Magic Quadrant pour les services de sécurité Edge

20 mai 2025 - ID G00815904 - 33 min de lecture

Par Charlie Winckless , Thomas **Lintemuth** et **2 autres**

Le marché des services de sécurité en périphérie est dynamique et regroupe plusieurs offres d'accès en une seule offre convergée centrée sur le cloud. Ce Magic Quadrant aidera les acheteurs à évaluer idéalement les principaux fournisseurs dans le cadre d'une stratégie SASE.

Définition/Description du marché

Gartner définit le service de sécurité Edge (SSE) comme une offre qui sécurise l'accès au web, aux services cloud et aux applications privées, indépendamment de la localisation de l'utilisateur, de l'appareil utilisé ou de l'hébergement de l'application. Le SSE protège les utilisateurs contre les contenus malveillants et inappropriés sur le web et offre une sécurité et une visibilité renforcées pour les applications SaaS et privées auxquelles les utilisateurs finaux accèdent.

Security Service Edge offre une solution principalement cloud pour contrôler l'accès des utilisateurs et des appareils aux applications, aux sites web et à Internet. Elle offre un éventail de fonctionnalités de sécurité, notamment l'accès adaptatif basé sur l'identité et le contexte, la protection contre les logiciels malveillants, la sécurité des données et la prévention des menaces, ainsi que les analyses et la visibilité associées. Elle permet une connectivité plus directe pour les utilisateurs hybrides en réduisant la latence et en offrant un potentiel d'amélioration de l'expérience utilisateur. L'intégration de fonctionnalités à plusieurs types de trafic et destinations assure une expérience plus fluide pour les utilisateurs et les administrateurs, tout en maintenant une sécurité cohérente.

Caractéristiques obligatoires

Les caractéristiques obligatoires de ce marché comprennent :

- Plans de gestion et de données principalement fournis dans le cloud
- Proxy de transfert sensible à l'identité avec capacités de décryptage et de protection
- Protection en ligne des données dans les applications SaaS et privées
- Protection hors bande des données dans les applications SaaS via l'intégration d'API
- Contrôle d'accès adaptatif et granulaire prenant en charge à la fois les appareils dotés d'un agent SSE (ou d'une méthode de pilotage du trafic similaire) et les appareils sans logiciel ni configuration SSE locaux
- Intégration avec des fournisseurs d'identité externes

Caractéristiques communes

Les caractéristiques communes de ce marché comprennent :

- Console intégrée unique prenant en charge toutes les fonctionnalités et fonctions de la plate-forme
- Capacité à appliquer des contrôles de manière cohérente sur plusieurs destinations réseau et applications
- Prise en charge de la gestion et de la sécurisation du trafic à partir de tous les points de terminaison courants (tels que les appareils Windows, macOS, iOS et Android)
- Intégration avec les technologies clés de l'entreprise telles que la gestion des informations et des événements de sécurité (SIEM), la détection et la réponse étendues (XDR), le SD-WAN et d'autres technologies adjacentes
- Prise en charge des API publiées et documentées, accessibles au client et permettant l'automatisation des tâches courantes et l'intégration avec d'autres plateformes de sécurité
- Catalogues d'applications SaaS organisés, gérés et évalués en fonction des risques
- Contrôle du trafic sur tous les ports et protocoles
- Isolation du navigateur à distance (RBI) pour améliorer la sécurité sur toutes les destinations et tous les canaux du réseau

- Gestion de la posture de sécurité SaaS pour la visibilité et la correction des configurations SaaS et la visibilité des applications plug-in SaaS
- Contrôles d'accès continus et adaptatifs sur tous les canaux en fonction de l'état de connexion initial et de tout changement d'état pendant la connexion
- Lire, écrire et agir sur les étiquettes des plateformes courantes de classification de données
- Analyse intégrée du comportement des entités utilisateur (UEBA) pour fournir une détection et une réponse automatisées aux comportements anormaux et risqués des appareils et des utilisateurs
- Capacité à appliquer des fonctionnalités avancées de protection des données

Quadrant magique

Figure 1 : Magic Quadrant pour les services de sécurité Edge

Gartner

Points forts et précautions du fournisseur

Broadcom

Broadcom est un acteur de niche dans ce Magic Quadrant. Il propose Symantec Network Protection, qui inclut une protection cloud et locale pour les sites web, et est pris en charge par Symantec DLP Cloud pour les clients nécessitant une protection contre la perte de données.

Les activités de Broadcom sont géographiquement diversifiées et ses clients sont généralement de très grandes entreprises de secteurs très variés. Au cours des 12 derniers mois, Broadcom a progressivement mis à jour son produit SSE, notamment un gestionnaire

de trafic d'agents permettant de contrôler le routage des agents connectés et la mise à disposition de son accès réseau Zero Trust (ZTNA) sur la Marketplace Microsoft Azure. Au cours de cette étude, Broadcom développait une console unifiée unique pour les fonctionnalités SSE.

Broadcom a refusé toute demande d'informations complémentaires. L'analyse de Gartner s'appuie donc sur d'autres sources crédibles.

Points forts

- Broadcom propose une intégration solide de la sécurité des données avec son offre de prévention des pertes de données d'entreprise (DLP), simplifiant ainsi l'intégration avec les environnements d'entreprise.
- L'approche du marché et la stratégie de soutien de Broadcom se concentrent sur les besoins des très grandes entreprises complexes et hautement réglementées.
- Broadcom propose une plate-forme de protection des points d'extrémité (EPP) et un produit de détection et de réponse des points d'extrémité (EDR) bien connus et largement installés et a convergé cela avec son agent SSE.

Précautions

- Broadcom se concentre sur la vente de licences d'entreprise à un sous-ensemble de très gros clients, ce qui a un impact sur sa capacité à soutenir de manière optimale les petites organisations.
- Le SSE de Broadcom s'adresse principalement aux clients existants et aux prospects déjà engagés dans le portefeuille plus large de technologies de cybersécurité et d'infrastructure que ce fournisseur fournit.
- Broadcom dispose de plusieurs consoles et d'une intégration moindre dans son SSE que ce qui est typique sur ce marché .

Cloudflare

Cloudflare est un acteur de niche dans ce Magic Quadrant. Il propose Cloudflare One, une offre SSE unifiée, soutenue par le plus grand réseau de points de présence physiques (POP) de cette évaluation. Cloudflare One propose une offre gratuite jusqu'à 50 utilisateurs.

Les activités de Cloudflare sont géographiquement diversifiées, et ses clients SSE sont généralement des petites organisations ou des déploiements de petite envergure au sein d'organisations plus importantes. Au cours des 12 derniers mois, Cloudflare a acquis BastionZero pour prendre en charge les cas ZTNA d'accès des développeurs et des infrastructures, ainsi que Kivera pour contrôler les modifications des configurations hyperscaler pilotées par API . L'entreprise a également amélioré ses offres de sécurité des données , en continuant d'ajouter des classificateurs regex pour davantage de types de données.

Points forts

- Cloudflare dispose d'un vaste réseau de diffusion de contenu (CDN) et d'une solution de protection des applications web et des API (WAAP). L'entreprise dispose également d'une approche de contractualisation de fonds communs de placement qu'elle peut exploiter pour des opportunités de ventes croisées, ce qui devrait contribuer à sa croissance et à son adéquation avec les besoins des utilisateurs finaux .
- Cloudflare dispose du plus grand réseau POP pour l'intégration du trafic vers son cloud dans cette évaluation et continue d'étendre et de développer ce réseau, lui permettant de soutenir les clients ayant des besoins de couverture dans les zones les plus reculées du monde.
- Cloudflare est une grande entreprise cotée en bourse avec un investissement solide dans SSE, ce qui aide l'entreprise à maintenir sa viabilité à long terme .

Précautions

- Les capacités techniques de Cloudflare sont à la traîne par rapport aux autres acteurs de ce marché dans des domaines tels que la sécurité des données, la découverte SaaS, la notation des risques et l'accès adaptatif.
- La stratégie de résilience de Cloudflare dépend uniquement de la solidité de son architecture réseau, ce qui n'est pas suffisant pour certains clients à la recherche de plans de données alternatifs .
- Les prix de Cloudflare, tels qu'évalués au cours de cette recherche, sont élevés pour le niveau de capacité fourni , et les clients de Gartner ont signalé que la tarification par service n'est pas claire lorsque Cloudflare regroupe son SSE avec d'autres services.

Fortinet

Fortinet est un Challenger dans ce Magic Quadrant. FortiSASE propose des fonctionnalités SSE intégrées et un CASB API distinct (FortiCASB). Toutes les fonctionnalités reposent sur FortiOS, la plateforme propriétaire de l'éditeur. Fortinet propose des POP sur Google Cloud et sur son propre matériel, et limite par défaut le nombre de POP utilisables par client. Les clients peuvent déployer une combinaison des deux infrastructures et augmenter le nombre de POP accessibles en achetant des niveaux de licence supérieurs.

Les activités de Fortinet sont géographiquement diversifiées, et ses clients SSE sont généralement des clients Fortinet existants en matière de pare-feu et de WAN défini par logiciel (SD-WAN), couvrant un large éventail de secteurs et de clients de toutes tailles. Au cours des 12 derniers mois, Fortinet a intégré la majorité de ses fonctionnalités SSE dans deux consoles, l'API CASB nécessitant une configuration distincte, et a ajouté le ZTNA sans agent à son portefeuille. L'éditeur a également introduit un agent unifié pour la protection des terminaux et les fonctionnalités SSE.

Points forts

- Fortinet est un fournisseur important et bien financé, disposant d'une base de clientèle solide et d'un engagement public à développer davantage son offre SSE et sa part de marché .
- Fortinet dispose d'une large base de clients existante qu'elle peut exploiter pour étendre sa présence SSE et se développer sur le marché grâce à sa forte orientation client .
- Les prix de Fortinet sont très compétitifs sur ce marché pour les fonctionnalités techniques offertes lorsque les POP hébergés sur Google Cloud Platform (GCP) de Fortinet peuvent être utilisés.

Précautions

- L'approche de Fortinet en matière de ZTNA, qui nécessite un appareil FortiOS exposé à chaque terminaison, et sa conception FortiOS partout limitent son attrait pour les clients non Fortinet et les clients qui ne souhaitent pas maintenir et mettre à jour ces systèmes exposés.
- Fortinet gère deux réseaux POP distincts et requiert des licences spécifiques de niveau supérieur, ainsi que des coûts plus élevés pour utiliser les POP provenant de son environnement hébergé par GCP, ou des deux environnements. Fortinet limite également le nombre de POP auxquels un utilisateur final peut se connecter et le nombre d'appareils pris en charge par utilisateur.

- Il est peu probable que l'approche centrée sur l'infrastructure de Fortinet fasse progresser efficacement le marché SSE, car elle nécessite l'utilisation d'appareils virtuels ou matériels pour adopter certains services SSE, orientant ainsi efficacement les consommateurs vers FortiSASE.

iboss

iboss est un acteur de niche dans ce Magic Quadrant. Il propose la solution SASE Zero Trust d'iboss , axée sur l'approche Zero Trust 800-207 du National Institute of Standards and Technology (NIST). Sa pile de sécurité SSE peut être déployée dans de multiples environnements, y compris le cloud privé , tout en étant gérée depuis le plan de gestion central. Ses points de présence sont hébergés sur de nombreux points d'échange Internet.

Les activités d'iboss sont principalement concentrées en Amérique du Nord et en Europe, et ses ventes SSE ciblent les très grandes entreprises . Au cours des 12 derniers mois, iboss a intégré le SD-WAN nativement à sa plateforme et peut désormais proposer son offre directement dans Azure depuis la Marketplace Azure.

Points forts

- iboss offre de solides capacités de sécurité Web ainsi que des capacités personnalisables de notation des risques par l'utilisateur.
- iboss étend ses efforts de vente et de marketing pour accroître sa présence sur le marché et permettre une croissance plus rapide .
- iboss dispose d'une bonne couverture POP mondiale, ce qui lui permet de prendre en charge des clients géographiquement dispersés.

Précautions

- Les informations financières concernant le fournisseur sont limitées, et iboss apparaît rarement dans les enquêtes Gartner ou sur les listes de présélection des concurrents. Les acheteurs devraient procéder à une validation supplémentaire de ce fournisseur.
- Le coût du produit d'iboss est plus élevé que celui des autres fournisseurs du marché pour des fonctionnalités équivalentes, selon notre évaluation.
- iboss offre moins de fonctionnalités de sécurité SaaS, comme le nombre d'intégrations d'API et la gestion de la posture de sécurité SaaS (SSPM), ainsi qu'une surveillance de l'expérience numérique (DEM) moins aboutie que ses concurrents. Iboss offre également

une protection des données moins avancée, notamment l'absence de chiffrement des données ou des champs, et l'absence de capacités d'intégration DLP d'entreprise.

Netskope

Netskope est leader dans ce Magic Quadrant. L'entreprise propose Netskope One SSE, basé sur son réseau propriétaire NewEdge prenant en charge les points de présence physiques.

Les activités de Netskope sont géographiquement diversifiées et ses clients SSE sont généralement de très grandes entreprises actives dans des secteurs très variés. Au cours des 12 derniers mois, Netskope a étendu ses capacités DEM en intégrant plus pleinement son acquisition Kadiska en 2023 et en étendant le support de l'IA aux fonctions d'accompagnement client.

Points forts

- Netskope offre de solides capacités techniques dans tous les domaines de l'ESS et peut prendre en charge la grande majorité des cas d'utilisation des clients.
- Netskope fait preuve d'une solide compréhension de ce marché et de ses tendances , prenant généralement en charge de nombreux parcours SSE des utilisateurs finaux.
- Netskope apparaît souvent sur les listes restreintes de clients, ce qui reflète la notoriété de la marque dont elle bénéficie et renforce sa capacité à se développer et à continuer à fournir des services sur ce marché .

Précautions

- Netskope ne cible pas efficacement le marché intermédiaire et concentre ses efforts de vente sur les grandes organisations.
- Netskope propose sa console uniquement en anglais, ce qui limite potentiellement son attrait sur de nombreux marchés .
- Netskope tarde à introduire de nouvelles fonctionnalités avancées, telles que le DEM complet, dans son produit par rapport aux autres fournisseurs de ce marché.

Palo Alto Networks

Palo Alto Networks est leader dans ce Magic Quadrant. L'entreprise propose Prisma Access, qui offre une gestion intégrée avec des plateformes de pare-feu sur site. Les points de

présence Prisma Access sont déployés chez les principaux fournisseurs de cloud hyperscale.

Les activités de Palo Alto Networks sont géographiquement diversifiées. Si ses clients SSE sont principalement des clients existants, l'entreprise s'est développée pour servir des entreprises de toutes tailles et de différents secteurs. Depuis 2024, Palo Alto Networks a intégré la technologie de navigateur sécurisé issue de l'acquisition de Talon Cyber Security sous le nom de Prisma Access Browser et continue d'investir dans les capacités d'IA de son produit.

Points forts

- Palo Alto Networks est une société bien établie, cotée en bourse, qui se concentre fortement sur sa division SSE et y investit, permettant aux clients de continuer à s'attendre à des capacités de la part de ce fournisseur.
- Palo Alto Networks a une vision claire de l'innovation avec les technologies d'IA dans sa plateforme , en s'alignant sur les exigences émergentes des entreprises.
- L'intégration de la configuration de Palo Alto Networks avec ses pare-feu existants (via Strata Cloud Manager) permet aux clients existants de tirer parti d'une interface unique.

Précautions

- Il est peu probable que la vision et l'accent mis par Palo Alto Networks sur les navigateurs d'entreprise sécurisés façonnent le marché SSE en raison de l'ensemble restreint de cas d'utilisation qu'il aborde efficacement.
- Les clients de Gartner décrivent la tarification de Prisma Access de Palo Alto comme complexe, coûteuse et parfois difficile à interpréter.
- Palo Alto propose principalement un support technique, une interface utilisateur et une documentation technique en anglais , ce qui limite potentiellement son attrait sur de nombreux marchés .

Sécurité Skyhigh

Skyhigh Security est un acteur de niche dans ce Magic Quadrant. Il propose Skyhigh SSE, une solution fortement axée sur la sécurité des données. L'éditeur exploite à la fois des points de présence physiques et des points de présence hébergés par un fournisseur de cloud , en fonction de la demande locale, et n'offre pas nécessairement tous les services dans tous les points de présence sans une demande suffisante de la part des clients.

Les activités de Skyhigh sont géographiquement diversifiées. Ses clients SSE évoluent généralement dans des secteurs hautement réglementés. Depuis 2024, Skyhigh a changé de direction et partage désormais un PDG avec Trellix . L'éditeur a ajouté la traduction automatique de sa documentation pour faciliter son adoption dans les zones non anglophones.

Points forts

- Skyhigh offre de solides capacités de sécurité des données et de sécurité SaaS via sa plateforme SSE .
- Selon notre évaluation, Skyhigh offre des fonctionnalités techniques pour un coût relativement faible.
- Skyhigh a fait ses preuves en répondant efficacement aux demandes et aux besoins techniques du marché .

Précautions

- La visibilité sur les finances de Skyhigh Security est limitée, et le fournisseur a une part de marché plus petite et apparaît rarement sur les listes restreintes de clients de Gartner ou en tant que fournisseur compétitif.
- Il est peu probable que la feuille de route des produits de sécurité des données et d'avenir de Skyhigh influence ou modifie le marché SSE .
- Les clients de Gartner expriment des incertitudes quant à l'impact des changements de direction sur l'orientation de Skyhigh Security. Les acheteurs devraient prendre des mesures supplémentaires pour vérifier cette orientation.

Versa Networks

Versa Networks est un acteur de niche dans ce Magic Quadrant. Il propose Versa SSE, qui fait partie d'une offre SASE plus large, incluant son SD-WAN. Versa exploite son propre backbone privé et ses points de présence (POP) basés sur son propre matériel physique.

Les activités de Versa sont géographiquement diversifiées et ses clients SSE sont de toutes tailles, avec une préférence pour les entreprises de taille moyenne. Depuis 2024, Versa a ajouté des fonctionnalités SASE souveraines et une détection des menaces basée sur l'IA pour identifier les menaces en s'appuyant moins sur les technologies sandbox.

Points forts

- Versa offre un large éventail de fonctionnalités sur l'ensemble du portefeuille SSE .
- Versa propose des POP à proximité des principaux centres de population, ce qui lui permet de servir des clients géographiquement dispersés.
- Versa propose des prix compétitifs pour les capacités techniques offertes.

Précautions

- Par rapport aux autres fournisseurs de cette étude, les informations financières disponibles sont limitées et les acheteurs doivent procéder à une validation supplémentaire de leur viabilité financière à long terme.
- La vision et l'accent mis par Versa sur les approches souveraines de sécurité SASE et des points de terminaison sont insuffisants en termes d'exhaustivité de la vision par rapport aux leaders du SSE.
- La documentation SSE de Versa est médiocre par rapport aux autres fournisseurs du marché SSE, et les clients peuvent avoir besoin d'une assistance supplémentaire de la part du fournisseur pendant le déploiement et l'exploitation.

Zscaler

Zscaler est leader dans ce Magic Quadrant. L'entreprise propose Zscaler Zero Trust Exchange, qui comprend Zscaler Internet Access et Zscaler Private Access.

Les activités de Zscaler sont géographiquement diversifiées et ses clients SSE sont généralement de très grandes entreprises. Depuis 2024, Zscaler a unifié ses multiples consoles en une seule et a lancé un modèle tarifaire simplifié. L'entreprise a diversifié ses activités sur des marchés non SSE en acquérant Airgap Networks pour la microsegmentation et Avalor pour faciliter l'agrégation et la corrélation des résultats de plusieurs outils de sécurité.

Points forts

- Zscaler a une forte présence marketing sur ce marché et figure souvent sur les listes restreintes des clients , ce qui renforce sa capacité à se développer et à continuer à servir les utilisateurs finaux.

- Zscaler a introduit un nouveau modèle de tarification qui simplifie considérablement les achats pour les nouveaux clients.
- Zscaler possède une solide compréhension du marché et de son orientation, ainsi qu'une solide expérience en matière de présence sur le marché avec de nombreuses fonctionnalités.

Précautions

- Zscaler est généralement l’un des fournisseurs les plus chers de ce marché pour les fonctionnalités qu’il fournit, et cela reste une préoccupation courante pour les clients de Gartner.
- Zscaler a diversifié ses capacités dans les opérations de sécurité, ce qui pourrait nuire à sa concentration sur le SSE.
- Les clients de Gartner observent des problèmes de performances avec les connexions Zscaler plus fréquemment que ce qui est typique pour les autres fournisseurs de ce marché.

Fournisseurs ajoutés et supprimés

Nous révisons et ajustons nos critères d'inclusion dans les Magic Quadrants en fonction de l'évolution des marchés. En conséquence, la composition des fournisseurs d'un Magic Quadrant peut évoluer au fil du temps. Le fait qu'un fournisseur figure dans un Magic Quadrant une année et non l'année suivante ne signifie pas nécessairement que nous avons changé d'avis à son égard. Cela peut refléter une évolution du marché et, par conséquent, des critères d'évaluation, ou un changement d'orientation de la part de ce fournisseur.

Ajouté

- Aucun fournisseur ajouté

Abandonné

- Lookout ne répondait pas aux exigences des clients de ce marché.

Critères d'inclusion et d'exclusion

Pour être admissible à l'inclusion, l'offre SSE du fournisseur doit :

- Fonctionner comme un service. L'offre doit être fournie sous forme de service cloud, sécurisant les utilisateurs autorisés sur les terminaux autorisés vers les services appropriés exécutés dans des clouds publics ou privés et des environnements sur site.
- Gartner doit démontrer de manière convaincante que le produit SSE est largement adopté, indépendamment d'un SD-WAN, d'un pare-feu ou de toute autre fonctionnalité réseau proposée par le même fournisseur. L'offre SSE principale d'un fournisseur doit inclure plusieurs fonctionnalités permettant de sécuriser les utilisateurs autorisés sur les terminaux autorisés pour accéder aux services appropriés. Ces fonctionnalités doivent être disponibles au plus tard le 31 octobre 2024. Ces fonctionnalités sont les suivantes :
  - Sécurisez l'accès à Internet depuis les terminaux courants, notamment Windows, macOS, iOS et Android via un proxy. Proposez un filtrage d'URL et une protection avancée contre les menaces pour protéger les utilisateurs et appliquer des politiques d'utilisation acceptables.
  - Utilisation sécurisée des logiciels en tant que service, en ligne et via API. Assurer la visibilité, le respect de la conformité, la sécurité des données et la protection contre les menaces pour l'utilisation des applications SaaS ; surveiller et corriger les problèmes via un produit proxy (en ligne) et des intégrations API. L'intégration API pour les fonctions CASB doit inclure au moins cinq suites logicielles d'entreprise majeures, telles que Microsoft Office 365, Google Workspace, Salesforce, Workday, Github, Atlassian et ServiceNow. Au moins une de ces intégrations doit être autre qu'une application de partage ou de stockage de fichiers. Les intégrations API avec les réseaux sociaux ou les plateformes SaaS gratuites, telles que Twitter, Reddit, YouTube ou Facebook, ne sont pas prises en compte. La sécurité doit inclure la protection contre les menaces, la protection des données et des capacités de détection et de prévention. La sécurité en ligne doit être assurée depuis les appareils gérés, y compris au moins Windows, macOS, iOS et Android, vers toute application SaaS et être applicable depuis les appareils non gérés vers les applications SaaS connues et explicitement autorisées.
  - 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
Vertical/Industry Strategy	NotRated
Innovation	Medium
Geographic Strategy	Low

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 and demonstrate a clear understanding of the market. Additionally, they possess a product strategy that aligns with the market trend for providing easy-to-use advanced features and making business investments for the future. Leaders have effective sales and distribution channels for their entire product portfolios, a well-diversified vertical and geographic strategy, and a vision for how SSE offerings are positioned within the context of organizations' wider SASE transformations.

Challengers

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

Visionaries

Visionaries are distinguished by technical and/or product strategies but lack either the track record of execution and the high visibility of Leaders or corporate resources, such as strong sales channels and strategic relationships. Buyers should expect 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:

- **Remplacement des VPN :** Les vulnérabilités des infrastructures sécurisées situées à la périphérie d'une organisation, telles que les appliances VPN, les pare-feu réseau et les passerelles, sont de plus en plus exploitées par des attaques visant à s'implanter dans les réseaux. Ces vulnérabilités ont favorisé l'essor des produits SSE, car leurs offres d'accès

privé permettent généralement aux organisations d'exploiter un centre de données « obscur » où aucun accès entrant n'est possible. Les fournisseurs ont amélioré leurs offres pour autoriser l'accès au réseau et le trafic sortant depuis les serveurs d'entreprise, permettant ainsi à de nombreuses organisations de remplacer ces systèmes hérités, bien que cela représente généralement un coût nettement plus élevé.

- **Adoption du SaaS et sécurité GenAI :** L'adoption et la croissance du SaaS, de la plateforme en tant que service (PaaS) et de l'infrastructure en tant que service (IaaS) continuent de progresser. Gartner estime que le SaaS est le principal générateur de revenus du cloud et qu'il connaîtra une croissance annuelle composée de plus de 15 % d'ici 2028 (voir **Prévisions : Services de cloud public, monde, 2022-2028, mise à jour du 4e trimestre 2024**) . L'adoption rapide du cloud crée un besoin de simplification et de consolidation de la sécurité fournie par le cloud pour le cloud, plutôt que de tenter de forcer le trafic via les réseaux et centres de données sur site pour sécuriser l'accès. Elle accroît également le besoin de sécurité et de contrôles communs, que les applications soient hébergées dans un hyperscaler, livrées sur site ou migrées vers le SaaS. De même, les applications GenAI, présentées comme des cas particuliers d' applications SaaS, prolifèrent. Elles peuvent être contrôlées en limitant l'accès aux applications approuvées et en filtrant les données qui peuvent être saisies et traitées par ces applications.

- **Réseautage Zero Trust :** L'intérêt pour l'harmonisation de la sécurité avec le Zero Trust reste fort, tant dans les secteurs où il est obligatoire qu'au niveau plus général. C'est en partie pour cette raison que le marketing Zero Trust est omniprésent dans le secteur de l'ESS. Quelles que soient les définitions présentées par les fournisseurs, l'ESS peut mettre en œuvre les principes du réseautage Zero Trust, comme expliqué dans **la réponse rapide : Qu'est-ce que le réseautage Zero Trust ?**

- Ces principes exigent que l'accès au réseau ne soit accordé qu'après authentification et autorisation ; que l'accès au réseau soit limité aux seules ressources nécessaires ; et que l'accès au réseau soit ajusté en permanence en temps quasi réel, en fonction du risque.

⊕ Preuve

⊕ Définitions des critères d'évaluation