Magic Quadrant pour Security Service Edge

10 avril 2023 - ID G00766751 - 44

Par **et 4 autres**Charlie Winckless, Aaron McQuaid,

Les solutions de périphérie de service de sécurité fournissent une sécurité sécurisée, cohérente et principalement fournie par le cloud pour le trafic des utilisateurs et des terminaux. Les responsables de la sécurité et de la gestion des risques peuvent utiliser cette recherche pour identifier les fournisseurs appropriés pour sécuriser l'accès au Web, aux services cloud et aux applications privées.

Hypothèses de planification stratégique

D'ici 2025, 70 % des organisations qui mettent en œuvre un accès réseau Zero Trust (ZTNA) basé sur des agents choisiront un fournisseur SASE (Secure Access Service Edge) ou un fournisseur de services de sécurité (SSE) pour ZTNA, plutôt qu'une offre autonome.

D'ici 2026, 85 % des organisations cherchant à se procurer des offres Cloud Access Security Broker, Secure Web Gateway ou Zero Trust Network Access les obtiendront à partir d'une solution convergée.

D'ici 2026, 45 % des organisations donneront la priorité aux fonctionnalités avancées de sécurité des données pour l'inspection des données au repos et en mouvement comme critère de sélection pour SSE.

Définition/description du marché

SSE sécurise l'accès au Web, aux services cloud et aux applications privées, quel que soit l'emplacement de l'utilisateur ou de l'appareil qu'il utilise ou l'endroit où cette application est hébergée. Il offre également une sécurité et une visibilité accrues pour les environnements SaaS (Software as a Service), PaaS (Platform as a Service) et IaaS (Infrastructure as a Service) auxquels accèdent les utilisateurs finaux.

Les capacités SSE obligatoires incluent :

- Proxy direct, y compris la protection contre les logiciels malveillants, la prévention des menaces et le filtrage d'URL
- Détection et protection en ligne (proxy) et hors bande (API) des applications SaaS en cours d'utilisation, y compris l'inspection du contenu pour détecter les données sensibles, la

protection contre les logiciels malveillants et la prévention des menaces

- Accès granulaire (contrôlé par l'identité et le contexte) aux applications privées par agent ou sans agent, ou de manière optimale les deux
- Possibilité d'appliquer des contrôles de manière cohérente sur plusieurs destinations réseau
- Prise en charge des appareils gérés et non gérés et possibilité de fournir un accès adaptatif aux applications SaaS et aux applications privées à partir de ces types d'appareils
- Prise en charge de la gestion et de la sécurisation du trafic provenant de terminaux courants tels que les appareils Windows, macOS, iOS et Android
- Intégration avec des technologies d'entreprise clés 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
- Intégration avec les fournisseurs d'identité pour le contexte et la validation des identités
- Déchiffrement et rechiffrement de Secure Sockets Layer/Transport Layer Security (SSL/TLS)

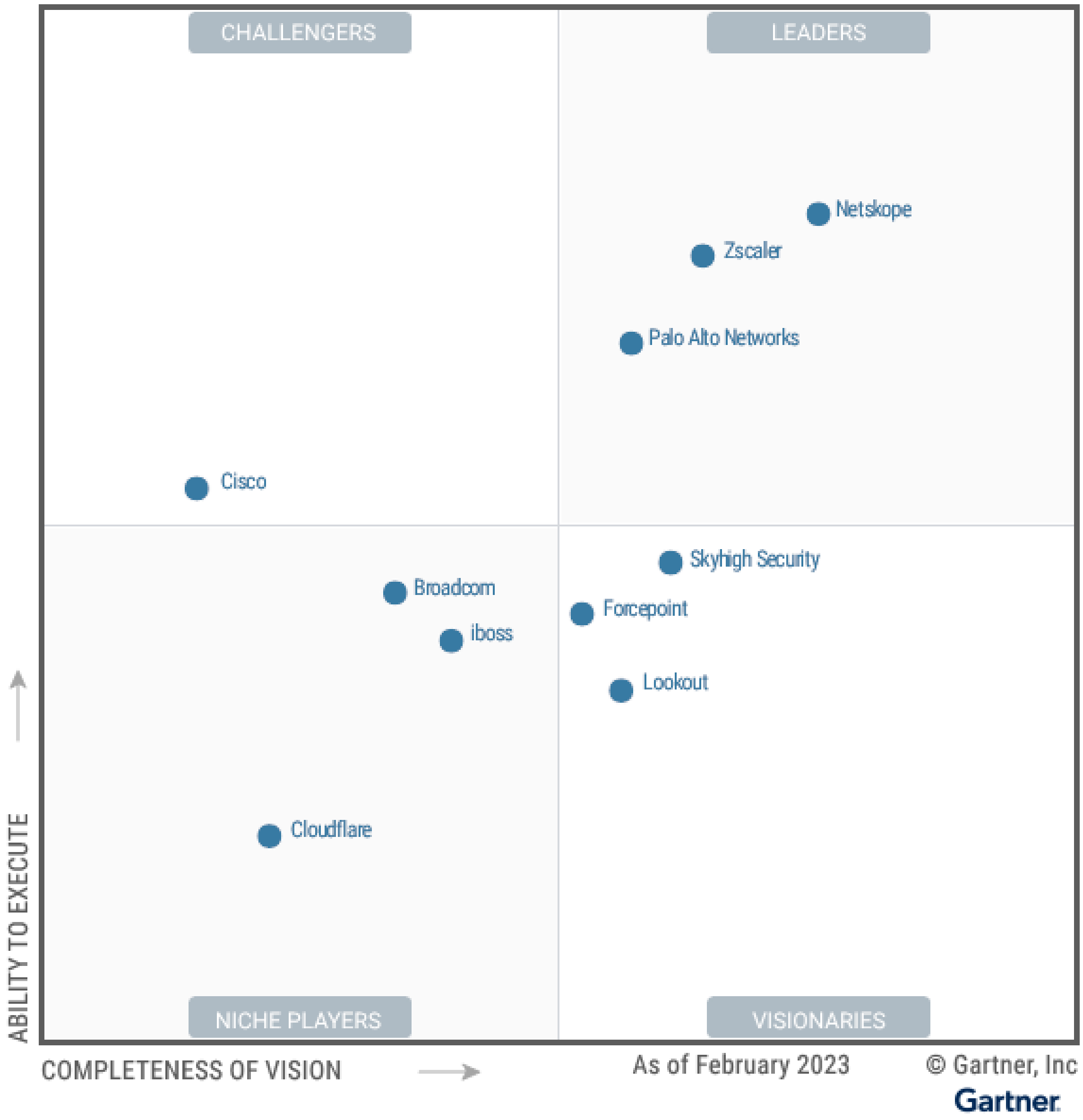
Fonctionnalités SSE en option :

- Capacité à fournir un contrôle 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 du cloud et gestion de la posture de sécurité SaaS pour la visibilité et la correction du SaaS et de l'IaaS
- Contrôles d'accès adaptatifs basés sur l'état initial de la connexion et tout changement d'état pendant la connexion
- Capacité de lire, d'écrire et d'agir sur les étiquettes des plates-formes de classification de données courantes
- Prise en charge des API publiées et documentées accessibles au client pour permettre l'automatisation des tâches courantes et l'intégration avec d'autres plates-formes de sécurité
- Analyse du comportement de l'entité utilisateur (UEBA) pour fournir une détection et une réponse automatisées aux comportements anormaux et risqués des appareils et des utilisateurs
- Fonctionnalités avancées de protection des données telles que la rédaction, la lapidation et le chiffrement à la volée (en ligne et hors bande)
- Capacités avancées de détection de données telles que l'appariement exact des données (EDM), la reconnaissance optique de caractères (OCR) et les classificateurs d'apprentissage

automatique

Magic Quadrant

Figure 1 : Magic Quadrant pour Security Service Edge



Forces et mises en garde des fournisseurs

Broadcom

Broadcom est un acteur de niche dans ce Magic Quadrant. L'offre SSE de Broadcom est composée de deux éléments : Symantec Network Protection et Symantec Data Loss Prevention (DLP) Cloud. Broadcom, dont le siège social est situé à San Jose, en Californie, aux États-Unis, est une grande entreprise ayant des activités mondiales. Ses clients ont tendance à être de grandes et très grandes entreprises de nombreux secteurs. Broadcom continue d'avoir une forte présence sur le marché avec son activité de passerelle Web sécurisée (SWG) basée sur des appliances.

Depuis son acquisition de Symantec en 2019, Broadcom s'est concentré sur la création d'une entreprise de logiciels d'entreprise. En mai 2022, Broadcom a annoncé son intention d'acquérir VMware. Parmi les autres changements apportés aux produits par Broadcom, citons la résiliation de son service OEM FWaaS et le lancement de sa propre offre et la création d'un agent combiné pour tous les services SSE et la prévention des pertes de données d'entreprise (DLP).

Forces

- Broadcom est une société publique bien financée et financièrement sûre qui possède un portefeuille de semi-conducteurs stratégiques de haute technologie et de logiciels d'entreprise.
- La sécurité des données de Broadcom dans SSE fait partie de son Symantec DLP Cloud, et les clients doivent acheter cette licence pour obtenir cette fonction. Cependant, il couvre un large éventail de domaines, y compris regex, regex personnalisé, EDM et OCR technologie. Il utilise les mêmes classificateurs sur plusieurs vecteurs. Cela étend la visibilité et permet une synergie accrue entre le cloud et le point de terminaison.
- L'offre SSE de Broadcom peut étendre la couverture aux cas d'utilisation sur site via son modèle de livraison hybride. Toutes les fonctionnalités SSE sont prises en charge avec ses appliances locales.
- La console d'administration de Broadcom est disponible en plusieurs langues, dont l'anglais, le français, l'espagnol et le japonais.

Précautions

- Broadcom se concentre sur les plus grandes entreprises du monde, ce qui limite son attrait pour les entreprises qui ne relèvent pas de cette catégorie. Les commentaires indiquent également que son offre SSE basée sur le cloud figure sur moins de listes restreintes que celles d'autres concurrents sur ce marché et est couramment citée comme cible de remplacement.
- Les fonctions SSE de base sont deux SKU, et Broadcom poursuit ses efforts pour intégrer plus étroitement les composants. Cependant, l'offre elle-même est composée de plusieurs produits et consoles intégrés via l'authentification unique (SSO). Les fonctions non essentielles (telles que l'UEBA) sont également des produits supplémentaires.
- Broadcom a été lent à introduire certaines fonctionnalités telles qu'une gestion intégrée de l'expérience numérique (DEM) sur le marché.
- Broadcom maintient actuellement relativement peu d'accréditations auprès d'organismes communs. Il n'est pas enregistré auprès de la Cloud Security Alliance Security, Trust, Assurance and Risk (CSA STAR) et ne dispose pas de plusieurs accréditations de sécurité géographiques telles que FedRAMP, Cyber Essentials, C5 et le programme Infosec Registered Assessors (IRAP).

Cisco

Cisco est un challenger dans ce Magic Quadrant. Les principaux produits Cisco pour SSE font partie de plusieurs gammes de produits, notamment Cisco Umbrella, Cisco+ Secure Connect et Duo. Elle dispose également d'un large portefeuille de produits d'infrastructure, de mise en réseau et de sécurité. Cisco a son siège social à San Jose, en Californie, aux États-Unis. Ses opérations sont géographiquement diversifiées et elle compte des clients de toutes tailles et de toutes industries.

En 2022, Cisco a lancé son service Cisco+ Secure Connect, axé sur SASE à fournisseur unique et intégrant des éléments de SSE à son SD-WAN Meraki existant (bien que cela ne prenne en charge que 5 000 utilisateurs). Cisco a également étendu ses capacités DLP pour inclure la GED et a fourni la possibilité de l'appliquer sur les canaux CASB (Cloud Access Security Broker) et Secure Web Gateway (SWG).

Forces

- Cisco a remplacé le ZTNA sans client Duo Beyond dans sa solution SSE ce cycle. Le nouveau ZTNA sans agent inclut une vérification de posture et prend en charge le Web, le shell sécurisé (SSH) et le protocole RDP (Remote Desktop Protocol) si le déploiement d'un agent éphémère est autorisé.

- Cisco est fortement représenté sur le marché, à la fois en termes de visibilité dans l'enquête de Gartner sur les capacités et dans son positionnement dans la dynamique du marché de Gartner dansle dex (MMI).

- Cisco a fait des progrès dans l'intégration de son offre SD-WAN Meraki (mais pas encore Viptela) dans son offre SSE ce cycle de recherche.

- ThousandEyes, bien qu'il ne soit pas intégré à la solution SSE, est une offre DEM complète (avec des capacités supplémentaires) disponible en tant que produit distinct.

Précautions

- Bien que Cisco ait amélioré l'intégration de sa plate-forme SSE au cours de ce cycle, sa plate-forme SSE complète repose toujours sur plusieurs produits discrets qui ne sont que partiellement intégrés.

- La solution d'accès privé basée sur les agents de Cisco est construite autour d'AnyConnect VPN-as-a-service (VPNaaS) et n'est pas une solution ZTNA. Ses contrôles d'accès adaptatifs ne s'appliquent qu'à l'accès privé (pas SaaS). Ils ne peuvent pas modifier la connectivité pendant une connexion et évaluent relativement peu de signaux lors de la connexion.

- Cisco ne fournit aucun contrat de niveau de service (SLA) pour la latence pour le traitement des données ou le temps aller-retour, bien qu'il maintienne un SLA de disponibilité de cinq neuf (ou 99,999%). Cisco ne fournit pas de visibilité sur les services pris en charge sur quels centres de données dans le cadre de son portail de confiance.

- Gartner observe que Cisco est fréquemment présélectionné par les clients, mais n'est généralement pas sélectionné comme solution SSE, sauf dans le cadre d'un accord Cisco plus large.

Cloudflare

Cloudflare est un acteur de niche dans ce Magic Quadrant. Cloudflare est un grand fournisseur d’infrastructure avec plus de 3 000 employés et propose un certain nombre de produits sur le marché. Elle est entrée sur le marché de l’ESS en 2022 avec l’acquisition de la technologie CASB pour fournir des fonctionnalités SSE de base.

La principale offre SSE de Cloudflare est Cloudflare Zero Trust. Il inclut la fonctionnalité intégrée pour SSE, et il existe une option freemium. En outre, Cloudflare offre une variété de services réseau et Zero Trust sous forme d’offres à la carte.

Au cours de la dernière année, Cloudflare a acquis Vectrix pour fournir une visibilité API sur les applications SaaS et la zone de sécurité 1 pour la sécurité des e-mails. Il a également publié l’isolation Web sans client et la journalisation des commandes SSH pour sa plate-forme.

Forces

- Cloudflare, bien que nouvelle dans l’espace SSE, est une grande entreprise mondiale axée sur la sécurité avec une forte présence dans plusieurs zones géographiques et clients dans un ensemble diversifié de secteurs verticaux.

- Cloudflare propose un niveau de tarification simple, y compris un niveau gratuit pour moins de 50 utilisateurs ou de grandes organisations qui souhaitent effectuer une preuve de concept comprenant SWG, ZTNA, CASB en ligne et un forum de support communautaire.

- Cloudflare offre le plus grand nombre de points de présence cloud (PoP) sur ce marché, et des fonctionnalités réseau grâce à son Magic WAN et à des intégrations avec plusieurs fournisseurs SD-WAN. Il offre un SLA à 100% pour la disponibilité (mais pas de SLA de latence) pour son Cloudflare Zero Trust payant. Cette anse géographiquesignifie qu’il y a rarement une latence significative pour atteindre un PoP Cloudflare.

- Alors que tous les journaux actifs sont traités en mémoire aux États-Unis continentaux, Cloudflare permet aux clients de désactiver les journaux ou d’utiliser son service Logpush pour diriger les journaux vers n’importe quel fournisseur de stockage dans la région de leur choix. En outre, Cloudflare Data Localization Suite peut restreindre l’inspection du trafic à n’importe quelle région en fonction des besoins des clients.

Précautions

- Cloudflare ne dispose pas d’une base installée significative au-delà des déploiements de petites entreprises et de preuve de concept (en partie en raison de son option gratuite pouvant accueillir jusqu’à 50 utilisateurs). Il fait mûrir sa plate-forme à partir de sa base initiale de clients ZTNA pour inclure les fonctions SWG et CASB. Aujourd’hui, Gartner voit rarement Cloudflare sur les listes de présélection des clients pour la sélection SSE.

- Cloudflare ne dispose que de fonctionnalités de sécurité des données naissantes dans sa plate-forme et ne peut pas prendre en charge la plupart des cas d’utilisation de la sécurité des données d’entreprise.

- Cloudflare n’a acquis la fonctionnalité CASB d’API critique qu’en 2022. Il s’intègre avec très peu de fournisseurs SaaS par API par rapport au marché et suit un petit nombre d’attributs pour le risque SaaS. Il n’intègre pas le risque SaaS dans sa politique.
- Cloudflare manque d’un certain nombre de fonctionnalités trouvées sur ce marché, telles que le sandboxing de logiciels malveillants, DEM et des rapports et analyses intégrés complets.

Point de force

Forcepoint est un visionnaire dans ce Magic Quadrant. Forcepoint propose l’ESS à travers son offre Forcepoint ONE, issue de l’achat de Bitglass en octobre 2021. Forcepoint fournit également des pare-feu réseau, DLP d’entreprise et d’autres produits de sécurité. Le siège social de Forcepoint est situé à Austin, au Texas, aux États-Unis. Ses opérations sont géographiquement diversifiées et ses clients vont des petites aux très grandes organisations dans de nombreux secteurs.

En 2022, Forcepoint a entamé le processus de retrait de ses anciens produits de sécurité cloud et d’offre des options de migration à ses anciens clients sur Forcepoint ONE. En 2022, Forcepoint a également intégré ses technologies Zero Trust Content Disarm and Reconstruction, DLP et RBI dans Forcepoint ONE.

Forces

- Forcepoint offre des contrôles de sécurité des données solides et personnalisables à l’aide de la fonction exclusive Field Programmable SASE Logic (FPSL) de l’entreprise. Il est intégré aux fonctions SWG, CASB et ZTNA.
- Forcepoint est bien présent à l’échelle mondiale et compte parmi ses clients un mélange de grandes et moyennes entreprises. L’acquisition de Bitglass fournit à Forcepoint une offre SSE plus consolidée pour ces clients par rapport à ses offres cloud traditionnelles.
- Forcepoint peut utiliser son agent SmartEdge pour effectuer le déchiffrement et l’inspection du contenu, y compris la prise en charge d’ESNI et de QUIC, car il ne s’agit pas d’un proxy traditionnel de l’homme du milieu. Cette approche peut réduire la latence sur les appareils et fournir une visibilité sur le trafic Web où l’agent peut être installé, y compris les sites distants avec une présence limitée dans le cloud.
- Forcepoint offre une expérience utilisateur solide avec de bonnes notifications aux utilisateurs finaux lorsqu’ils enfreignent une politique, même à partir d’appareils non gérés lors de l’utilisation de sa capacité ZTNA sans client et de proxy inverse pour les applications SaaS sanctionnées.

Précautions

- Forcepoint poursuit sa stratégie de consolidation des capacités de Forcepoint dans la plate-forme Forcepoint ONE. Cependant, toutes les fonctionnalités de Forcepoint ne sont pas intégrées à sa plate-forme et l’agent Forcepoint ONE SmartEdge n’est disponible que sous Windows et macOS. Des exemples de technologies non intégrées incluent certaines qui sont actuellement gérées à partir d'une console distincte (bien qu'intégrées à Forcepoint ONE via SSO). Par exemple, la protection adaptative aux risques de Forcepoint et la DLP des terminaux de Forcepoint nécessitent le déploiement d'un agent distinct, bien que les stratégies DLP des points de terminaison puissent être importées dans Forcepoint ONE.

- Forcepoint fournit uniquement l'accès TCP sur ZTNA basé sur un agent, et seules les applications Web sont prises en charge dans le cas d'utilisation sans agent.
- Forcepoint apparaît rarement dans les évaluations concurrentielles et les listes restreintes pour l'ESS des clients de Gartner. Les clients existants de Forcepoint et les anciens clients de Bitglass citent souvent la mauvaise expérience du support client de Gartner comme une raison de les exclure.
- Forcepoint a introduit moins de nouvelles fonctionnalités nettes à sa plate-forme SSE au cours de ce cycle de recherche, car elle s'est concentrée sur la consolidation de la plate-forme Forcepoint ONE et des éléments de la pile de sécurité existante de Forcepoint.

iBoss

iboss est un joueur de niche dans ce Magic Quadrant. Son offre SSE principale est la plate-forme cloud iboss Zero Trust Edge. Basée à Boston, Massachusetts, États-Unis, iboss est une société privée avec des opérations mondiales et des clients principalement basés en Amérique du Nord. Il a une présence plus petite dans la région EMEA et en Asie/Pacifique. Ses clients sont principalement dans le secteur financier vertical avec une représentation plus faible dans d'autres domaines.

En 2022, iboss a étendu la notation des risques pour les utilisateurs de la plate-forme Zero Trust Edge et a ajouté de nouvelles fonctionnalités DLP à la plate-forme. Il a étendu ses partenariats de fournisseur de services de sécurité gérés (MSSP) pour inclure Verizon et a ajouté des intégrations technologiques avec SentinelOne et CrowdStrike. iboss a également obtenu la certification FedRAMP Moderate en 2022 et s'est fortement concentré sur son alignement sur NIST 800-207 en tant qu'approche du marché.

Forces

- iBoss offre un SLA de forte disponibilité de sept-neuf, ainsi qu'un SLA de latence de 100ms. Il offre des crédits progressifs basés sur le non-respect de ces SLA à ses clients.
- iboss inclut plusieurs fonctionnalités en standard à tous les niveaux de sa plate-forme, y compris les FWaaS et ZTNA de base, bien qu'il soit toujours l'une des offres les moins chères.
- Bien qu'il s'agisse d'un fournisseur relativement petit sur le marché, les clients de Gartner font état d'une équipe de support client efficace et réactive, et le mandat du personnel de support d'iboss est supérieur à la normale pour cette comparaison.
- Le modèle SSE d'iboss peut être déployé dans des emplacements flexibles, y compris sur site et dans des environnements cloud hébergés par le client. Cela permet à la fois des opérations ZTNA universelles et la prise en charge des zones géographiques soumises à des restrictions de conformité.

Précautions

- iboss se concentre fortement sur les clients basés en Amérique du Nord et se trouve dans un ensemble limité de secteurs verticaux. Clients en dehors des États-Unis Les régions géographiques devraient valider qu'il y a suffisamment de personnel et de ressources pour répondre à leurs besoins.

- iboss ne se concentre pas sur le support SaaS, en particulier avec les intégrations d'API. Il manque de capacités de gestion de la posture de sécurité SaaS (SSPM), ne dispose que d'un petit catalogue d'applications SaaS pour lesquelles il fournit des évaluations de risque et a peu d'applications SaaS intégrées à son produit pour API CASB.

- Bien qu'iboss se concentre extrêmement fortement sur NIST 800-207 et le zero trust, il montre moins d'innovation autour des fonctionnalités communes à ce marché, notamment les fonctions DEM, CSPM et SSPM.

- Gartner voit rarement iboss cité sur les listes restreintes pour les clients ni comme un concurrent de premier plan par d'autres fournisseurs sur ce marché.

Guetteur

Lookout est un visionnaire dans ce Magic Quadrant. L'offre SSE de Lookout comprend les services CASB, SWG et ZTNA. Lookout propose également des produits de sécurité des terminaux mobiles. Lookout a son siège social à San Francisco, Californie, États-Unis. Ses activités sont concentrées en Amérique du Nord et dans la région EMEA, et sa présence est plus faible en Asie/Pacifique. Il sert principalement les moyennes et grandes entreprises dans de nombreux secteurs.

Lookout a procédé à une intégration supplémentaire de ses services RBI et a ajouté une capacité FWaaS à sa plateforme. Bien qu'il ne soit pas directement lié à l'ESS, Lookout a également acquis SaferPass pour la gestion des mots de passe afin de soutenir sa stratégie globale de travail à domicile.

Forces

- Lookout dispose de solides capacités de sécurité des données, y compris plusieurs fonctionnalités avancées. Il a intégré les politiques et les applications de sécurité des données profondément dans les applications Web, SaaS et privées.

- Bien qu'il s'agisse d'un fournisseur plus petit, Lookout bénéficie de bons canaux de revendeurs grâce à ses relations avec les FAI de niveau 1, les MSSP et les opérateurs de télécommunications du monde entier.

- Lookout propose un produit unifié et complet couvrant tous les types de cas d'utilisation SSE de base, quels que soient l'utilisateur, l'appareil, les données ou le service cloud. Sa stratégie reste cependant plus axée sur les cas d'utilisation mobile.

- Lookout dispose de capacités avancées d’analyse et de tableau de bord qui présentent des méthodes puissantes pour visualiser les données de sa plateforme SSE.

Précautions

- L’offre SSE de Lookout a moins de parts de marché et de visibilité que celles de la plupart des autres fournisseurs SSE. Il apparaît moins fréquemment sur les listes de présélection concurrentielles vues par Gartner, n’a pas été très bien classé dans l’indice de momentum du marché de Gartner et est mentionné moins souvent par les utilisateurs du service de demande de renseignements des clients de Gartner.

- Lookout a peu de partenariats SD-WAN et se concentre sur la défense contre les menaces pour les systèmes d’exploitation mobiles plutôt que pour les appareils non mobiles. Les clients potentiels qui ont besoin de connecter des succursales doivent examiner les partenariats SD-WAN de Lookout et tester attentivement la connectivité des succursales.

- La perception de Gartner à partir de l’enquête indique que Lookout se développe plus lentement à partir d’une base plus petite et a moins de clients que de nombreux fournisseurs sur ce marché. Cela est particulièrement vrai pour les grands clients de Gartner.

- Lookout ne dispose pas d’une fonctionnalité DEM mature pour mesurer les performances de bout en bout du trafic utilisateur-application. Sa vision produit reste axée sur les marchés du mobile et de la sécurité des données plutôt que sur le marché plus large de l’ESS.

Netskope

Netskope is a Leader in this Magic Quadrant. Its primary SSE offerings, available as part of the Netskope Intelligent SSE platform, include the Next Gen Secure Web Gateway, CASB and Netskope Private Access (NPA). Netskope is headquartered in Santa Clara, California, U.S. Its operations are geographically diversified, and its customers range from midsize to very large organizations across many industries.

In 2022, Netskope acquired Infiot to support single-vendor SASE and WootCloud to enhance visibility into the Internet of Things (IoT) ecosystem. It expanded its DLP to encompass endpoint use cases, and expanded its ZTNA to allow for on-premises termination to support universal ZTNA use cases. In the SSPM arena, it continued to integrate the Kloudless acquisition from 2021, including launching a dedicated SSPM query language.

Strengths

- Netskope is a well-funded, privately held company. Gartner estimates Netskope has strong revenue and growth relative to other vendors in the market. Feedback from Gartner clients indicates that Netskope appears frequently on SSE shortlists and has a strong mind share in the SSE market.

- Netskope offers advanced data security capabilities, including a lightweight on-premises capability via its agent. For example, Netskope offers machine learning to identify image types and text based on classifiers trained on end-user data.

- Netskope has simplified its SKU and packaging model to provide a less complex purchasing experience for its customers. In addition, Netskope has no surcharge based on the location of the Netskope PoP used by a customer.

- Netskope offers a strong ZTNA capability including in-line DLP inspection, on connect and continuous context validation, and clientless support for web, SSH, RDP, virtual network computing (VNC) and Telnet protocols.

Cautions

- Netskope has a single login for its admin console. However, administration is complicated by then splitting it into two primary management environments: settings and functions. Settings include technical configurations for the platform, while functions include a mix of dashboards, policies, event monitoring and an integration to the Advanced Analytics dashboard. Advanced Analytics is a separate license, though it is included in some higher-tier Netskope packages.

- Gartner clients report that Netskope is usually one of the most expensive options in a competitive pricing situation.

- While Netskope has purchased a vendor with many SD-WAN capabilities, this is not yet fully integrated with the Netskope platform and the installed base is small. This purchase may strain existing SD-WAN partnerships and relationships.

- Netskope does not offer some advanced DEM capabilities as part of its SSE platform. Additionally, while it has added Layer 7 firewall capabilities, it still has a low adoption rate for its advanced cloud firewall.

Palo Alto Networks

Palo Alto Networks is a Leader in this Magic Quadrant. Its SSE offering is primarily composed of Prisma Access and SaaS security services. It offers a stand-alone cloud native application protection platform under the Prisma Cloud brand. It also provides a range of other network and cloud security products. It is headquartered in Santa Clara, California, U.S. Its operations are geographically diversified, and it has customers of all sizes from all industries.

Palo Alto Networks extended Prisma Access capabilities in 2022. New features include better integration with Prisma SD-WAN, enhancements to the explicit proxy and its ZTNA component as well as initial SSPM capabilities. New features are seen first in the Innovation edition of the platform. Palo Alto Networks acquired Crusoe Security for RBI in July of 2022.

Strengths

- Palo Alto Networks is financially strong. 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.

- Palo Alto Networks offers a complete unified console for SSE and has simplified management of the platform in its Prisma Access Cloud Management.

- Palo Alto Networks ZTNA remains in-line for traffic between endpoints and applications, and applies its object-based rules to segment users and applications. Palo Alto Networks supports a connector-based architecture, subapplication filtering capability, adaptive trust changes during an existing connection, and stronger integrated DLP and management capabilities.

- Palo Alto Networks SSE includes AI/ML features including deep learning categorization of URL categories, advanced DNS security without a requirement to be a resolver and extensive integration into collaboration applications. In addition, its DEM offering allows for user self-service.

Cautions

- Palo Alto Networks Cloud Management Console offers a full-featured SSE, but clients must choose between this and the Panorama plug-in on license activation and cannot change this after the fact. There remain feature differences between the Cloud Management Console and the Panorama plug-in.

- Gartner clients indicate that Prisma Access licensing remains complex and confusing, with multiple potentially overlapping models and capabilities. For example, customers must license multiple modules and then choose the Prisma Access security features to secure users, branches or both.

- Palo Alto Networks does not yet offer native RBI capabilities despite its acquisition of Crusoe Security, but relies on CloudBlade integration with a third-party RBI vendor. Palo Alto Networks risk scoring cannot be adjusted or tuned by the end user to meet their individual priorities and risk needs.

- Palo Alto Networks Prisma Access still appeals primarily to existing Palo Alto Networks customers.

Skyhigh Security

Skyhigh Security is a Visionary in this Magic Quadrant. Its SSE offering is the Skyhigh Security Service Edge. Headquartered in San Jose, California, U.S., Skyhigh has a wide geographic presence. Its customers range in size from small to very large, and come from all industries.

At the start of 2022, Symphony Technology Group separated McAfee enterprise into the cloud business (now Skyhigh Security) and the endpoint business (now Trellix). Skyhigh Security continues to integrate with Trellix products, and they share the same DLP classifiers for the Trellix Enterprise DLP and Skyhigh's Cloud DLP. Skyhigh Security is responsible for development of the DLP engine that both companies use.

Strengths

- Skyhigh Security offers a robust and mature set of security controls including a powerful and intuitive ability to adjust risk ratings to tune for individual customer use cases. Skyhigh Security has tight integration with the Trellix security solution suite but will support major UEM and XDR vendors to provide integration into the Skyhigh Security platform to enrich the posture information.

- Skyhigh Security has excellent data security capabilities overall with support for a range of base selectors, OCR, ML and EDM. It can tie data security with user, device, cloud service, personal versus corporate instances of cloud services, and stand-alone on-premises use cases. This allows for an end user to have a comprehensive view of all sensitive data entering or leaving an organization.

- Skyhigh Security has been adding SSPM capabilities to its existing CSPM capabilities in this market, and has the ability to discover applications connected to O365 and apply risk ratings to these connections.

- Skyhigh Security has a large catalog of risk-rated SaaS applications, and offers users a flexible and powerful interface for both adjusting these ratings and using these ratings in their policy engine.

Cautions

- Skyhigh Security does not run all services in all PoPs. Customers of Skyhigh Security, particularly from regions outside of North America and Europe, must test and validate if the features they need are available and performant from the Skyhigh PoPs to which they need to connect.

- Skyhigh Security's presence in the market and channel program is weaker than many other leading competitors. Skyhigh Security today is not represented on many Gartner client RFPs and shortlists despite the feature set of the solution.

- The split of businesses from McAfee Enterprise into and between Skyhigh Security and Trellix has disrupted Skyhigh's sales motion and has had an impact on its growth in this evaluation cycle, especially in this rapidly growing market.

- Skyhigh Security has an extensive and robust set of controls within the portfolio; however, it has not demonstrated significant advancement in its portfolio this evaluation cycle while the business addressed the business split.

Zscaler

Zscaler is a Leader in this Magic Quadrant. Its primary SSE offerings are Zscaler for Users (a unified SSE) and discrete products including Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA) and Zscaler Digital Experience (ZDX). It also offers Zscaler for Workloads (focusing on CNAPP) and Zscaler for OT and IoT. Zscaler is headquartered in San Jose, California, U.S. Its operations are geographically diversified, and its customers range from midsize to very large organizations across all industries.

In 2022, Zscaler acquired Priatta Networks for IoT discovery and ShiftRight for security workflow automation. It also announced a partnership with Siemens to integrate ZPA into Siemens' SCALANCE OT devices to facilitate remote administration of these devices. Zscaler also strengthened its data security offering by introducing automated data classification, enhanced inspection for endpoint and email DLP, and increased support for automation.

Strengths

- Zscaler continues to see strong revenue growth from a large base. It continues to grow faster than the overall market.

- 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.

- Zscaler's network is extensive, with a large number of its own PoPs, and some of the solutions also run on hyperscaler cloud provider infrastructure. It provides support in China, which is rare for vendors in this space. Zscaler has a strong suite of accreditations, including FedRAMP High, C5, IRAP and UK Cyber Essentials.

- Zscaler's ecosystem of partners and API integration is strong, and they provide good integration across multiple adjacent markets such as EDR, SIEM and SD-WAN.

Cautions

- Gartner sees Zscaler's clients often report pricing and perceived sales arrogance as top complaints, particularly at renewal time, while SMEs often tell Gartner that Zscaler can be hard to do business with. For example, those renewing from Zscaler's Bundle SKU line items find prices have increased with the newer Zscaler Edition SKU pricing though inclusive of extra features.

- Zscaler's platform uses multiple consoles for configuration, though these consoles are integrated by SSO. The console is not a leading example of UX in this market, and some capabilities/functions (such as DLP on ZTNA being part of ZIA, not ZPA) can be convoluted to configure.

- Zscaler has been slow to release several common features of a leading SSE platform. A number of features for Zscaler were introduced in the middle of the evaluation cycle in late 2022. Gartner has limited client feedback on their user and device risk scoring, advanced AI/ML data scoring, endpoint DLP and automation, and these were not considered in this evaluation.

- Zscaler lacks some advanced features expected in this market, such as consistent ZTNA and CASB posture checks. While Zscaler's agent polls periodically for posture check, it cannot force a change during an existing session (which Gartner identifies as a key zero trust capability).

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

Cloudflare was added this year after acquiring Vectrix for API CASB.

Dropped

Versa was dropped because it did not meet the MMI requirement as it did not rank in the top 20 organizations in the MMI criteria this year.

Inclusion and Exclusion Criteria

Vendors of SSE offerings (as defined in the Market Definition/Description section) were considered for inclusion in this Magic Quadrant under the following conditions:

- The provider’s SSE offering must be owned and operated as a primarily cloud-delivered service to ensure a better end-user experience when securing authorized users on allowed endpoints to appropriate services running in public or private clouds.
- The core SSE offering includes the following minimum capabilities:
  - Secure access to the internet via proxy
    - Provide URL filtering and a range of advanced threat defense (ATD) methods to protect organizations and enforce internet use and compliance with acceptable use policies.
  - Secure usage of cloud services in-line and via API
    - Provide critical and consolidated controls for the secure use of cloud services including visibility, compliance enforcement, data security and threat protection. These protections can span SaaS, IaaS and PaaS.
    - API integration for CASB functions must include at least three major enterprise suites, such as O365, G Suite, Salesforce, Workday, GitHub, Atlassian and ServiceNow. API integrations with social media or free SaaS platforms (such as Twitter, Reddit, YouTube and Facebook) are not included in this count.
  - Provide secure remote access to private applications
    - Create an identity- and context-based logical boundary that encompasses an enterprise user and an internally hosted application or set of applications.
    - Hide applications from discovery and restrict access via a trust broker that verifies identity, context and policy adherence of the participants before allowing access.
    - Minimize options for lateral movement elsewhere in the network.
- Each of these core capabilities must support securing authorized users on allowed endpoints to appropriate services. These capabilities must have been generally available by 30 August 2022.

- The offering is wholly independent of deploying with a physical SD-WAN, device or other edge networking component, but can be connected to existing edge devices, endpoints, or by optional partnerships with networking or network firewall providers.
- SSE vendors demonstrate scale relevant to enterprise-class organizations. At least two of the three criteria below must be met:
  - They generated $40 million in revenue from SSE offerings during CY2021.
  - At least 500 paid enterprise customers use SSE under support as of 1 September 2022.
  - At least four million seats for SSE under paid support as of 1 September 2022.
- SSE Vendors must show relevance to global organizations by:
  - Demonstrating their SSE service offers a minimum of 20 PoPs globally with at least two PoPs in each major global region (North America, EMEA and APAC).
  - Gartner receiving strong evidence that 10% or more of its customer base is outside its home region (North America, EMEA or APAC).
- Rank among the top 20 organizations in the market momentum index defined by Gartner for this Magic Quadrant. Data inputs used to calculate SSE market momentum 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

SSE vendors not included in this Magic Quadrant were excluded for one or more of the following reasons:

- The vendor’s SSE functionality was not primarily delivered as a cloud service.
- The vendor’s SSE functionality is primarily delivered with an SD-WAN platform as part of a single-vendor SASE offering.
- The vendor is primarily a managed services provider, and SSE offerings mostly come as part of broader MSP provider contracts, or is a service provider leveraging third-party SSE services.

- The vendor did not natively offer one of the core capabilities of cloud-based SSE service (SWG, CASB or ZTNA) prior to 30 August 2022. (Vendors cannot rely on OEM partnerships for SWG, CASB or ZTNA core capabilities.)

Honorable Mentions

- **Akamai:** This vendor provides a proxy-based SWG solution (Secure Internet Access Enterprise), which includes some CASB in-line DLP and application control capabilities, as well as ZTNA (Enterprise Application Access). We excluded Akamai from this Magic Quadrant because it did not offer API integrations as part of its CASB as of 1 September 2022.

- **Cato Networks:** This vendor provides its SSE 360 platform including FWaaS, in-line web and SaaS security controls, and ZTNA functions. We excluded Cato from this Magic Quadrant because Cato SSE 360 is primarily delivered with an SD-WAN platform as part of a single-vendor SASE offering and only supported monitoring of SaaS applications via API CASB as of 1 September 2022.

- **Fortinet:** Fortinet provides a cloud-delivered SWG, CASB and ZTNA via ForitSASE and a universal ZTNA offering based on its next-generation firewall (NGFW) acting as an in-line proxy. Fortinet has a large globally diverse client base. We excluded Fortinet because as of 1 September 2022, it did not meet Gartner's required minimum points of presence globally for direct customers of FortiSASE.

- **Microsoft:** This vendor provides a multimode CASB (Microsoft Defender for Cloud Apps) with inspection in-line and at rest via API integrations, and some ZTNA (Azure AD Application Proxy). It has a large client base. We excluded Microsoft from this Magic Quadrant because it did not provide a generally available proxy-based SWG as of 1 September 2022.

- **Trend Micro:** This vendor provides an SWG, CASB and ZTNA called Zero Trust Secure Access as part of its Vision One platform. We excluded Trend Micro because it did not demonstrate its SSE offering met the scale and coverage relevant to enterprise-class organizations as of 1 September 2022.

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, etc., whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Subcriteria:

- Evaluation of core and additional capabilities for securing web, cloud services and private applications.

- Core capabilities evaluated include:

    - Cloud-delivered service
    - Forward proxy
    - Advanced threat defense
    - Data security controls
    - In-line SaaS security controls
    - API-based SaaS security controls
    - ZTNA
- Additional capabilities evaluated included, but were not limited to:
    - SD-WAN integration
    - FWaaS
    - RBI
    - Advanced analytics
    - UEBA
    - Adaptive access controls
    - CSPM
    - DEM

Overall Viability: This includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and 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. This includes 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: 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 a wide range of use cases across SSE functionality.
- Enabling 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 the product/brand and 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 and services/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), 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.

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

Subcriteria:

- Effective support and organization to address geographic presence.
- Strong leadership with clear articulation of vision and direction.
- Effective partnerships between sales, engineering, and marketing to align results and direction and minimize customer confusion and complications.

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	Low

Source: Gartner (April 2023)

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 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 that extend the scope and depth of a vendor's 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, SD-WAN) owned or provided by partnerships.

Vertical/Industry Strategy: The strategy to direct resources (sales, product, development), skills and products to meet the specific needs of individual market segments, including verticals.

Subcriteria:

- Displays an offering that aligns with key managed security providers and vendors.
- Shows an ability to target and effectively support and sell to key SSE targets and horizontal segments.
- Displays success and strength in tackling key verticals for the SSE market as identified by Gartner.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, 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 consumers to purchase the service consistently regardless of customer location.

Table 2: Completeness of Vision Evaluation Criteria

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

Source: Gartner (April 2023)

Quadrant Descriptions

Leaders

Leaders are vendors of strong momentum (in terms of sales and mind share growth). They have track records for 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 are established vendors that offer SSE components that may not be tightly integrated or lack sophisticated features. Challengers may be lacking advanced features or have gaps in their product offerings. Buyers of Challengers' products and services are typically motivated by strategic relationships with these vendors.

Visionaries

Visionaries are distinguished by technical and/or product innovation, but lack either the track record of execution and high visibility of Leaders or the corporate resources of Challengers. Buyers should expect advanced, integrated SSE offerings from Visionaries, but be wary of strategic reliance on these vendors and monitor their viability closely. Often, Visionaries 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 they lack the sophistication, advanced capabilities or integration of Visionaries' offerings. Additionally, Niche Players lack either the market presence or resources of Challengers. Niche Players may have a strong presence in a specific region or target organizations of a specific size. They deserve attention from the types of buyers on which they focus.

Context

In 2019, Gartner defined secure access service edge as an emerging architecture that combined comprehensive network as a service (most notably, SD-WAN) capabilities with comprehensive network security functions (including the protection of the web, cloud services and private applications) to support the dynamic secure-access needs of diverse organizations ranging from small and midsize businesses (SMBs) to large enterprises.

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 that application is hosted. In today's market, a set of security-focused vendors offers 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. While some vendors offer a single vendor SASE product (see our Market Guide for Single Vendor SASE), Gartner's 2022 CISO Security Vendor Consolidation XDR & SASE Trends Survey shows that a majority of buyers are planning for a two-vendor strategy for SASE

SSE customers are primarily looking to secure remote or hybrid workers who are accessing the public internet, cloud services and private applications. SSE customers may also be looking to secure remote users when the organization is virtual, is a heavy cloud consumer, or has no complex networking requirements for satellite locations.

Market Overview

Vendor innovation slowed in the SSE market in 2022 as vendors focused on improvement in their core capabilities. Vendors continue to advance their functionality and integrate their capabilities into fewer distinct products. In addition, more vendors in adjacent markets are adding in-line security features for web, SaaS and private applications to compete against full SSE vendors for opportunities where full SSE functionality is not a requirement.

Vendors differ in terms of the architecture of their SSE offerings. Overall, most vendors have now integrated their discrete components into a unified SSE platform; be wary of those still offering distinct capabilities even if tied to an SSE offering. SSE can be delivered from a hyperscaler-based, private-cloud-based or hybrid model, and different vendors continue to espouse these separate architectural approaches.

Across all the vendors, there are varying levels of maturity in terms of components, such as in the depth and breadth of cloud service security and data security capabilities, cloud infrastructures, and anti-malware defenses. Vendors are improving their DEM capabilities to provide further depth and analysis for web, SaaS and private application performance to help customers quantifiably answer end users who ask: “Why is everything I try to access so slow?” ZTNA also shows marked separation, with strong vendors having well-balanced agent- and agentless-focused capabilities, and others offering only one or the other.

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

- **The human-centric workforce:** Human-centric design is defined as “a model for work that recognizes human beings are at the center of work, not secondary components of the work environment.“ [1] Human-centric work designs drive far superior employee performance, higher intent to stay and lower fatigue than any other models tested. [2] As organizations adopt a hybrid workforce, they are moving to a human-centric design and must align cybersecurity models as well. SSE supports building security around the user rather than the location and applies unified security policies for workers regardless of their location.

- **SD-WAN transformation:** Network transformations to enable direct internet access and reduce dedicated circuit costs continue at an accelerating pace. In Forecast: Enterprise Network Equipment by Market Segment, Worldwide, 2021-2027, 1Q23 Update, Gartner estimates that the SD-WAN equipment market amounted to $4.1 billion in 2022 and that it will grow at a compound annual rate of 15.5% over the period 2021 through 2027. Clients report that fully implemented SSE service subscription costs may exceed the savings from reducing Multiprotocol Label Switching (MPLS) backhaul costs. Therefore, the move to SSE is not driven by ROI but by better end-user experiences in terms of lower latency, consistent security experiences, and increased flexibility to secure the hybrid workforce and branch locations through a unified, cloud-hosted security stack.

- **Cloud adoption:** Adoption and growth rates for SaaS, PaaS and IaaS continue to climb. In Forecast Analysis: Public Cloud Services, Worldwide, 3Q21 Update, Gartner estimates that SaaS is the largest cloud revenue generator and that it will grow at a compound annual rate of around 20% through 2025, while the PaaS and IaaS sectors are smaller but growing much faster. Rapid cloud adoption creates a need to simplify and consolidate security delivered from the cloud for the cloud, rather than try to force traffic through on-premises networks and data centers to secure access.

- **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 the 2022 Strategic Roadmap for SASE Convergence, Gartner recommends having representatives from networking, workforce transformation, branch office transformation and security work as a joint team to develop a long-term strategic roadmap for SASE. 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.

Acronym Key and Glossary Terms

Hybrid workforce model	A hybrid workforce model is one in which a significant part of the workforce flows through various work sites as "flexible workers." These sites range from remote solo locations to remote microsites of small populations and traditional concentrated facilities (such as offices, factories and retail premises).

Evidence

[1] Future of Work Reinvented: Human-Centric Work Design

[2] Human-Centric Work Models Proven to Drive Performance the Most

Other sources used as part of the fact base: Throughout the course of a year, Gartner receives many inquiries about 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. Most of the Peer Insights reviews relevant to this Magic Quadrant were for subcategories of SSE, primarily CASB and SWG.

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.