IDC MarketScape

IDC MarketScape: Worldwide Managed SASE Services 2025 Vendor Assessment

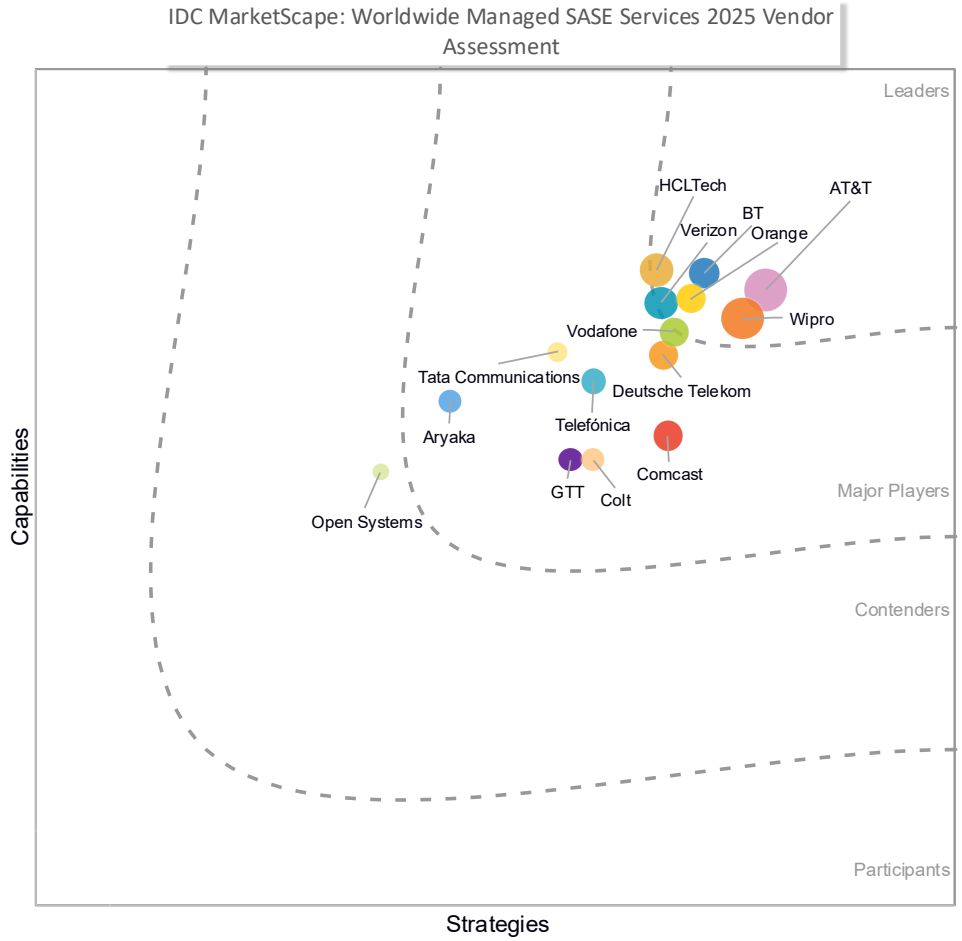
Ghassan Abdo James Eibisch Yogesh Shivhare

THIS EXCERPT FEATURES ORANGE AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Managed SASE Services Vendor Assessment



Source: IDC, 2025

October 2025, IDC #US53011425e

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: Worldwide Managed SASE Services 2025 Vendor Assessment (Doc # US53011425).

IDC OPINION

This IDC MarketScape evaluates global communications service providers (SPs) offering managed secure access services edge (SASE) services.

SASE emerged as an architectural framework that integrates software-defined networking with security services such as advanced firewalls, cloud access security broker (CASB), secure web gateways (SWGs), and zero trust network access (ZTNA). As IT decision-makers navigate the complexities of network transformation, SASE promised to reduce friction in the decision process and simplify the implementation and deployment of networking and security services. SASE builds on the momentum of SD-WAN services and increased pressure on enterprises to secure the network and related applications. This has become a strategic imperative as enterprises shift workloads to the cloud, manage remote workers, implement the latest AI technologies, and deal with increasing bandwidth demand. Application performance, high availability, and zero trust are more critical for enterprises as they digitize their internal and external business processes — they are becoming the lifeblood of a thriving enterprise.

Despite the grand promises of SASE, reality indicates significant challenges in adoption and shows a fragmented market. Friction remains among networking and security decision-makers, dealing with legacy security services slows implementation of cloud-based security services, and lack of maturity of managed SASE offers by providers slows adoption. This IDC MarketScape details many lessons from briefings with the participating service providers and calls with end users, detailed in the following sections.

Market Adoption

Conversations with service providers and end users reveal the following:

- SASE adoption is still in early stages, with enterprises prioritizing adoption of SD-WAN and some basic security services such as firewall and secure cloud access.
- Managed SASE service offers are fragmented, with varying approaches to security solutions or security services edge (SSE). SSE spans multiple services,

with no clear definition of what is included or excluded in a proper implementation of SASE. This is in addition to the complexity of dealing with legacy services.

- Consulting services are key to SASE adoption due to the complexity of security portfolios, which include integrating with legacy and deciding from several permutations of best-of-breed, multivendor, or single-vendor options.

Orchestration and Client Portals

IDC's communications for this IDC MarketScape reveal the following:

- All global service providers provide a client portal to enable customers to change configurations, obtain reports, and request analytics data.
- Most portals enable direct access to supported vendor portals/consoles. While service providers continue to evolve their own orchestration layer and improve their ability to orchestrate across vendors, there are practical and economic limits to how much vendor capability they can and should replicate themselves. They continue to rely on access to interfaces of the underlying vendor portal. This limits the extent to which they and customers can manage multivendor deployments within a single portal.
- Real-time reporting of network anomalies and the level of granularity of these reports are among enterprises' key complaints. This is an area that deserves significant attention from service providers.
- Most global service providers claim to use AI/machine learning (ML) technologies to enhance predictive maintenance and improve the use of customer data. We believe there are opportunities for improvement here, especially in the use of generative AI (GenAI) to simplify access to data and analytics.

Support Services

Conversations with service providers and end users reveal the following:

- Most enterprises opt for a fully managed service. However, co-managed services, where customers and service providers agree and share management responsibilities, have been increasing in popularity in recent years.
- Global service providers are pivoting toward security consulting to help enterprises navigate the complexity of choosing and deploying the right security services within the context of SASE services. This favors systems integrators (SIs) and managed security SPs as consulting is their key strength.
- Most multinational corporations (MNCs) prefer to sign a single service-level agreement (SLA) with the managed service provider, with the expectation that

the underlay services provided by third-party internet SPs are handled under that single contractual framework.

Technology and Vendors

IDC's conversations with service providers and users also showed the following:

- Global providers have established strategic partnerships with major technology providers of SD-WAN and SSE. They typically offer three to five vendor solutions with a tendency to reduce the number of vendors.
- Multivendor SASE services seem to dominate current deployments while a pivot toward a single-vendor SASE solution is accelerating.

Go to Market and Branding

IDC's communications for this IDC MarketScape also revealed the following:

- Despite progress, most providers lack a cohesive marketing and branding communication plan for their managed SASE services, including business and technical rationale to evolve SD-WAN toward SASE services.
- Most global providers rely on channel partners to target the midmarket and SMB segments, which are generally underserved and represent a greenfield opportunity. These segments require standardized and automated solutions to reduce the need for in-house expertise.
- Most global services eye expansion into geographies they do not currently serve. This can be challenging due to increased global competition and required investments in go-to-market (GTM) and support services.

In summary, the adoption of SASE is transformative in network security because SASE is heavily integrated with other security products and tools. This makes it a critical component of the decision-making process for firewall, ZTNA, data loss prevention (DLP), and other security technologies. Its transformative nature does not necessarily mean that the SASE adoption process will be quick for buyers. While more organizations are looking to embrace SASE, migration is a slow and involved process that benefits from a well-planned, measured approach to adoption.

Given the complexities of integration and the volume of capabilities that modern SASE solutions bring to the table, global service providers must help enterprises with migrating toward SASE and choosing the right solution and capabilities. This will help enterprises balance the number of features they adopt, the percentage of the workforce for which SASE rolls out, and the number of critical applications it supports.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

This IDC MarketScape includes service providers from all regions (the Americas, EMEA, and APJ) that meet the following criteria:

- The service providers must have global capability and serves global MNCs.
- The service provider has a minimum $25 million annual revenue in 2024.
- The service provider must demonstrate commitment to further development of its managed SASE services.
- The service provider is driving innovation in its SASE road map.

ADVICE FOR TECHNOLOGY BUYERS

Network transformation is a strategic imperative for enterprises. IDC's September 2024 *Future Enterprise Resiliency and Spending Survey* indicated that the top drivers of IT spending in 2025 include enhancing cyber-recovery/cyber-resiliency and modernizing core enterprise applications. Organizations can only achieve these business drivers with a holistic network transformation that aligns with business outcomes. Security needs to protect business outcomes and not just act as a barrier to threats.

Enterprises face the choice of adopting SD-WAN and security services as disparate services or adopting SASE as an integrated architecture for both networking and security. Despite some of the fragmentation of SASE and ongoing evolution, it is a promising technology and architectural framework. Enterprises should consider the following in their decision for SASE:

- Prioritize service providers with proven experience in providing managed services spanning the full life cycle of design, implementation, deployment, and operation.
- Consider service providers that provide choices in SASE technologies, including best-of-breed, multivendor, or single-vendor solutions, but with an integrated orchestration layer. The integrated orchestration layer will manage networking and security policies holistically and consistently across the enterprise network.
- Seek service providers that are aligned with your business priorities, understand the network transformation outcomes, and provide needed consultancy and advisory services to help you achieve these business goals.
- Ensure that the service provider has a comprehensive road map and needed resources to integrate AI into the full life cycle of SASE services. These will have a major impact on optimizing operations, improving customer service, and increasing productivity.

- Ensure that single-vendor SASE options do not result in lock-in as services evolve and new players may have differentiated offers.

VENDOR SUMMARY PROFILES

This section briefly 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 and challenges.

Orange

Orange is positioned in the Leaders category in the 2025 IDC MarketScape for worldwide managed SASE services.

Headquartered in Paris, France, Orange serves over 200 countries via more than 650 POPs and operates global NOCs in Brazil, Egypt, and India. It offers SD-WAN, SASE, and SD-branch to multinational and regional customers. The Evolution Platform, the centerpiece of its next-gen network service strategy, enables customers to design, orchestrate, and manage SD-WAN, SASE, and SSE solutions, underpinned by carrier-grade reliability and performance.

Orange delivers SASE using partners such as Cisco, Fortinet, Palo Alto Networks, HPE Aruba, Netskope, and Zscaler (Versa joining late 2025), integrated as VNFs in Orange Super POPs. The platform features modular composability, enabling customers to choose and chain network and security functions as well as adjust control between fully managed, co-managed, or self-managed models.

The Orange Evolution Platform provides a unified digital interface for end-to-end solution creation, automated provisioning, orchestration, configuration, ticketing, observability, and billing. Advanced tools enable solution designers to automate configuration, validate compliance, and chain network and security services. Single-pane-of-glass access provides high-level and detailed management, with the ability to access underlying partner consoles for fine-tuning and vendor-specific analytics.

Orange is actively developing AIOps for anomaly detection, incident prediction, and GenAI-based copilots for configuration and customer interactions. Evolution Platform will bring AI-driven compliance assessment and automated ticket classification and resolution, further enhancing operational efficiency.

Orange's proprietary threat intelligence, powered by Orange Cyberdefense and its EU CERT, is embedded in all SASE deployments, augmenting industry-leading SSE capabilities from Netskope, Palo Alto, Zscaler, and Fortinet. 24 x 7 SOC coverage and

continuous monitoring ensure global regulatory compliance and advanced risk detection.

Strengths

Orange's strengths and differentiators in the managed SASE market include the following:

- Extensive, resilient network infrastructure and certified expertise across all key SASE partner technologies
- Evolution Platform, which enables modular, flexible, carrier-grade solution design — combining telco resilience with SI-like customization options
- Converged security intelligence from Orange Cyberdefense, global threat research, and automatic protection workflows within SASE deployments
- Robust consulting, advisory, and operational support paired with deep automation and orchestration capabilities

Challenges

To maintain its competitive advantage, Orange will benefit from the following:

- Increased global brand recognition and expansion of Evolution Platform are priorities for market differentiation.
- Continued investment is required to launch further AI-driven features, expand solution composability, and integrate new SASE partners.
- Streamlining commercial risk management (proofs of concept, pilot programs) could accelerate customer decision-making in large-scale SASE transformations.

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 builds and delivers 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

Managed SASE brings SD-WAN together with a combination of SSE technologies, such as firewall as a service, SWG, CASB, ZTNA, and DLP, along with service provider day 0 to day 2 configuration, monitoring, and management provided as a monthly recurring revenue (MRR) service.

Managed SD-WAN combines SD-WAN and, in many cases, next-generation firewall security as a premise-based service, along with provider day 0 to day 2 configuration, monitoring, and management provided as an MRR service. The provision of a self-service portal enables organizations to configure, manage, and obtain reporting on the health and performance of the WAN.

LEARN MORE

Related Research

- *IDC MarketScape: Worldwide Managed SD-WAN Services 2025 Vendor Assessment* (IDC #US52980125, September 2025)
- *IDC MarketScape: Worldwide Managed Security Service Edge Services 2025 Vendor Assessment* (IDC #US52992425, September 2025)
- *Worldwide Managed Edge Services Forecast, 2025–2029* (IDC #US53507526, June 2025)

- *NaaS Market Trends 2025* (IDC #US51677424, May 2025)
- *Inference at the Edge: Implication for Service Providers* (IDC #US53114325, March 2025)
- *Top 5 Trends in Managed Edge and Content Delivery Services in 2025* (IDC #US52277225, February 2025)

Synopsis

This IDC study assesses 15 providers that provide managed SASE services on a global basis. The assessment is based on their current capabilities and strategies for delivering managed SASE services. This comprehensive analysis by IDC on this rapidly growing market provides insights into enterprises deciding on the adoption of managed SASE services in their journey toward network transformation.

"By unifying network and security under a common architecture, SASE provides a compelling framework to achieve zero trust networking paradigm. It behooves service providers and technology providers to communicate the value of a unified SASE framework and how it mitigates typical friction in networking and security decision process," said Ghassan Abdo, research VP, Worldwide Telecom.

"Managed SASE services are increasingly distinguished by how effectively they embed security into converged architectures. Providers that unify SSE, SD-WAN, and threat intelligence into a managed framework are best positioned to deliver connectivity and performance as well as continuous risk reduction and zero trust execution at scale," added Yogesh Shivhare, research manager, Security and Trust.

"SASE promises to converge networking and security into a single manageable entity, but the reality is that enterprises have diverse needs and preferences as well as established ways of managing security so that there is no one-size-fits-all solution. Service providers need to retain flexibility and customer choice in their offerings," said James Eibisch, research director, European Enterprise Communications Services.

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