IDC MarketScape

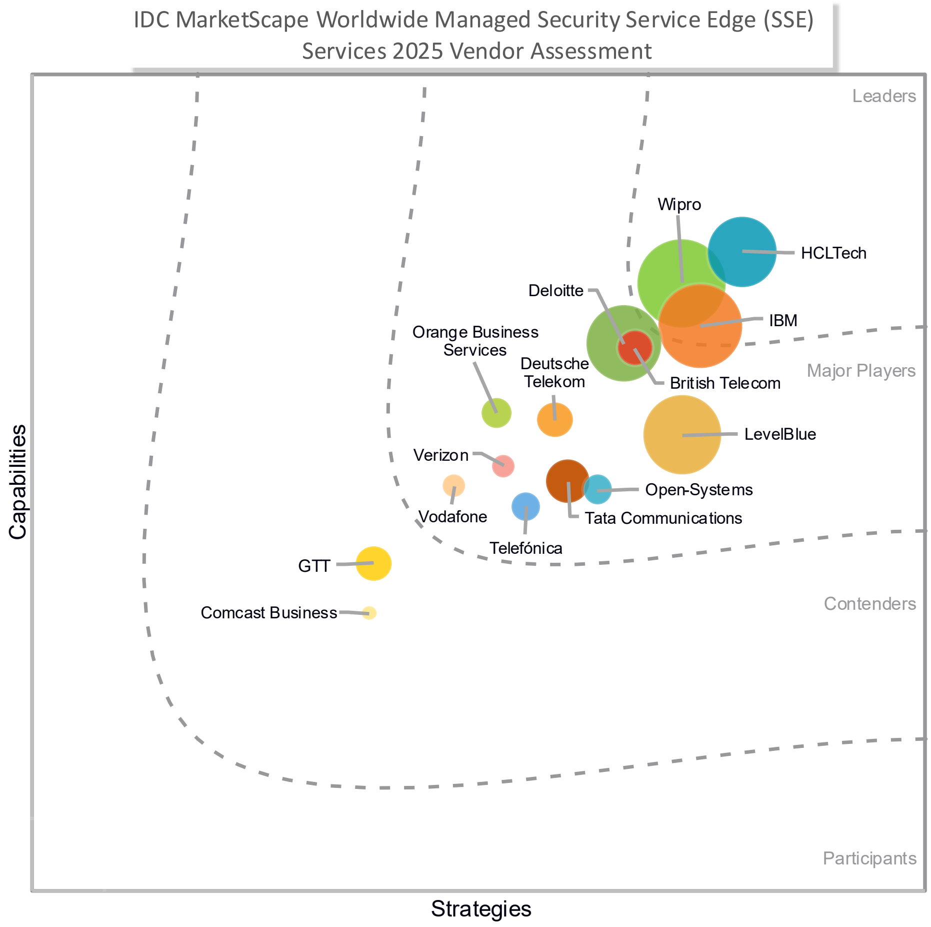
# IDC MarketScape: Worldwide Managed Security Service Edge Services 2025 Vendor Assessment

Yogesh Shivhare

## IDC MARKETSCAPE FIGURE

### FIGURE 1

### IDC MarketScape Worldwide Managed Security Service Edge Services Vendor Assessment



Source: IDC, 2025

September 2025, IDC #US52992425

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

## IDC OPINION

Managed security service edge (SSE) has matured into a cornerstone of enterprise security architecture as organizations adapt to cloud adoption and hybrid work models. The shift from appliance-based web gateways and VPNs toward unified, cloud-delivered services reflects the demand for consistent policy enforcement, consolidated visibility, and improved user experience across distributed environments. By converging various network security functions, SSE provides a scalable foundation for zero trust strategies while reducing operational complexity.

The market's evolution is now shaped less by whether SSE is adopted and more by how it is delivered and managed. Providers differentiate through breadth of technology partnerships, depth of managed services, and their ability to embed automation into policy management, reporting, and incident response. Integration with adjacent domains such as identity management and managed detection and response (MDR) is increasingly viewed as a requirement, as enterprises want to align access control and threat response with a common zero trust framework. The most advanced offerings extend value through customer portals with real-time visibility and compliance reporting, as well as globally distributed enforcement nodes that ensure low-latency, policy-consistent access worldwide.

IDC views the key differentiators among managed SSE providers as:

- Diversity and maturity of vendor technology partnerships, including leading SSE platforms
- Integration of identity and access management (IAM) to operationalize zero trust
- Seamless linkage with managed extended detection and response (MXDR) and security operations center (SOC) services to improve detection fidelity and accelerate response
- Customer-facing portals with transparent controls, reporting, and compliance evidence
- Global enforcement presence to guarantee user experience and consistent policy application
- Embedded data protection aligned to regulatory frameworks across industries

## IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

To be included in the 2025 worldwide managed security service edge service provider vendor assessment, providers had to meet the following criteria:

- **Portfolio of managed SSE services:** The security service provider must have an established portfolio of managed SSE services. Managed SSE services provide organizations with cloud-delivered security solutions focused on protecting users and data, regardless of location, as a single converged solution. This includes, but not limited to, firewall as a service (FWaaS), secure web gateway (SWG), cloud access security broker (CASB), and zero trust network access (ZTNA). The managed SSE service provider offers deployment, integration, management, and operations for these solutions.
- **Time threshold:** The provider must have offered these managed SSE services for at least one year prior to this assessment.
- **Multiregion footprint:** The service provider must have an active customer base spanning at least two of the four major global regions — North America, EMEA, APAC, and LATAM.
- **Revenue threshold:** The provider must have generated at least $10 million in global revenue in calendar year 2024 specifically attributable to its managed SSE services portfolio.

## ADVICE FOR TECHNOLOGY BUYERS

Organizations evaluating managed SSE should adopt a dual lens: near-term needs for secure connectivity and access and long-term goals for architectural transformation. IDC recommends buyers focus on the following considerations:

- **Clarify use cases early:** Identify whether the priority is secure remote access, SaaS visibility, or full policy consolidation. Many organizations deploy SSE in phases, often beginning with ZTNA or SWG.
- **Assess reporting depth:** Go beyond surface metrics. Demand dashboards that show policy change outcomes, chronic offenders, user/app impact, and predictive trendlines. Continuous improvement depends on proactive, business-oriented reporting rather than reactive ticket histories.
- **Define the operating model:** Decide upfront whether you want fully managed or comanaged service. For comanaged delivery, require a documented runbook with RACI, change windows, rollback plans, and emergency contacts to avoid gaps in accountability.

- **Pilot with business-critical flows:** Don't rely on synthetic testing. Validate SSE performance and policy impact on your top 3 applications with live users, ensuring break-glass access and SD-WAN failover are tested under production conditions.
- **Scrutinize service-level agreements (SLAs):** Look for providers that go beyond uptime guarantees. Differentiated SLAs should include commitments around time to detection, time to remediation, change accuracy, SOC feed availability, and security update cadence.
- **Evaluate integration depth:** Ensure the provider can unify SWG, CASB, and ZTNA policy and extend into identity, MDR, and compliance reporting for stronger zero trust execution.
- **Keep industry and regulatory alignment:** Prioritize providers with vertical expertise and proof of compliance support in your industry (e.g., HIPAA, PCI DSS, and GDPR).
- **Insist on migration playbooks:** Insist on detailed plans for transitioning from VPNs and on-premises gateways, including coexistence strategies and user adoption support.
- **Look for long-term road map:** Select providers whose vision extends SSE into broader secure access service edge (SASE) or zero trust architectures, with integration to SD-WAN, IAM, and advanced SOC capabilities.

## 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.

### British Telecom

British Telecom is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide managed SSE services vendor assessment.

British Telecom (BT), headquartered in London, United Kingdom, offers managed security service edge services as part of its broader secure networking portfolio. The company launched its managed SSE offering in 2022, leveraging its experience in delivering SD-WAN and global connectivity services to enterprise clients. BT's SSE portfolio is built around partnerships with prominent SSE technology vendors and is designed to offer deployment flexibility, service consistency, and integration with other BT-managed services.

BT structures its managed SSE services into three modular service tiers. The "Foundation" tier allows customers to set up the SSE environment, with BT managing it in life. The "Foundation Plus" tier adds deployment services, with BT responsible for both setup and ongoing management with proactive monitoring. The "Premium" tier builds on Foundation Plus by adding advanced security optimization and in-life technical design. Customers can choose their preferred level of involvement through a flexible service model that supports full management, comanagement, or self-service, depending on operational maturity and internal resourcing.

At the core of BT's managed SSE service is Eagle-i, BT's security orchestration and automation engine, which monitors customer traffic for threats and enriches alerts with business context. This includes identifying the infected endpoint, providing attribution intelligence on the threat actor, and assessing the risk to the organization. The system supports proactive customer notification and can trigger remediation actions across the portfolio, such as quarantining endpoints when availed by customers. In addition, BT's OneTest database supports internal testing and benchmarking of vendor features, allowing BT to identify gaps in partner solutions and collaborate on product improvements. This continuous feedback loop enhances BT's deployment expertise and helps ensure alignment between vendor capabilities and customer expectations.

Service delivery and management are underpinned by BT's Security Hub customer portal, where customers can view security posture, policy status, incident insights, and integration points with broader threat management systems. The portal also supports future road map initiatives, such as Risk360, a CISO-focused dashboard for visualizing cyber-risks and SaaS posture, and modular options for tailoring service requests and customer journeys.

In addition to the SSE components, BT's role as a global telco supports integration of underlay connectivity and SD-WAN, which can be bundled with SSE depending on the customer's architecture. While the focus remains on SSE, this network visibility enables BT to support unified policy enforcement across connectivity and security.

BT plans to continue investing in AI/ML-enabled capabilities within its SOC ecosystem. The Future SOC initiative will introduce user and entity behavior analytics (UEBA), autonomous threat sweeps, and deeper AI-assisted automation. These enhancements will be tightly integrated with the SSE offering, extending coverage from edge protection to endpoint and cloud detection and response.

## Strengths

BT's Eagle-i platform provides integrated analytics by correlating SSE, SD-WAN, and endpoint telemetry, enabling automated responses within a unified security context for faster, more efficient threat mitigation.

Through OneTest, BT offers real-world benchmarking across vendor solutions, helping customers evaluate capabilities and make more informed technology choices.

## Challenges

BT applies significant automation and orchestration across its network and SD-WAN services, and there is an opportunity to extend these same capabilities more deeply into its SSE operations. Expanding automation for policy management, provisioning, and routine incident handling could further streamline service delivery and reduce operational overhead for customers. BT is already investing in its Future SOC initiative, which incorporates AI/ML for analytics and threat detection, as well as automation of service support requests (SSRs) to drive efficiency and consistent customer experience for its customers.

## Consider British Telecom When

Consider BT when looking for a managed SSE service that supports multiple vendor technologies with flexible service tiers and strong integration with global SD-WAN and connectivity services.

# Comcast Business

Comcast Business is positioned in the Contenders category in the 2025 IDC MarketScape for worldwide managed SSE services vendor assessment.

Comcast Business (CB), headquartered in Philadelphia, United States, offers managed security service edge services as part of its broader managed networking and security portfolio. The service is delivered alongside its managed SD-WAN and SASE offerings, leveraging partnerships with multiple technology vendors, including Cisco, Fortinet, Versa, and Palo Alto Networks. CB supports both single-vendor and multivendor SSE architectures, allowing customers to deploy a complete stack from one OEM or combine components of network security functions from supported solution providers.

The managed SSE service is underpinned by CB's Managed Solutions Platform, which combines monitoring, orchestration, automation, and analytics. This platform uses third-party tools, along with vendor APIs and standard protocols, to collect and process network and security telemetry. Capabilities include automated configuration synchronization across devices, advanced fault correlation, AI/ML-driven performance monitoring, security event categorization, and severity-based alerting. A 24 x 7 security operations team monitors alerts, conducts triage, and coordinates incident response.

CB offers multiple delivery models to meet different operational preferences, including fully managed, comanaged, platform as a service, and managed takeover of existing customer infrastructure. Customers access the service through a digital portal providing visibility into service delivery, network performance, inventory, user management, billing, and comanagement integration with OEM platforms through SSO.

The service is designed to operate across hybrid and multicloud environments, supporting connectivity to public clouds, private clouds, and SaaS applications. CB's approach enables consistent policy enforcement and monitoring across network and security domains. Comcast Business combines its managed SSE with its broader connectivity portfolio, allowing integration with underlay services such as DIA, Ethernet, MPLS, LTE, satellite, and private 5G where required. This integration supports unified network and security policy management.

Future developments for the managed SSE service include further application of AI/ML in network and security operations and expansion of automation use cases. The acquisition of Nitel is expected to enhance service delivery scale and reach, particularly on the indirect channel.

## Strengths

Comcast Business delivers a flexible managed SSE architecture supporting both single-vendor and multivendor deployments. The service is complemented by managed EDR and MDR for expanded threat management and is underpinned by a broad connectivity portfolio that extends unified policy enforcement across security and network domains.

Comcast Business can also meet industry-specific compliance needs, offering FedRAMP-certified solutions for public sector clients and PCIaaS for retail and payment environments.

## Challenges

Current SLA commitments for the managed SSE service focus primarily on uptime and incident response time, with less definition around timelines for change management and incident resolution.

In addition, while CB has embedded extensive automation and AI within its network management services, the application of these capabilities to security provisioning, monitoring, remediation, and change requests is still developing. The provider is actively expanding its AI/ML road map, increasing automation use cases in security operations, and enhancing orchestration across network and security domains to address these areas over time.

### Consider Comcast Business When

Organizations that require a managed SSE service closely integrated with SD-WAN and underlay connectivity, with flexible vendor and deployment options, should consider Comcast Business' managed SSE offering.

## Deloitte

Deloitte is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide managed SSE services vendor assessment.

IDC notes that Deloitte did not actively participate in this IDC MarketScape, and its evaluation is based on IDC's knowledge of its managed SSE service.

Deloitte offers managed SSE as part of its broader managed SASE services portfolio, combining deep consulting expertise with operational delivery. Its approach is anchored in a consult-to-operate model that integrates advisory, solution design, and managed services, ensuring that SSE adoption is aligned with each client's digital transformation and risk management goals. With a global presence and a large delivery footprint, Deloitte positions itself as a partner capable of managing complex environments across industries and geographies.

The service is underpinned by strong alliances with various SSE vendors, including Netskope, Palo Alto Networks (Prisma Access), Zscaler, and Cisco, providing clients with flexibility to select the technology stack that better aligns with their existing infrastructure and strategic priorities. Beyond partnerships, Deloitte differentiates itself by embedding SSE within its broader managed services ecosystem. Planned integration with Deloitte's proprietary Cybersphere platform will provide enterprises with enhanced visibility, threat intelligence, and AI-driven automation, creating a unifying layer across multiple security domains.

Deloitte also leverages its Operate services to accelerate the value of SSE adoption. For example, digital identity services support zero trust access management, ensuring that policies extend seamlessly across SSE deployments. Similarly, Deloitte's MXDR services integrate with SSE enforcement points to provide rapid detection, correlation, and response to threats in real time. This cross-service alignment allows enterprises not only to deploy SSE but also to realize its business value faster, embedding SSE controls into a wider security operating model.

### Strengths

Deloitte's strength lies in its ability to embed SSE within complex global transformations, ensuring alignment with business and risk strategies. Its broad vendor partnerships and upcoming Cybersphere integration position it as a differentiated provider for enterprises seeking an end-to-end managed SSE experience.

### Challenges

Deloitte's consulting-heavy delivery model may be less suited for SMBs or organizations seeking turnkey, prepackaged SSE services.

Current operational automation is less mature than that of specialized providers, though investments in Cybersphere are aimed at closing this gap.

### Consider Deloitte When

Organizations with complex, global environments that require SSE to be tightly integrated into wider managed security programs should consider Deloitte's managed SSE offering.

## Deutsche Telekom

Deutsche Telekom is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide managed SSE services vendor assessment.

Deutsche Telekom (DT), headquartered in Bonn, Germany, offers managed security service edge services as part of its wider secure networking portfolio. The service builds on DT's experience in delivering managed network and security solutions to enterprise customers across Europe and globally, with integration into its extensive fixed and mobile connectivity capabilities. This enables unified policy enforcement and visibility across both network and security environments.

DT's managed SSE is vendor agnostic, supporting both single-vendor and multivendor deployments from a range of technology partners like Fortinet, Cisco, Zscaler, and Palo Alto Networks. Customers can align the service to their preferred technology stack while DT provides design, deployment, and operational management. Integration with DT's managed SD-WAN allows consistent security policy application across distributed locations and cloud environments. All SSE customers receive protection enhanced by DT's proprietary threat intelligence, derived from its telco network visibility and a global honeypot network of approximately 6,000 sensors, which is used to detect and respond to emerging threats.

The service is delivered through DT's global 24 x 7 security operations centers, providing centralized policy management, continuous monitoring, and incident response. Customers can opt for fully managed or comanaged service models, supported by a defined service-level agreement for critical incident resolution within four hours. The Secure Networking Platform serves as the customer portal, giving access to service delivery insights, inventory management, and network reporting, as well as management-plane integration with vendor platforms via single sign-on.

DT is expanding its automation capabilities with the development of EVA, an AI-driven interface that will allow customers to interact with their service inventory and operational data through natural language queries. As part of its road map, DT is also integrating a market-leading security information and event management (SIEM) platform into the Secure Networking Platform to enhance monitoring, unify SSE incident management, and improve reporting. Additional investments in AI/ML are planned to automate provisioning, policy enforcement, and threat detection, aiming to improve operational efficiency and responsiveness.

## Strengths

DT's proprietary threat intelligence, combining telco network data with insights from a global honeypot network, enhances the ability to identify and mitigate threats before they impact customers, supporting proactive risk reduction. The vendor-agnostic approach allows customers to align SSE delivery with existing technology strategies while maintaining consistent service management. Defined SLAs for critical incidents provide predictable resolution timelines, helping customers meet compliance and operational continuity objectives. Ongoing developments such as EVA and integrated SIEM aim to give customers faster access to actionable insights, streamlined incident management, and improved security reporting.

## Challenges

Deutsche Telekom continues to evolve the Secure Networking Platform to provide more integrated visibility across networking and security services. While customers can already access SSE security insights through connected vendor portals, DT is investing in the addition of a market-leading SIEM and automation features to further enhance unified monitoring, incident management, and reporting. These planned enhancements are designed to give customers more comprehensive and streamlined security visibility in the future.

## Consider Deutsche Telekom When

Organizations that require a flexible, vendor-agnostic managed SSE service with proprietary threat intelligence and integration into global connectivity and SD-WAN services should consider Deutsche Telekom's offering.

## GTT

GTT is positioned in the Contenders category in the 2025 IDC MarketScape for worldwide managed SSE services vendor assessment.

GTT, headquartered in Arlington, Virginia, offers managed security service edge services as part of its broader managed networking and security portfolio. The service builds on GTT's global tier 1 backbone, SD-WAN capabilities, and managed security operations to provide integrated policy enforcement and visibility across security and network environments.

GTT's managed SSE offering is available through technology partnerships with Fortinet and Palo Alto Networks, supporting both single-vendor and multivendor SASE architectures. Customers can deploy SSE as a cloud-delivered solution or through a customer premises equipment (CPE)-based approach via a vendor-specific device or GTT EnvisionEDGE. With EnvisionEDGE, customers can dynamically connect and sequence up to 10 virtualized network and security services, including routing, SD-WAN from multiple vendors, managed firewalls, monitoring tools, and observability agents. This platform enables rapid deployment of up to 16 pretailored configurations, allowing customers to align security and networking functions to specific business requirements.

The service is offered in three tiers. The Standard tier provides baseline deployment and operational management of SSE functions with access to the EnvisionDX portal for service visibility. The Premium tier adds enhanced monitoring, proactive optimization, and broader policy management. The Enterprise tier extends these capabilities with advanced customization, integration into complex environments, and increased service governance options. Across all tiers, GTT offers fully managed or comanaged operational models. The EnvisionDX portal consolidates network and service performance metrics, security event summaries, and service status tracking.

SSE delivery is supported by GTT's 24 x 7 security operations centers and a critical incident notification SLA of 15 minutes, although SLAs for resolution times and change management are not defined. All customers can also access adjacent security services, including managed detection and response, distributed denial-of-service (DDoS) protection, and web application and API protection (WAAP). GTT is developing an additional SSE single-vendor architecture based on the HPE Aruba technology stack, expanding deployment flexibility for future customers.

## Strengths

GTT leverages its global tier 1 backbone and extensive network infrastructure to deliver SSE with optimized performance for distributed workforces, branch locations, and cloud workloads. This integration enables consistent policy enforcement and reduced latency, allowing customers to maintain a unified security posture without compromising user experience.

## Challenges

While EnvisionDX provides consolidated service visibility, additional integrated SSE security reporting continues to evolve and may require customers to use technology partner portals for more detailed analytics. SLAs define incident notification timelines but do not cover resolution times or change management, which may require clarification during service scoping. GTT is addressing these areas through planned integration of enhanced incident management and reporting capabilities within the portal.

## Consider GTT When

Organizations seeking a managed SSE service integrated with a global tier 1 backbone, complemented by additional security services and centralized service visibility, should consider GTT's offering.

# HCLTech

HCLTech is positioned in the Leaders category in the 2025 IDC MarketScape for worldwide managed SSE services vendor assessment.

HCLTech, headquartered in Noida, India, offers managed security service edge services as part of its broader secure digital workplace and network transformation portfolio. The company delivers SSE as a vendor-agnostic service, integrating solutions from multiple technology partners, including Palo Alto Networks, Fortinet, Cisco, Netskope, and Zscaler, to address customer requirements across industries and geographies. Its proprietary SPADE framework is used to assess a customer's environment, determine solution fitment, and design the deployment architecture. This consultative assessment approach allows HCLTech to align SSE deployments with each customer's existing infrastructure, operational maturity, and security objectives.

The managed SSE service is operated within HCLTech's Cyber Security Fusion Center (CSFC) platform, which provides 24 x 7 monitoring, orchestration, and incident management. All SSE customers benefit from HCLTech's proprietary advanced threat intelligence, which combines curated feeds, analytics, and correlation across threat surfaces. The standard SSE package includes zero trust network access, secure web gateway, and firewall as a service. Additional capabilities, such as cloud access security broker, data loss prevention (DLP), and digital experience monitoring (DEM), are available as add-ons to extend the security stack based on customer requirements.

HCLTech offers flexible contracting models, including standard terms, the shortest contract commitment of six months, and on-demand contracts for proof-of-concept (POC) engagements. Service tiers provide different levels of operational support and integration, allowing customers to scale management depth and feature sets over time.

Service delivery is supported through a customer portal that integrates with ServiceNow and vendor management planes, with an automation layer in between. This automation platform, iNetBot, enables policy push into SSE components and accelerates configuration changes. The portal also provides advanced dashboarding by aggregating and integrating data from multiple vendor solutions for consolidated visibility. A new role-based access control (RBAC)–enabled AI dashboarding portal is planned for release, designed to enhance security event visualization, analytics, and user-specific access control.

HCLTech's future development focus includes expanding its lab infrastructure to test and validate SSE architectures, integrating generative AI (GenAI) use cases for threat detection, incident analysis, and automated policy recommendations, and further enhancing the automation capabilities within its operational framework.

## Strengths

HCLTech offers comprehensive SLA frameworks, covering not only availability and incident response but also a broad set of operational and performance parameters. This allows customers to set clear service expectations across multiple aspects of delivery. The SLA structure is supported by the SPADE assessment framework, CSFC-based management, proprietary advanced threat intelligence, and the iNetBot automation layer, which together provide consistent policy enforcement, faster configuration changes, and reduced operational effort. Flexible contracting options, including short-term commitments and on-demand POC agreements, give customers the ability to evaluate and scale services with minimal risk.

## Challenges

HCLTech's automation capabilities are strong in areas such as GenAI-enabled customer experience, SSE migration, and incident management, where they apply advanced orchestration to accelerate processes and improve outcomes. However, customer feedback indicates that automation for routine level 1 and level 2 service requests is less mature, requiring more manual handling than other parts of the service. HCLTech is addressing this gap by expanding its automation framework within the iNetBot platform to include more self-service and preconfigured workflows for common operational tasks.

### Consider HCLTech When

Organizations operating in complex, compliance-driven, and highly distributed environments that require a large systems integrator and managed service provider capable of delivering and managing SSE at scale should consider HCLTech's offering.

## IBM

IBM is positioned in the Leaders category in the 2025 IDC MarketScape for worldwide managed SSE services vendor assessment.

IBM, headquartered in Armonk, New York, delivers managed security service edge services as part of its global network security and transformation portfolio. The company takes a vendor-agnostic approach, partnering with multiple SSE technology providers, including Palo Alto Networks, Zscaler, Netskope, Cloudflare, and Cisco. This enables customers to align SSE deployments with preferred platforms while leveraging IBM's integration, operational management, and service delivery expertise.

The managed SSE service is operated through IBM's Virtual Security Operations Center (VSOC) platform, which integrates IT service management (ITSM) functions with vendor management portals to provide a single view of policies, incidents, and service requests. The platform supports both fully managed and comanaged models, with IBM providing 24 x 7 monitoring, policy enforcement, and change management through its global SOC network.

IBM has developed a set of AI-enabled capabilities aimed at accelerating provisioning, migration, and operational efficiency. AI agents can automate change requests initiated from chat and email, extract information from service support request tickets, and perform resolution tasks. Additional AI models are being developed to automate up to 60–80% of SSR handling, simulate deployment scenarios to support customer decision-making, and deliver SSE security posture assessments to measure compliance with industry and regulatory standards. For customers migrating between platforms, IBM offers an SSE migration toolkit to streamline the transition process.

A key differentiator in IBM's delivery approach is this agentic AI framework codenamed PULSE, designed to achieve faster time to value. PULSE can translate existing security policies, configurations, and compliance documents into SSE policy constructs, then automatically configure them on the target platform. It supports the creation of custom SSE policies and generates project artifacts such as implementation checklists, policy documentation, and references to solution configuration guides. PULSE also provides architecture design support, ensuring alignment between business requirements and technical implementation.

IBM's SSE service is available in modular tiers, allowing customers to start with core functions, such as secure web gateway, zero trust network access, and firewall as a service, and add capabilities like cloud access security broker, data loss prevention, and digital experience monitoring as required. While IBM X-Force threat intelligence is available, it is offered as an optional add-on rather than a default inclusion.

IBM plans to extend its offering to a fully managed SASE service by integrating its SSE capabilities with managed SD-WAN and networking services. Future enhancements will also expand the role of AI in automation, incident resolution, and policy management, along with further developing decision-support tools that allow customers to simulate the impact of different deployment and policy options before implementation.

### Strengths

IBM's broad ecosystem of SSE partnerships allows customers to deploy their preferred platform with centralized management, supported by a global SOC footprint. The PULSE framework accelerates time to value by translating and automating security policy configuration, reducing manual effort in deployment, and providing structured project deliverables. AI-enabled automation across change management, SSR handling, and migration tasks helps improve operational efficiency and streamline service delivery.

### Challenges

IBM provides strong service-level objectives (SLOs) as part of its standard service offering, and these can be tailored or made more aggressive based on individual customer requirements. However, unlike some providers, these commitments are positioned as SLOs rather than contractual SLAs, which may be a consideration for organizations in highly regulated or compliance-driven environments. Expanding the scope of formal SLA coverage would strengthen IBM's ability to meet the needs of customers that require enforceable service guarantees.

### Consider IBM When

Organizations seeking a vendor-agnostic managed SSE service with accelerated deployment capabilities, strong automation for policy translation and migration, and integration with existing ITSM and vendor portals should consider IBM's offering.

## LevelBlue

LevelBlue is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide managed SSE services vendor assessment.

LevelBlue is headquartered in Texas, United States. The company was spun off from AT&T in 2024 as a joint venture, with AT&T retaining a minority investment and two board seats. AT&T launched its managed SSE/SASE services in 2021, inherited by LevelBlue with the spin-off, which now serves clients globally through a network of security operations centers with follow-the-sun coverage.

LevelBlue's managed SSE services combine consulting and professional services to assess readiness, design strategies, and execute phased transformations. The service is delivered using an ITIL-based model and will be available in three tiers in 2026: Essentials, Advanced, and Premium. The Essentials tier will include deployment support such as integration, setup, and fine-tuning of policy and comanaged operations, providing basic monitoring and incident response. The Advanced tier will offer fully managed services, while the Premium tier will add compliance reporting, SLAs, and risk management add-ons. LevelBlue supports multiple vendors for SSE, including Palo Alto Networks (Prisma Access), Fortinet, Zscaler, and Cisco, allowing clients to integrate with existing infrastructures or select new solutions.

The service includes life-cycle support from design to ongoing management. Clients can request changes via email, a self-service portal or API, with LevelBlue handling configuration, policy updates, and fine-tuning. Automation features within vendor platforms are augmented by LevelBlue's proprietary Automated Policy Management (APM) platform for firewall management, which provides a consistent interface for interacting with multivendor firewalls. For SSE, this enables centralized threat detection and response. LevelBlue also offers adjacent services like risk management and continuous compliance support, integrating SSE with MDR for cross-environment visibility.

In 2025, LevelBlue expanded its existing MDR foundation and other adjacent security capabilities through the acquisitions of Trustwave, Stroz Friedberg, and Elysium from Aon. These additions strengthen the company's global footprint and extend its capabilities in risk management and digital forensics/incident response. For customers, this means enhanced MDR and digital forensics and incident response (DFIR) services, available to be integrated with SSE deployments, providing deeper threat intelligence, improved risk management, and broader access to LevelBlue's global SOC network and intelligence sources, including SpiderLabs.

LevelBlue maintains a partner ecosystem with various software vendors, ensuring interoperability and compliance with standards like GDPR and PCI DSS. The service emphasizes data residency through vendor platforms that support regional cloud instances. For multicloud environments, LevelBlue uses API integrations to apply consistent security policies across AWS, Azure, and Google Cloud.

LevelBlue plans to consolidate its USM Anywhere (for MDR) and APM platform into a unified security management platform by 2026, incorporating GenAI for policy recommendations and automation. Customers can expect expanded hosted SSE options for midmarket clients, deeper AI integration for threat intelligence, and enhanced cross-service dashboards for observability. This will likely reduce operational complexity and improve response times, with a focus on regulatory compliance.

### Strengths

LevelBlue's multivendor support for SSE allows clients to leverage existing investments in platforms like Palo Alto Networks or Zscaler while benefiting from centralized management.

LevelBlue has established MDR and threat intelligence capabilities, which are being expanded further through acquisitions. This expansion strengthens the company's ability to deliver integrated threat detection, risk management, and digital forensics/incident response alongside its SSE services. For customers, this translates into improved resilience, enriched context for security events, and faster response to complex threats.

### Challenges

LevelBlue's current customer portal lacks unified visibility across its full-service portfolio, requiring clients to navigate multiple interfaces for comprehensive management. The company is addressing this with a unified digital platform, planned for completion by 2026, which will consolidate visibility, policy management, and self-service capabilities into a single interface with AI-driven recommendations and role-based access control.

### Consider LevelBlue When

Enterprises seeking a managed SSE service with multivendor flexibility and strong MDR integration should consider LevelBlue. Midmarket clients looking for cost-effective managed SSE options may also benefit from LevelBlue's tiered model.

## Open Systems

Open Systems is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide managed SSE services vendor assessment.

Open Systems, headquartered in Zürich, Switzerland, delivers managed security service edge services as part of its broader managed security portfolio. The company operates its SSE offering on a proprietary architecture designed to provide high levels of automation, orchestration, and integration across customer environments. Delivery is comanaged, with services delivered through Open Systems' own security experts, designated account consultants and specialists from their global operations center, or with customers leveraging self-service tools in the customer portal. Centralized oversight and operational comanagement are made available through its custom-built configuration management database (CMDB).

The custom CMDB enables end-to-end orchestration and automated validation for any change or remediation, ensuring accuracy and reducing manual intervention during operational updates. This capability extends to provisioning, incident handling, and security policy enforcement, with the goal of maintaining consistency across distributed customer deployments. Open Systems is also extending its agentic AI capabilities directly to customers, enabling them to manage change requests and incidents through natural language interaction with the platform.

The SSE service integrates multiple threat intelligence feeds, which are available in two tiers to match different customer needs. Proprietary threat intelligence is applied directly to SSE policy and detection workflows, enhancing situational awareness and enabling faster threat prioritization. Customers can choose from modular service options to align SSE deployment with their existing architecture, and the service can be delivered standalone or integrated with other Open Systems managed network offerings.

Service commitments are backed by defined SLAs, including a 15-minute notification time for priority 1 incidents, one-hour time to start response, four-hour resolution time, and delivery of root cause analysis within three days. The customer portal offers visibility into SSE status, incident details, service metrics, and service reports and supports integration with customer ITSM platforms. Clients that are interested in detailed security and compliance reporting can get customized and tailored insights through their account management team.

Open Systems plans to introduce user and device risk scoring to all SSE services to enable more adaptive policy enforcement in addition to CASB, as well as a Copilot capability that will allow customers to query security data directly through the platform. These enhancements aim to further improve security decision-making and operational agility for customers.

## Strengths

Open Systems' proprietary CMDB and fully orchestrated change and remediation workflows reduce operational errors, improve accuracy, and shorten execution times. The extension of agentic AI to customers provides an additional layer of operational efficiency, allowing natural language interaction for incident and change management tasks.

### Challenges

Open Systems' broader security services portfolio, including managed email security and managed SSE, is relatively limited, with offerings such as managed detection and response delivered through partners rather than fully in house. While the SSE service is comprehensive, customers seeking a single provider for managed security services, including response, may need to supplement it with additional vendors. The company continues to focus on enhancing its SSE platform capabilities and building integrations to address more customer security needs over time.

### Consider Open Systems When

Organizations seeking a flexible and comanaged managed SSE service with high levels of automation, strong incident response SLAs, integrated threat intelligence, and the ability to directly interact with the platform through AI-enabled interfaces should consider Open Systems' offering.

## Orange Business

Orange Business is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide managed SSE services vendor assessment.

Orange Business, headquartered in Paris, France, delivers managed security service edge services as part of its broader secure networking and connectivity portfolio. Leveraging its position as a global telecommunications provider, Orange Business integrates SSE delivery with its managed SD-WAN, SASE, and underlay connectivity services to support unified policy enforcement and operational consistency across distributed environments. The service is supported by Orange Business' global operational footprint and SOC infrastructure, with delivery integrated into its Evolution platform for centralized customer visibility and control.

The company's SSE portfolio is vendor agnostic, integrating with various technology partners, including Netskope, Zscaler, Palo Alto Networks, and Fortinet, while applying Orange Cyberdefense's proprietary threat intelligence to all SSE customers. This intelligence, sourced from its global network visibility and internal research, is embedded into detection, analysis, and threat response workflows. The service can be delivered standalone or as part of a converged SASE deployment, providing flexibility in design and integration with existing security architectures.

Orange Business uses a modular delivery approach that allows customers to align SSE functions with their operational priorities. The service is backed by robust SLAs covering initial response time, incident updates, and resolution commitments for high-priority incidents, with differentiated service levels across Core, Standard, and Premium offerings. The Evolution platform provides the customer interface for SSE monitoring, configuration, and integration with other managed services. The company plans to expand this platform to provide end-to-end visibility of the customer's security environment, enabling a single-pane-of-glass experience across connectivity, network security, and SSE components.

Future enhancements include the integration of AI-driven compliance assessment for SSE configurations and designs, as well as generative AI capabilities for automated ticket classification, prioritization, routing, and resolution of complex, multi-provider incidents. Additional AI use cases under development include configuration anomaly detection and automated remediation, aimed at increasing operational accuracy and reducing time to resolution.

## Strengths

Orange Business' position as a global telco allows it to tightly integrate managed SSE with SD-WAN, SASE, and connectivity services, enabling consistent security policy enforcement across network layers. The application of proprietary threat intelligence to all SSE customers enhances detection accuracy and response prioritization, while the planned AI-driven compliance and ticket automation capabilities signal a continued focus on operational efficiency and service quality improvements.

## Challenges

Orange Business already invests in derisking SSE adoption through consulting support, outcome-focused workshops, and solution demonstrations that help customers align deployments with business and financial objectives. Expanding further into commercial derisking measures, such as structured pilot programs, try-and-buy options, or paid proof of concepts for complex environments, would provide prospects with even greater confidence in large-scale SSE transformations. These additions could complement Orange's current presales engagement model and strengthen customer decision-making at critical investment stages.

## Consider Orange Business When

Organizations seeking a managed SSE service with strong integration into global connectivity and SD-WAN, backed by proprietary threat intelligence and an evolving AI-driven operations road map, should consider the Orange Business offering.

# Tata Communications

Tata Communications is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide managed SSE services vendor assessment.

Tata Communications, headquartered in Mumbai, India, offers managed security service edge services as part of its broader secure networking portfolio. The company delivers SSE in partnership with various technology vendors, including Zscaler, Netskope, Palo Alto Networks, Cisco, and Fortinet, providing flexibility for customers to align technology selection with their security architecture and operational requirements. SSE can be deployed as a standalone service or integrated into broader managed SASE offerings alongside Tata Communications' SD-WAN and global connectivity services. Enterprises can align the service to their scale and requirements, with small and midsized organizations benefiting from a simplified, unified SASE offering built on Tata's global infrastructure to improve performance and optimize cost efficiency, while large enterprises with complex security needs can leverage consulting-led assessments and seamless integration through partnerships with various technology providers to address advanced use cases.

The TCx platform serves as Tata Communications' central service management and automation layer for SSE and other managed security services. For SSE, it provides management plane integration with partner solutions, enabling customers to view service health, initiate and track incidents, and implement policy changes from a single interface. TCx applies automation to routine operational processes such as firewall rule updates, configuration changes, and provisioning, reducing manual effort and ensuring consistent policy enforcement across environments. The platform's integration with vendor management planes allows near–real-time synchronization of changes, while embedded workflow orchestration helps standardize service requests and accelerate response times.

The SSE service integrates with Tata Communications' broader managed security ecosystem and global SOC operations. The service is backed by comprehensive SLAs that cover not only incident notification and resolution times but also change management activities.

Tata Communications Hosted SASE leverages its extensive global network infrastructure to support consistent performance and secure access for distributed workforces. Customers benefit from integration options that unify SSE policies with network-level controls, enabling consistent enforcement across multiple regions and user groups.

Tata Communications is focused on enhancing the TCx platform's automation capabilities, deepening integration with SSE vendor ecosystems. Future development efforts will also target broader visibility features, additional reporting capabilities, and more advanced orchestration to improve time to value for customers adopting SSE.

## Strengths

Tata Communications' TCx platform provides centralized service management with integrated visibility across network and SSE environments, simplifying operational control and enabling consistent policy management. The company's broad set of technology partnerships offers customers flexibility in selecting SSE components aligned to their specific architecture, supported by a global service delivery footprint.

## Challenges

While Tata Communications provides strong service management through the TCx platform, its automation capabilities for day-to-day operational tasks such as policy life-cycle management and fulfillment of standard service requests are still developing. Much of the focus today is on enabling policy administration and integrating with vendor management planes but opportunities remain to expand automation into closed-loop policy enforcement, auto-remediation of common SSRs, and proactive policy optimization. Enhancing automation in these areas would further reduce manual overhead, speed up service delivery, and improve the consistency of customer experience across complex multivendor SSE environments.

## Consider Tata Communications When

Organizations seeking a managed SSE service integrated with a global network backbone, vendor choice flexibility, and centralized service management through a unified platform should consider Tata Communications' offering.

# Telefónica

Telefónica is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide managed SSE services vendor assessment.

Telefónica, headquartered in Madrid, Spain, delivers managed security service edge services as part of its wider secure networking and cybersecurity portfolio. The company offers SSE in partnership with Zscaler, Netskope, Palo Alto Networks, and Cisco, providing customers with flexibility to align technology choices with their operational requirements and security architecture. Telefónica's SSE services can be deployed as a standalone managed security layer or integrated with broader SASE solutions that combine network security with the company's global connectivity and SD-WAN capabilities.

The service is supported by Telefónica's dedicated threat intelligence (TI) team, which operates its own threat intelligence platform (TIP). This intelligence is applied to all SSE customers, enhancing detection and prevention by incorporating indicators of compromise, adversary tactics, and emerging threat trends into protection policies. Telefónica delivers its managed SSE services through a centralized service portal that integrates ITSM capabilities, including ticket management, change requests, and incident tracking, with vendor management planes for configuration and monitoring. While the portal provides strong operational control, reporting and dashboarding are delivered through the native capabilities of the underlying vendor platforms rather than a proprietary interface.

Service performance is governed by service-level objectives rather than contractual SLAs. For priority 1 service disruptions, Telefónica targets a maximum resolution time of four hours for 95% of cases, and for priority 1 security incidents, the SLO for time to start responding is 30 minutes.

Telefónica is enhancing its SSE offering by integrating it with the company's SIEM and SOAR platforms to enable improved threat analysis, AI-driven threat detection, and tighter orchestration of incident response. These enhancements will also enable closer integration with the company's managed detection and response and digital forensics and incident response services. Additional planned capabilities include AI assistants to support SSE implementations and migrations, along with unified querying across vendor documentation to improve operational efficiency.

### Strengths

Telefónica's use of in-house threat intelligence from its dedicated TI team ensures that SSE policies and detections benefit from global adversary insights and tailored threat data. Its planned integration of SSE with SIEM, SOAR, MDR, and DFIR capabilities positions the service to deliver more comprehensive threat analysis and incident response for customers requiring deeper security orchestration.

### Challenges

While Telefónica's service portal offers robust ITSM functionality and seamless integration with SSE solutions' management planes, it currently offers a monthly service performance report and recommendations to improve security posture and controls but lacks proprietary unified reporting and consolidated dashboarding. Customers rely on the native reporting capabilities of the vendor solutions, which may limit cross-platform visibility.

### Consider Telefónica When

Organizations seeking a managed SSE service that integrates global threat intelligence with strong vendor technology choice and that can be extended into broader SOC workflows and managed detection services should consider Telefónica's offering.

## Verizon

Verizon is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide managed SSE services vendor assessment.

Verizon, headquartered in New York, United States, delivers managed security service edge services as part of its broader secure networking and cybersecurity portfolio. The company partners with Palo Alto Networks, Zscaler, and Versa Networks, giving customers flexibility in technology selection while leveraging Verizon's extensive global network and longstanding expertise in connectivity and network management. The offering is currently delivered as a fully managed service, with Verizon overseeing deployment, policy configuration, and day-to-day operations. In 2024, Verizon launched its Trusted Connection service, which will extend this model to allow customers to self-manage SSE components, providing additional flexibility in operational control.

Advanced threat intelligence is applied to all SSE customers, drawing on Verizon's global network visibility and security research to enhance detection, prevention, and policy tuning. SSE service delivery is supported by the Verizon Network-as-a-Service (NaaS) portal, which integrates directly with the management planes of partner SSE. Operational processes such as ticketing, change requests, and incident tracking are handled through Verizon's ServiceNow-based ITSM portal, ensuring mature process governance.

Unlike tiered offerings, Verizon's SSE service is delivered on a bespoke basis, tailoring scope, features, and operational workflows to match customer requirements, compliance needs, and existing security operations capabilities. This approach is particularly suited to organizations with complex architectures or multiregional deployments, where network integration and service customization are key.

Verizon plans to expand its Trusted Connection model to provide broader self-service capabilities and enhanced automation within the NaaS portal. Future development efforts will also focus on deeper integration between SSE and adjacent managed security services, leveraging Verizon's global reach and operational scale to deliver more cohesive security and network service experiences.

## Strengths

Verizon combines advanced threat intelligence integration with its global connectivity and network management expertise, enabling customers to unify network performance and SSE security operations under a single managed framework. The direct management plane integration via the NaaS portal, coupled with mature ITSM-based operational workflows, provides centralized visibility and streamlined control for complex, distributed environments.

## Challenges

Verizon does not currently provide defined SLAs for incident resolution. Organizations with strict compliance or governance requirements may need to define these parameters during the contracting phase to ensure alignment with internal service expectations.

### Consider Verizon When

Organizations requiring a managed SSE service that leverages global connectivity expertise, integrated threat intelligence, and the ability to customize delivery for complex, multisite, or compliance-driven environments should consider Verizon's offering.

## Vodafone

Vodafone is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide managed SSE services vendor assessment.

Vodafone, headquartered in London, United Kingdom, offers managed security service edge services as part of its broader secure networking portfolio. Leveraging its global telecommunications footprint, Vodafone combines network management, connectivity services, and security functions to support the delivery of integrated secure access service edge architectures. The managed SSE offering is built in partnership with Zscaler, Cisco, and Fortinet, providing customers with technology choice while benefiting from Vodafone's operational scale and established service delivery processes.

Vodafone structures its managed SSE services into three tiers: Lite, Standard, and Premium, enabling organizations to select the level of support and features that align with their operational maturity and resource availability. Customers can opt for "True Forward" Enterprise Agreements or Managed Services Enterprise Agreements, both of which are designed to protect against midyear overage charges, offering greater predictability in service costs.

For SSE migration and deployment, Vodafone applies its proprietary Vodafone Business DNA Design framework. This framework integrates feasibility tools to assess requirements and SLAs, then recommends optimal designs based on performance and operational considerations. For SSE services, the framework supports integration with provisioning systems through Vodafone Business DNA Provisioning, which enables bulk provisioning of configurations. AI/ML models are incorporated into the design process to accelerate architecture and template development, although the process does not include automated translation of security policies between platforms.

Service management is handled via Vodafone's customer portal, which provides ITSM capabilities and single sign-on access to partner vendor portals for detailed configuration and reporting. In the future, the portal will be enhanced with a GenAI-powered Copilot to support knowledge management and generate AI-driven insights, aimed at improving operational efficiency and decision-making. Vodafone supports its managed SSE offering with service-level agreements that go beyond notification. In addition to the 15-minute commitment for priority 1 incident notification, the company also provides SLAs for incident resolution and change management.

Vodafone plans to continue investing in AI-driven enhancements to its service delivery processes, including deeper integration of GenAI capabilities into its customer portal and expanded automation for architecture design and provisioning. These developments are expected to provide customers with more responsive, data-informed, and efficient SSE operations, further aligning with Vodafone's broader secure networking and connectivity portfolio.

## Strengths

Vodafone's ability to deliver managed SSE alongside its global connectivity and network management services supports cohesive SASE deployments, enabling unified operational oversight and consistent policy enforcement across network and security functions. The Vodafone Business DNA Design and Provisioning framework provides a structured and scalable approach to SSE migration and deployment, with embedded AI/ML models to accelerate architecture and template creation.

## Challenges

Vodafone's customer portal today provides ITSM capabilities and single sign-on access to partner vendor portals for detailed configuration and reporting. While this supports service management, customers still depend on vendor dashboards for deeper visibility and analytics. Vodafone plans to enhance the portal with a GenAI-powered Copilot for knowledge management and AI-driven insights, which should strengthen its ability to deliver unified, predictive reporting. Until then, expanding integrated analytics within the portal remains an opportunity to improve customer experience.

In addition, while SSE services are informed by the threat intelligence capabilities of its technology partners, the lack of proprietary advanced threat intelligence may limit differentiation for customers seeking deeper, customized threat analysis.

## Consider Vodafone When

Organizations seeking an integrated SASE deployment that combines global connectivity, managed network services, and flexible SSE delivery tiers should consider Vodafone's offering.

# Wipro

Wipro is positioned in the Leaders category in the 2025 IDC MarketScape for worldwide managed SSE services vendor assessment.

Wipro, headquartered in Bengaluru, India, delivers managed security service edge services as part of its broader cybersecurity and managed security offerings. The company partners with Netskope, Zscaler, Palo Alto Networks, and Cisco to provide customers with technology choice while leveraging Wipro's global MSSP capabilities and security operations experience.

Wipro's managed SSE is structured into three service tiers, designed to align with different customer maturity levels and operational needs. The entry tier provides foundational SSE management capabilities, including policy enforcement, monitoring, and vendor portal integration. The midtier builds on this with enhanced analytics, additional automation, and more proactive policy management. The highest tier offers fully managed SSE operations, advanced reporting, and tighter integration with Wipro's security operations framework for customers seeking end-to-end operational coverage.

To improve time to value, Wipro applies its proprietary ZTview framework for SSE readiness assessment and solution fitment. ZTview simulates user-to-application access scenarios to map needs, identify weaknesses, and generate optimized architectures based on those simulations. This process automates security policy design, enhances existing policies, and uses automated bots to validate policy effectiveness before deployment. These capabilities aim to shorten deployment cycles while improving the precision and relevance of applied security controls.

Service management is delivered through Wipro's MSSP customer dashboard, which integrates with SSE tools at the management layer to consolidate operational views. The dashboard supports the creation of trends and visualizations from aggregated data, helping customers track performance and security posture over time. This is enhanced by SMC AI, Wipro's AI-enabled platform that provides a natural language interface for querying security data and generates exclusive reporting by pulling data through APIs and overlaying risk scoring. SMC AI also powers a GenAI-based chatbot that assists with incident investigation, reporting queries, and operational decision support.

For operational assurance, Wipro offers an SLA for SSE services that includes a 15-minute notification time for priority 1 incidents and a four-hour resolution time, providing defined expectations for incident responsiveness. Wipro's automation capabilities, enabled by SMC AI and the ZTview framework, are also applied to policy life-cycle management, SSE posture monitoring, and remediation processes, supporting more efficient day-to-day operations.

Wipro plans to continue expanding the AI capabilities within its managed SSE portfolio, including deeper integration of SMC AI into its customer portal, expanded simulation and testing capabilities within ZTview, and greater automation of service requests and policy changes. These developments are expected to further streamline SSE operations and enhance the speed and accuracy of security decision-making for customers.

### Strengths

Wipro's combination of the ZTview framework and SMC AI provides customers with structured readiness assessments, policy simulation, and AI-driven operational insights, helping accelerate deployment timelines and enhance security policy precision.

### Challenges

Wipro's managed SSE services are optimized for solving complex, large-scale security and networking challenges, which may make the offering less aligned with the needs and budgets of SMB customers.

While the company has enhanced its services with AI use cases for deployment, migration, reporting, and visualization, its automation for certain operational use cases, such as routine service requests and low-level change management, is less mature. Wipro is actively working to expand these automation capabilities to deliver greater efficiency across day-to-day SSE operations.

### Consider Wipro When

Organizations operating in complex, compliance-driven, and highly distributed environments that require deep integration of SSE with a broad suite of managed security and IT services should consider Wipro's offering.

# 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

Managed security service edge (SSE) services provide organizations with a unified, cloud-delivered security architecture designed to protect users, applications, and data regardless of location. Delivered as a single converged solution, Managed SSE integrates core security capabilities, including secure web gateway (SWG), cloud access security broker (CASB), zero trust network access (ZTNA), and firewall as a service (FWaaS). Beyond technology delivery, managed SSE services encompass provider-led deployment, integration, ongoing policy management, and operation.

## Strategies and Capabilities Criteria

This section includes an introduction of market-specific weighting definitions and weighting values (see Tables 1 and 2).

## TABLE 1

## Key Strategy Measures for Success: Worldwide Managed Security Service Edge Services Provider

| Strategies Criteria | Definition | Weight (%) |
|---|---|---|
| Functionality or offering strategy | Plans to expand delivery capabilities, strengthen partnerships with SSE technology vendors, and enhance core functionalities; including the road map for automation and orchestration using AI/ML for policy enforcement, log analysis, and security actions, as well as R&D investments and targeted areas for service innovation | 40.0 |
| Customer experience and satisfaction strategy | Enhancements to customer portal capabilities, self-service features, and planned programs to increase customer involvement in road map development through executive advisory boards and advocacy initiatives | 18.0 |
| Portfolio benefits strategy | Road map for integrating and enhancing SSE services with other adjacent security offerings, along with the planned use of proprietary or third-party threat intelligence to strengthen security enforcement | 15.0 |
| Go-to-market and thought leadership strategy | Plans to improve sales decision support tools for derisking SSE adoption, thought leadership activities such as contributions to industry frameworks, publications, research, and active engagement in security forums, along with alignment of services to specific industry requirements | 15.0 |
| Pricing and packaging strategy | Planned developments in pricing models, service tier structures, and contract flexibility, including adjustments to enterprise agreements and options that improve customer value | 7.0 |
| Financial outlook strategy | Projected financial performance for SSE services, including funding, profitability, and growth expectations over the planning horizon | 5.0 |
| Total | | 100.0 |

Source: IDC, 2025

## TABLE 2

## Key Capability Measures for Success: Worldwide Managed Security Service Edge Services Provider

| Capabilities Criteria | Definition | Weight (%) |
|---|---|---|
| Functionality or offering | Breadth of SSE solution partnerships, global and regional service coverage, and delivery center network, including support for data sovereignty and localization requirements; incorporating current automation and orchestration capabilities using AI/ML for policy enforcement, log analysis, and customer-specific risk-based policy refinement; and assessing availability of proprietary frameworks, automation tools, and preconfigured templates for accelerating migrations and deployments, as well as current service SLAs beyond uptime | 45.0 |
| Customer experience and satisfaction | Quality and usability of customer portals, dashboards, and self-service capabilities, including operational, executive, and compliance reporting, with the ability to generate custom dashboards, policy enforcement insights, and compliance reports; also including customer satisfaction indicators such as CSAT, NPS, retention rates, and engagement through advisory boards | 18.0 |
| Portfolio benefits | Availability of additional security offerings that complement SSE, such as SOC services, incident response, security consulting, and MDR/XDR integration; including the use of proprietary or third-party threat intelligence to enhance SSE policy enforcement and threat detection | 15.0 |
| Go-to-market and thought leadership | Current tools and resources provided to support customer decision-making, such as ROI calculators, cyber-risk reduction quantification, and trial programs; including thought leadership activities, contributions to security frameworks, research publications, industry forum engagement, and alignment of services to specific industries with tailored accelerators, use cases, and reporting capabilities | 15.0 |
| Pricing and packaging | Current pricing models, service tier structures, and contract flexibility, including options for short-term, long-term, scale-up/down, and on-demand contracts; multiyear agreements; volume discounts; and flexible renewals | 7.0 |
| Total | | 100.0 |

Source: IDC, 2025

## LEARN MORE

### Related Research

- *Worldwide Managed Security Services Market Shares, 2024: Opportunity for All, in All Managed Security Areas* (IDC #US53101625, September 2025)
- *Secure Access Service Edge (SASE): Network and Security Convergence for the Hyper-Distributed Enterprise* (IDC #US53328325, May 2025)
- *IDC's Worldwide Security Services Taxonomy, 2025* (IDC #US53294625, April 2025)
- *Bridging the Gap: The Missing Piece in Managed SSE Providers' Market Messaging* (IDC #US53267425, March 2025)

### Synopsis

This IDC study presents a vendor assessment of worldwide managed security service edge (SSE) service providers through the IDC MarketScape model. Using the IDC MarketScape methodology, 15 providers with active managed SSE offerings were evaluated. The process included direct briefings with 14 providers and feedback from two or more customer references for each, while one provider's evaluation was based on IDC's independent knowledge of its services and capabilities. Providers were assessed on both their current capabilities and future strategies for delivering managed SSE services across regions worldwide.

"The managed security service edge (SSE) services market is evolving quickly as enterprises converge web, cloud, and private app security into unified, cloud-delivered frameworks. Providers bring diverse approaches, giving organizations more tailored options to accelerate zero trust adoption and simplify operations." — Yogesh Shivhare, research manager, Security and Trust, 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.