Magic Quadrant for Security Service Edge

29 July 2026 - ID G00835657 - 33 min read

By John Watts, Thomas Lintemuth, and 2 more

Security service edge is a mature market that consolidates multiple access-related security point offerings into a single cloud-centric, converged platform driven by hybrid work and cloud adoption. Evaluate security-focused vendors in the context of a dual-vendor secure access service edge strategy.

Market Definition/Description

Gartner defines security service edge (SSE) as an offering that secures access to the web, cloud services and private applications regardless of the location of the user, the device they are using or where that application is hosted. SSE protects users from malicious and inappropriate content on the web and provides enhanced security and visibility for the SaaS, generative AI and private applications accessed by end users.

Security service edge provides a primarily cloud-delivered solution to control access by end users and devices to applications, websites and the internet. It provides a range of security capabilities, including adaptive access based on identity and context, malware protection, data security and threat prevention, as well as the associated analytics and visibility.

SSE reduces latency by enabling more direct connectivity for hybrid users and providing the potential for improved user experience. Capabilities that are integrated across multiple traffic types and destinations allow a more seamless experience for both users and administrators while maintaining a consistent security stance.

Mandatory Features

The mandatory features of this market include:

- Management and data planes that are primarily cloud-delivered
- Identity-aware forward proxy with decryption for data- and threat-protection capabilities
- In-line threat and protection of data in generative AI, SaaS and private apps
- Out-of-band protection of data in SaaS apps via API integration
- Adaptive and granular access control supporting both devices with an SSE agent (or similar traffic steering method) and devices with no local SSE software or configurations
- Integration with an identity provider

Optional Features

The optional features of this market include:

- Single integrated console supporting all features and functions of the platform
- Ability to apply controls consistently across multiple network and application destinations
- Support for managing and securing traffic from all common endpoints (such as Windows, macOS, iOS and Android devices)
- Support for managing and securing traffic from a full stack secure enterprise browser or extension
- Integration with key enterprise technologies such as security information and event management (SIEM), workspace security, SD-WAN and other adjacent technologies
- Support for published and documented APIs that are accessible to the customer and that allow automation of common tasks and integration with other security platforms
- Curated, managed and risk-scored catalogs of SaaS and generative AI applications
- Control of traffic on all ports and protocols
- Remote browser isolation (RBI) to enhance security across all network destinations and channels
- SaaS security posture management for visibility and remediation of SaaS configurations and visibility into SaaS plug-in applications and connections

- Read, write and act-upon labels from common data classification platforms
- Embedded user entity behavior analytics (UEBA) to provide automated detection and response for anomalous and risky devices and user behaviors

Magic Quadrant

Figure 1: Magic Quadrant for Security Service Edge

Gartner

Vendor Strengths and Cautions

Broadcom

Broadcom is a Niche Player in this Magic Quadrant. It offers Symantec Cloud Secure Web Gateway (SWG) with add-ons for Symantec ZTNA, full browser isolation, Symantec CloudSOC cloud access security broker (CASB), Symantec Data Loss Prevention and cloud sandboxing.

Broadcom's operations are geographically diversified, and its clients tend to be very large enterprises across a wide variety of sectors. Over the last 12 months, Broadcom divested the VeloCloud product line, which delivered SD-WAN capabilities. It migrated discrete SSE component consoles into a unified Symantec Enterprise Console, introduced more granularity for policy controls for ZTNA and Cloud SWG, and added a dedicated Microsoft Copilot Gatelet and an integrated system for cross-domain identity management (SCIM) support for user provisioning in its CASB.

Broadcom declined requests for supplemental information. Gartner's analysis is therefore based on other credible sources.

Strengths

- **Geographic Strategy:** Broadcom offers a hybrid SWG as part of its SSE offering that meets the needs for organizations with on-premises proxy and sovereignty requirements.
- **Overall Viability:** Broadcom scores highest for financial strength overall with significant investments in its broader cybersecurity portfolio, including Symantec SSE products.
- **Innovation:** Broadcom continues to invest in research and development for cloud-delivered security services and aligns innovations with the needs of its legacy proxy customer base.

Cautions

- **Market Understanding:** Broadcom divested VeloCloud in 2025 and no longer has a clear path to evolve SSE into a secure access service edge (SASE) platform offering long term.
- **Product:** Broadcom only provides a few Gatelets for deeper, granular controls to secure the use of generative AI.
- **Market Responsiveness/Record:** Compared to other providers, Broadcom exhibits a slower pace in addressing new market demands, such as the implementation of generative AI controls.

Cisco

Cisco is a Challenger in this Magic Quadrant. It offers Cisco Secure Access, which focuses on enabling customers to secure a hybrid workforce from the cloud and includes domain name system (DNS) defense essentials that upgrade to full SSE suite capabilities with higher licensing tiers.

Cisco's operations are geographically diversified, and it is growing its enterprise customer base for its stand-alone SSE product. Over the past 12 months, Cisco announced or acquired companies to integrate with its product lines including Astrix for nonhuman identities. It has expanded its cloud points of presence on its Cisco Edge V2 architecture and announced "Zero Trust Access (ZTA) for Internet Destinations" to secure all internet-bound transmission control protocol (TCP) and user datagram protocol (UDP) traffic.

Strengths

- **Sales Strategy:** Cisco's sales strategies, including its plan to upsell and migrate its large, existing Cisco Umbrella customer base, are likely to increase its SSE adoption.
- **Product:** Cisco Secure Access offers strong digital experience monitoring (DEM) and DNS security relative to other SSE vendors in the market.
- **Market Responsiveness/Record:** Cisco was early addressing the need for generative AI security as part of SSE, compared to other vendors in the market.

Cautions

- **Overall Viability:** Cisco has reported flat revenue for its security division the past few quarters, and its investments focus on expanding and investing in SASE platforms more than stand-alone SSE.
- **Innovation:** Cisco's recent innovations, such as its flexible single-pass security pipeline, are catching up to the market, and planned future innovations around AI agent security are unlikely to shape the SSE market.
- **Offering (Product) Strategy:** Cisco's product strategy focuses on endpoint security, AI identity and data security posture management (DSPM) expansion which are adjacencies to the SSE market.

Cloudflare

Cloudflare is a Visionary in this Magic Quadrant. It offers Cloudflare One, a unified SSE offering supported by the largest network of physical POPs in this evaluation. Cloudflare One recently simplified licensing for SSE to three bundled tiers of Interna package offerings.

Cloudflare's operations are geographically diversified, with a significant percentage of its enterprise customer base made up of midsize organizations. Over the last 12 months, Cloudflare acquired companies to integrate with its product lines outside of Cloudflare One. It released end-to-end postquantum SSE and SASE encryption supporting hybrid module-lattice-based key-encapsulation mechanism (ML-KEM) for Cloudflare IPsec, artificial intelligence security posture management (AISPM) capabilities and a Model Context Protocol (MCP) server portal.

Cloudflare announced a reduction of 1,100 positions, or approximately 20% of their workforce, on 7 May 2026. This announcement occurred outside Gartner's analysis window and was not assessed in this evaluation.

Strengths

- **Innovation:** Cloudflare's planned innovations for postquantum readiness are increasingly important to SSE buyers.
- **Pricing:** Cloudflare simplified its pricing for Cloudflare One and offers a midtier package covering basic SSE requirements at a low cost relative to others in the market.
- **Geographic Strategy:** Cloudflare offers a strong option of cloud points of presence globally and supports more languages in its administrative UI than many vendors in this market.

Cautions

- **Product:** Many of the core product features for Cloudflare One, such as the number of software as a service (SaaS) supported for application programming interface (API) integrations and adaptive access controls, are weaker compared to Leaders in this market.
- **Marketing Execution:** Cloudflare lacks visibility in the market and is often not cited on shortlists of Gartner clients when evaluating SSE providers.
- **Market Responsiveness/Record:** Cloudflare's market responsiveness lags behind other vendors in the SSE market when introducing certain features, such as sovereign SSE and generative AI security.

iboss

iboss is a Niche Player in this Magic Quadrant. It offers the iboss AI-Powered SASE Platform. Its SSE security stack can be deployed in multiple environments, including private cloud or as a hosted service, and supports local repatriation requirements by design.

iboss's operations are mainly focused in North America and Europe, and its SSE sales focus is on very large enterprises. In the last 12 months, iboss launched its AI-powered CASB and dual-risk scoring for application and data loss assessments to improve visibility and control of vibe-coded applications.

Strengths

- **Product:** iboss offers a strong web security, in-line SaaS security and private application access capability relative to others in the market.
- **Market Understanding:** iboss focuses on the SSE market with a current direction toward SASE platforms by including SD-WAN in its offering rather than as a paid add-on.
- **Market Responsiveness/Record:** iboss was early, relative to other vendors evaluated in this research, in providing sovereign options to run the full SSE technology stack across cloud, local and colocated locations.

Cautions

- **Sales Execution:** Gartner estimates that iboss is growing its SSE customers at a slower rate compared to other vendors in the market.
- **Marketing Execution:** iboss lacks visibility in the market and is rarely cited on shortlists of Gartner clients.
- **Marketing Strategy:** The vendor's plan to target roles outside of the traditional SSE buying center, such as AI security leaders, is unlikely to improve visibility on prospects' shortlists when assessing SSE vendors.

Netskope

Netskope is a Leader in this Magic Quadrant. It offers Netskope One SSE, which prioritizes cloud and data security.

Netskope's operations are geographically diversified, and its SSE clients tend to be very large enterprises across a wide range of industries. In the last 12 months, Netskope executed its

initial public offering and is now a publicly traded company. It launched AgentSkope, an architectural foundation for deploying AI agents supporting SSE workflows; an AI security suite; and Netskope One Copilot for Private Access to make ZTNA policy recommendations.

Strengths

- **Customer Experience:** Netskope has above-average customer experience relative to the SSE market, based on a mix of internal and public data sources.
- **Marketing Execution:** Netskope has high market visibility relative to others in the market and is often cited on client shortlists when evaluating SSE vendors.
- **Innovation:** Netskope's AgentSkope is positioned to accelerate its ability to provide agentic operations in the future, which is likely to shape the SSE market.

Cautions

- **Pricing:** Netskope offers comparatively complicated licensing, and feedback from Gartner clients indicates that pricing tends to be higher than average.
- **Sales Strategy:** Netskope's focus on selling broader AI security and governance is unlikely to resonate with SSE buyers not responsible for securing AI application development pipelines.
- **Market Understanding:** Netskope's assessment of its strengths and weaknesses within the competitive landscape is overly focused on in its core differentiators, compared to competitors that have closed the gaps over the past few years.

Palo Alto Networks

Palo Alto Networks is a Leader in this Magic Quadrant. It offers Palo Alto Networks Prisma Access SSE and focuses on security efficacy to secure hybrid work, and deploys Prisma Access POPs across major hyperscaler cloud providers.

Palo Alto Networks' operations are geographically diversified with a large customer base across multiple industries and sizes. In the past 12 months, Palo Alto Networks acquired companies including CyberArk for identity management to integrate with its products. It launched AI Access Security based on its Precision AI framework to deliver AI usage control capabilities and Prisma Access 6.1, which includes improved capabilities such as SASE Private Location to improve user-to-application performance and disaster recovery.

Strengths

- **Overall Viability:** Palo Alto is one of the strongest vendors financially in this market and positioned to invest and expand its SSE offering as part of its platform strategy.
- **Marketing Execution:** Palo Alto has high visibility relative to others in the market and is often cited on client shortlists when evaluating SSE vendors.
- **Market Understanding:** Palo Alto shows an understanding of how to address product weaknesses, such as administrative complexity, and is likely to shape the future of the SSE market with its dual-vendor and SASE platform deployments.

Cautions

- **Offering (Product) Strategy:** Palo Alto's product platform strategy creates risk in that its SSE overlaps and requires investments in products out of scope for the SSE buyer, such as AI runtime defense and nonhuman AI agent identity management.
- **Pricing:** Gartner client feedback and internal assessments show Palo Alto is one of the most complex and expensive vendors to procure relative to others in the SSE market.
- **Innovation:** Palo Alto's planned innovations, such as autonomous defense focused on protecting legacy and OT environments, are more aligned with hybrid mesh firewalls and SASE platforms than with SSE buyers.

Skyhigh Security

Skyhigh Security is a Niche Player in this Magic Quadrant. It offers Skyhigh Security Service Edge, which focuses on data security capabilities. The vendor operates both physical and cloud-provider-hosted POPs, depending on local demand, and may dynamically provision services on-demand at some POPs to balance efficiency and performance SLA attainment.

Skyhigh's operations are geographically diversified, and its SSE clients tend to be larger, highly regulated industries. In the past 12 months, Skyhigh launched Secure Browser Controls focused on securing any browser through JavaScript injection, and a hybrid SSE architecture.

Strengths

- **Customer Experience:** Skyhigh has above-average customer experience feedback relative to others in the market, primarily reflected in internal Gartner client data and public sources.

- **Sales Strategy:** Skyhigh's sales strategy focused on key verticals is likely to resonate with prospects in its target market.
- **Product:** Skyhigh's SSE supports one of the strongest data security capabilities relative to other vendors in the market.

Cautions

- **Sales Execution:** Gartner estimates Skyhigh is growing its SSE customers at a slower rate compared to other vendors in the market.
- **Offering (Product) Strategy:** Skyhigh's product strategy primarily centers on data security rather than an evolution toward SASE platforms.
- **Innovation:** Skyhigh's recent and planned innovations regarding DSPM align more with data security buyers than the broader needs of SSE buyers.

Zscaler

Zscaler is a Leader in this Magic Quadrant. It offers the Zscaler Zero Trust Exchange platform as its SSE product, which includes zero-trust capabilities delivered via its proxy-based architecture.

Zscaler's operations are geographically diversified, and its SSE clients tend to be very large enterprises. Zscaler has acquired several companies to integrate with its SSE, including SPLX (in May 2025) for AI security, SquareX (in February 2026) for secure enterprise browser capabilities, and Red Canary (August 2025) for managed detection and response (MDR) services. Zscaler launched its B2B exchange for direct Zscaler Private Access (ZPA) connectivity, the Zscaler AI Security Suite to improve visibility and control of AI, and its quantum-ready capabilities for Zscaler Internet Access (ZIA).

Strengths

- **Product:** Zscaler has strong AI usage and control capabilities relative to others in the SSE market.
- **Innovation:** Zscaler's planned and recent innovations for agentic operations and building out a separate AI security platform integrated with SSE are well aligned with the emerging needs of SSE buyers.

- **Marketing Execution:** Zscaler has high visibility relative to others in the market and is often cited on client shortlists when evaluating SSE vendors.

Cautions

- **Sales Strategy:** Zscaler's sales strategy focuses on using SSE to advance SASE platform sales and is unlikely to increase stand-alone SSE sales.
- **Pricing:** Gartner client feedback indicates that Zscaler's platform packaging includes adjacent capabilities and requires multiple add-on SKUs for advanced core SSE capabilities.
- **Customer Experience:** Zscaler has lower-than-average customer experience compared to others in the SSE market, based on a mix of internal and public data sources.

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

- Cisco

Dropped

- Fortinet
- Versa

Inclusion and Exclusion Criteria

To qualify for inclusion, the provider's SSE offering must:

- Be operated as a service. The offering must be delivered primarily as a cloud-hosted ("SaaS") service securing authorized users on allowed endpoints to appropriate services

running in public or private clouds and on-premises environments.

- Demonstrate broad market adoption as an independently deployed SSE offering, separate from any SD-WAN or other networking capabilities provided by the same vendor, with strong supporting evidence available to Gartner. These capabilities must have been generally available by 1 May 2026. The capabilities are:
  - Secure access to the internet from common managed devices (including, at minimum, Windows, macOS, Android, and iOS) via proxy. Provide URL filtering and advanced threat defense to protect users and enforce acceptable use policies.
  - Secure usage of software-as-a-service both through in-line visibility and controls AND via API integration
- Provide visibility, compliance enforcement, data security and threat protection for the use of SaaS and generative AI applications.
- Both monitor and remediate issues via a proxy product (in-line) and API integrations:
  - API integration for CASB functions must include coverage of at least five of the following SaaS apps: Microsoft Office 365, Google Workspace, Salesforce, Workday, Oracle Fusion/Oracle Business Suite, Microsoft Dynamics/Dynamic 365, ServiceNow, Snowflake, Palantir, Atlassian Suite, GitHub. Security must include threat protection, data protection, and both detection and prevention capabilities.
  - In-line security must be provided from managed devices to any SaaS application. It must be enforceable from unmanaged devices via integration with an identity provider (IdP) to control access to SaaS applications integrated with the IdP. Security must include threat protection, data protection, and both detection and prevention capabilities.
- Provide secure remote access to private applications hosted on-premises or in the public cloud using zero-trust principles by incorporating identity and context-based logical access boundaries for access.
- Provide visibility, basic controls (e.g., block, warn, allow) and inspection for sensitive data for at least three of the following generative AI apps: Microsoft Copilot, OpenAI Chat GPT, Google Gemini, Grok AI, Perplexity, DeepSeek, Anthropic Claude and initiated by an end user from the endpoint.

- Provide visibility to the state of common, managed endpoints through a native agent for third-party integrations on Windows, macOS, Android and iOS, and enable access decisions in that context.

An SSE vendor must also demonstrate scale relevant to enterprise-class organizations measured by all of the following criteria:

- As of 1 March 2026, have at least 300 large enterprise customers securing web, SaaS and private applications using their primary SSE product independent of their SD-WAN, or grew at least 50% in number in the past 12 months.
- As of 1 March 2026, have at least three million seats securing web, SaaS and private applications using their primary SSE product independent of their SD-WAN under paid support, or grew at least 50% in number of seats under paid support in the past 12 months.

An SSE vendor must also demonstrate relevance to global organizations by:

- Leveraging POP infrastructure meeting all the following requirements:
- Presence in at least 15 distinct geographic metropolitan cities globally, with at least three distinct metropolitan cities in each of the three major regions: EMEA, North and South America, and the Asia/Pacific region.
- POPs are in a highly secure facility and offer all of the following services locally (intra-POP) generally available to all enterprise customers: web proxy, private access and in-line SaaS control with high availability.
- Provide a publicly available URL with POP metropolitan cities list, POP monitoring/status capability and a documented POP SLA.
- Strong evidence that 10% or more of its customer base is outside its home region (North America, EMEA or the Asia/Pacific region) and that it is actively marketing and enhancing its SSE offering.
- Primarily selling its SSE functionality independent of its SD-WAN or SASE platform offering, strategic roadmap investments for SSE independent of SASE platforms, and/or showing Gartner evidence that customers are primarily evaluating SSE as a stand-alone capability independent of the vendor’s SASE platform offering.

Honorable Mentions

- **Check Point Software Technologies** is investing in SSE as part of its SASE platform.
- **Fortinet** is investing in SSE as part of its SASE platform.
- **Fortra** is investing in the SSE market and expanding its capabilities.
- **HPE Networking** is investing in SSE as part of its SASE platform.
- **Microsoft** is investing in the SSE market and expanding its capabilities.
- **Versa Networks** is investing in SSE as part of its SASE platform.

Evaluation Criteria

Ability to Execute

Product or Service: The capabilities, features and overall quality of the core goods and services that compete in and or serve the defined market.

We assess specific current product capabilities, quality and feature sets, whether offered natively or through original equipment manufacturer (OEM) agreements or partnerships, as defined in the Market Definition section and detailed in the subcriteria. Capabilities assessed include: securing private applications, in-line cloud-enforced security, SaaS app control and visibility, ease of administration, data security, threat protection, adaptive access, AI security, enterprise integration, and sovereignty.

Overall Viability: The organization's overall financial health, as well as the financial and practical success of the relevant business unit. This includes the likelihood that the organization can continue to offer and invest in the product, as well as the product's position in the organization's portfolio.

We evaluate the vendor across multiple areas such as marketing, sales, product development and support in the business unit and their investments to expand their SSE offering.

Sales Execution/Pricing: The organization's capabilities in all presales activities and the structures that support these activities. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

We evaluate the growth of the business, how pricing and licensing is offered to customers and its relative ease of consumption, evidence of the ability to build and maintain strong relationships with end customers, and the value of the product for its cost.

Market Responsiveness/Record: The ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This includes the provider's history of responsiveness to changing market demands.

We evaluate the vendor's track record in delivering the right capabilities at the right time to address customer needs, compared with competitors. We also evaluate the vendor's history of responsiveness in terms of changing market demands and addressing limitations to remain competitive. Our assessment is not limited to SSE product responsiveness as it also involves responsiveness for the supporting activities around a product offering, including pricing, licensing models, go-to-market and overall competitive dynamics.

Marketing Execution: The ability to deliver clear, high-quality, creative and effective messaging via publicity, promotional activity, thought leadership, social media, referrals and sales activities. This includes the organization's ability to influence the market, promote the brand, increase awareness of products and establish a positive reputation among customers.

We evaluate the clarity of messaging and its efficiency, as well as if it is clearly differentiated and aligned with their product capabilities. We also assess investments in marketing, and if these investments are delivering results in how prominently clients consider the vendor.

Customer Experience: The degree to which a vendor's products, services and programs enable customers to achieve their desired results. This includes the quality of supplier/buyer interactions, technical support or account support, as well as ancillary tools, customer support programs, availability of user groups and service-level agreements.

We evaluate the customer experience inclusive of presales and postsales activities. This includes the customer's experience with the vendor. Additionally, we assess how the vendor manages customer experience and employee engagement.

Ability to Execute Evaluation Criteria

Evaluation Criteria	*Weighting*
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	Low
Marketing Execution	Medium
Customer Experience	High
Operations	NotRated

Source: Gartner (July 2026)

Completeness of Vision

Market Understanding: The ability to understand customer needs and translate that understanding into products and services. Vendors with a clear vision of the market listen to and understand customer demands, and they can shape or enhance market changes with their vision.

This criterion assesses the vendor's ability to understand the emerging 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: The ability to clearly communicate differentiated messaging, both internally and externally, through social media, advertising, customer programs and positioning statements.

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 that vendors reach customers, how they reach evolving customer buyer personas, and how they plan to communicate their message to drive market demand.

Sales Strategy: The ability to create a sound strategy for selling that uses the appropriate networks including direct and indirect sales, marketing, service and communication. This includes partnerships that extend the scope and depth of a provider's market reach, expertise, technologies, services and their customer base.

We assess the vendor's proposed use of direct and indirect sales and related investments to add new customers and/or extend sales within existing customers. We also assess how a vendor articulates a clear, relevant and differentiated sales strategy that resonates with customers and reaches new buyer personas and go-to-market strategies and emerging pricing models.

Offering (Product) Strategy: The ability to approach product development and delivery in a way that meets current and future requirements, with an emphasis on market differentiation, functionality, methodology and features.

We evaluate the vendor's SSE product around existing and future capabilities. This evaluation includes not just the raw features, but also the vendor's overall architecture, and how this architecture provides value to the end customer. We also assess whether the vendor closes key gaps in its existing offering and strategy across various capabilities.

Innovation: Marshaling of resources, expertise or capital for competitive advantage, investment, consolidation or defense against acquisition.

We evaluate plans for differentiated capabilities that will enhance the vendor's ability to attract customers and drive business. We assess recent and planned innovations and if they are true "game changers" with an emphasis on future innovations, and assess if these innovations will disrupt the market via shifting customer expectations and/or will force competitors to react.

Geographic Strategy: The ability to direct resources, skills and offerings to meet the specific needs of regions outside the providers' home region, either directly or through partners, channels and subsidiaries.

We assess whether the strategy is clear and will resonate with customers in order to grow adoption on a global basis including messaging, partnerships, and sales channels. We assess a vendor's plans to address specific needs within geographies and the vendor's ability to address any unique requirements such as regional sovereignty.

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

Source: Gartner (July 2026)

Quadrant Descriptions

Leaders

Leaders are vendors with strong momentum in terms of sales and mind share. They have track records of delivering well-integrated SSE components with advanced functionality and demonstrate a clear understanding of the market. Additionally, they possess a product strategy that aligns with the market trend for providing easy-to-use advanced features and

making business investments for the future. Leaders have effective sales and distribution channels for their entire product portfolios, a well-diversified vertical and geographic strategy, and a vision for how SSE offerings are positioned within the context of organizations' wider SASE transformations.

Challengers

Challengers offer SSE components that may not be tightly integrated or may lack sophisticated features and alignment with the market's direction. They may compensate for this with a strong sales channel (possibly in adjacent security areas), strategic relationships or extensive visibility in the market. They are often late to introduce new features and lack a complete, unified product strategy. Challengers appeal largely to clients that have established strategic relationships with them.

Visionaries

Visionaries are distinguished by technical and/or product strategies but lack either the track record of execution and the high visibility of Leaders or corporate resources, such as strong sales channels and strategic relationships. Buyers should expect a complete SSE offering with some advanced features or unique approaches to the market, but be wary of strategic reliance on them and monitor their viability closely.

Niche Players

Niche Players' products are typically solid offerings in terms of one or more discrete SSE components but are focused on fewer areas, such as technical capabilities, geographic support or vertical industries. Additionally, Niche Players lack the market presence and resources of Challengers and the forward-looking vision and market alignment of Visionaries. They merit attention from the types of buyers on which they focus.

Context

This Magic Quadrant focuses on vendors relevant to large enterprises with a broad global footprint offering stand-alone SSE capabilities as part of a dual SASE deployment often integrated with a multivendor edge networking capability. SSE buyers are led by security teams that do not have the budget or remit to change their edge networking at the same time they are buying the security capabilities of a SASE framework. Vendors selling and marketing

stand-alone SSE put an emphasis on partnerships and interoperability with third-party SD-WAN providers rather than their own SD-WAN offering. However, the trend in the market is toward SASE platforms, and vendors in this Magic Quadrant with a product direction and offering for SASE platform tend to score better on vision.

Gartner sees impacts to SSE buyers due to geopolitical landscape changes and an increased interest in sourcing vendors from regional providers with less dependency on foreign-provided security products. All vendors assessed in this Magic Quadrant are headquartered in North America and typically have legal entities or subsidiaries in other countries. Most vendors offer large cloud POPs and various sovereignty options to address a growing demand by organizations to control networking and data within specific geographic boundaries.

The shift in SSE buying evaluations due to the rapid adoption of AI shapes buyer priority in the market, but most SSE buyers are not responsible for all AI security and governance. Vendors score better when targeting the needs of SSE security buyers with capabilities to secure the use of AI by end users specifically rather than the whole of AI security more tightly coupled with SSE product offerings.

Finally, evaluations by SSE buyers increasingly include questions about postquantum readiness and crypto agility. Vendors generally score better by offering postquantum support today and a vision to enable postquantum readiness in the future.

Market Overview

SSE Architecture

Vendors vary in the architecture and delivery models of their SSE offerings. Most offer a multitenant cloud architecture that uses custom-built cloud POPs in colocated data centers, POPs of major hyperscaler cloud tenants or a mixture of both. Increasingly, vendors provide virtual or hardware-based appliances that extend the SSE data plane from the cloud to on-premises locations. This enables local traffic processing and resilience against unplanned cloud downtime.

Prospective customers typically care about POP proximity to their end users and rely on proof of concept (POC) testing to evaluate a vendor's ability to deliver acceptable latency, reduce the attack surface and maintain stable access to the SSE data plane across diverse endpoints and locations. Features such as Layer 3 VPN, IP address retention, full packet capture (PCAP),

secure ICAP and other capabilities found in legacy on-premises point solutions remain important for a subset of organizations that must support legacy third-party connections or specific cybersecurity architecture requirements.

Vendors Differentiating in Adjacent Features

Vendors in this market display varying levels of maturity across components and capabilities, especially in the depth and breadth of their SaaS security, GenAI security, advanced data security features and DEM. Capabilities such as protection of all ports and protocols from user devices are now common and no longer seen as differentiators by most Gartner clients.

Some vendors have added Layer 3 VPN and local enforcement points to augment their proxy-based zero-trust network access (ZTNA), enabling a “universal ZTNA” capability for accessing all applications from any location using zero-trust principles.

SASE Platforms and Overconsolidation Risk

Many vendors in the SSE space are positioned to compete for SASE platform opportunities by adding at least a lightweight SD-WAN option to their offerings, but they still document or promote third-party SD-WAN partnerships or integrations. This is important for SSE buyers who may not be able or may not desire to deploy SD-WAN tied to their choice of SSE. Many are also building broader cybersecurity platforms that extend into adjacent markets such as endpoint security, DSPM and security operations functions. This expansion creates friction and buyer frustration, making it harder to compare vendors on SSE capabilities because features are tied to adjacent products, such as AI assistants accessed from a console tied to security operations capabilities.

New platform licensing models are often more expensive but provide access to at least basic versions of adjacent tools, encouraging adoption. Extending SSE into adjacent areas creates overlaps with existing technologies and forces teams to rationalize their cybersecurity tool stack to eliminate overhead and waste from underutilized products.

Market Evolution

The SSE market is mature, with vendors expanding beyond core features. Gartner estimates the 2026 SSE revenue component of SASE will approach $13 billion worldwide (see Forecast Analysis: Secure Access Service Edge, Worldwide, 2025-2030). Most vendors have integrated their discrete components into a unified SSE platform that can be configured from a single

console with a single agent, a single data model and a single-pass inspection data plane. Vendors from adjacent markets target displacement of SSE vendors with narrowly focused, less expensive and limited capabilities. These vendors tend to focus on browser-only or endpoint-only security, limited URL filtering, basic data security capabilities, in-line-only SaaS controls, or stand-alone secure remote access for private applications.

Broad market trends driving the market evolution of SSE include:

- **AI transformation:** Traditional drivers for SSE, such as replacing perimeter security to support hybrid work access to workloads in any location, are giving way to AI-driven transformation initiatives. Customers report gaps in secure use of AI from existing SSE providers.
- **VPN replacement:** Attackers are increasing their focus on vulnerabilities in secure infrastructure located on an organization's perimeter, such as Layer 4 VPN appliances, network firewalls and gateways. SSE offers an alternative access method using ZTNA technologies.
- **Zero-trust networking:** Zero-trust initiatives are reaching higher levels of maturity, transitioning from pilots and experiments to full-scale operations. SSE vendors offer secure "user-to-application" access when integrated with identity and endpoint security solutions.
- **Geopolitics:** The continued fracture of regulations and requirements for data residency and processing across geographies creates opportunities for regional SSE providers, and global SSE vendors are increasingly adding the ability to geopatriate workloads to customer or regional data centers.

⊕ Evidence

⊕ Evaluation Criteria Definitions

With unmatched, proprietary AI insights from Gartner

Explore the AI Hub ↗