

IDC MarketScape: Asia/Pacific Managed SD-WAN/SASE Services 2025–2026 Vendor Assessment

Nikhil Batra

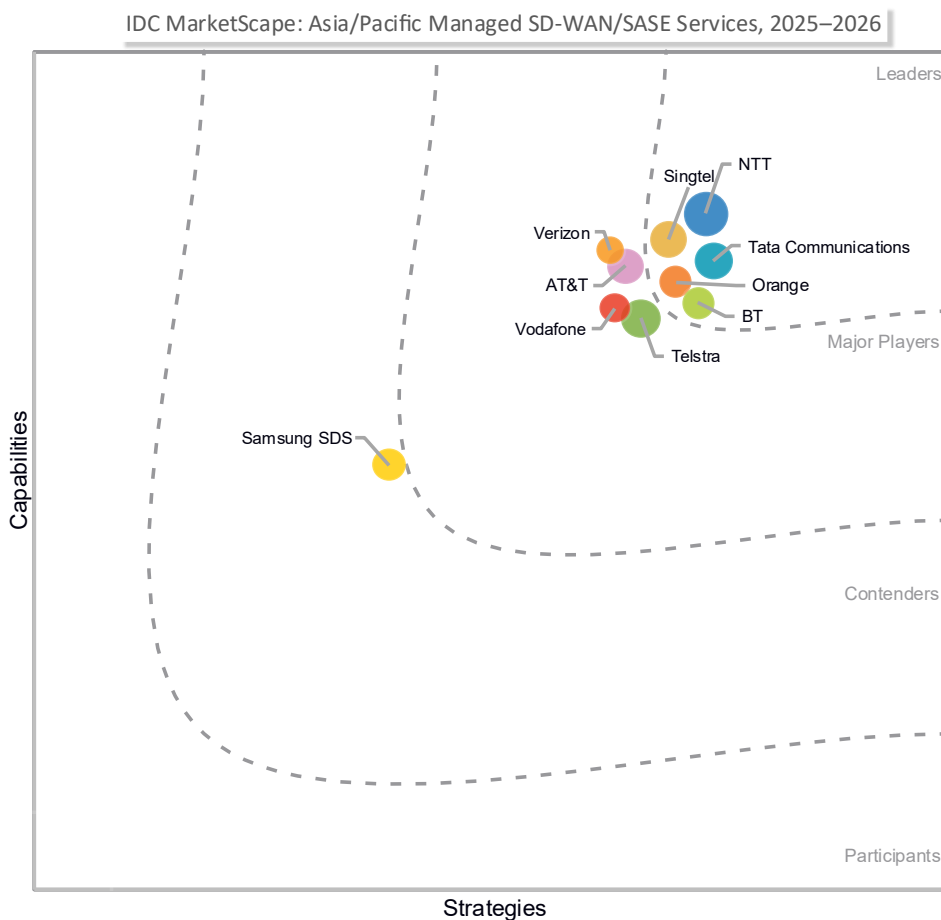
Sakshi Grover

THIS EXCERPT FEATURES TATA COMMUNICATIONS AS A LEADER

IDC MARKETScape FIGURE

FIGURE 1

IDC MarketScape Asia/Pacific Managed SD-WAN/SASE Services Vendor Assessment



Source: IDC, 2025

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: Asia/Pacific Managed SD-WAN/SASE Services 2025–2026 Vendor Assessment (Doc # AP52998525).

IDC OPINION

The 2025 IDC MarketScape on Asia/Pacific managed software-defined WAN (SD-WAN)/secure access service edge (SASE) services reflects how organizations in the region are moving beyond the first wave of SD-WAN adoption toward a broader focus on secure SD networking (SDN). SD-WAN is now a table-stakes capability, a baseline that every major provider must deliver. IDC's *Asia/Pacific Enterprise Connectivity Survey* highlights that 48% of organizations have already adopted SD-WAN, with another 30% expected to do so by mid-2026. The real key focus now lies in how service providers combine SD-WAN with security service edge (SSE) functions to deliver a complete SASE experience that integrates networking, security, automation, and observability under one operating model.

The study highlights that the managed SASE services market in Asia/Pacific has matured to a point where core SD-WAN capabilities are largely standardized. Service providers should offer depth of integration, automation, and life-cycle services. IDC's analysis of this year's study highlights the following set of capabilities for service providers:

Operating as a “platform” rather than a portal. Moving on from orchestration to full life-cycle automation, spanning provisioning, policy synchronization, and assurance, has become a key indicator of platform maturity. Service providers that integrate these capabilities through open application programming interfaces (APIs) and expose them to customers as comprehensive platforms, rather than as collections of managed tools, will have better traction in the market. Examples such as Singtel CUBΣ, Global Fabric, Evolution Platform, and Adaptive Networks demonstrate how automation depth, not interface design, is now defining the SP platform approach.

Unified multivendor observability and control. The ability to ingest telemetry and policy data from different SD-WAN and SSE stacks into a unified operational model will be an important factor for organizations. Service providers are investing in proprietary software layers that harmonize data, analytics, and alerts, enabling customers to manage their environments through a single pane of glass.

Making NaaS functional and measurable. Service providers that have evolved Network as a Service (NaaS) from a flexible pricing mechanism into a functional

model are placing greater emphasis on customer transparency and control. By defining which functions are automated, which are managed, and which are self-service, they are giving organizations predictable experiences that mirror cloudlike consumption models. This transition allows them to demonstrate flexibility aligned with their customer requirements.

Consulting and life-cycle integration as part of service design. Helping customers align their networking and security teams, design hybrid SASE solutions, and migrate with runbooks and pretested blueprints, while keeping their technology choices in mind, facilitates deeper conversations. Service providers with an integration heritage are winning complex rollouts because they reduce both organizational friction and technical risk.

AI for IT operations (AIOps) as an assurance framework. The use of AI and automation for proactive fault isolation, predictive routing, and guided remediation is moving from experimentation to standard practice. Service providers that can demonstrate measurable improvement in metrics such as mean time to repair (MTTR) and provisioning times showcase reliability and transparency.

Ecosystem expansion with governance. Scaling business with indirect channels (domestic telcos, systems integrators [SIs], etc.), while enforcing design standards, certification, and shared key performance indicators (KPIs), so delivery quality stays uniform across markets, provides Asia/Pacific SPs with additional growth avenues.

Regional delivery excellence as proof of consistency. In Asia/Pacific, execution quality is essential, and service providers that can demonstrate in-country delivery capabilities, publish their point of presence (POP) distribution, and showcase operational case studies are building greater confidence with enterprises seeking a consistent experience across countries.

IDC MARKETSCOPE VENDOR INCLUSION CRITERIA

This IDC MarketScape included communications SPs from Asia/Pacific region that meet the following criteria:

- Regional and global SPs that have the capability to serve large enterprises and multinational corporations (MNCs)
- Service providers that are offering managed SD-WAN and SASE services in the region
- Service providers demonstrating commitment to further development of SD-WAN and SASE services portfolio
- Service providers that are driving innovation in SDN services

ADVICE FOR TECHNOLOGY BUYERS

For organizations, the growing maturity of managed SASE platforms has redefined what to look for in a service provider. With most vendors now capable of delivering secure connectivity, the real difference lies in operational consistency, transparency, and the ability to support hybrid, multivendor environments. The following highlights practical checks that can help organizations choose the right partner for their secure networking journey:

Evaluate platform maturity, not just vendor logos. Ask the provider to demonstrate end-to-end tasks such as site addition, policy change, configuration rollbacks, and ticket/issue management, in one place. Verify API availability and how the SP platform addresses your technology mix of SD-WAN and SSE vendors.

Validate AIOps scope and outcomes. Confirm whether AI is only about alerts and highlighting anomalies, or also correlates across underlay, overlay, and security to trigger guided or automated fixes. Inquire about MTTR improvements and example incidents in which issues were prevented rather than detected.

Clarify NaaS in a formal structure. Request a matrix that shows what is metered, what is fixed, what you can self-serve, and which service-level agreements (SLAs) apply to the internet underlay as well as multiprotocol label switching (MPLS). Run proof of concepts (POCs), increasing bandwidth or a cloud connection yourself via APIs or the service provider's self-service portal.

Plan multivendor policy governance upfront. If you prefer hybrid SASE, work with your service provider to have consistent, single policy enforcement across your chosen SD-WAN and SSE stacks. Ask how telemetry is normalized and how conflicts are detected and resolved.

Assess life-cycle support before you buy. Look for design blueprints, migration runbooks, bulk provisioning capabilities, and Day-2 optimization to reduce risk when network and security teams are still operating in silos.

Inspect regional delivery specifics. Ask for a map of the POPs used for your users and applications, typical latencies, and named escalation contacts per country. Request information on recent local incidents and examine how they were handled end-to-end.

Test comanaged roles and audit trails. In a live portal, verify approval workflows and configuration history for policy changes to ensure you can make changes without needing to open tickets. This is where many "comanaged" offers differ in practice.

Plan for an internet-first approach, but with protection. When you shift from MPLS, evaluate service provider options for business-grade internet alternatives with AI-routed paths, distributed denial of service (DDoS) controls, and performance

SLAs. Validate how the provider proves path quality and switches routes proactively (AI routing).

Insist on transparency for partner-delivered work. If the provider uses SIs or local telcos for fulfilment for some locations, request shared dashboards, joint KPIs, and accountability for the joint operations. Your experience should be uniform regardless of who performs the work.

Overall, organizations should approach the adoption of managed SD-WAN or SASE services and the selection of their preferred partner with a greater focus on life-cycle outcomes, from planning and design to ongoing assurance and optimization, rather than being technology feature-led.

VENDOR SUMMARY PROFILES

This section provides a brief explanation of IDC's key observations that inform 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 opportunities.

Tata Communications

Tata Communications is positioned in the Leaders category in the 2025–2026 IDC MarketScape on Asia/Pacific managed SD-WAN/SASE services.

Tata Communications continues to evolve from a global network operator into a digital ecosystem enabler, integrating connectivity, cloud, and security with a unified platform strategy. This transformation is anchored in its Digital Fabric strategy, which brings together the Network Fabric, Cloud and Security Fabric, Interaction Fabric, and IoT Fabric, aimed at helping organizations interconnect their infrastructure, applications, people, and things.

In Asia/Pacific, this approach has translated into tangible momentum, with the service provider highlighting good growth across all three areas: managed SD-WAN, managed SSE, and managed SASE services. The company also noted its growing relevance among organizations seeking a single technology partner capable of integrating networking ownership and the full life cycle of managed services. Building on this foundation, Tata Communications' strategy emphasizes automation, outcome-driven delivery, and flexibility in engagement models to help enterprises modernize connectivity and security simultaneously.

The core of Tata Communications' enterprise portfolio is now structured around the Digital Fabric, a framework designed to enable organizations to adopt modular capabilities — from underlay to edge — under a unified governance and observability layer. Supporting this strategy is its IZO portfolio, which includes IZO SD-WAN, IZO Cloud, SSE offerings, and interconnect services, with the aim of providing secure software-defined connectivity. The TC^x platform sits at the heart of

this architecture, functioning as the orchestration, analytics, and policy engine that binds network and security domains. It also collects telemetry across underlay and overlay layers, without fragmenting policy control or visibility.

This integration between architectural design and operational execution enables Tata Communications to offer a wide range of managed services, including its SD-WAN, SSE, and SASE framework-based offerings, delivered through a life-cycle methodology. The IZO SD-WAN portfolio, in partnership with technology vendors such as Versa, Cisco, HPE Aruba, and Fortinet, has transitioned to SD-WAN 2.0, characterized by AI-driven automation and orchestration capabilities. Complementing the SD-WAN offerings, Tata Communications' SSE offerings integrate SWG, CASB, ZTNA, and FWaaS. These are delivered in partnership with companies such as Fortinet, Zscaler, Palo Alto Networks, Netskope, and Versa, and are managed through the unified TC^X platform, which provides consolidated policy orchestration and analytics.

Building on the foundations of SD-WAN and SSE, Tata Communications' managed SASE services framework offers enterprises two deployment options:

- Hybrid SASE, which integrates multivendor SD-WAN and SSE components through TC^X for unified policy management and observability.
- Hosted SASE, a single-vendor solution delivered in partnership with Versa, hosted on Tata's globally distributed POPs and provisioned through automated activation workflows.

For enterprises, this means a single operational plane for network and security visibility, reducing blind spots between connectivity and cloud-based controls. The company's SSE infrastructure operates with a stated 99.999% platform uptime, and incident-response parameters are mapped to priority classes within its SLA framework. This integration of network-aware security capabilities not only strengthens the threat posture but also simplifies management for organizations seeking to converge their security operations with network governance.

Commercially, Tata Communications employs a three-part pricing structure that separates technology investments (license), implementation (onetime, nonrecurring charges [NRC]), and management (monthly recurring charges [MRC]), allowing enterprises to align their spend with scope and operational ownership. The company also provides contract terms ranging from 12 to 60 months, with options for phased activation and flexibility that supports incremental rollouts. Underlay connectivity services can also be bundled or sourced separately by organizations. Together, these constructs allow Tata Communications to act as a partner that balances architectural offerings with flexible commercial engagement — a combination that is increasingly valued by Asia/Pacific enterprises.

Strengths

Hybrid and hosted SASE flexibility that matches customer requirements. Tata Communications' SASE strategy offers two well-defined paths to its customers that mirror how enterprises typically advance on their networking and security convergence journey: Hybrid SASE for specialized integration and Hosted SASE for a unified, cloud-delivered option. The Hybrid SASE model enables organizations to integrate SD-WAN and SSE technologies from various vendors, maintaining a single operational plane through the TC^X platform for unified policy enforcement, threat visibility, and real-time analytics. In contrast, Hosted SASE, delivered in partnership with Versa, is hosted across Tata Communications' globally distributed POPs and offered as a fully managed service that can be ordered through a simplified digital interface and activated automatically with light or zero-touch provisioning.

This dual-option structure enables enterprises to move at their own pace — preserving existing investments where needed or shifting to a standardized, as-a-service environment in which speed and uniformity are paramount. Since both deployment modes are anchored in the TC^X fabric, customers retain a single set of policies and insights across architectures, ensuring consistent control and visibility throughout the transformation.

IDC believes that this combination of architectural choice and unified governance is a significant capability that helps reduce migration risk and sustain Day-2 operational consistency as SASE adoption expands for an organization.

Digital Fabric and TC^X integration for intelligent, life cycle–led delivery. The Digital Fabric's layered architecture and TC^X orchestration capabilities unify network, cloud, and security domains, simplifying policy enforcement and observability across multivendor environments. This model resonates with enterprises seeking coherence between networking and security functions, reducing the friction that typically arises in siloed operations.

Operationally, Tata Communications integrates its proprietary design-to-run model, the Assess, Execute, Integrate, Operate, and Manage (AXIOM) methodology, with TC^X in a continuous feedback loop to reduce deployment risk and compress time-to-value, especially in large, geographically dispersed organizations. AI/ML models embedded in TC^X monitor event streams across network and security layers, applying component-level severity scoring that rolls up to a site-level health view. When anomalies exceed defined thresholds, automated tickets are generated and prioritized by risk, ensuring timely escalation and response. The Quality Management Bot (QM-Bot) then evaluates postclosure performance to detect recurring patterns and recommend targeted improvements.

The overall effect is a structured, self-learning delivery fabric in which every deployment feeds insights back into the operating model, reinforcing consistency, predictability, and continuous service optimization. This disciplined, automation-

driven approach has become a defining strength of Tata Communications' managed SD-WAN and SASE delivery.

Challenges

Maintaining a strong presence in security-led conversations. Although Tata Communications owns significant global network infrastructure, enterprises are now more focused on software-defined agility and integrated security solutions. The growing prominence of SASE framework-based solutions means that networking conversations increasingly revolve around security capabilities rather than connectivity alone. Although Tata Communications also offers a full suite of managed security services, it should focus on developing and expanding its cybersecurity capabilities to strengthen its service offering in the region.

Having said that, the Digital Fabric strategy, along with its options for Hybrid and Hosted SASE services in the portfolio, is resulting in good traction, as evidenced by the service providers' results. Tata Communications will need to continue translating its infrastructure strength into measurable service advantages and highlighting its Day-2 performance commitments and experience KPIs to demonstrate value.

Shifting market perception from carrier to platform partner. Despite its progress, Tata Communications continues to address the legacy perception of being a connectivity provider. Reinforcing its identity as a services-led, automation-driven transformation partner — particularly in managed SASE services engagements — will be key to sustaining its growth in the region and further underscoring its position as a transformation partner rather than a carrier-led one.

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, as well as how well aligned the vendor is with customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will assess how effectively a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or the strategy 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.

This document gives equal weight to the strategies and the capabilities criteria using a 50:50 ratio. The managed SASE services market continues to evolve, driven by ongoing changes in service provider offerings and strategies. Hence, the study gives equal weightage to current capabilities and midterm/long-term strategies that drive growth and differentiation.

IDC MarketScape Methodology

The IDC MarketScape criteria selection, weightings, and vendor scores represent IDC's well-researched 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, drawing on detailed surveys and interviews with vendors, publicly available information, and end-user experiences. This approach enables an accurate and consistent assessment of each vendor's characteristics, behavior, and capabilities.

Market Definition

Since its inception in 2015, SD-WAN has been viewed as a transformational technology that addresses the enterprise needs for cloud adoption, flexible service introduction, and dynamic bandwidth allocation. It has since been elevated as the underpinning of network transformation, fundamental to the digitization of enterprises. The demands on the network are constantly evolving, particularly with the adoption of AI and generative AI (GenAI) technologies, which require higher bandwidth and variable traffic patterns.

Global communications SPs initially offered network-based SD-WAN managed services primarily based on Cisco IWAN. They later incorporated over-the-top (OTT) solutions from start-ups such as Viptela, VeloCloud, and Versa in response to enterprise demand and to fend off against competition from these vendors.

2019 witnessed an acceleration of managed SD-WAN adoption and an increase in commercial deployments. SD-WAN architecture has evolved to integrate security services under the umbrella of secure access service edge (SASE). From a commercial perspective, SD-WAN/SASE is increasingly bundled under the network-as-a-service (NaaS) commercial framework. NaaS provides a cloud consumption model of networking services and integrates them under a single SLA.

Managed SD-WAN services continue to experience strong growth. We expect this growth to accelerate with the rollout of SASE services, driven by strong demand for

security services. Managed SASE combines SD-WAN with a suite of SSE technologies, including firewall as a service, SWG, CASB, ZTNA, and DLP, along with service provider Day 0 to Day 2 configuration, monitoring, and management, all provided as a monthly recurring revenue (MRR) service.

LEARN MORE

Related Research

- *Asia/Pacific (Excluding Japan and China) Managed SD-WAN Services Forecast, 2025–2029*, (IDC #AP52210825, March 2025)
- *IDC FutureScape: Worldwide Enterprise Connectivity 2025 Predictions — Asia/Pacific Implications* (IDC #AP51576924, December 2024)
- *Sustainable Networking in Asia/Pacific — Only If It Makes Business Sense* (IDC #AP50970924, June 2024)
- *Seizing the Opportunity: SP and Enterprise Multivendor Management Challenges* (IDC #AP50970724, April 2024)

Synopsis

This IDC study presents an assessment of 10 communications SPs that provide managed SD-WAN and SASE services in the Asia/Pacific region. The assessment is based on their current capabilities, go-to-market (GTM) strategies, growth, innovation, and plans for delivering managed software-defined WAN (SD-WAN) and secure access service edge (SASE) services. This is an evolution of the *IDC MarketScape: Asia/Pacific Managed SD-WAN/SASE Services 2024–2025 Vendor Assessment* in 2024, and the second comprehensive analysis by IDC in a rapidly evolving market. It provides insights into enterprises deciding on the adoption of managed SASE services in Asia/Pacific.

“The Asia/Pacific region has witnessed a significant shift in software-defined networking, moving from SD-WAN to a more comprehensive range of SASE framework-based solutions. This evolution is driven by the increasing demand from enterprises for flexible, reliable, and secure networking solutions. To this end, communications SPs are offering a broader range of services, including SASE framework-driven solutions that combine networking and security capabilities. However, not all offerings are created equal, and various service providers are positioning themselves in different ways to stand out in a highly competitive market,” says Nikhil Batra, senior research director, IDC Asia/Pacific Telecom Practice.

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.).

IDC Asia/Pacific Headquarters (Singapore)

168 Robinson Road
Capital Tower, Level 20
Singapore 068912
65.6226.0330
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 2025 IDC. Reproduction is forbidden unless authorized. All rights reserved.