Magic Quadrant for Security Service Edge

15 April 2024 - ID G00792702 - 38 min read

By Charlie Winckless, Thomas Lintemuth, **and 1 more**

Security service edge is a dynamic market focused on consolidating cloud-delivered point solutions and replacing or augmenting legacy hardware. This Magic Quadrant will help buyers evaluate 10 key vendors, ideally in the context of a SASE strategy and long before contracts are due for renewal.

Strategic Planning Assumptions

By 2026, 85% of organizations seeking to secure their web, SaaS and private applications will obtain the security capabilities from a security service edge (SSE) offering.

By 2026, 45% of organizations will prioritize advanced data security features for inspection and protection of data at rest and in motion as a selection criterion for SSE.

Market Definition/Description

This document was revised on 18 April 2024. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Gartner defines security service edge (SSE) as a solution that secures access to the web, cloud services and private applications regardless of the location of the user or 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 edge devices to applications (private or delivered via SaaS) as well as websites (and to a lesser extent general internet traffic). 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 a hybrid workforce more efficiently than traditional on-premises solutions. Capabilities that are integrated across multiple traffic types and destinations allow a more seamless experience for both users and admins while maintaining a consistent security stance.

Must-Have Capabilities

The must-have capabilities of this market include:

- Identity-aware forward proxy (including encrypted traffic visibility and control, malware protection, threat prevention and URL filtering).
- Both inline (via identity-aware proxy supporting managed and unmanaged devices) and out-of-band (via API) protection of in-use SaaS apps including adaptive access, encrypted traffic visibility and control, data loss prevention (DLP), malware protection and threat prevention.
- Adaptive and granular access (controlled by identity and context) to private and SaaS applications by both agent and agentless methods, and from managed and unmanaged devices.
- Integration with identity providers for identity context and validation.

Standard Capabilities

The standard capabilities of this market include:

- Ability to apply controls consistently across multiple network and application destinations.
- Support for managing and securing traffic from 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 catalog of SaaS applications.
- Support for controlled access from managed and unmanaged devices.

Optional Capabilities

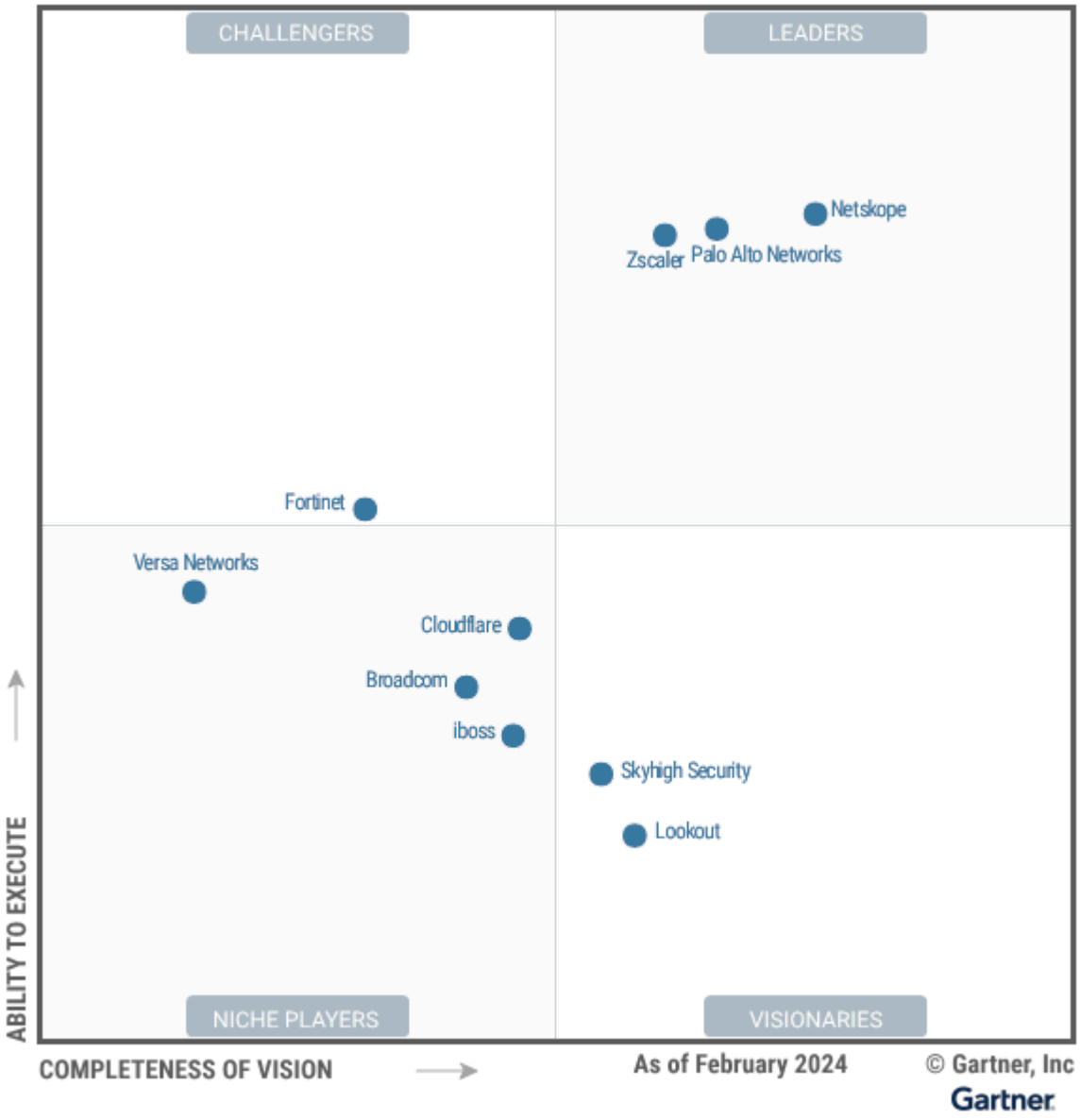
The optional capabilities of this market include:

- Control over 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.
- Advanced data protection capabilities such as redaction, tombstoning, and on-the-fly encryption (both in-line and out-of-band) and advanced data detection capabilities such as exact data matching (EDM), optical character recognition (OCR) and machine learning (ML) classifiers.

Magic Quadrant

Figure 1: Magic Quadrant for Security Service Edge



Vendor Strengths and Cautions

Broadcom

Broadcom is a Niche Player in this Magic Quadrant. It is a very large organization, headquartered in Palo Alto, California, U.S. Its SSE offering consists of Symantec Network Protection and Symantec Data Loss Prevention (DLP) Cloud. These are administered via multiple single sign-on

(SSO) integrated consoles. Other SSE functionality is provided by Symantec Endpoint Security Complete and Symantec DLP Core.

Broadcom's operations are geographically diversified. Its clients tend to be very large enterprises in a wide variety of sectors.

Broadcom plans to combine the components of its SSE offering into a single SKU.

Broadcom completed the acquisition of VMware in November 2023 and plans to integrate it with its SSE offering. At the time of evaluation, however, Broadcom and VMware operated as separate entities, so the combined organization is not considered in this Magic Quadrant.

Strengths

- **Overall viability:** Broadcom is a very large and financially very strong company with a range of hardware and software products.
- **Product offering:** Broadcom's SSE offering has strong threat prevention and data security capabilities. In particular, it can use the same classifiers, enforcement and engine as Broadcom's Symantec DLP Core enterprise DLP offering.
- **Market record:** Broadcom is a well-established vendor in the SSE space. It can integrate SSE with its on-premises web gateways and other ecosystem products, such as endpoint protection and enterprise DLP products.

Cautions

- **Customer experience:** Broadcom focuses its sales and support primarily on the largest companies worldwide. Feedback from Gartner clients indicates that they continue to seek to replace Broadcom products with products from other vendors, being dissatisfied with many aspects of Broadcom, including its sales approach and ongoing support.
- **Product offering:** Broadcom lacks a unified console and control plane for administration, and its multiple consoles have disparate appearances and approaches.
- **Geographic strategy:** Broadcom holds few regional security accreditations. Key omissions include Cyber Essentials in the U.K., Cloud Computing Compliance Controls Catalog (C5) in Germany and Infosec Registered Assessors Program (IRAP) in Australia.

Cloudflare

Cloudflare is a Niche Player in this Magic Quadrant. It is a large infrastructure provider, headquartered in San Francisco, California, U.S. It has several security and infrastructure offerings. Its SSE offering, Cloudflare One, is administered by a single unified console and includes a free tier for up to 50 users.

Cloudflare's operations are geographically diversified. Its SSE clients tend to be small organizations or large organizations with small deployments.

In 2023, Cloudflare focused on expanding its DLP functionality and adding API integrations to support additional SaaS applications, as well as enhancing its zero-trust network access (ZTNA) to allow bidirectional connectivity. It plans to continue to extend DLP and reporting capabilities in 2024.

Strengths

- **Sales strategy:** Cloudflare has a large and established customer base and the opportunity to expand within this base with its SSE product.
- **Geographic strategy:** Cloudflare maintains a very strong presence near major population centers worldwide.
- **Sales execution:** Cloudflare offers a simple pricing model, with a tiered approach, including a free tier. It does not include a separate support line item in its quotes.

Cautions

- **Product offering:** Cloudflare lacks some key features in this market, including sandboxing of content, advanced DLP functionality, and customizable reporting and management. It maintains only a minimal collection of discoverable cloud services and lacks risk ratings for them.
- **Market responsiveness:** As a late entrant to this market, Cloudflare has yet to fully respond to demand for common SSE features such as advanced DLP and file sandboxing. This reduces its appeal to the market's more sophisticated security teams.
- **Innovation:** Cloudflare's R&D appears to be focused on closing technical gaps in its product (such as DLP and SaaS support) to catch up with mature players.

Fortinet

Fortinet is a Challenger in this Magic Quadrant. It is a large security equipment and software provider, headquartered in Sunnyvale, California U.S. Its SSE offering is FortiSASE, which comprises loosely integrated offerings and consoles from the Fortinet product catalog. FortiSASE requires Fortinet virtual machines or appliances from Fortinet's catalog with inbound internet access open to support ZTNA use cases.

Fortinet's operations are geographically diversified. Its clients cover a wide range of industries and are of all sizes.

Fortinet is focused on expanding its point of presence (POP) coverage, both organically and through a partnership with Google (Google Cloud), though Fortinet still limits the number of POPs a client can access. The Google-hosted and Fortinet-owned POP networks do not interoperate. Fortinet is also striving to integrate capabilities across its disparate product lines.

Strengths

- **Sales strategy:** In our assessment, Fortinet has a strong sales strategy to upsell and cross-sell to its sizable installed base.

- **Customer experience:** Fortinet's customer support is robust and well regarded by Gartner clients.
- **Overall viability:** Fortinet is a large, well-funded company that has stated publicly that it plans to invest in FortiSASE.

Cautions

- **Product offering:** Our assessment is that Fortinet's product is weaker than those of its competitors in all areas of evaluation for this Magic Quadrant. Its disparate consoles and loose integration of products under one SKU make for a solution suited primarily to existing Fortinet customers.
- **Geographic strategy:** Fortinet's POP coverage is less than expected in this market, and the expanded network of Google-hosted POPs does not currently integrate with Fortinet's existing POP infrastructure. Customers can select only four POPs, unless they pay extra per POP for the option to select up to eight.
- **Market responsiveness:** Fortinet entered this market late and lacks common SSE features such as advanced DLP, an integrated console and a unified control plane. It continues to require on-premises Fortinet appliances or virtual machines with inbound internet access open for ZTNA access.

iboss

iboss is a Niche Player in this Magic Quadrant. It is a relatively small vendor, headquartered in Boston, Massachusetts, U.S. Its SSE offering is iboss Zero Trust SSE, which is the vendor's primary product. It is managed via a single, unified console.

iboss's operations are focused in North America, but it maintains a global presence. It focuses on highly regulated industries.

iboss remains highly focused on alignment with the U.S. National Institute of Standards and Technology (NIST) SP 800-207 Zero Trust Architecture publication. It is one of several vendors in this Magic Quadrant that announced enhanced integration with the CrowdStrike Falcon endpoint protection platform in 2023. This integration enables iboss to ingest threat signals and take enforcement actions from Falcon endpoint tools. iboss focuses more on secure web gateway (SWG) use cases than on SaaS security capabilities.

Strengths

- **Product offering:** iboss offers good web security and adaptive access capabilities in its product.
- **Sales strategy:** iboss's pricing model is simple, with additional features such as RBI included for all users, regardless of volume.
- **Geographic strategy:** iboss has POPs located close to major population centers in most regions of the world, and can closely control data storage and processing.

Cautions

- **Product offering:** iboss has very few API integrations for SaaS applications. Its offering lacks other SaaS security features, such as SaaS security posture management (SSPM), and support for advanced API DLP use cases such as masking and tokenization of data records.
- **Overall viability:** iboss is growing slower than other vendors in this market, and Gartner rarely sees it included on competitive shortlists.
- **Product strategy:** In our opinion, iboss's planned product enhancements, such as SD-WAN capabilities, employee monitoring and other roadmap items evaluated for this Magic Quadrant are unlikely to influence the shape of the broader enterprise SSE market.

Lookout

Lookout is a Visionary in this Magic Quadrant. It is a relatively small vendor, headquartered in San Francisco, California, U.S. In addition to SSE, it offers mobile device security products. Its SSE platform, the Lookout Cloud Security Platform, includes Lookout Secure Internet Access, Lookout Secure Private Access and Lookout Secure Cloud Access offerings. These are managed via a single, unified console.

Lookout's operations are concentrated in North America and EMEA, but the company also has a smaller presence in Asia/Pacific. Its clients tend to be midsize and large enterprises from multiple sectors.

In 2023, Lookout extended the ZTNA capabilities of Lookout Secure Private Access to support all ports and protocols, and partnered with Fortra to utilize its data classification capabilities in the Lookout Cloud Security Platform. Lookout also divested its consumer mobile security division to F-Secure, although this move was not directly related to SSE.

Strengths

- **Product offering:** Lookout offers strong data security capabilities in its SSE platform. These are integrated across all SSE traffic channels.
- **Market understanding:** In our assessment, Lookout has a good understanding of the SSE market's direction and its competitors.
- **Sales strategy:** Lookout's integration of its SSE offering with its mobile security offering may appeal to industries with a strong need for mobile SSE security.

Cautions

- **Geographic strategy:** Lookout does not operate as many POPs close to major population centers as do other vendors in this Magic Quadrant.
- **Sales execution:** Lookout charges for extra elements. There are, for example, charges per SaaS application for API connections and cloud sandboxing.

- **Sales strategy:** Lookout has fewer channel partners than other vendors in this Magic Quadrant (across all geographies). It relies instead on its relationships with Tier 1 telcos. Indications from Gartner clients are that Lookout rarely appears on competitive shortlists.

Netskope

Netskope is a Leader in this Magic Quadrant. It is a large organization, headquartered in Santa Clara, California, U.S. Its primary focus is SSE. Its SSE product is Netskope Intelligent Security Service Edge, which is managed via a single, unified console.

Netskope's operations are geographically diversified. It has clients of all sizes in multiple industries.

Netskope has incorporated software-defined WAN (SD-WAN) technology from its 2022 acquisition of Infiot into its agent and made its Borderless SD-WAN generally available. Additionally, in September 2023, Netskope announced the acquisition of Kadiska to extend its digital experience monitoring (DEM) capabilities. Netskope has moved the functionality from its formerly separate Advanced Analytics SKU into its base product.

Strengths

- **Geographic strategy:** Netskope maintains POPs close to most major population centers, and claims that all its POPs have consistent bandwidth and feature availability.
- **Product offering:** Netskope has a strong set of controls across all supported traffic channels, with particular strength in data security.
- **Market understanding:** Netskope shows excellent understanding of the market's direction and has a leading roadmap.

Cautions

- **Innovation:** Netskope has been slow to introduce DEM features to its platform and to enhance them.
- **Sales execution:** Although Netskope offers consolidated SKUs for some of its offerings, Gartner clients report that its licensing remains hard to interpret in many cases. In addition, Netskope's offering remains one of the more expensive in this market.
- **Marketing execution:** Gartner estimates that Netskope's ZTNA market share and growth in 2023 were lower than those of several other vendors in this market.

Palo Alto Networks

Palo Alto Networks is a Leader in this Magic Quadrant. It is a large company, headquartered in Santa Clara, California, U.S. It offers a range of security products, in addition to SSE. Its SSE offering is Prisma Access, which can be managed from a single, unified console that can also manage on-premises firewalls.

Palo Alto Networks' operations are geographically diversified. It has clients of all sizes from a wide range of industries.

Palo Alto Networks has acquired Talon Cyber Security, a provider of an enterprise browser, which it plans to integrate with Prisma Access.

Strengths

- **Overall viability:** Palo Alto Networks is financially secure. It continues to invest in, and develop, its SSE offering into a competitive offering to support the transition of its sizable customer base to cloud-delivered security services.
- **Product offering:** Palo Alto Networks recently launched a new console (Strata Cloud Manager) that unifies the management of both on-premises firewalls and SSE and removes the requirement to select a management approach upon deployment.
- **Innovation:** Palo Alto Networks continues to invest in engineering talent for its SSE business unit. It is also investing in its AI assistant and strong industry partnerships.

Cautions

- **Sales execution:** Gartner clients report that Palo Alto Networks' licensing model is complex and difficult to understand, with inflexible and inflated pricing during sales motions.
- **Market responsiveness:** Our assessment is that Palo Alto Networks' product roadmap for RBI is insufficiently differentiated to have a significant impact on the SSE market.
- **Sales strategy:** Feedback from Gartner clients indicates that Palo Alto Networks' Prisma Access still appeals primarily to the company's existing customers.

Skyhigh Security

Skyhigh Security is a Visionary in this Magic Quadrant. Formerly the SSE business of McAfee Enterprise, Skyhigh Security is a relatively small vendor, headquartered in San Jose, California, U.S. Its SSE offering is Skyhigh Security Service Edge, which is administered from a single, unified console.

Skyhigh Security's operations are geographically diversified. Its clients range from small to very large, with a bias toward the financial services, healthcare and government sectors.

Skyhigh Security moved to rebuild its channel partner network in 2023, under new leadership. It is one of several vendors in this Magic Quadrant that have announced closer integrations with CrowdStrike products in the past year. It also has tight integrations with Trellix.

Strengths

- **Product offering:** Skyhigh Security has strong data security and SaaS security capabilities.
- **Sales strategy:** Skyhigh Security has invested in reestablishing its channel presence, including by hiring new leaders to drive this initiative.

- **Market understanding:** Skyhigh Security maintains a clear vision of the market across all key capabilities, with a focus on a more data-centric approach.

Cautions

- **Geographic strategy:** Skyhigh Security does not run all its services in all its POPs but bases their availability on customer demand in an area. This is especially true for ZTNA and advanced services such as RBI.
- **Overall viability:** Skyhigh Security is growing more slowly than other vendors in this market, and Gartner rarely sees it included on competitive shortlists.
- **Sales execution:** Gartner sees Skyhigh Security as being focused largely on the government and financial services sectors and having less appeal to clients outside these areas.

Versa Networks

Versa Networks is a Niche Player in this Magic Quadrant. It is headquartered in Santa Clara, California, U.S. It offers both SSE and single-vendor secure access services edge (SASE). Its SSE product is Versa Security Service Edge, which is administered via a single, unified console.

Versa Networks' operations are geographically diversified. Its clients tend to be small, midsize and large enterprises.

Versa Networks has extended some SSE functionality to on-premises deployments via both its own network infrastructure and software capable of running on some other vendors' switches under the label of Versa Zero Trust Everywhere.

Strengths

- **Customer experience:** Gartner clients generally rate the support they receive from Versa Networks as good.
- **Product offering:** Versa Networks' offering provides a flexible and configurable capability for assigning and adjusting dynamic risk scores to both users and devices.
- **Geographic strategy:** Versa Networks' POP network covers the majority of major population centers. A log's storage location is determined by the location of the POP that a user connects to.

Cautions

- **Sales strategy:** Gartner observes that Versa Networks sells through large global carriers, managed service providers, managed security service providers and distribution partners. There is limited consumer awareness of Versa Networks' presence in the SSE market.
- **Marketing execution:** Versa Networks is rarely seen on shortlists in this market. There is less awareness of its offerings in this market among Gartner clients.

- **Product strategy:** Versa's SSE platform is still catching up with capabilities such as DEM and endpoint detection and response that are already generally available in the market.

Zscaler

Zscaler is a Leader in this Magic Quadrant. It is a relatively large organization headquartered in San Jose, California, U.S. It focuses on its SSE offering, Zscaler for Users, use of which involves multiple consoles, integrated via SSO.

Zscaler's operations are geographically diversified. Its clients tend to be large and extra-large organizations across a wide range of industries.

In February 2023, Zscaler acquired Canonic Security for its SSPM technology, which it has since integrated with its SSE offering. At its annual user conference in June 2023, Zscaler announced a hardware Branch Connector to simplify forwarding of traffic to its SSE platform. Furthermore, Zscaler is one of several vendors in this Magic Quadrant offering enhanced integration with CrowdStrike for endpoint security signals.

Strengths

- **Overall viability:** Zscaler is a publicly traded company that continues to register strong revenue growth from a large base of customers. It continues to grow faster than the overall market.
- **Geographic strategy:** Zscaler has POPs close to most major population centers, and operates in China. This presence is supported by a strong set of regional accreditations.
- **Marketing strategy:** Zscaler has a strong marketing message that appeals to many organizations looking for a cloud-native security provider, and that generates strong mind share in this market. This results in Zscaler being frequently seen on shortlists.

Cautions

- **Sales execution:** Zscaler has a complex price list. In addition, Gartner clients have expressed frustration with Zscaler's periodic licensing updates, the need for per-bandwidth SKU add-ons for some use cases, and cost increases at renewal time.
- **Customer experience:** Gartner receives feedback about performance and latency problems more frequently from Zscaler customers than is typical for other vendors in this market.
- **Product strategy:** Zscaler's planned product enhancements, such as "zero-trust" SD-WAN capabilities and other roadmap items evaluated for this Magic Quadrant, are less likely to shape the broader enterprise SSE 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

- Fortinet
- Versa Networks

Dropped

- Cisco Systems, as its primary SSE offering, Cisco Secure Access, did not meet the customer and seat counts required as of 15 October 2023.
- Forcepoint, as it did not satisfy the requirement for mobile device agent support as of 15 October 2023.

Inclusion and Exclusion Criteria

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

- Operated as a service. The offering must be delivered as a cloud service to ensure a better end-user experience when securing authorized users on allowed endpoints to appropriate services running in public or private clouds and on-premises environments.
- Broadly adopted independently of an SD-WAN capability offered by the same vendor. The product must be wholly independent of deploying with a physical SD-WAN, device or other edge networking component, but can be connected to existing edge devices and endpoints or by optional partnerships with networking or network firewall providers.

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 15 October 2023. The capabilities are:

- Secure access to the web via proxy. Provide URL filtering and advanced threat defense to protect users and enforce acceptable use policies.
- Secure usage of cloud services, 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 solution (in-line) and API integrations:
    - API integration for cloud access security broker (CASB) functions must include at least five major enterprise suites (such as Microsoft 365, Google Workspace, Salesforce, Workday, GitHub, Atlassian and ServiceNow). At least one of these integrations must be with something other than a file-sharing or file storage application. API integrations with

social media or free SaaS platforms (such as X [formerly Twitter], Reddit, YouTube or Facebook) are not included in this count.
    - 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 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 and agentless connection methods.
- Connectivity must be provided from common operating systems, including at least Windows, macOS, iOS and Android.

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 September 2022 and 30 September 2023.
- Have at least 500 enterprise customers (over 1,000 seats) using at least two of the three must-have capabilities (excluding identity integration) of the evaluated SSE offering under support as of 1 October 2023.
- Have at least 4 million seats for the evaluated SSE offering under paid support as of 1 October 2023.

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 two in each major global region (North America, EMEA and Asia/Pacific). Each counted POP must be hosted in a secure and managed facility and be locally supported, and have enabled capabilities for all the must-have capabilities of an SSE product.
- Gartner receiving strong evidence that 10% or more of its customer base is outside its home region (North America, EMEA or Asia/Pacific).

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 it failed to satisfy the inclusion criteria or if:

- Its SSE functionality is primarily delivered with an SD-WAN platform as part of a single-vendor SASE offering, or its primary direction is toward a single-vendor SASE solution incorporating its own SD-WAN.
- It is primarily a managed services provider and its SSE offering(s) mostly come as part of broader managed services provider contracts, or if it is a service provider leveraging third-party SSE services.
- It did not natively offer one or more of the must-have capabilities of an SSE offering prior to 15 October 2023. Vendors cannot rely on OEM partnerships for must-have capabilities.

Honorable Mentions

- **Cisco Systems:** This vendor announced general availability of Cisco Secure Access on 13 September 2023, but lacked the required number of customers and seats to be included in this report.
- **Forcepoint:** This vendor provides cloud-delivered SWG, CASB, ZTNA, firewall as a service (FWaaS), RBI and DLP functionality with the Forcepoint ONE platform, but did not support a mobile traffic steering agent as of 15 October 2023.
- **Microsoft:** This vendor provides a multimode CASB (Microsoft Defender for Cloud Apps) that offers inspection in-line and at rest via API integrations, and had SWG and ZTNA capabilities (Entra Internet Access and Entra Private Access) in public preview as of 11 July 2023. It has a large client base. We excluded Microsoft from this Magic Quadrant because it did not provide URL filtering and advanced threat defense to protect users and enforce acceptable use policies via proxy as of 15 October 2023.
- **Trend Micro:** This vendor provides SWG, CASB and ZTNA by enabling Zero Trust Secure Access as part of its Trend Vision One platform. We excluded Trend Micro from this Magic Quadrant because it did not demonstrate that its SSE offering had the required scale and coverage relevant to enterprise-class organizations as of 15 October 2023.

Evaluation Criteria

Ability to Execute

Product or Service: Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships, as defined in the market definition and detailed in the subcriteria.

Subcriteria:

- Evaluation of key features for securing web, cloud services and private applications:
  - Adaptive access controls
  - Advanced threat defense
  - API-based SaaS security controls
  - Cloud-delivered service
  - Data security visibility and controls
  - Forward proxy
  - In-line SaaS security controls
  - ZTNA
- Evaluation of other features, including (but not limited to):
  - Advanced analytics
  - DEM
  - FWaaS
  - RBI
  - SD-WAN integration
  - SSPM
  - UEBA

Overall Viability: This includes an assessment of the overall organization's financial health and the financial and practical success of the business unit. It also reflects the likelihood of the individual business unit continuing to invest in and offer the product and advance the state of the art within the organization's portfolio of products.

Subcriteria:

- Sustained funding sources (venture capital or otherwise), including positive year-over-year growth in customers, seats and revenue.
- The company's overall ability to continue to serve new and existing customers through sufficient staffing and company growth.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. Included are deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Subcriteria:

- Pricing that is competitive and places few restrictions on which SSE features can be used.
- Successful competition in deals that displace incumbents because of better value and customer use-case alignment, with effective sales, presales and marketing teams.
- Wins in highly competitive shortlists.

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 criterion also considers the vendor's history of responsiveness.

Subcriteria:

- Track record of developing key SSE features faster than competitors.
- Addressing of a wide range of use cases across SSE functionality.
- Enabling of the SSE portion of a SASE architecture for customers and the ability to support their transformation strategies.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand and business, increase awareness of products, and establish a positive identification with products, brands and the organization in the minds of buyers. This mind share can be driven by a combination of publicity, promotional, thought leadership, word-of-mouth and sales activities.

Subcriteria:

- Ability to capture mind share by frequently appearing on prospective customers' shortlists for SSE.
- Demonstrated leadership for the SSE portion of SASE frameworks, including thought-leading research and clarity about the advantages of a stand-alone, integrated SSE service offering.

Customer Experience: Relationships, products, services and programs that enable clients to be successful with the products evaluated. Included are the ways in which customers receive technical support or account support. Also relevant are ancillary tools, customer support programs (and the quality thereof), the availability of user groups and SLAs.

Subcriteria:

- Overall satisfaction of customers across the entire cycle (from sales to support), based on input from multiple sources, including feedback from Gartner clients, Gartner Peer Insights feedback and other public sources of customer sentiment.
- Evidence of strong, actionable SLAs that demonstrate ongoing stability of operations and remediations when breaches occur.

Table 1: Ability to Execute Evaluation Criteria

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

Source: Gartner (April 2024)

Completeness of Vision

Market Understanding: The vendor's ability to understand buyers' needs and to translate those needs into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those wants and needs with their added vision.

Subcriteria:

- Ability to respond to customers' feature requests through internal development or well-executed technology acquisitions and integrations with vendors' SSE services.
- Ability to meet customers' requirements in a timely manner, but also to decline customers' requests if they do not add sufficient value or align with SSE services.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Subcriteria:

- Ability to craft succinct marketing messages and efficiently communicate the value of an SSE offering to prospective customers.
- Ability to target the right roles for SSE services (such as chief information security officer, CIO and non-IT buyer roles), as these services may be purchased by different organizational buyers.

Sales Strategy: The vendor's strategy for selling products that uses an appropriate network of direct and indirect sales, marketing, service, and communication affiliates to extend the scope and depth of its market reach, skills, expertise, technologies, services and customer base.

Subcriteria:

- Ability to create strategic alliances with the right partners to resell SSE services.
- A good mix of sales channels to reach prospective buyers across different markets, and a comprehensive channel partner strategy.

Offering (Product) Strategy: The vendor's approach to product development and delivery, with emphasis on differentiation, functionality, methodology and feature set as they relate to current and future requirements.

Subcriteria:

- A comprehensive SSE strategic vision aligned with overall SASE customer requirements.
- An actionable roadmap for the short term to address any gaps in the SSE offering, and development of differentiating features.

- Understanding of the value of integration of SSE features and alignment with adjacent technologies (such as identity and access management [IAM], SIEM, XDR and SD-WAN) owned or provided by partnerships.

Innovation: Direct, related, complementary, and synergistic layouts of resources, expertise or capital for investment, consolidation, and defensive or preemptive purposes.

Subcriteria:

- Evidence of continued in-house research and development resulting in clear differentiators strongly aligned with the needs of the SSE market (for example, cloud service security, SSE cloud service delivery, web security and private application access).
- Track record of consistently delivering roadmap features that are innovative in the market, rather than just developments to catch up with competitors' offerings.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside its "home" or native geography, either directly or through partners, channels and subsidiaries, as appropriate for that geography and market.

Subcriteria:

- Strong sales and support for different geographic regions, including strong regional channel support and regional certifications (such as FedRAMP, ISO 27001 and SOC 2).
- Consistent pricing across geographies to enable customers to purchase the service(s) consistently, regardless of customers' location.

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Market Understanding	High
Marketing Strategy	Low
Sales Strategy	High
Offering (Product) Strategy	High

Evaluation Criteria ↓	Weighting ↓
Business Model	NotRated
Vertical/Industry Strategy	NotRated
Innovation	Medium
Geographic Strategy	Low

Source: Gartner (April 2024)

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, as well as 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 that may lack sophisticated features, and that lack 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 innovation, 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 solutions 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 or the device they are using or where the application is hosted. Various security-focused vendors offer the SSE portion of a 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 indicates that most buyers are planning for a two-vendor strategy for SASE. More and more vendors, however, are taking a single-vendor SASE approach (see Magic Quadrant for Single-Vendor SASE), so we expect to see more purchases from these vendors, even if only their SSE capabilities are deployed.

SSE customers are primarily looking to secure remote or hybrid workers who are accessing the public internet, cloud services and private applications. These 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. Most vendors have integrated their discrete components into a unified SSE platform configured from a single console. Customers should be wary of those still offering distinct capabilities and multiple consoles, even if these are tied to an SSE offering or integrated via SSO.

Vendors continue to improve their functionality and integrate their capabilities into fewer distinct products and SKUs. They are adding ease-of-use and administration features such as advanced reporting, DEM, and better SaaS support both in terms of number of integrations and SSPM features. Vendor-owned SD-WAN is becoming more common, but, especially in larger organizations, dual-vendor SASE is still preferred and strong integrations with third parties are a requirement.

Enterprise Integration

Enterprise integration continues in areas such as XDR, where many vendors have partnered in the past year or offered integration touchpoints. Vendor-supplied XDR remains primarily a small-to-

midsize enterprise area, and one where existing EPP vendors are likely to have an advantage.

The hype about generative AI is likely to be reflected in the SSE market. Wexpect vendors to add AI-enabled policy creation and optimization, reporting and analysis, and even data security capabilities to their SSE offerings.

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, while 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.

Vendor Differentiation

Vendors in this market display varying levels of maturity in terms of components and capabilities, such as in the depth and breadth of their SaaS security and data security capabilities, adaptive access capability, and anti-malware defenses. 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. ZTNA is increasingly homogeneous, with all the vendors in this year's Magic Quadrant being required to have both agent- and agentless capabilities and agents running on all major platforms.

Market Drivers

Broad market trends that are driving adoption of SSE offerings include:

- **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 require that access to the network be granted only after access is authenticated and authorized, that network access be restricted to only necessary resources, and that network access be continuously adjusted in near real time, based on risk.

- **SaaS adoption:** Adoption and growth rates for SaaS, platform as a service (PaaS) and IaaS continue to climb. Gartner estimates that SaaS is the largest cloud revenue generator (see **Forecast: Public Cloud Services, Worldwide, 2021-2027, 4Q23 Update**), and that it will grow at a compound annual rate of over 17% through 2027 (again, see **Forecast: Public Cloud Services, Worldwide, 2021-2027, 4Q23 Update**). Rapid cloud adoption creates a need to simplify and consolidate security delivered from the cloud for the cloud, rather than to try and 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.

- **Organizational silos:** Most large organizations have separate networking and security teams. This creates two buying centers for SASE offerings, though in smaller enterprises more organizations are considering single-vendor SASE. In **2024 Strategic Roadmap for SASE Convergence**, Gartner recommends consolidating existing networking and security contracts, and engaging networking and security engineers, before any technology evaluations. This will help to minimize duplicate spending, as well as to engage with stakeholders aiming to modernize branch office connectivity, pursue a zero-trust strategy, or secure and connect hybrid workers. In the long term, some organizations may create a unified team responsible for access engineering, spanning remote workers, branch office and edge locations. A single-vendor approach to implementing a SASE architecture is not required, but Gartner recommends that organizations have a strategic goal of reducing their SASE suppliers to either one vendor or two explicitly integrated vendors over the next few years.

Evidence

Throughout the course of a year, Gartner receives many inquiries about SSE and SASE technology. These inquiries help shape our views about the market and its vendors, as do other sources of publicly accessible data

Where possible, we also have drawn on customer reviews posted on Gartner's Peer Insights platform.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

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

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase

awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.