end-user requirements in the market. Leaders have offerings that address multiple use cases via a unified platform that provides a consolidated easy-to-use administrative interface. Additionally, a Leader's strategy is well-aligned with emerging user needs and has the potential to shape and transform the market going forward. A Leader has strong demand-side market visibility and a sizable installed base. A Leader typically is increasing its investments, demonstrating its commitment to the future of the SASE platform market.

Challengers

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

Visionaries

Visionaries often focus on shaping and transforming the market — from driving new product innovations and new pricing models to solving enterprise challenges in new ways. While Visionaries often have a solid relevant and differentiated strategy going forward, they often lack a consistent, proven ability to address customer challenges at a broader level that actually change market dynamics. For example, a Visionary may have a limited installed base of customers, lack demand-side market visibility, offer only partial geographic coverage or lack key 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 particular use case, geography or product specialty. They have a viable product but have not shown the ability to drive the broader market or sustain execution in the broad enterprise market. Niche Players typically have a near-complete SASE platform offering, with some limitations that manifest outside of their core focus areas. These limitations often include feature depth/breadth, geographic reach, demand-side market visibility, go-to-market and/or 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 continues to drive a unified approach to enterprise access requirements. Customers are looking to converge the number of vendors for simplicity or sourcing, management and security posture. SASE platforms can improve and simplify the end-user and operator experience by enabling the same access to applications, regardless of their location or the location of the application accessed. SASE can help organizations adopt a zero-trust security posture by applying consistent identity and context-based policies in near real time, regardless of the type of resource the user is accessing. SASE platforms consolidate this functionality into a unified platform offering.

At the same time, enterprises are moving beyond merely pursuing zero-trust strategies to now focusing on securing user access to GenAI apps and AI agent traffic, addressing sovereignty concerns, leveraging AI to improve Day 2 operations and implementing PQC. We also see

vendors extending their offerings beyond traditional SASE functions and risk over platforming, which can have collateral impacts by reducing choice, limiting innovation and focusing less on the intended targeted SASE buyers.

Market Overview

The overall SASE market is projected to reach over $18 billion in 2026, with a 2025 through 2030 compound annual growth rate (CAGR) of 23% (see Forecast Analysis: Secure Access Service Edge, Worldwide, 2025-2030). But only a small portion of this revenue is in the form of a SASE platform today. Over time, however, we expect more SASE platform adoption, when compared with dual-vendor SASE.

The market for converged SASE platform offerings is maturing, with new vendors introducing solutions, some vendors consolidating and others exiting. End-user client interest continues to increase, and Gartner estimates that over 25,000 enterprises are using a SASE platform offering for some functionality. However, most customers have not yet fully enabled all core features of the vendor's SASE platform offerings. We expect that to take more time as enterprises go through refresh cycles, with a focus on consolidating vendors.

Many SD-WAN and security service edge (SSE) vendors now have a SASE platform offering. However, not all vendors offer the required breadth and depth of functionality, integration across all components, and a single management plane.

The following are the current trends that Gartner observes in the SASE platform market.

Demand Side

Buyers typically prioritize security functionality over networking functionality when making purchasing decisions. This conclusion is based on end-user Gartner client inquiries and market surveys. They also prefer simplicity and unified offerings, including a single management console, agent, policy engine, and easy-to-understand pricing models. Furthermore, buyers expect point of presence (POP) coverage with full-service functionality that aligns with where their users and branches are located. Increasingly, we also see interest in data and infrastructure sovereignty, including where traffic is routed, where it is inspected and where logs are stored.

Buyers typically start their SASE platform journey with SD-WAN and at least one SSE component, but rarely use all functions. They are also extending zero-trust network access

(ZTNA) to branch locations from being only for remote and mobile users. The goal is to leverage the consistent identity, context- based policies and risk in near real time of ZTNA and apply it everywhere as a single offering, regardless of the user's location. We see the increasing desire for users to access the network in the office environment in a similar way to when they are in a coffee shop. Known as "coffee shop networking," even with return-to-office mandates, we see this use case being relevant when applications are served primarily from the cloud (where there is minimal need for on-premises security for local East/West security) and there is a limited number of users/employees in the office.

There is a desire for NetSecOps operational simplicity by using AI agents increasingly to automate and streamline workflows. Customers are also increasingly concerned about securing nonhuman identities (e.g., AI agents and APIs) that can be transient and not sanctioned by the organization. There are new concerns in response to the frontier AI models, which autonomously find infrastructure vulnerabilities that can be exploited by bad actors. Previously, patches were delayed or not even done, as infrastructure could be in production past their end-of-life date. The risk of infrastructure vulnerabilities in the market is driving organizations to accelerate their patching windows to reduce risk.

Supply Side

New vendors continue entering the SASE platform market from adjacent markets, such as SD-WAN and SSE. We estimate that there are approximately 15 to 20 vendors with viable offerings or plans to build a full-featured, fully converged SASE platform offering. We also expect mergers and acquisitions (M&As) to continue in this market and vendors to cease their participation. Few vendors have a solid breadth of functionality across network and security (and both on-premises and cloud). Additionally, with an increasing number of vendors in the market offering a unified platform, it still remains a work in progress for some others. SD-WAN and SSE vendors that do not participate in the SASE platform market will have limited growth opportunities going forward.

Generative AI (GenAI) assistants are mainstream, but some vendors are also investing in agentic NetSecOps capabilities to drive more automation. Most vendors have capabilities to manage access (allow or block) to GenAI applications and provide prompt inspection to ensure that no sensitive data is inadvertently uploaded or released in a response. Many vendors are focused on discovering and securing AI agents, securing their traffic to and from MCP servers, and securing their traffic to the web, SaaS application and private applications.

An increasing number of vendors are offering private/sovereign SASE capabilities that provide flexibility as to where SASE policies are enforced, encryption is performed, logs can be stored and traffic is routed across on-premises appliances, the vendor's POPs and local POPs. Just because a vendor can deploy a solution on-premises, doesn't necessarily make it sovereign.

Some other areas where we observe vendors focusing their offerings are:

- Converging their SD-branch with SASE offerings to drive further simplicity of networking and network security offerings.
- Introducing secure enterprise browsers, while others are taking a more agnostic approach that secures the browser that the enterprise chooses to use.
- Extending their SASE platform offerings to SASE adjacencies such as network detect and response (NDR) with the intention of being a one-stop shop for end customers. But, this approach has the risk of overplatforming by reducing innovation and increasing lock-in.

Market Evolution

In the next two years, we expect the following evolution in the SASE platform market:

- Increased adoption of SASE platforms and a shift away from dual-vendor SASE will continue as capabilities improve, refresh cycles come up, and security and networking teams collaborate.
- Vendor consolidation typically is more important than protecting against vendor lock-in, but customers with distinct networking and security requirements will likely stay with dual-vendor SASE.
- We expect more vendors to exit the market due to the high cost of maintaining a solution from a core competency, technology and investment perspective.
- At the same time, we expect more regional suppliers will enter the market to address sovereign use cases in areas such as Europe.

AI advances will continue in the SASE platform market, where GenAI assistants will become standard capabilities for both network security and networking use cases. Vendors will improve the security of GenAI applications and inspection of end-user prompts, and will extend security of GenAI applications to private GenAI-enabled applications and models. AI agents with process automation within the SASE platform will advance so that more of the

day-to-day networking and network security functions are automated. AI will be leveraged for capabilities such as near-real-time network troubleshooting, threat intelligence and microsegmentation. Support for unmanaged and nonhuman devices/users will expand into several options, including reverse proxies, dissolvable agents, browser plug-ins, remote browser isolation and local browser isolation (either through a separate secure enterprise browser or tighter integration with browser security capabilities exposed by Google and Microsoft).

SASE platform vendors will expand into adjacent markets, such as endpoint security, endpoint DLP, data security posture management (DSPM), SaaS security posture management (SSPM), microsegmentation, NDR, network access control, and wired and wireless LAN to support SD-Branch. As a result, while some aspects are beneficial to customers, there will be a risk of overplatformed solutions which may impact the quality of individual solutions meant for SASE buyers.

We also expect vendors will offer postquantum cryptography (PQC) algorithms as standard to enhance data security and prevent harvest now/decrypt later attacks. Vendors will increasingly have their vulnerabilities exposed quicker and risk attackers compromising enterprise infrastructure. The result will be a much faster response to offering patches and accelerate the patch management process for customers.

⊕ Evidence

⊕ Evaluation Criteria Definitions