Gartner. Licensed for Distribution

Magic Quadrant for Security Service Edge

Updated 30 March 2022, Published 15 February 2022 - ID G00757036 - 46 min read

UPDATED This Magic Quadrant now includes links to relevant Corporate Transaction Notification research.

By John Watts, Craig Lawson, **and 2 more**

The emergence of a market for security service edge solutions reflects the need for organizations with hybrid workforces to apply consistent security from the cloud. This Magic Quadrant will help you identify suitable vendors to secure access to the web, cloud services and private applications.

Strategic Planning Assumptions

By 2025, 70% of organizations that implement agent-based zero trust network access (ZTNA) will choose a security service edge (SSE) provider for ZTNA, rather than a stand-alone offering, up from 20% in 2021.

By 2025, 80% of organizations seeking to procure SSE-related security services will purchase a consolidated SSE solution, rather than stand-alone cloud access security broker, secure web gateway and ZTNA offerings, up from 15% in 2021.

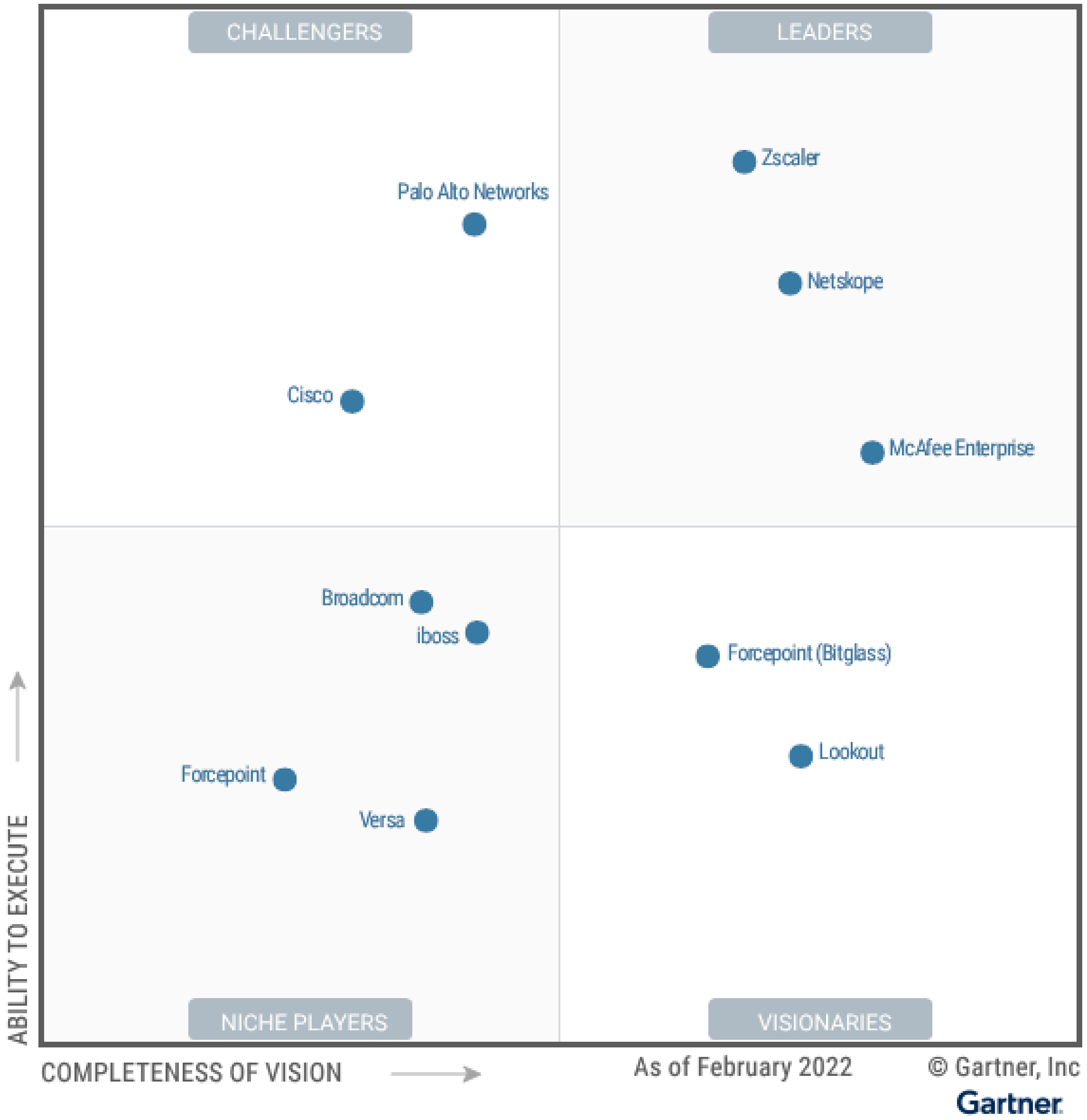
By 2026, 50% of organizations will prioritize advanced data security features for inspection of data at rest and in motion as a selection criterion for SSE, up from 15% in 2021.

Market Definition/Description

Security service edge (SSE) secures access to the web, cloud services and private applications. Capabilities include access control, threat protection, data security, security monitoring, and acceptable-use control enforced by network-based and API-based integration. SSE is primarily delivered as a cloud-based service, and may include on-premises or agent-based components.

Magic Quadrant

Figure 1: Magic Quadrant for Security Service Edge



Source: Gartner (February 2022)

Vendor Strengths and Cautions

Broadcom

Broadcom is a Niche Player in this Magic Quadrant. Broadcom's SSE offering comprises Symantec Web Security Service, CloudSOC (a cloud access security broker [CASB]) and Symantec Secure Access Cloud (for zero trust network access [ZTNA]). Headquartered in San Jose, California, U.S., Broadcom is a large company with operations globally. Its customers tend to be large and very large enterprises, and they come from many industries. Broadcom still has a strong presence in the market with its appliance-based secure web gateway (SWG) business.

Since its acquisition of Symantec in 2019, Broadcom has focused on building an enterprise software business and struggled to retain some key Symantec talent. In April 2021, Broadcom and Google Cloud announced further strategic collaboration partnerships. Also in 2021, Broadcom delivered its Symantec CloudSOC Mirror Gateway, which uses remote browser isolation (RBI) to secure unmanaged device access to software as a service (SaaS) and private applications.

Strengths

- Broadcom is a well-funded, financially secure public company with a portfolio of strategic high-tech semiconductor and enterprise software products. It maintains a high level of investment in its software business.
- Broadcom's offering provides a good view of end-user risk scores and the reasons why some users have a high risk rating. It traces each attribute and how it contributes to users' risk ratings. In addition, Broadcom's enterprise data loss prevention (DLP) engine has advanced data security controls, such as for optical character recognition (OCR), fingerprinting and vector machine learning, that can be extended beyond the SSE offering to other channels.
- Broadcom has simplified its pricing by selling only cloud-based SSE licenses. If a customer requires appliances on-premises, the hardware costs extra.
- Broadcom was among the first in the market to have core SWG, CASB and ZTNA components. Its strategy now focuses on tightly integrating these components to improve its unified SSE service.

Cautions

- Broadcom is often mentioned by Gartner clients as a target for replacement. Feedback also indicates that its cloud-based SSE offering appears on fewer shortlists than those of other competitors in this market.
- Broadcom's sales strategy focuses on the largest companies worldwide, to which it sells a large portfolio of products and services under a comprehensive Portfolio License Agreement. This focus limits its appeal to companies that fall outside this category. Feedback from Gartner clients is that both prospective and current customers outside this category find it difficult to purchase or receive support from Broadcom.
- Broadcom's SSE offering is not well integrated. Customers who want to utilize the full SSE offering must deploy multiple agents and manage it through different consoles, including, at minimum, SWG, CASB, ZTNA, DLP and reporting consoles. The lack of integration also results in confusing product features — for example, high scores are assigned to less risky cloud apps ("more ready cloud apps" in the vendor's terminology) but also to "more risky end users."

- Feedback from Broadcom customers indicates that, despite some improvement since Broadcom's acquisition of Symantec, technical support challenges persist.

Cisco

Cisco is a Challenger in this Magic Quadrant. Cisco's primary products for SSE are part of its Cloud Security line, including Cisco Umbrella, Cloudlock and Duo Beyond. It also has a large portfolio of infrastructure, networking and security products. Cisco is headquartered in San Jose, California, U.S. Its operations are geographically diversified, and it has customers of all sizes and from all industries.

In 2021, Cisco added in-line DLP and an identity proofing service to its Umbrella Cloud Security Service and introduced RBI capability. It also introduced a cloud-based secure managed remote access service based on its AnyConnect VPN technology.

Strengths

- Cisco is financially strong and has a large employee base. It has a large market share in the SSE market, primarily for its Umbrella product line. It continues to invest significantly in its products.

- Cisco shows up frequently on Gartner clients' shortlists for SSE. It is often mentioned by users of Gartner's client inquiry service, particularly if they are looking to combine Cisco SSE technologies with Cisco software-defined wide-area network (SD-WAN) offerings.

- Cisco's customers like the affordability, ease of use and method of deployment of its entry-level SSE offerings, such as Umbrella DNS Security Essentials and Umbrella DNS Security Advantage integrated with SecureX, an extended detection and response (XDR) offering. Customers find that the AnyConnect VPN meets many remote access requirements, and it is often paired with Umbrella via a single agent.

- Cisco has integrated Umbrella with Meraki and Viptela using its SD-WAN Cloud OnRamp feature. It offers Talos threat intelligence, can ingest Structured Threat Information eXpression (STIX)/Trusted Automated Exchange of Intelligence Information (TAXII)-based threat intelligence, and use the enforcement API in its SSE offerings to create a custom threat intelligence list.

Cautions

- Cisco provides limited security options for unmanaged device access to SaaS applications outside a corporate network. It also offers only basic data security controls, applied through separate policies for in-line data and for data at rest. Cisco also lacks automated advanced analytics functionality. For example, although it is possible to configure a maximum speed of travel by a user between two locations, this cannot be done automatically.

- Cisco does not have a well-integrated, cloud-based SSE service offering. Instead, it offers SWG, firewall as a service (FWaaS) and forward-proxy CASB services through Umbrella; a loosely integrated API-based CASB as part of the Cloudlock offering; ZTNA through Duo Beyond; AnyConnect VPN services; and Stealthwatch Cloud for some cloud security posture management (CSPM) functionality.

- Customer feedback indicates that, although the basic tiers of Cisco's SSE products are inexpensive, a complete set of SSE functionality is relatively expensive. Additionally, Gartner clients have reported that it is difficult to understand what is required to gain complete SSE functionality from Cisco.

- Cisco often lags behind other vendors in this Magic Quadrant when it comes to introducing new features and functions related to SSE. For example, Cisco has yet to release an agent-based ZTNA feature, and it only recently added browser isolation.

Forcepoint

Since the initial publication of this Magic Quadrant (15 February 2022), Forcepoint was a party in the following significant corporate transaction(s). For Key Background and Considerations for Technology and Service Selection, see:

- *"Closed Corporate Transaction Notification: Forcepoint, Security Service Edge" (30 March 2022)*

Analysis within this Magic Quadrant remains as originally published.

Forcepoint is a Niche Player in this Magic Quadrant. The core of Forcepoint's SSE service comprises its Cloud Security Gateway, Cloud Access Security Broker and Private Access products. Forcepoint also provides firewalls, enterprise DLP and other security products. Forcepoint is headquartered in Austin, Texas, U.S. Its operations are geographically diversified, and its customers range from small to very large organizations across many industries.

In January 2021, Forcepoint was acquired by private equity firm Francisco Partners from Raytheon Technologies. In May 2021, Forcepoint purchased Cyberinc, an RBI vendor, and integrated its Isla platform into its SSE offering. In August 2021, Forcepoint acquired Deep Secure for its Content, Disarm & Reconstruction (CDR) technology. It also released a new agent, the Neo endpoint agent, which further enhances its enterprise DLP functionality. In October 2021, Forcepoint completed the acquisition of SSE vendor Bitglass, which is evaluated separately in this Magic Quadrant. As with any acquisition, it will take time to see how the effects of this acquisition play out.

Strengths

- Forcepoint's SSE offering provides a dashboard view of risky users. Customers can build custom policies for assessing risks and taking actions, with a flexible policy builder ingesting inputs from multiple telemetry sources.

- Since acquiring Forcepoint, Francisco Partners has invested in the business. Gartner estimates that Forcepoint has healthy revenue and a healthy customer base.

- Forcepoint continues to invest in innovation for its SSE offering. The recently released Neo agent provides the ability to implement "intelligent auto-switching." This feature automatically optimizes functionality for the endpoint between direct connect (policy defined in the cloud and enforced on the endpoint) and proxy connect (policy defined and enforced in the cloud) modes.

- Forcepoint's SSE package includes features such as integrated cloud DLP and native RBI capabilities. Forcepoint does not charge separately for these.

Cautions

- Gartner clients primarily consider Forcepoint when they value a mix of on-premises appliances and cloud security or want to utilize Forcepoint's enterprise DLP. Forcepoint's legacy appliances are often targets for replacement. In addition, client feedback indicates that Forcepoint appears less frequently on shortlists for SSE than many of its competitors.

- Forcepoint's SSE offering lacks strong integration between components at the management and reporting layers. As a result, multiple consoles are required to access different aspects of the service. In addition, Forcepoint lacks mobile agents for iOS and Android.

- Clients indicate challenges with troubleshooting Forcepoint's Forcepoint One Endpoint (F1E) endpoint agents. Their comments also point to a decline in overall support quality and responsiveness over the past year.

- Forcepoint's strategy to build a ZTNA feature that supports only web application access has resulted in low ZTNA adoption across its customer base.

Forcepoint (Bitglass)

Since the initial publication of this Magic Quadrant (15 February 2022), Forcepoint (Bitglass) was a party in the following significant corporate transaction(s). For Key Background and Considerations for Technology and Service Selection, see:

- *"Closed Corporate Transaction Notification: Forcepoint (Bitglass), Security Service Edge" (30 March 2022)*

Analysis within this Magic Quadrant remains as originally published.

Forcepoint (Bitglass) is a Visionary in this Magic Quadrant. Its primary SSE offerings are Secure Web Gateway, Cloud Access Security Broker, and Zero Trust Network Access. It is headquartered in Campbell, California, U.S. Its operations are mostly in North America and Europe, but it also has a smaller presence in Asia/Pacific and South America. Its customers tend to be large enterprises from many industries.

In August 2021, Forcepoint (Bitglass) announced cloud-managed SmartEdge Secure Web Gateway (SWG) virtual appliances for branch offices, which provide SWG services to all devices at a branch. It also achieved ISO/IEC 27001:2013 certification for the data security management system that supports its CASB system, and received a FedRAMP Moderate Agency Authority to Operate (ATO) for its Total Cloud Security Platform.

Bitglass was acquired by Forcepoint in October 2021. Forcepoint has another SSE solution, for which it is assessed separately in this Magic Quadrant. As with any acquisition, it will take time to see how the effects of the Forcepoint acquisition play out.

Strengths

- Forcepoint (Bitglass) offers a strong set of data security controls. These are customizable using the company's proprietary Field Programmable SASE Logic (FPSL) feature, and integrated across SWG, CASB and ZTNA functions. In addition, the company's AJAX-VM technology can enable agentless access, including via "bring your own device" (BYOD), to cloud services.

- Forcepoint (Bitglass) has received positive feedback from customers about its support responsiveness, powerful features for data security and Field Programmable SASE Logic (FPSL) feature for power users.

- Forcepoint (Bitglass) has a good presence globally and offers over 300 cloud points of presence (POPs) built on Amazon Web Services (AWS), including local edge data centers in typically underserved regions such as China and Africa. As it uses its SmartEdge agent to perform decryption and inspection of content, it is less dependent on processing in the cloud. This approach improves overall latency on devices in remote locations where this agent can be installed.

- Forcepoint (Bitglass) is expanding its unique FPSL feature to other parts of its SSE offerings. The company also has a strong investment roadmap to improve the existing features of these offerings.

Cautions

- Although Forcepoint (Bitglass) has released a new virtual machine to connect branches to its SWG, customer feedback about its focus on the SmartEdge agent indicates that it is challenging to connect endpoints where an agent cannot be installed. In addition, Forcepoint (Bitglass) does not support UDP applications for ZTNA.

- Gartner's research indicates that Forcepoint (Bitglass) does not have the same levels of market share and client visibility as leading SSE vendors, and it appears less frequently on competitive shortlists seen by Gartner and in client inquiries.

- According to Gartner's estimates of revenue, Forcepoint (Bitglass) is one of the smallest companies in this market. It has received less funding than other private companies in this market.

- Responses by Forcepoint (Bitglass) to the market have slowed in the past year. For example, it has focused its efforts on expanding its cloud POPs and extending its FPSL feature to additional modules within its existing platform, rather than adding new functionality such as FWaaS.

iboss

Iboss is a Niche Player in this Magic Quadrant. Its core SSE offering is the Secure Access Service Edge (SASE) cloud platform. Headquartered in Boston, Massachusetts, U.S., iboss is a privately held company with global operations and customers concentrated in North America and Europe. It has a smaller presence in Asia/Pacific. Its customers come from many industries.

In 2021, iboss hired a number of new executive leaders from other vendors in the SSE market to bolster its marketing and sales channels and product. In January 2021, iboss received a fresh round of $145 million of Series B funding led by NightDragon and Francisco Partners. In August 2021, iboss released a new RBI capability and eliminated its dependency on Microsoft Cloud App Security (MCAS) for advanced CASB functionality in order to launch its first integrated SSE offering.

Strengths

- All iboss customers receive ZTNA licenses — no separate license is required. This increases the overall value of the platform. Client and customer feedback indicates that iboss' pricing in this market is competitive.

- Feedback from iboss customers about its technical support capabilities and response times is positive, and customers like the functionality of its endpoint agent, which can be extended to Linux and Chromebooks. The vendor offers an SLA for seven nines of availability in the SSE market, which also includes a 100-millisecond (ms) latency guarantee.

- The cloud security platform’s new RBI function and data security capabilities are well integrated and applied across web, cloud services and private applications.

- Iboss continues to build SSE features into its core cloud security platform, with a more tightly integrated offering that leverages the underlying proprietary containerized architecture. Customers can deploy enforcement nodes in their own data centers or utilize the iboss cloud service offering.

Cautions

- This vendor’s SSE offering integrates with few SaaS applications via API. Additionally, its cloud app risk scoring is opaque and not customizable by clients, and there is very limited agent posture checking for ZTNA.

- Feedback from Gartner clients indicates that iboss appears less frequently than some other vendors on competitive shortlists — and has less visibility in this market — when API-based CASB and DLP functionality are key drivers.

- Gartner has observed iboss adding some SSE features after their introduction by other vendors. For example, in August 2021, it delivered native RBI and CASB API integrations, which other vendors had built or introduced before 2021.

- Iboss has fewer strategic Tier 1 sales partners and managed security service provider (MSSP) partners to sell its solution than is the case with other vendors in this market. Furthermore, as the market evolves, some of its existing partnerships and technology alliances may be at risk, such as its partnership with FireEye (now part of McAfee Enterprise, which is also evaluated in this Magic Quadrant).

Lookout

Lookout is a Visionary in this Magic Quadrant. Lookout’s SSE offering includes CASB, SWG and ZTNA services. Lookout also offers mobile endpoint security products. Lookout has headquarters in San Francisco, California, U.S. Its operations are concentrated in North America and EMEA, but it also has a smaller presence in Asia/Pacific. It serves primarily midsize and large enterprises across many industries.

In March 2021, Lookout acquired CipherCloud to expand its Mobile Endpoint Security product offerings into the SSE market. In May 2021, Lookout integrated CipherCloud’s SSE technology into its product and rebranded it as Lookout’s first generally available integrated SSE offering.

Strengths

- Lookout has strong data security capabilities in the SSE market, including advanced features like watermarking, encryption, tokenization and the ability to automatically apply data classification labels to content. Lookout has integrated policies and data security enforcements deeply across web, SaaS and private applications. These include policies on managed desktops enforced through its unified agent.

- Lookout has a strong sales strategy for a relatively small vendor. It benefits from good reseller channels, as a result of relationships with Tier 1 ISPs, MSSPs and telcos worldwide.

- Over the past year, Lookout has added relevant SSE components from CipherCloud to its mobile threat defense offerings. This move aligns with the needs of its existing customers.

- Lookout's acquisition of CipherCloud demonstrates a commitment to invest in SSE technology. Lookout is one of the better funded, but smaller, private companies in the SSE market, having received an estimated total of $282.3 million over nine funding rounds.

Cautions

- Lookout's SSE offering appears not to have as much market share and visibility as those of most other SSE vendors. It appears less frequently on competitive shortlists seen by Gartner and is mentioned less often by users of Gartner's client inquiry service.

- Lookout has few SD-WAN partnerships, and focuses on threat defense for mobile operating systems rather than nonmobile devices. Prospective customers that need to connect branch office locations should examine Lookout's SD-WAN partnerships and test branch connectivity carefully.

- Lookout lacks an FWaaS offering and did not introduce RBI until August 2021 (via an OEM partnership). Compared with other vendors, RBI is not as deeply integrated into its SSE offering. For example, isolating access is not an action you can choose on a policy — you must create separate policies specifically for isolation.

- Gartner's research indicates that Lookout has fewer customers than many vendors in this market, and is weaker in terms of large customers globally. Large, worldwide organizations should request customer references and check Lookout's ability to support them globally.

McAfee Enterprise

On 22 March 2022, McAfee Enterprise's SSE business was rebranded as Skyhigh Security.

McAfee Enterprise is a Leader in this Magic Quadrant. Its SSE offering is the MVISION Unified Cloud Edge (UCE) service. It also offers other security products, such as XDR and endpoint security offerings. Headquartered in San Jose, California, U.S., McAfee Enterprise has a wide geographic presence. Its customers range in size from small to very large, and come from all industries.

In July 2021, Symphony Technology Group (STG) purchased McAfee's enterprise business and formed McAfee Enterprise as a private company. In October 2021, STG completed the acquisition of FireEye and merged the two acquisitions into a single company. In January 2022, STG launched a new business unit, Trellix, for its XDR products, which are separate from its McAfee Enterprise SSE portfolio.

Strengths

- McAfee Enterprise offers a complete and tightly integrated suite of SSE services, which includes integrated RBI and advanced data security capabilities across SWG, CASB and ZTNA offerings. It also offers CSPM and SaaS security posture management (SSPM) functions, digital experience monitoring (DEM), and native integration with its enterprise DLP technology through a common endpoint agent.
- McAfee Enterprise has one of the simplest and most competitive pricing models in the market. Packages are provided in three tiers, based on features included, such as private access and FWaaS. All bundles include RBI for risky websites at no additional cost.
- McAfee Enterprise has acquired and integrated RBI technology in several unique ways to improve the efficacy of its SSE service. It has, for example, made it part of the forward proxy by default.
- McAfee Enterprise has a strong presence globally, offers differentiated pricing by geography, and is gaining momentum in relatively small but fast-growing markets for SSE offerings, such as those of the Middle East and Latin America.

Cautions

- McAfee's multiple ownership changes and legacy brand name impact the perception of McAfee Enterprise, especially when compared with the market's newer, cloud-native security vendors.
- McAfee Enterprise developed and released ZTNA and FWaaS capabilities for its SSE offering later than other vendors in this market. These are fully featured capabilities, but they are new and, so far, the subject of limited feedback from customers.
- McAfee Enterprise lacks tight integration with its certified SD-WAN providers, offering only basic integration and setup.
- McAfee Enterprise has a large installed base, but we estimate that its growth in SSE seats and new customers is slower than that of other Leaders in this market.

Netskope

Netskope is a Leader in this Magic Quadrant. Its primary SSE offerings, available as part of the Netskope Security Cloud 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 2021, Netskope received a fresh round of $300 million in funding led by ICONIQ Growth. Also in 2021, Netskope announced that it had acquired Randed (for RBI) and integrated it into its SSE offerings, and released a new in-house-built FWaaS offering as part of its platform. Netskope also acquired Kloudless in order to offer SSPM functionality in addition to Netskope's CSPM capabilities.

Strengths

- Feedback from Gartner clients indicates that Netskope appears frequently on SSE shortlists. This is partly because Netskope positions its SSE as a modular cloud-native platform hosted on its in-house-built NewEdge cloud infrastructure.
- Netskope offers advanced data security capabilities. For example, in addition to OCR for parsing text within an image, Netskope offers machine learning to identify image types and text based on trained classifiers.
- Netskope's total private funding of an estimated $1 billion makes it one of the best-funded private companies in the SSE market.
- Netskope offers a strong SLA for uptime and latency. Its SLA offers a standard five nines of availability, along with guarantees of less than 10 ms of latency for unencrypted web traffic and 50 ms for encrypted traffic.

Cautions

- Netskope released the first phase of DEM to select tenants in August 2021 and, unlike some competitors, Netskope's cloud firewall does not support Layer 7 firewall controls outside of HTTP and HTTPS applications. In addition, Netskope provides only basic VPN tunnel configurations in conjunction with its SD-WAN partners.
- Netskope introduced its agent-based ZTNA service, NPA, in early 2020, and added a clientless option in 2021. But we believe, based on Gartner market share estimates and other sources of information, that NPA is not selling as well to Netskope's client base as its Next Gen Secure Web Gateway and CASB.

- Netskope's cautious approach to releasing new features for its platform results in it being left off some shortlists. It often relies on lengthy beta tests before releasing features. The process by which it released native RBI and FWaaS offerings exemplifies Netskope's cautious approach.
- Netskope offers enterprise agreements and combined SSE SKUs, but otherwise has a relatively complicated set of SKUs. Additionally, client feedback indicates that Netskope is less competitive on pricing than other vendors.

Palo Alto Networks

Palo Alto Networks is a Challenger in this Magic Quadrant. Its SSE offering is primarily composed of Prisma Access and SaaS Security services. 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.

In February 2021, Palo Alto Networks announced Prisma Access 2.0, which includes updated cloud management capabilities, DEM, an explicit proxy for its SWG, and CloudBlades to support API integration with third-party technologies such as RBI. It also announced a single SASE SKU for SD-WAN and SSE bundles, and improved on the SWG workflows from its cloud management console.

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 successfully positions Prisma Access as a viable alternative to other SSE offerings, with hybrid (on-premises and cloud) benefits for customers. As a result, Palo Alto Networks appears more frequently than many other vendors on client shortlists seen by Gartner.
- Palo Alto Networks is a very large security portfolio vendor that has responded positively to market demands by supporting the proxying of traffic to Prisma Access. This has eliminated the need to deploy the vendor's GlobalProtect agent to all remote endpoints.
- Palo Alto Networks remains in-line of traffic between endpoints and applications for ZTNA, and applies its object-based rules to segment users and applications. As a result, Prisma Access can apply the same consistent ZTNA access rules for users off- and on-premises.

Cautions

- Palo Alto Networks' SSE offering is not well integrated. It requires multiple modules for full SSE functionality and configuration of certain components in different modules, such as those for user and entity behavior analytics (UEBA) and data security. Also, rather than use OEM technology for RBI, it depends on partners, and it relies on its CloudBlades architecture for integration.

- Gartner clients indicate that Prisma Access is relatively complicated to set up and manage. For example, it requires configurations of network routes over VPN tunnels called “service connections” to connect to private applications and relies on separate modules for CASB API integrations and UEBA functionality.

- Palo Alto Networks’ SSE product strategy builds on acquired functionality and the use of firewall rules. For example, its ZTNA functionality draws on the GlobalProtect agent and uses object-based firewall rules for user-to-application segmentation. Client feedback indicates that this approach appeals primarily to Palo Alto Networks’ existing customer base and that it has limited appeal elsewhere.

- Client feedback indicates that it is expensive and confusing to achieve full SSE functionality with Palo Alto Networks. For example, customers must license multiple modules and then choose the Prisma Access security features they need for global or regional deployments to secure users, branches or both.

Versa

Versa is a Niche Player in this Magic Quadrant. Its SSE offering is Versa SASE. It also offers WAN edge infrastructure products. Headquartered in San Jose, California, U.S., Versa operates globally. Its customers range from midsize to very large organizations across many industries.

Versa received $84 million in series D funding in June 2021. Versa released its SSE functionality on the Versa Operating System (VOS) in the fourth quarter of 2020, enabling its Versa SASE security services to be part of an overall SASE framework.

Strengths

- Versa has a strong set of data security controls that can be applied both in-line and for data at rest in SaaS applications. These controls include support for fingerprinting, encryption, watermarking, redaction and other advanced actions.

- Versa built its SSE on its VOS, which enables it to build a tightly integrated set of SSE features that can be used as part of its cloud service or within its range of hardware offerings.

- Client feedback indicates that Versa is known mostly for networking, but Versa has also invested in, developed and released an integrated set of SSE services with the help of its in-house R&D team.

- Versa has responded positively to market demands. It has got ahead of many other SD-WAN-focused vendors by seizing the opportunity to add cloud-native security to its strong networking stack.

Cautions

- Versa SASE's UI is complicated when it comes to building security policies and undertaking troubleshooting. In addition, Versa's SSE SaaS support is limited. For example, it does not support the importation of proxy logs to provide "shadow IT" SaaS reporting. Also, Versa supports unmanaged device access to a limited number of SaaS applications outside a corporate network.
- Feedback from Gartner clients indicates that Versa has limited market visibility and market share as a security vendor, and that its marketing lags behind the availability of features. For example, Versa released API integration with SaaS vendors in mid-2021, but its website had no mention of this as of August 2021.
- Client feedback indicates that Versa SASE appeals primarily to existing Versa SD-WAN customers. It appears on client shortlists for SSE functionality less frequently.
- Versa customers have indicated that the vendor releases new features with bugs and a steep learning curve, due to poor documentation. Additionally, feedback from Versa customers indicates that presales and postsales support, including professional services, is not strong — customers have to be technically savvy to test, implement and operate the product.

Zscaler

Zscaler is a Leader in this Magic Quadrant. Its primary SSE offering includes Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA) and Zscaler Digital Experience (ZDX) services. It also offers CSPM and Zscaler Cloud Protection, which includes identity-based segmentation of workloads. 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 mid-2021, Zscaler acquired Trustdome (a cloud infrastructure entitlement management [CIEM] vendor) and Smokescreen (a vendor of deception technology). In the past year, Zscaler has improved its CASB offering by introducing API integrations with more SaaS applications, improving its data security features and integrating RBI.

Strengths

- Zscaler invests in a very large sales organization, and has grown its revenue and number of new customers quickly, relative to the 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. Gartner estimates that it has a large share of the market for cloud-based SWGs and ZTNA.

- Zscaler has a solid track record of innovation and continues to invest before its competitors in efforts to provide interesting innovations in the SSE market. For example, it was the first to introduce DEM, which enables it to collect and analyze end-user experiences wherever its agent is installed.

- Zscaler offers a single agent for steering traffic to the Zscaler cloud for security, along with strong SWG capabilities and an easy-to-use ZTNA product. It also offers an integrated management console for managing and reporting across SSE features. In addition, it has stronger SD-WAN partnerships (with tighter integrations) than other vendors.

Cautions

- Zscaler's clients frequently identify its pricing as their top complaint, particularly at renewal time. For example, those renewing from Zscaler's Bundle SKU line items find prices have increased with the newer Zscaler Edition SKU pricing.

- Zscaler lags behind other vendors in terms of advanced data security capabilities and cloud security capabilities. For DLP, for example, it does not use advanced artificial intelligence such as trained image classifiers to detect sensitive data, nor does it enable DLP directly in ZPA. For cloud security, Zscaler's cloud discovery database tracks fewer attributes for cloud risk than is the case with some vendors in this market.

- Some of Zscaler's recent acquisitions, such as Smokescreen and Edgewise Networks (acquired for its cloud workload protection platform), have technologies adjacent to its core SSE technology. This may distract Zscaler from the need to advance its core SSE features and to increase what Gartner estimates to be relatively few customers using its advanced CASB functionality, compared with other SSE vendors.

- Client feedback indicates that Zscaler's dashboarding and reporting features can suffer from performance issues and have limitations when it comes to large datasets and advanced reporting requirements. As a result, clients rely on Zscaler's Nanolog Streaming Service to send logs to a security information and event management (SIEM) product for more advanced analysis.

Inclusion and Exclusion Criteria

Vendors of SSE offerings corresponding to the contents of the Market Definition/Description section were considered for inclusion in this Magic Quadrant under the following conditions:

- The offering was operated as a service and delivered as a cloud service to deliver better end-user experiences when securing any user on any device to any service running in public or private clouds.
- The core SSE offering included the ability to secure web access via proxy (SWG functionality), secure SaaS access via API and proxy modes (CASB functionality), and provide secure remote access to private applications (ZTNA functionality). Each of these core capabilities must support the securing of any user from any device or location. Native SWG, CASB and ZTNA functions had to be generally available by 30 August 2021.
- The offering provided controls for a minimum of 10 SaaS applications in in-line modes and integration with a minimum of two distinct enterprise SaaS suites (from, for example, Microsoft [Microsoft 365], Google [Google Workspace] or Salesforce) via API for security functions such as data inspection at rest and monitoring of user behavior.
- The offering did not have to be deployed with a physical SD-WAN device or other edge networking component, but could be connected to existing edge devices, endpoints, or technologies from optional networking or network firewall provider partners.
- The vendor demonstrated global presence, and features and scale relevant to enterprise-class organizations, on the basis that:
  - It generated $40 million in total SSE service revenue during 2020.
  - It had at least 500 enterprise customers using its SSE offering under support as of 1 September 2021.
  - It had at least 4 million seats for its SSE offering under paid support.
  - Its service offered a minimum of 20 points of presence (POPs) globally, with at least two POPs in each major global region (North America, EMEA and Asia/Pacific).
  - Gartner received strong evidence that 10% or more of its customers were outside its home region (North America, EMEA or Asia/Pacific).

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 delivered as a stand-alone cloud offering.

- The vendor is primarily a managed services provider and its SSE offering(s) mostly come as part of broader managed service provider contracts, or is a service provider using third-party SSE services.
- The vendor did not natively offer one of the core components of a cloud-based SSE service (SWG, CASB or ZTNA) prior to 30 August 2021 (vendors could not rely on OEM partnerships for SWG, CASB or ZTNA services).

Honorable Mentions

- **Akamai:** This vendor provides a proxy-based SWG solution (Enterprise Threat Protector), 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 30 August 2021.
- **Cato Networks:** This vendor provides SD-WAN, FWaaS and SWG solutions, as well as ZTNA. We excluded Cato Networks from this Magic Quadrant because it did not offer a full, generally available set of CASB controls as of 30 August 2021.
- **Cloudflare:** This vendor provides proxy-based SWG solutions, including RBI and CASB in-line DLP and application control, as well as ZTNA. We excluded Cloudflare from this Magic Quadrant because it did not offer API integrations as part of its CASB as of 30 August 2021.
- **Menlo Security:** Clients who see high value in malware prevention may consider the Menlo Security Secure Web Gateway (SWG) based on its Isolation Core product. We excluded Menlo Security from this Magic Quadrant because it did not satisfy the minimum required financial inclusion criterion as of 30 August 2021.
- **Microsoft:** This vendor provides a multimode CASB (Microsoft Defender for Cloud Apps) with inspection in-line and at rest via API integrations, and 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 30 August 2021.
- **Proofpoint:** This vendor did not qualify for inclusion as it had retired its ZTNA functionality as of 31 December 2021. Clients interested in SWG and CASB functionality may consider Proofpoint, which introduced a new cloud-based SWG offering in June 2021.

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 of a wide range of use cases across SSE functionality.
- Enabling of the SSE portion of a SASE architecture for customers and the ability to support their transformation strategies.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand and business, increase awareness of products, and establish a positive identification with 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.

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	***Weighting*** ↓
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	Low

Evaluation Criteria	***Weighting***
Market Responsiveness/Record	Medium
Marketing Execution	Medium
Customer Experience	High
Operations	NotRated

Source: Gartner (February 2022)

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 trends.
- 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.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive 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	NotRated
Innovation	Medium
Geographic Strategy	Low

Evaluation Criteria ↓	***Weighting*** ↓

Source: Gartner (February 2022)

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 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 which may not be tightly integrated or which lack sophisticated features. Challengers perform well for a significant market segment, but they may be lacking advanced features or have gaps in their product offerings. Buyers of Challengers' products and services typically focus on individual SSE components, rather than the full range of SSE requirements, or are 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 (SASE) as an emerging offering that combined comprehensive network as a service (most notably, SD-WAN) capabilities with comprehensive network security functions (such as SWG, CASB, FWaaS and ZTNA) to support the dynamic secure-access needs of digital enterprises.

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.

SSE customers are comparing vendors that offer security capabilities, and may pair these with existing edge networking components such as SD-WAN equipment, firewalls and other networking equipment (perhaps in the process of being replaced). 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.

Most large organizations have separate networking and security teams that make independent purchasing decisions or have yet to integrate their SASE planning efforts.

Market Overview

Revenue in the SSE market amounted to between $2.4 and $2.6 billion in fiscal 2020 and is growing by 19% to 21% year over year, according to Gartner's estimates. Vendors in this market have primarily improved their SWG or CASB offerings to compete more directly with vendors in the SWG and CASB sectors, but a few notable entrants have added both functions to compete for SSE opportunities.

Vendors differ in terms of the architecture of their SSE offerings. Some vendors have an integrated SSE platform. Others have loosely integrated various components into a packaged offering. Some vendors are very agent-dependent, while others provide strong agentless networking and agent-based controls.

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 increasingly adding DEM to their offerings to help customers quantifiably answer end users who ask "Why is everything I try to access so slow?"

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

- **The hybrid workforce model:** Many organizations are now remote-working organizations principally, rather than by exception. In the 2021 Gartner View From the Board of Directors Survey, remote work was identified by 50% of respondents as the No. 1 extraordinary change expected to persist as part of the new long-term norm as a response to COVID-19. Even though a return to the workplace is occurring as lockdowns ease, organizations are adopting a hybrid approach of “remote first,” as opposed to “remote by exception.” This change demands different approaches to traditional perimeter-based security in order to secure the workforce.

- **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, 2019-2025, 3Q21 Update, Gartner estimates that the SD-WAN equipment market amounts to $3.5 billion and that it will grow at a compound annual rate of 18% over the period 2021 through 2025. 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, platform as a service (PaaS) and infrastructure as a service (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, which creates two buying centers for SASE offerings. In the 2021 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

Information Protection and Cloud Security Product Updates Announcement for Q1 2022, Proofpoint, 10 January 2022.

2021 Gartner View From the Board of Directors Survey: This survey was conducted to find out how boards of directors view the evolution of the digital-business-driven business model and its impact on their enterprises. It was also conducted to help us understand boards' expectations of executive leaders and how boards' focus is translated into executive actions and overall corporate performance.

The survey was conducted online from May through June 2020 among 265 respondents from the U.S., EMEA and Asia/Pacific. Companies were screened to be midsize, large or global enterprises. Respondents were required to be board directors or members of a corporate board of directors. If respondents serve on multiple boards, they answered for the largest company, defined by its annual revenue, for which they were a board member.

The survey was developed by Gartner analysts and Gartner's Research Data, Analytics and Tools team.

Disclaimer: The results of this survey do not represent global findings or the market as a whole. They reflect the sentiments of the respondents and companies surveyed.

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.

About Careers Newsroom Policies Site Index IT Glossary Gartner Blog Network Contact Send Feedback