Magic Quadrant for Security Service Edge

20 May 2025 - ID G00815904 - 33 min read

By Charlie Winckless, Thomas Lintemuth, and 2 more

Security service edge is a dynamic market that consolidates multiple access-related point offerings into a single cloud-centric converged offering. This Magic Quadrant will help buyers evaluate key vendors ideally in the context of a SASE 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 and private applications accessed by end users.

Security service edge provides a primarily cloud-delivered solution to control access from end users and devices to applications, as well as 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. It enables more direct connectivity for hybrid users by reducing latency 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 and protection capabilities
- In-line protection of data in 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 external identity providers

Common Features

The common 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)
- Integration with key enterprise technologies such as security information and event management (SIEM), extended detection and response (XDR), 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 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
- Continuous adaptive access controls across all channels based on initial connection status and any change in state during connection
- 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 device and user behaviors
- Ability to apply advanced data protection capabilities

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 Network Protection, which includes both cloud and local protection for websites, and is supported by Symantec DLP Cloud for clients who need data loss protection functionality.

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 has made incremental updates to its SSE product, including an Agent Traffic Manager that allows control of routing on connected agents and making its zero-trust network access (ZTNA) available on Microsoft Azure Marketplace. It was developing a single unified console for SSE features during the period of this research.

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

Strengths

- Broadcom offers strong data security integration with its enterprise data loss prevention (DLP) offering, simplifying integration with enterprise environments.
- Broadcom's market approach and support strategy focus on the needs of very large, complex and highly regulated enterprises.
- Broadcom offers a well-known and broadly installed endpoint protection platform (EPP) and endpoint detection and response (EDR) product and has converged this with its SSE agent.

Cautions

- Broadcom focuses on selling enterprise licenses to a subset of very large clients, which impacts its ability to optimally support smaller organizations.
- Broadcom's SSE appeals primarily to existing customers and prospects already committed to the broader portfolio of cybersecurity and infrastructure technologies that this vendor supplies.
- Broadcom has multiple consoles and less integration in its SSE than is typical in this market.

Cloudflare

Cloudflare is a Niche Player in this Magic Quadrant. It offers Cloudflare One, a unified SSE offering supported by the largest network of physical points of presence (POPs) in this evaluation. Cloudflare One offers a free tier for up to 50 users.

Cloudflare's operations are geographically diversified, and its SSE clients tend to be smaller organizations or small deployments within larger organizations. Over the last 12 months, Cloudflare has acquired BastionZero to support developer and infrastructure access ZTNA cases and Kivera to control API-driven changes to hyperscaler configurations. It has also enhanced its data security offerings, continuing to add regex classifiers for more data types.

Strengths

- Cloudflare has an extensive set of existing content delivery network (CDN) and web application and API protection (WAAP) customers. It also has a pool of funds contracting approach it can leverage for cross-sell opportunities, which should help the company grow and maintain relevance to end users.
- Cloudflare has the largest POP network for onramping traffic to its cloud in this evaluation and continues to expand and grow this network, enabling it to support clients with coverage needs in more remote areas of the world.
- Cloudflare is a large and publicly traded company with a solid investment in SSE, which helps the company sustain viability long term.

Cautions

- Cloudflare's technical capabilities lag behind others in this market in areas such as data security, SaaS discovery, risk scoring and adaptive access.
- Cloudflare's strategy for resilience depends solely on the strength of its network architecture, which isn't sufficient for some customers seeking alternate data planes.
- Cloudflare's pricing as evaluated during this research is high for the level of capability delivered, and Gartner clients have reported that per-service pricing is not clear when Cloudflare bundles its SSE with other services.

Fortinet

Fortinet is a Challenger in this Magic Quadrant. It offers FortiSASE, which includes integrated SSE capabilities and a separate API CASB (FortiCASB). All functions are based on the vendor's proprietary FortiOS. Fortinet offers POPs on both Google Cloud and Fortinet's own

hardware and by default limits the number of POPs a client can use. Customers can deploy a combination of both infrastructures and increase POPs accessed by purchasing higher license tiers.

Fortinet's operations are geographically diversified, and its SSE clients tend to be existing Fortinet firewall and software-defined WAN (SD-WAN) clients, which covers a range of industries and clients of all sizes. Over the last 12 months, Fortinet has integrated the majority of its SSE features into two consoles, with API CASB requiring a separate configuration, and added agentless ZTNA to its portfolio. The vendor also introduced a unified agent for its endpoint protection and SSE features.

Strengths

- Fortinet is a large and well-funded vendor with a strong customer base and a public commitment to grow its SSE offering and market share further.
- Fortinet has a large existing customer base that it can leverage to expand its SSE presence and grow in the market through strength in customer focus.
- Fortinet's pricing is highly competitive in this market for the technical features offered when Fortinet's own non-Google Cloud Platform (GCP)-hosted POPs can be used.

Cautions

- Fortinet's approach to ZTNA, which requires an exposed FortiOS appliance at every termination, and its FortiOS-everywhere design limit its appeal to non-Fortinet customers and customers who do not want to maintain and update these exposed systems.
- Fortinet maintains two separate POP networks and requires specific higher tier licenses, and increased costs to use POPs from either their larger GCP-hosted environment or from both environments. Fortinet also limits both the number of POPs an end user can select to connect to and the devices supported per user.
- Fortinet's infrastructure-centric approach is unlikely to effectively advance the SSE market as it necessitates the use of virtual or hardware appliances to adopt some SSE services, effectively steering consumers toward FortiSASE.

iboss

iboss is a Niche Player in this Magic Quadrant. It offers iboss Zero Trust SASE, which is focused on the National Institute of Standards and Technology (NIST) 800-207 approach to

zero trust. Its SSE security stack can be deployed in multiple environments, including private cloud, while still being managed from the central management plane, and its POPs are hosted in many internet exchanges.

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 has integrated SD-WAN natively into its platform and can now deliver its offering directly in Azure from the Azure Marketplace.

Strengths

- iboss offers strong web security capabilities as well as customizable user-risk-scoring capabilities.
- iboss is expanding its sales and marketing efforts to grow its presence in the market and enable faster growth.
- iboss has good global POP coverage, enabling it to support geographically dispersed clients.

Cautions

- Financial information about the vendor is limited, and iboss rarely appears in Gartner inquiry or on competitive shortlists. Buyers should perform additional validation of this vendor.
- iboss' product cost is higher than that of other vendors in the market for equivalent functionality based on our assessment.
- iboss offers fewer SaaS security capabilities such as the number of API integrations and SaaS security posture management (SSPM), as well as less mature digital experience monitoring (DEM) than its competitors. It also provides less advanced data protection, such as lacking data or field encryption and lacking enterprise DLP integration capabilities.

Netskope

Netskope is a Leader in this Magic Quadrant. It offers Netskope One SSE, which is built on the vendor's proprietary NewEdge network supporting physical POPs.

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 has

extended its DEM capabilities by more fully integrating its 2023 Kadiska acquisition and extended AI support for customer-enablement functions.

Strengths

- Netskope offers strong technical capabilities across all areas of SSE and can support the vast majority of customer use cases.
- Netskope shows a strong understanding of this market and its trends, typically supporting many end-user SSE journeys.
- Netskope is often seen on customer shortlists, reflecting the brand awareness it enjoys and enhancing its ability to grow and continue to supply services in this market.

Cautions

- Netskope does not target the midmarket effectively and focuses its sales efforts on large organizations.
- Netskope offers its console only in English, which potentially limits its appeal in many markets.
- Netskope is slow to introduce new advanced features, such as comprehensive DEM, to its product compared to other vendors in this market.

Palo Alto Networks

Palo Alto Networks is a Leader in this Magic Quadrant. It offers Prisma Access, which provides integrated management with on-premises firewall platforms. Prisma Access POPs are deployed across major hyperscale cloud providers.

Palo Alto Networks' operations are geographically diversified, and while its SSE clients have primarily been existing customers, the company has expanded to serve businesses of various industry sizes across different sectors. Since 2024, Palo Alto Networks has incorporated the secure browser technology from its Talon Cyber Security acquisition as Prisma Access Browser and continues to invest in AI capabilities within its product.

Strengths

- Palo Alto Networks is a well-established, publicly traded company with a strong focus and investment in its SSE division, enabling clients to continue to expect capabilities from this vendor.

- Palo Alto Networks has a clear vision for innovating with AI technologies in its platform, aligning with emerging enterprise requirements.
- Palo Alto Networks' configuration integration with its existing firewalls (via Strata Cloud Manager) allows existing customers to leverage a single interface.

Cautions

- Palo Alto Networks' vision and focus on secure enterprise browsers are unlikely to shape the SSE market due to the narrow set of use cases it effectively addresses.
- Gartner clients describe Palo Alto's Prisma Access pricing as complex, expensive and sometimes difficult to interpret.
- Palo Alto offers primarily English-speaking tech support, user interface and technical documentation, potentially limiting its appeal in many markets.

Skyhigh Security

Skyhigh Security is a Niche Player in this Magic Quadrant. It offers Skyhigh SSE, which is heavily focused on data security outcomes. The vendor operates both physical POPs and cloud-provider-hosted POPs, depending on local demand, and does not necessarily offer all services in all POPs without seeing sufficient demand and requests from clients.

Skyhigh's operations are geographically diversified. Its SSE clients tend to be in highly regulated industries. Since 2024, Skyhigh has changed leadership roles and now shares a CEO with Trellix. The vendor has added automatic translation of its documentation to facilitate adoption in non-English-speaking areas.

Strengths

- Skyhigh offers strong data security and SaaS security capabilities via its SSE platform.
- In our assessment, Skyhigh offers technical functionality for a relatively low cost.
- Skyhigh has a track record of responding effectively to the technical demands and needs of the market.

Cautions

- There is limited visibility into Skyhigh Security's financials, and the vendor has a smaller market share and rarely appears on Gartner client shortlists or as a competitive vendor.

- Skyhigh's data security, forward-looking product roadmap is unlikely to influence or change the SSE market.
- Gartner clients express uncertainty about the impact of senior management changes on Skyhigh Security's direction. Buyers should take additional steps to verify its direction.

Versa Networks

Versa Networks is a Niche Player in this Magic Quadrant. It offers Versa SSE, which is part of a larger SASE offering, including its SD-WAN. Versa operates its own private backbone and POPs based on its own physical hardware.

Versa's operations are geographically diversified, and its SSE clients are of all sizes, with some bias toward medium enterprises. Since 2024, Versa has added more sovereign SASE features and AI-based threat detection to identify threats with less reliance on sandbox technologies.

Strengths

- Versa offers a broad set of capabilities across the entire SSE portfolio.
- Versa offers POPs near major population centers, enabling it to serve geographically dispersed clients.
- Versa offers competitive pricing for the technical capabilities offered.

Cautions

- Compared to other vendors in this research, there is limited financial information available, and buyers should perform additional validation of its long-term financial viability.
- Versa's vision and focus are on sovereign SASE and endpoint security approaches and therefore fall short on completeness of vision compared to the leaders in SSE.
- Versa's SSE documentation is poor relative to other vendors in the SSE market, and customers may require additional support from the vendor during deployment and operation.

Zscaler

Zscaler is a Leader in this Magic Quadrant. It offers the Zscaler Zero Trust Exchange, which includes Zscaler Internet Access and Zscaler Private Access.

Zscaler's operations are geographically diversified, and its SSE clients tend to be very large enterprises. Since 2024, Zscaler has unified its multiple consoles into a single console and launched a simplified pricing model. It has diversified its operations into non-SSE markets by acquiring Airgap Networks for microsegmentation and Avalor to help aggregate and correlate findings from multiple security tools.

Strengths

- Zscaler has a strong marketing presence in this market and is often on client shortlists, which enhances its ability to grow and continue to serve end users.
- Zscaler introduced a new pricing model that significantly simplifies purchasing for new clients.
- Zscaler has a strong understanding of the market and its direction, as well as a track record of being early to market with many capabilities.

Cautions

- Zscaler is typically one of the most expensive vendors in this market for the functionality it provides, and this remains a common concern for Gartner clients.
- Zscaler has diversified its capabilities into security operations, potentially detracting from its focus on SSE.
- Gartner clients observe performance issues with Zscaler connections more frequently than is typical for other vendors in this market.

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

- No vendors added

Dropped

- Lookout did not satisfy the requirements for customers in this market.

Inclusion and Exclusion Criteria

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

- Operate as a service. The offering must be delivered as a cloud service securing authorized users on allowed endpoints to appropriate services running in public or private clouds and on-premises environments.
- Gartner must have strong evidence that the SSE product is broadly adopted independently of an SD-WAN, firewall or other networking capability offered by the same vendor. A vendor's core SSE offering must include several capabilities that support securing authorized users on allowed endpoints to appropriate services. These capabilities must have been generally available by 31 October 2024. The capabilities are:
  - Secure access to the internet from common endpoints, including at a minimum Windows, macOS, iOS and Android 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 in-line and via API. Provide visibility, compliance enforcement, data security and threat protection for the use of SaaS applications; both monitor and remediate issues via a proxy product (in-line) and API integrations. API integration for CASB functions must include at least five major enterprise suites, such as Microsoft Office 365, Google Workspace, Salesforce, Workday, Github, Atlassian and ServiceNow. At least one of these integrations must be something other than a file-sharing or file-storage application. API integrations with social media or free SaaS platforms, such as Twitter, Reddit, YouTube or Facebook, are not included in this count. Security must include threat protection, data protection and both detection and prevention capabilities. In-line security must be provided from managed devices, including at least Windows, macOS, iOS and Android, to any SaaS

application and be enforceable from unmanaged devices to known and explicitly sanctioned SaaS applications.

- Provide secure remote access to private applications. Create an identity- and context-based logical access boundary that encompasses an enterprise user and associated device separated from an internally hosted application or set of applications. Applications must be hidden from discovery and have access restricted via a trust broker to a named set of entities; support both agent (or full integration with native OS functions) and agentless connection methods from all common endpoints, including at a minimum Windows, macOS, iOS and Android. Agent-based, or full integration with native OS functions, support must be provided to access these private applications using both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) from all common endpoints, including at least Windows, macOS, iOS and Android.

- Provide visibility into the state of common endpoints, including at least Windows, macOS, iOS and Android, and be able to use that context in access decisions.

An SSE vendor must also demonstrate scale relevant to enterprise-class organizations. At least two of the three criteria below must be met:

- Generated $40 million in revenue from the evaluated SSE offering between 1 November 2023 and 31 October 2024.

- As of 31 October 2024, have at least 500 enterprise customers (each of over 1,000 seats) securing two out of three of:

  - Private applications; SaaS applications (both in-line and API); general access to www. sites capabilities (excluding identity integration) of the evaluated SSE under support; have at least 4 million seats for the evaluated SSE under paid support as of 31 October 2024.

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

- Demonstrating that its SSE service offers a minimum of 20 POPs globally, with at least five POPs in each major global region (North America, EMEA and Asia/Pacific [APAC]). Each counted POP must be hosted in a secure and managed facility and locally supported and have enabled capabilities for all the must-have capabilities of an SSE product.

- Providing Gartner with strong evidence that 10% or more of its customer base is outside its home region (North America, EMEA or APAC).

Lastly, an SSE vendor must rank among the top 20 organizations in Gartner's Customer Interest Index for this Magic Quadrant. Data inputs used to calculate the Customer Interest Index for SSE included a balanced set of measures:

- Gartner end-user inquiry volume per vendor
- Gartner.com search data
- Gartner Peer Insights competitor mentions
- Google trends data
- Social media analysis

An SSE vendor is excluded from this Magic Quadrant if:

- The vendor's SSE functionality is primarily delivered with an SD-WAN platform as part of a single-vendor SASE offering, or the vendor's primary direction is toward a single-vendor SASE solution incorporating their own SD-WAN.
- The vendor is primarily a managed services provider and SSE offerings mostly come as part of broader managed services provider contracts or is a service provider leveraging third-party SSE services.
- The vendor did not natively offer one or more of the must-have capabilities from the SSE market definition prior to 31 October 2024. Vendors cannot rely on OEM partnerships for must-have capabilities.

Honorable Mentions

- **Check Point Software Technologies** supplies a cloud-delivered offering to support security for the web and access to private applications, as well as auxiliary services. However, it did not have the capability to provide multimode protection for SaaS applications in general availability as of 31 October 2024, preventing it from qualifying for this Magic Quadrant.
- **Cisco Systems** supplies a cloud-delivered offering to support security for the web, cloud services and private applications, as well as auxiliary services through Cisco Secure Access. However, it lacked the required number of customers and seats for its primary SSE offering as of 31 October 2024, preventing it from qualifying for this Magic Quadrant.

- **HPE (Aruba Networking)** supplies a cloud-delivered offering to support security for the web and access to private applications, as well as auxiliary services. However, it did not have the capability to provide out-of-band protection for SaaS applications as of 31 October 2024, preventing it from qualifying for this Magic Quadrant.
- **Lookout** supplies a cloud-delivered offering to support security for the web and access to private applications, as well as auxiliary services. However, it lacked a sufficient number of large enterprise customers as of 31 October 2024, preventing it from qualifying for this Magic Quadrant.
- **Microsoft** provides partial support for SSE through its Microsoft Defender for Cloud Apps, Entra for Internet Access, and Entra for Private Access products. It has a very large customer base. However, it lacked support for all common endpoint platforms and advanced threat defense for its secure web gateway (SWG) as of 31 October 2024, preventing it from qualifying for this Magic Quadrant.

Evaluation Criteria

Ability to Execute

Product or Service: Key areas assessed include: Ease of administration, securing private applications, securing web traffic, SaaS control and visibility, unified platform, data security, threat protection, adaptive access, and enterprise integration.

Overall Viability: We assess the health of the vendor, the business unit, and whether they will continue to invest across multiple areas, such as product, marketing, support, to continue to grow their SSE offering

Sales Execution/Pricing: Key areas to be evaluated will include growth of the business, how pricing and licensing are offered to customers and its relative consumability, 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: This assesses the vendor's track record compared to competitors of delivering effective and customer aligned capabilities, not just in product but in other key SSE areas. It addresses the vendor's demonstrated historical ability to address the changing market and changing customer demands and address their own limitations.

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

Customer Experience: We will assess and consider all aspects of the customer experience, including presales and postsales experience, availability and quality of documentation, technical support, and end-user satisfaction with the product.

Ability to Execute Evaluation Criteria

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

Source: Gartner (May 2025)

Completeness of Vision

Market Understanding: This includes the ability to understand and address client needs, identify likely competitors for the vendor's product now and in the future, and clearly understand their own strengths and weaknesses in the market.

Marketing Strategy: The vendor shows novel and effective approaches to communicating and differentiating, as well as forward-looking investments in their marketing program and messaging.

Sales Strategy: This assesses how the vendor intends to build out channels, deal strategies, pricing and sales organization, and how these align with customer demands and needs.

Offering (Product) Strategy: This includes delivering new features that are relevant to the market, addressing end users' current and emerging needs, and are delivered in a timely fashion.

Innovation: This evaluates the key planned future innovations across technology, sales, partnerships and features, and how the vendor will bring unique value to the market to address end-user challenges most effectively. We assess whether these innovations provide customer value and are game changers to the market.

Geographic Strategy: This examines their delivery, sales and marketing strategies for different geographies, top initiatives for expanding market share, regional compliance localization capabilities, and language support. It also assesses their plans to increase presence, staff count, customers and channel partners to fill gaps in their geographic coverage.

Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	High
Marketing Strategy	Low
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	NotRated

Evaluation Criteria	*Weighting*
Vertical/Industry Strategy	NotRated
Innovation	Medium

Source: Gartner (May 2025)

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 ar 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 advanced, integrated SSE offerings from Visionaries but be wary of strategic reliance on them and monitor their

viability closely. Visionaries often represent good candidates for acquisition by other vendors. Thus, Visionaries' customers run a slightly higher risk of business disruption.

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

SSE secures access to the web, cloud services and private applications regardless of the location of the user, the device they are using or where the application is hosted. This places these products in a critical path for access to much of an organization's data, especially data accessed via private applications.

Various security-focused vendors offer the SSE portion of an SASE architecture for purchase and use by security buyers. At the same time, vendors in the WAN edge infrastructure market cover the networking portion of the SASE framework considered by networking buyers.

Data from Gartner surveys and client inquiries indicate that most buyers are planning for a two-vendor strategy for SASE. However, more are taking a single-vendor SASE approach (see **Magic Quadrant for Single-Vendor SASE**), and the difference in capability between SSE vendors and SASE platform vendors is rapidly closing. This technical match has made clients increasingly willing to consider single-vendor offerings, especially in the small to medium enterprise space. Return-to-office mandates and the decrease in fully remote work are also impacting demand for SSE, particularly in organizations with small geographic footprints.

SSE customers are primarily looking to secure remote or hybrid workers who are accessing the public internet, cloud services and private applications. Where users are largely on-premises, SSE provides flexibility but may incur higher costs than on-premises controls. SSE customers may also want to secure remote users when their organization is virtual, is a heavy cloud consumer or has no complex networking requirements for satellite locations.

Market Overview

Product Evolution

The SSE market is maturing, with changes increasingly being evolutionary rather than revolutionary. The changes vendors are making are largely either incremental or, from late-entering vendors, designed to meet the standard for "good enough" demanded by end users. Most vendors have integrated their discrete components into a unified SSE platform configured from a single console. Customers should be wary of vendors still offering distinct capabilities, such as API SaaS protection functions, and multiple consoles, even if these are tied to an SSE offering or integrated via single sign-on (SSO). Additionally, caution should be exercised with vendors that require elements to be exposed on the perimeter of networks in order to support core SSE functions like ZTNA. Many features, such as protection of web access and associated threats, seamless remote browser isolation (RBI), firewall as a service (FWaaS) and even core DLP functions, are largely commoditized, with the differences occurring in edge cases that are of interest to fewer and generally more advanced clients.

Vendors continue to improve their functionality and integrate their capabilities into fewer distinct products. Innovators and leading vendors in this space are adding (or already have) ease of use and administration features such as:

- Advanced reporting
- DEM
- GenAI-based AI assistant
- Extensive user coaching, both in-line and from the agent
- Enhanced SaaS support, both in terms of the number of integrations and SSPM features

The vast majority of vendors are now offering, or plan to offer in the immediate future, an organic SD-WAN, though capabilities vary widely and large organizations still mostly prefer a dual-vendor architecture. However, we see increased consolidation between SSE vendors' offerings and SASE vendors' platform offerings.

Lastly, since these products are in-line for critical applications and cloud delivery is not a guarantee of availability, vendors are expanding their support for operational resilience.

There is significant value in vendors who have a simple, transparent and productized ability to extend their edge to an on-premises gateway, largely for business continuity.

Generative AI Protection

Generative AI (GenAI) has been heavily hyped for the past year, yet it presents possible advantages to many organizations when used correctly. SSE products offer strong controls against the inappropriate use of public GenAI platforms and tools, as they sit in-line with this traffic and have visibility into its data. Vendors are either treating these as use cases for SaaS protection (API or in-line) or adding new licenses that treat them similarly but incur additional cost. While these tools do not provide complete protection against GenAI data exposure threats, they are a valuable tool in the necessary arsenal of protection.

SSE Architecture

Vendors differ in terms of the architecture of their SSE offerings and delivery models. Vendor-owned POPs theoretically offer a lower cost of goods sold and, therefore, possibly lower price points (though this rarely appears true in practice). In contrast, cloud-service-provided POPs add more flexibility and the potential for faster deployments. Some vendors use a hybrid model, and increasingly, some level of capability is offered on client premises for disaster recovery or universal ZTNA use cases. Several vendors also operate their own networks, and most have extensive peering with major cloud service providers and SaaS providers to offset the latency that inevitably arises from decryption and traffic analysis. However, these architectural differences rarely provide significant differences in the end-user outcomes and are not a priority for most Gartner clients during evaluations.

Vendor Differentiation

Vendors in this market display varying levels of maturity in terms of some components and capabilities, such as in the depth and breadth of their SaaS security and advanced data security capabilities, as well as DEM. Capabilities such as protection of all ports and protocols from user devices are now common, and, therefore, are not seen as differentiating by the majority of Gartner clients. Access to private applications is increasingly homogeneous, with all the vendors in this year's Magic Quadrant required to have both agent and agentless capabilities, TCP and UDP support, and agents running on all major platforms. ZTNA architectures vary. Be cautious of those that do not allow you to run a dark data center and require you to run an exposed and listening port of any nature.

Market Drivers

Broad market trends driving the adoption of SSE offerings include:

- **VPN replacement:** Vulnerabilities in secure infrastructure located on an organization's perimeter, such as VPN appliances, network firewalls and gateways, have been increasingly exploited by attacks to gain a foothold in networks. These vulnerabilities have created tailwinds for SSE products since their private access offerings usually allow organizations to run a "dark" data center where no inbound access is possible. Vendors have enhanced their offerings to allow network access and traffic outbound from corporate servers, enabling many organizations to replace these legacy systems, albeit usually at a significantly higher cost.

- **SaaS adoption and GenAI security:** Adoption and growth rates for SaaS, platform as a service (PaaS) and infrastructure as a service (IaaS) continue to climb. Gartner estimates that SaaS is the largest cloud revenue generator and that it will grow at a compound annual rate of over 15% through 2028 (see **Forecast: Public Cloud Services, Worldwide, 2022-2028, 4Q24 Update**). Rapid cloud adoption creates a need to simplify and consolidate security delivered from the cloud for the cloud, rather than trying to force traffic through on-premises networks and data centers to secure access. It also increases the need for common security and controls, whether applications are hosted in a hyperscaler, delivered on-premises or moved to SaaS. Similarly, GenAI applications presented as special cases of SaaS applications are proliferating. They can be controlled by limiting access to approved applications and filtering data that can be entered into and subsequently processed by these applications.

- **Zero-trust networking:** Interest in aligning security with zero trust remains strong, both in verticals where it is mandated and more generally. Partially as a consequence, zero-trust marketing abounds in the SSE space. Regardless of the definitions presented by vendors, SSE can enable zero-trust networking principles, as defined in **Quick Answer: What Is Zero-Trust Networking?**

- These principles require that access to the network be granted only after authentication and authorization; that network access be restricted to only necessary resources; and that network access be continuously adjusted in near real time, based on risk.

⊕ Evidence

⊕ Evaluation Criteria Definitions