IDC MarketScape

IDC MarketScape: Worldwide Secure Access Service Edge (SASE) 2026 Vendor Assessment

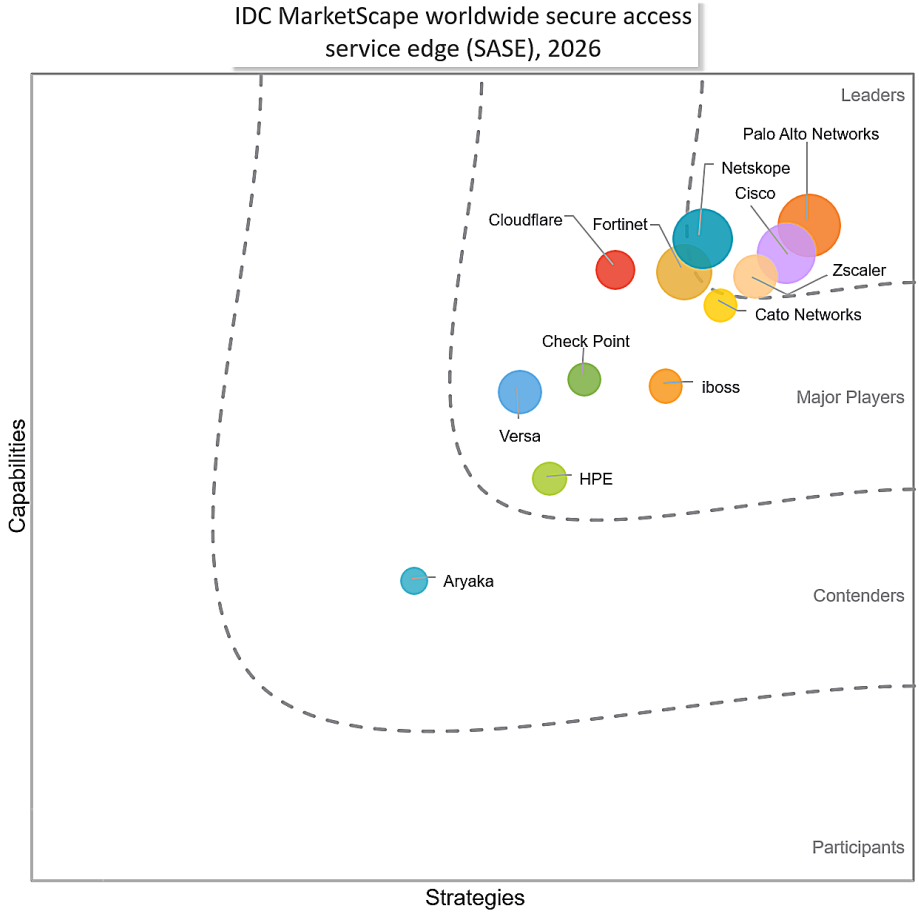
Brandon Butler Pete Finalle

THIS EXCERPT FEATURES PALO ALTO NETWORKS AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape worldwide secure access service edge (SASE) vendor assessment



Source: IDC, 2026

July 2026, IDC #US52978425e

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: IDC MarketScape: Worldwide Secure Access Service Edge (SASE) 2026 Vendor Assessment (Doc # US52978425).

IDC OPINION

Secure access service edge (SASE) architectures represent a fundamental convergence of the traditionally siloed networking and security markets and a next-generation strategy for connectivity and security for modern distributed enterprises in the AI era.

The rise of cloud-native application delivery, hybrid work models, and increasingly sophisticated AI-powered cyberthreats has driven organizations to rethink legacy perimeter-based architectures that were never designed for today's distributed enterprise realities. As workloads migrate to multicloud and SaaS environments and users connect from an expanding array of locations and devices, the limitations of discrete, point-based networking and security tools have become untenable, creating both the demand and the urgency for a more unified architectural approach. SASE architectures are a direct response, converging SD-WAN with cloud-delivered security capabilities, including secure web gateway (SWG), zero trust network access (ZTNA), and cloud access security broker (CASB), into an integrated framework.

The AI era is fundamentally reshaping the requirements for enterprise networking and security architecture. AI is simultaneously a powerful tool for defenders and an accelerant for adversaries, raising the stakes for organizations that have yet to modernize their access and security posture. Beyond the threat landscape, AI-driven workloads are placing new demands on network performance, latency, and capacity, forcing a rethink of how enterprises connect users, devices, and applications at scale. SASE has moved well beyond early adopter status and is now a mainstream strategic priority, with vendors competing on platform integration depth, security capability breadth, global point-of-presence (POP) scale, and AI-powered automation.

This IDC MarketScape evaluates the leading vendors across aforementioned dimensions, offering guidance for organizations navigating a dynamic and fast-moving market.

A diverse and differentiated competitive landscape

The 2026 SASE competitive landscape includes a diverse array of vendors approaching the market from different heritages, customer bases, and technology philosophies. Understanding where a vendor started helps buyers anticipate where capabilities are most

mature, where integration is native versus assembled, and where gaps are most likely to persist. This is a useful lens for evaluation, even as vendors have evolved, in some cases significantly, beyond their origins. These varied starting points appeal to meaningfully different buyers, and there is no single vendor that excels across every use case. IDC identifies three primary heritage categories, with several vendors spanning more than one:

- **Firewall and network security heritage:** Vendors in this category have built cloud-delivered security services by extending and modernizing established firewall and threat prevention capabilities, leveraging deep expertise in network security policy enforcement and perimeter defense.
- **Cloud-native secure service edge (SSE) heritage:** Vendors in this category anchor their SASE strategies in cloud-delivered security and purpose-built global private network backbones, delivering ZTNA, SWG, and CASB through a distributed proxy model designed from the ground up for cloud and mobile-first environments.
- **SD-WAN and branch networking heritage:** Vendors in this category approach SASE from established positions in edge infrastructure, drawing on expertise in SD-WAN, branch networking, and wired and wireless local area network (LAN) to extend connectivity-led platforms toward converged security.

Despite the similar origins for many vendors, the SASE product stack and its relative strengths and weaknesses are highly diverse between products. This is largely because of the complexity and scope of the products themselves, existing IP, expertise and new acquisitions, and a vast industry of unique environments, threats, and opportunities. Thus swimming lanes within these categories have developed, and no vendor has the single best solution for all SASE scenarios imaginable. However, some products solve more problems and reach more customers than others, and thus this research focuses on the broadest appeal, feature set, and strategy.

SASE buyer requirements are not universal

SASE is a singular product that integrates networking and security functionality into a unified solution. However, SASE buyers often do not approach these products as "one size fits all," and their search for a suitable solution can significantly narrow the list of viable vendors based on their specific requirements. The variance in the crucial KPIs of SASE buyers has yielded a market that thrives on product differentiation.

Vendor relevance with buyers is influenced by specific use cases, ecosystem requirements, regional and industry compliance standards, and existing networking and security investments. IDC's end-user research has shown that there is a range of requirements important to competing in the SASE market: security efficacy, geographic reach and POP coverage, advanced feature sets and extended portfolios, networking versatility and performance, and forward-looking AI and quantum capabilities. The cost of capabilities and

features also varies greatly, which can have a significant impact on platform alignment with a given size of business segment.

Balancing broad appeal with specialized capabilities

The dilemma facing many vendors in this market is whether to focus on specialized capabilities and appeal or to broaden their relevancy to expand their pool of potential customers. No vendor possesses the capability or capacity to be all things to everyone. On the other hand, vendors should not pigeonhole themselves with too narrow a focus, which could limit potential customer relevancy and reach. Most vendors included in this research have well-developed positioning within the customer, reseller, and managed service provider (SP)/managed security service provider community, which is essential for reputation, relevancy, and continued success.

Security capabilities across the evaluated vendors range from partial SASE to complete SASE to extended SASE, with varying degrees of integration. Networking capabilities similarly range from SD-WAN as a feature developed specifically for SASE to SD-WAN as a robust networking platform in its own right to private network backbones. This breadth of capabilities allows buyers to select vendors that meet their prioritized needs.

Foundational capabilities remain nonnegotiable

SASE solutions covered in this research are still evolving, and vendors are making significant investments in new features and advanced functionality, improved coverage and performance, and adherence to the latest market demands. A strong foundation is inherently the ideal scenario to build upon. SASE essentials, including SD-WAN, ZTNA, SWG, and API/inline CASB, are a baseline priority.

Critically, full-functioning CASB with both API and inline capabilities has emerged as essential for a SASE solution to meaningfully replace a standalone CASB. Equally, SD-WAN should not be a light feature or checkbox item. A SASE offering must be capable of functioning as a robust networking platform; if it cannot, buyers are likely to treat the solution as an SSE. Networking in general, and SD-WAN specifically, provides the foundational connectivity capabilities of a SASE platform, assuring high levels of user experiences and application performance, optimizing connectivity to cloud and AI applications, and providing advanced AI-powered connectivity management capabilities.

Emerging capabilities are becoming table stakes

Beyond the core SASE components, a set of capabilities that were once considered differentiating features have become broadly expected. These include digital experience monitoring (DEM), remote browser isolation (RBI), data loss prevention (DLP), and enterprise browser or browser extension capabilities. IDC recommends DEM in particular as a component of SASE, as it provides buyers with the visibility needed to maintain a high

level of performance and troubleshoot issues, both within the SASE solution and across components external to it.

Buyers can also further narrow their search by regional POP coverage, owned POP hardware or infrastructure, and sovereign controls that reflect a SASE vendor's ability to meet regional compliance requirements. POP coverage, including footprint, performance, and sovereign capabilities, defines the practical limits of a SASE solution's appeal, and strategic investments in POP architecture represent a meaningful lever for vendors looking to increase their addressable market.

At the same time, the industry is experiencing a rapid expansion of what buyers expect from a SASE platform when it comes to artificial intelligence. Security threats are now moving at AI speed, and AI-powered, autonomous security enforcement is quickly becoming important. Buyers are looking for immediate answers to these problems, but given the early stage of many AI capabilities, road map items and piloted capabilities should be taken into account alongside the generally available feature set of each vendor.

Management preferences and go-to-market considerations

Ease of deployment and ongoing management remain critically important evaluation criteria for SASE buyers. IDC's 2025 *SASE Buyer Insights Survey* shows that 45.2% of buyers prefer the easiest route to adoption, trusting a managed service provider to help them overcome the technical hurdles to deployment. Another 32.5% prefer the traditional do-it-yourself approach, while 22.3% are seeking the complete control offered by sovereign SASE. Vendors must be prepared to serve all three segments while maintaining simplicity as a North Star for product and go-to-market design.

Vendors must also be prepared for both partial and complete adoption among their customer base. The appetite of buyers for single-vendor SASE can sometimes exceed their capacity to adopt all of the security components offered by their vendor of choice. Third-party integrations are therefore essential to enabling buyers to achieve a smooth transition as they modernize their network and security architecture.

IDC's evaluation approach

For this research, IDC took a comprehensive view of the SASE market when evaluating vendors, focused on broad market relevance and capability, and aligned with IDC's 2026 *SASE Buyer Adoption Survey,* with niche or vertical-specific capabilities treated as differentiators rather than core criteria. Given the diversity of vendor approaches and buyer requirements outlined previously, no single vendor will be the right fit for every organization, and the profiles described in the Vendor Summary Profiles section are intended to help buyers identify the vendors best aligned to their specific priorities.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC used an inclusive interpretation of the SASE market for this research, which at a minimum required the integration of SD-WAN, ZTNA, SWG, and CASB as a single, consolidated product. Business, performance, and security outcomes were valued equally to technical and definitional alignment. While the presence of individual SD-WAN, SSE, or à la carte security SKUs did not impact inclusion, a single consolidated SASE SKU was a requirement for consideration.

All four primary SASE components must be present in a vendor's offering. Although considered essential, API CASB was not present in all solutions covered in this research. In addition, for a SASE solution to be considered for inclusion, it must have been generally available for at least 12 months at the start of the research process in the fourth quarter of 2025.

Vendors included in this research must have a global regional presence, with significant business across North America, Latin America, EMEA, and APAC. Regionally limited vendors were not included. This research also focuses specifically on SASE vendors serving the large enterprise market; vendors primarily focused on the small and medium-sized enterprise market are not included.

IDC implemented a minimum revenue threshold for inclusion in this research. As a result, the top 12 revenue-generating SASE providers were included. While vendors varied in how much of their SASE revenue was attributable to networking versus security components, SASE revenue was counted in totality for inclusion purposes. Revenue performance was calculated internally by IDC using IDC trackers and data sets, with vendor feedback from a qualification survey shared at the beginning of the research also taken into account.

ADVICE FOR TECHNOLOGY BUYERS

The SASE market has matured significantly, yet selecting the right vendor remains a complex, high-stakes decision. The range of architectural approaches, deployment models, and capability sets across vendors means there is no universal best choice, only the best fit for a given organization's infrastructure, security posture, and transformation goals. Buyers should resist the temptation to evaluate SASE platforms on feature breadth alone. Instead, the most effective evaluations begin with a clear articulation of immediate requirements, a realistic assessment of operational readiness, and a forward-looking view of how networking and security needs are likely to evolve. The following guidance is intended to help buyers structure that evaluation:

- **Start with immediate requirements.** Before evaluating vendors, buyers should define their nonnegotiable requirements across network coverage, performance, and

security. Regional POP proximity, sovereign controls, bandwidth availability, latency tolerances, and encrypted traffic performance must align with operational realities. On the security side, buyers should identify existing capability gaps and prioritize vendors that can natively address them. SASE adoption should improve security posture from the earliest stages of deployment, not defer it.

- **Prioritize coverage and consistency over feature completeness.** Deployment track record matters, but buyers should distinguish between time to deploy and time to value at scale. Request case studies that mirror your own deployment goals rather than vendor-selected best cases. Focus first on the breadth of users, devices, and applications covered under consistent policy enforcement before optimizing for feature depth. Licensing structures should support a clear migration path that delivers measurable ROI early, without requiring payment for capabilities that won't be utilized for years.
- **Evaluate for the journey, not just the starting point.** SASE adoption is an iterative process, and vendor selection should account for how requirements will evolve. Buyers should assess vendor road maps for alignment with emerging priorities such as AI governance, post-quantum cryptography, and dynamic threat response. Vendors with in-house threat research capabilities and a demonstrated track record of responding rapidly to emerging risks offer a more durable security foundation than those relying solely on third-party intelligence feeds.
- **Assess organizational readiness before selecting a platform.** SASE consolidates functions that are often owned by separate networking and security teams, and misaligned internal ownership is one of the most common causes of stalled deployments. Buyers should evaluate their readiness for that convergence, including how procurement, operations, and policy management will be structured across teams. Vendors with strong professional services and training resources can ease the transition, but organizational alignment is ultimately a buyer-side prerequisite that no platform can resolve on its own.
- **Inventory existing investments before committing to a platform.** Few enterprises approach SASE from a greenfield state, and integration complexity is frequently underestimated during vendor evaluation. Buyers should map their existing identity providers, endpoint security tools, SIEMs, and network monitoring infrastructure against each vendor's native integration capabilities and API openness. Platforms that require extensive custom integration work to coexist with incumbent tools introduce operational risk and can significantly extend time to value.
- **Match networking architecture to your use case.** SASE vendors vary significantly in their networking depth and architecture. Buyers with large branch or campus environments should evaluate the depth of SD-WAN capability and integration with wired and wireless LAN infrastructure. Cloud-first organizations may place greater value on a robust global backbone and hyperscaler interconnects. Understanding

where your traffic originates and where it needs to go and how the vendor's network architecture supports that flow is essential to avoiding performance and coverage gaps post-deployment.

VENDOR SUMMARY PROFILES

This section explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths, challenges, and opportunities.

Palo Alto Networks

Palo Alto Networks is positioned in the Leaders category in this 2026 IDC MarketScape for worldwide SASE.

Palo Alto Networks' SASE offering, delivered through the company's Prisma SASE platform, reflects a strategy centered on unifying networking, security, data protection, and operations into a single, cloud-delivered architecture. The company positions SASE as evolving beyond the combination of SD-WAN and SSE toward a broader platform that incorporates identity, data security, and AI-driven capabilities.

Prisma SASE integrates Prisma Access (SSE) with Prisma SD-WAN and extends security enforcement across multiple control points, including cloud points of presence, branch infrastructure, endpoints, and Prisma Browser Extension. A core architectural principle is policy abstraction, where policies are defined centrally and enforced across distributed environments depending on user, device, and application context.

The platform incorporates a wide range of security services, including secure web gateway, CASB, ZTNA, firewall as a service, and data loss prevention, alongside expanded capabilities for data security posture management and AI application governance. Palo Alto Networks places particular emphasis on extending SASE controls to emerging areas such as browser-based activity and AI-driven workflows.

The vendor is also advancing a converged networking and security model at the branch. Prisma SD-WAN supports application-aware routing and integrates security functions directly at the edge, with a road map toward a unified appliance combining SD-WAN and next-generation firewall capabilities. In addition, full integration with PAN-OS SD-WAN also enables customers to maximize the value of their Palo Alto firewalls along with SASE.

Management is delivered through Strata Cloud Manager, which provides centralized visibility, policy control, and workflow automation. The platform incorporates AI-driven

operational capabilities, including natural language interfaces, automated troubleshooting, and guided remediation, with a road map toward more autonomous operations.

Palo Alto Networks also emphasizes infrastructure resiliency and flexibility, leveraging a multicloud architecture and supporting sovereignty controls, distributed enforcement, and post-quantum cryptography initiatives. Overall, the company's approach reflects an expansion of SASE into a broader platform addressing networking, security, data, and AI-driven operational requirements.

Strengths

- **Technology leadership:** Palo Alto Networks has a long history of making best-of-breed technology investments, and this orientation continues to shape its SASE and AI security strategy. The company consistently brings mature, high-capability technology to market across networking, security, and data protection — including a strong SD-WAN offering that supports flexible deployment across physical, virtual, and cloud-managed environments — making it a strong fit for enterprises that prioritize technical depth and innovation.
- **Adaptive interface:** Prisma SASE's management experience is delivered through a flexible AI dashboard and interface that can be custom configured to suit different use cases and operational roles. This adaptability allows security and networking teams to tailor their operational views and workflows rather than conforming to a fixed interface model.
- **Autonomous security:** Palo Alto Networks has introduced autonomous security policy and configuration capabilities, enabling the platform to adapt to a rapidly evolving threat landscape with reduced manual intervention. This positions Prisma SASE among the more advanced offerings in terms of AI-driven, self-adjusting security operations. Unit 42, Palo Alto's threat intelligence function, delivers hourly threat updates, ensuring that security services across the platform are continuously refreshed with current intelligence on emerging attacks and threat actor behavior.
- **Emerging protections:** Palo Alto Networks is one of a small number of SASE vendors that has advanced post-quantum cryptography readiness to a production-relevant state, offering enterprises a forward-looking posture against emerging cryptographic threats. The platform also extends beyond traditional SSE capabilities into data security and AI governance, with AI-driven classification models and visibility into a large number of SaaS and generative AI applications, reflecting a focus on data exposure risks associated with distributed work and AI adoption.

Challenges

- **Multivendor limitations:** While Palo Alto Networks supports a broad range of extended technology integrations, it does not accommodate multivendor SASE scenarios effectively. Organizations with heterogeneous environments or those

seeking to mix SASE components across vendors may find the platform less flexible in supporting such architectures.

- **Infrastructure ownership:** Palo Alto Networks delivers much of its network reach through POPs deployed in partner and hyperscaler datacenters rather than through wholly owned, purpose-built facilities. This model supports strong SLA commitments, including 99.999% uptime and competitive bandwidth and latency metrics, and provides access to advanced hyperscaler capabilities such as GPU-accelerated processing. However, buyers with strict data sovereignty or regional compliance requirements may prefer vendors that operate a higher proportion of dedicated, owned POP infrastructure within their jurisdiction.
- **Premium pricing:** Prisma SASE offers a strong and comprehensive feature set but typically at a price premium relative to more budget-oriented alternatives. This positions the platform well for large enterprises with mature security requirements but may make it less competitive in the SMB market or for cost-sensitive buyers that do not require the full breadth of capabilities on offer.
- **Adoption complexity:** Palo Alto Networks' expansion of SASE into a broad platform that includes data security, AI protection, and operational tooling introduces complexity in positioning and adoption. Organizations evaluating SASE primarily for connectivity or SSE use cases may need to navigate a wider set of capabilities than required for initial deployments.
- **Evolving road map:** Palo Alto Networks continues to evolve its platform toward deeper convergence between its SD-WAN appliance portfolio and security functions, as well as toward fully autonomous operations. Customers should evaluate current versus planned capabilities carefully, particularly in areas such as unified policy management across networking and security functions.

Consider Palo Alto Networks when

Palo Alto Networks is well suited for large enterprises and global organizations seeking to align networking, security, and data protection within a single platform strategy. It is appropriate for organizations with distributed users, branch environments, and cloud-first application architectures that require consistent policy enforcement across multiple control points. The platform aligns with enterprises prioritizing zero trust models, data-centric security, and governance of generative AI usage. It is also relevant for organizations with dedicated security and networking teams that can leverage integrated operational tooling and AI-driven workflows across complex environments.

APPENDIX

Reading an IDC MarketScape graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market definition

SASE

Secure access service edge (SASE) architectures are a converged network and security offering made up of software-defined wide area network (SD-WAN) technology, with cloud-based secure service edge (SSE) security tools, including secure web gateway (SWG), zero trust network access (ZTNA), and cloud access security broker (CASB) as core components.

SSE

SSE is a converged solution for security, and sometimes connectivity, which is delivered as a service. SSE typically includes any combination of ZTNA, CASB, and SWG. These products can also include many additional features, such as firewall as a service (FWaaS), intrusion detection system/intrusion prevention system (IDS/IPS), and virtual private network (VPN). For the purposes of this research, SSE encompasses all security capabilities of a SASE offering while excluding networking functionality.

SD-WAN

Software-defined wide area network infrastructure encompasses the hardware and software products offered commercially by vendors. SD-WAN includes a centralized, application-based policy controller; a software overlay that abstracts underlying networks, analytics, and/or telemetry for application and network visibility; and an optional SD-WAN forwarder (routing capability). SD-WAN also provides automated management of hybrid WANs, defined as at least two WAN connections from each edge site, leveraging two or more underlying transport networks (e.g., MPLS, broadband internet, 4G/LTE/5G, LEO satellite). Together, these capabilities provide intelligent path selection across WAN links based on application policies defined on the controller. For the purposes of this research, SD-WAN includes all the networking components of an SD-WAN/SASE offering while excluding the security/SSE functionality.

Zero trust network access

ZTNA establishes secure connections from an authenticated user to only authorized applications based on context-aware, identity-aware, and device-aware policies. ZTNA is built on distributed integrity principles of application- and user-centric protections and least privilege access, thereby preventing unauthenticated users from connecting or sending any traffic to unauthorized applications.

Cloud access security broker

Cloud access security brokers are security enforcement points that monitor cloud application usage by organizations to provide discovery, monitoring, and protection. CASB incorporates multiple security controls, including policy enforcement, threat detection, data loss prevention (DLP), and user behavior analysis. CASB may operate as inline proxies and/or leverage API connectors to monitor traffic between users and cloud applications, as well as cloud-to-cloud communications.

Secure web gateway

Secure web gateways are security appliances or services that protect devices and data while users access and interact with websites. SWGs utilize multiple techniques, including

URL filtering, web content filtering, and threat protection, and may include remote browser isolation capabilities.

LEARN MORE

Related research

- *IDC Market Glance: Enterprise Network Infrastructure, 3Q26* (IDC #US53482825, June 2026)
- *IDC Survey Spotlight: How Have SSE/SASE Deployment Issues Changed Over the Past 24 Months?* (IDC #US54626526, June 2026)
- *IDC Survey Spotlight: How Has Single Vendor SSE/SASE Importance Evolved Over the Past Two Years?* (IDC #US54626826, June 2026)
- *IDC Survey Spotlight: Has the Importance of Existing Networking and Security Investments Waned in the Past Two Years?* (IDC #US54629326, June 2026)
- *IDC Survey Spotlight: Which Team Has Authority Over SSE/SASE Purchasing in 2026?* (IDC #US54629226, June 2026)
- *IDC's Worldwide Security Products Taxonomy, 2026* (IDC #US54501526, June 2026)
- *Key Considerations for Leveraging AI Agents in Network Management* (IDC #US54378526, March 2026)
- *How Is the Strategic Business Value of Connectivity Changing in the AI Era?* (IDC #US53918025, November 2025)
- *Secure Access Service Edge (SASE): Network and Security Convergence for the Hyper-Distributed Enterprise* (IDC #US53328325, May 2025)
- *IDC MarketScape: Worldwide SD-WAN Infrastructure 2023 Vendor Assessment* (IDC #US50471623, September 2023)

Synopsis

This IDC study provides a comprehensive evaluation of the leading vendors competing in the rapidly evolving SASE market, assessing the depth of their integrated networking and security capabilities, architectural approaches, and the ability to support enterprise transformation across distributed environments.

"Networking is a foundational element of any SASE architecture, and today's leading vendors are delivering a compelling and diverse range of approaches to integrated networking functionality. Whether organizations prioritize global POP-based architectures with impressive performance, standalone SD-WAN depth, or campus and branch integration, the market offers strong options that balance optimal connectivity and enhanced end-user experience with the robust security capabilities that define modern SASE

platforms." — Brandon Butler, senior research manager, Network Infrastructure and Services, IDC

"The SASE network security stack has matured greatly over the past 24 months, and few vendors struggle with providing the basics (ZTNA, SWG, inline CASB, and API CASB). However, in the face of increasingly fragmented ecosystems, AI usage and AI-powered threats, quantum computing development, and data/security sovereignty concerns, the basics are no longer good enough. For competing vendor products in this research, keeping one step ahead of the game/buyer requirements has never been more imperative or more difficult." — Pete Finalle, research manager, Trusted Access and Network Security, IDC

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, and web conference and conference event proceedings. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/about/worldwideoffices. Please contact IDC at customerservice@idc.com for information on additional copies, web rights, or applying the price of this document toward the purchase of an IDC service.

Copyright 2026 IDC. Reproduction is forbidden unless authorized. All rights reserved.