Singtel

2025 COMPANY OF THE YEAR

Driving impact across the customer value chain

RECOGNIZED FOR BEST PRACTICES IN THE SINGAPORE CYBERSECURITY SERVICES INDUSTRY

FROST & SULLIVAN

Table of Contents

Best Practices Criteria for World-class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each recognition category before determining the final recognition recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. Singtel excels in many of the criteria in the cybersecurity services space.

RECOGNITION CRITERIA

Visionary Innovation & Performance	*Customer Impact*
Addressing Unmet Needs	Price/Performance Value
Visionary Scenarios Through Megatrends	Customer Purchase Experience
Leadership Focus	Customer Ownership Experience
Best Practices Implementation	Customer Service Experience
Financial Performance	Brand Equity

The Transformation of the Cybersecurity Services Industry

The global cybersecurity services market continues to evolve as organizations encounter escalating volume and complication of cyber threats. Enterprises face a broader attack surface driven by hybrid cloud adoption, operational and information technology integration, remote work, and connected devices proliferation. These structural changes expose networks, data, and endpoints to increasingly complex risks, amplifying the need for real-time visibility, automated defense, and expert-led response.

Managed security service providers (MSSP) are essential partners in enabling digital resilience. Businesses across industries outsource cybersecurity operations to address talent scarcity, manage cost pressures, and navigate complex threat landscapes. The demand for continuous monitoring, incident response, and regulatory compliance drives organizations to adopt managed and professional security services that combine advanced technology, analytics, and domain expertise.

Within this broader market, the managed detection and response (MDR) segment has emerged as one of the fastest growing areas in cybersecurity services. This growth reflects various factors including cybersecurity talent shortages, high cost of establishing internal security operations centers (SOC), and rise of state-sponsored and criminal cyberattacks. MDR and MSS solutions leverage artificial intelligence (AI), machine learning, and automation to accelerate detection, investigation, and containment, creating scalable and adaptive security operations.

AI-driven analytics and automation continue to transform managed security. Generative and agentic AI support human analysts, automate repetitive tasks, and provide context-aware insights. MSSPs integrate these capabilities into unified security architectures that merge detection, response, and compliance functions within a single platform. This convergence enables higher precision, operational efficiency, and consistent protection across distributed environments.

> *"Frost & Sullivan finds that by aligning commercial strategy with national priorities, Singtel builds sustained customer confidence, supporting its leadership in Singapore's evolving cybersecurity space."*
>
> ***- Vivien Pua***
> ***Senior Industry Analyst***

Asia-Pacific (APAC) has become a focal region for cybersecurity services. While North America and Europe lead in maturity and revenue, APAC's rapid digital transformation, evolving regulatory frameworks, and growing enterprise security awareness sustain growth potential. Organizations in this region prioritize local service delivery, data sovereignty, and compliance alignment.

Small and medium-sized businesses (SMB) are an expanding market segment. Many operate with limited resources and insufficient in-house expertise. Governments and service providers collaborate to deliver bundled, affordable managed protection and training programs that enhance resilience. Human Risk Management solutions, driven by AI and behavioral analytics, complement these efforts by addressing the human dimension of cybersecurity.

Cybersecurity service providers differentiate through platform unification, automation depth, and integration breadth. Leading MSSPs embed identity threat detection, behavioral analytics, and continuous threat exposure management frameworks to improve prevention capabilities. They also invest in regional SOC presence, strengthen partnerships, and apply AI-enhanced orchestration to increase precision, efficiency, and scalability. Across markets, proactive prevention and regulatory alignment define the benchmark for modern cybersecurity operations, delivering resilience in an evolving digital environment.

Advancing National Cyber Resilience through Integrated Quantum Safe Security

Singapore Telecommunications Limited (Singtel) strengthens Singapore's cybersecurity industry through an integrated model that combines infrastructure control with advanced security capabilities. The company positions cybersecurity as a fundamental pillar of national digital resilience by integrating security across network, cloud, and connectivity assets. This structure enables consistent protection from enterprise environments to national programs.

Singtel advances the country's cyber readiness through partnerships with Singapore's Infocomm Media Development Authority (IMDA). The company has been appointed to develop Singapore's National Quantum-Safe Network Plus, establishing a quantum-resilient communication backbone to protect national systems against future quantum threats. It deployed quantum key distribution (QKD) nodes across Singapore and built a multi-vendor quantum ecosystem through partnerships with technology leaders including ID Quantique (IDQ), Cisco, Fortinet, and Palo Alto Networks. This model provides flexibility to integrate quantum-safe protection into existing infrastructure without vendor lock-in.

The company supports this strategy through the launch of its Hybrid Quantum-Safe Network (QSN) for enterprises. Hybrid QSN combines QKD with post-quantum cryptography (PQC), enabling enterprises to apply physics-based protection for mission critical links and use software-based PQC for remote, regional, and international sites. Singtel offers Hybrid QSN as a managed service as part of its broader cyber security collaboration with ecosystem partners including IDQ, Cisco, Fortinet, and Palo Alto Networks. Taken together with NQSN+, this milestone positions Singapore as the first country in Southeast Asia to offer both nationwide and hybrid commercial quantum-safe communications for enterprises at scale.

Singtel accelerates quantum adoption through a structured customer engagement program that includes education workshops, integration testbeds, and full operational assessment. This path reduces uncertainty and gives enterprises hands-on validation in real environments. Early adoption spans public and private sectors, including financial services and critical infrastructure operators.

The company also contributes to national resilience by enabling cybersecurity adoption among SMBs in Singapore. Partnering with IMDA and Enterprise Singapore, Singtel introduced the Cyber Protect Programme. The program targets to provide 49,000 SMBs with complimentary Mobile Protect and Broadband Security for the first year, along with subsidized access in the second year.[1] It bundles network-level protections such as malicious URL filtering and content screening into broadband and mobile subscriptions. This public–private partnership is designed to close the protection gap between large enterprises and smaller organizations**.**

Through these initiatives, the company sets a national benchmark for practical and scalable cybersecurity adoption. Frost & Sullivan finds that by aligning commercial strategy with national priorities, Singtel builds sustained customer confidence, supporting its leadership in Singapore's evolving cybersecurity space.

Delivering High Performance Managed Security Operations through Centralized Control

Singtel maintains full operational control of its MSS through a centralized multi-tenant security operations center. Its Advanced Security Operations Centre (ASOC) delivers round-the-clock managed security services across industries while maintaining strict client segregation and consistent service quality. The ASOC operates on a unified case management and analytics platform that integrates proprietary threat intelligence, automation, and big data analytics to provide a 360-degree view of the threat landscape.

Frost & Sullivan notes that Singtel's tiered analyst structure ensures speed and specialization throughout the incident-handling process. Level 1 analysts manage triage, Level 2 engineers conduct in-depth investigations and refine detection rules, and Level 3 specialists perform proactive threat hunting and incident response. Each escalation follows codified playbooks and runbooks that embed lessons from previous incidents, creating a continuous-learning cycle that improves operational consistency. Automation through security orchestration, automation, and response systems accelerates containment and recovery while maintaining human validation at critical decision points. These measures balance efficiency with analytical oversight to maintain high service quality.

The company applies AI-driven analytics and behavioral modeling to identify new risks, reduce false positives, and accelerate containment. Singtel integrates advanced detection rules and customized behavioral analytics into a unified platform that allows faster response times and minimizes analyst

[1] https://www.singtel.com/about-us/media-centre/news-releases/singtel-enterprise-singapore-and-infocomm-media-development-authority-launch-cyber-protect-programme0

workload. Analysts leverage global threat intelligence from its ecosystem partners to contextualize alerts, ensuring timely and precise mitigation.

The company complements its operations with an MSS portfolio that extends its ASOC capabilities across services that provide Managed Threat Monitoring and Detection, Managed Security Devices and Platforms and DDoS protect. Each service provides real-time monitoring, AI-powered analytics, and 24/7 protection supported by certified security specialists trained in penetration testing, digital forensics, and incident response. Through its Managed Security Devices portfolio, Singtel also monitors firewalls, intrusion detection/prevention system, email gateways, and endpoint protection systems.

Singtel further differentiates its operational excellence through its Managed Security Platforms, which unify threat management across networks, endpoints, and cloud environments. This platform consolidates security controls, threat intelligence, and compliance reporting into a single interface, enabling customers to maintain visibility, reduce operational complexity, and align with regulatory requirements. Its locally supported, globally benchmarked model gives enterprises cost-effective protection with predictable investment and scalable performance.

> *"Frost & Sullivan observes that Singtel delivers reliable MSS through full infrastructure oversight, standardized procedures, and a defined compliance roadmap. The company's framework represents a sustainable model for cybersecurity operations."*
>
> ***- Ain Sarah Aishah***
> ***Best Practices Research Analyst***

These automated and procedural safeguards operate under strict governance and measurement frameworks. Singtel's ASOC is ISO 27001-certified, and its infrastructure services carry additional attestations such as Outsourced Service Provider Audit Report (OSPAR) relevant to financial-sector requirements. The company continues to expand its compliance coverage in line with global standards such as SOC 2.[2] It reinforces operational assurance through post-incident retrospectives and regular red-team simulations and purple-team exercises that evaluate detection accuracy and analyst readiness.

Frost & Sullivan observes that Singtel delivers reliable MSS through full infrastructure oversight, standardized procedures, and a defined compliance roadmap. The company's framework represents a sustainable model for cybersecurity operations. This structure enhances service reliability, reduces operational friction, and ensures a consistent customer experience.

Providing Converged Connectivity and Security through Infrastructure Integration

Singtel integrates cybersecurity into its connectivity and cloud infrastructure, turning the network into a built-in security layer. This convergence differentiates it from security vendors that rely on overlay models or third-party gateways. Through this approach, the company ensures consistent protection and visibility across distributed environments, aligning security enforcement with network performance.

Its Secure Access Service Edge and Secure Service Edge (SSE) offerings unify secure internet access, private access, and Software-Defined Wide Area Network (SD-WAN) for hybrid and global enterprises. Enterprises use Singtel's global network, SD-WAN and SSE integration to maintain consistent security policies across

[2] Ibid

regions. The company extends this integration through CUBΣ, which applies advanced AI-driven analytics to network and security telemetry. The platform consolidates multi-source data into real-time dashboards, enabling faster anomaly detection, and enhanced proactive response across environments.

Singtel's ability to integrate network, cloud, and security functions into a unified operating model establishes a differentiated position in the regional cybersecurity landscape. Frost & Sullivan finds that this model combines extensive network reach, embedded analytics, and ecosystem collaboration to create measurable performance and operational transparency. The company enables enterprises to scale security consistently across environments while maintaining compliance with global standards.

Expanding Cybersecurity Adoption through Accessible Programs and Education

The Cyber Protect Programme provides a funded pathway for SMBs to adopt security through bundled network-level safeguards. Mobile Protect and Broadband Security filter malicious traffic at the network layer and remove cost barriers that commonly prevent smaller companies from adopting protection. Singtel complements this strategy with the Cyber Elevate Programme, offering awareness training and advisory programs tailored to varying organizational maturity levels. It extends these initiatives through the Cyber Security Institute (CSI), delivering targeted programs from board briefings and management training to Cyber Range exercises, First Incident Responder training, and automated phishing campaigns, enabling organizations to build capability across leadership, technical operations, and end users.

These initiatives strengthen the human layer of defense, complementing Singtel's technological offerings. CSI programs help enterprises shorten breach containment times and improve coordination between technical and non-technical functions, fostering a unified cyber readiness culture. Aligning technical capability with user education reduces operational risk and enhances customers' ability to manage threats independently.

Operationally, Singtel reinforces its empowerment model through transparent onboarding and service delivery practices. Customers receive structured reporting, defined escalation paths, and periodic performance reviews aligned with service-level objectives. These standards apply consistently across enterprise and SMB clients, ensuring reliability and accountability regardless of customer size.

This inclusive model differentiates Singtel from global MSS providers that primarily target large enterprises. In Singapore, the company's dual focus on enterprise and SMB segments enables broader market reach and strengthens brand trust. Its national presence and infrastructure ownership further enhance accessibility, allowing security features to be efficiently distributed.

Through these initiatives, Singtel drives widespread cybersecurity adoption across Singapore's business space. Frost & Sullivan acknowledges the company for transforming cybersecurity from a specialized function into an accessible business capability, solidifying digital confidence and long-term customer relationships built on trust, value, and measurable outcomes.

Conclusion

Singtel demonstrates the strength of an enterprise that unites national purpose with commercial execution. The company integrates cybersecurity, connectivity, and cloud infrastructure to transform digital protection into a measurable and scalable service capability. Its initiatives reflect strategic discipline that links innovation to real outcomes. Each development aligns with Singapore's long-term digital priorities and creates a defensible leadership position grounded in infrastructure ownership, operational control, and trusted ecosystem partnerships. Singtel also shows the maturity expected of a leading cybersecurity service provider. Its Advanced Security Operations Centre, artificial intelligence driven analytics, and unified security platforms create a consistent framework for proactive defense. The company embeds automation, threat intelligence, and behavioral modeling into service delivery to ensure reliability and transparency. This operational precision extends to its governance, training programs, and regional collaborations, strengthening customer confidence and reducing systemic risk across sectors. Its combination of human expertise, data-driven intelligence, and continuous innovation establishes a sustainable foundation for regional leadership. Singtel's integrated model sets a forward-looking standard for cybersecurity service delivery.

With its strong overall performance, Singtel earns Frost & Sullivan's 2025 Singapore Company of the Year Recognition in the cybersecurity services industry.

What You Need to Know about the Company of the Year Recognition

Frost & Sullivan's Company of the Year Recognition is its top honor and recognizes the market participant that exemplifies visionary innovation, market-leading performance, and unmatched customer care.

Best Practices Recognition Analysis

For the Company of the Year Recognition, Frost & Sullivan analysts independently evaluated the criteria listed below.

Visionary Innovation & Performance

Addressing Unmet Needs: Customers' unmet or under-served needs are unearthed and addressed to create growth opportunities across the entire value chain

Visionary Scenarios Through Megatrends: Long-range scenarios are incorporated into the innovation strategy by leveraging mega trends and cutting-edge technologies, thereby accelerating the transformational growth journey

Leadership Focus: The company focuses on building a leadership position in core markets to create stiff barriers to entry for new competitors and enhance its future growth potential

Best Practices Implementation: Best-in-class implementation is characterized by processes, tools, or activities that generate consistent, repeatable, and scalable success

Financial Performance: Strong overall business performance is achieved by striking the optimal balance between investing in revenue growth and maximizing operating margin

Customer Impact

Price/Performance Value: Products or services offer the best ROI and superior value compared to similar market offerings

Customer Purchase Experience: Purchase experience with minimal friction and high transparency assures customers that they are buying the optimal solution to address both their needs and constraints

Customer Ownership Excellence: Products and solutions evolve continuously in sync with the customers' own growth journeys, engendering pride of ownership and enhanced customer experience

Customer Service Experience: Customer service is readily accessible and stress-free, and delivered with high quality, high availability, and fast response time

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty, which is regularly measured and confirmed through a high Net Promoter Score®

Best Practices Recognition Analytics Methodology

Inspire the World to Support True Leaders

This long-term process spans 12 months, beginning with the prioritization of the sector. It involves a rigorous approach that includes comprehensive scanning and analytics to identify key best practice trends. A dedicated team of analysts, advisors, coaches, and experts collaborates closely, ensuring thorough review and input. The goal is to maximize the company's long-term value by leveraging unique perspectives to support each Best Practice Recognition and identify meaningful transformation and impact.

		VALUE IMPACT	
STEP		WHAT	WHY
1	**Opportunity Universe**	Identify Sectors with the Greatest Impact on the Global Economy	Value to Economic Development
2	**Transformational Model**	Analyze Strategic Imperatives That Drive Transformation	Understand and Create a Winning Strategy
3	**Ecosystem**	Map Critical Value Chains	Comprehensive Community that Shapes the Sector
4	**Growth Generator**	Data Foundation That Provides Decision Support System	Spark Opportunities and Accelerate Decision-making
5	**Growth Opportunities**	Identify Opportunities Generated by Companies	Drive the Transformation of the Industry
6	**Frost Radar**	Benchmark Companies on Future Growth Potential	Identify Most Powerful Companies to Action
7	**Best Practices**	Identify Companies Achieving Best Practices in All Critical Perspectives	Inspire the World
8	**Companies to Action**	Tell Your Story to the World (BICEP*)	Ecosystem Community Supporting Future Success

*Board of Directors, Investors, Customers, Employees, Partners

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

The Growth Pipeline Generator™

Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.

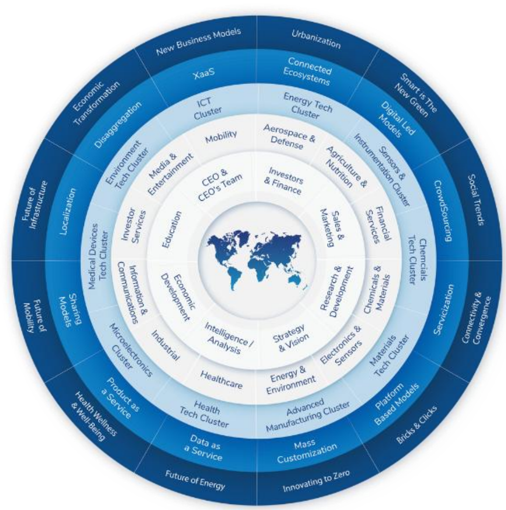
Learn more.

Key Impacts:

- **Growth Pipeline:** Continuous Flow of Growth Opportunities
- **Growth Strategies:** Proven Best Practices
- **Innovation Culture:** Optimized Customer Experience
- **ROI & Margin:** *Implementation Excellence*
- **Transformational Growth:** Industry Leadership

The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.



Analytical Perspectives:

- Megatrend (MT)
- Business Model (BM)
- Technology (TE)
- Industries (IN)
- Customer (CU)
- Geographies (GE)