FROST & SULLIVAN

BEST PRACTICES

2026 SINGAPORE CYBERSECURITY SERVICES

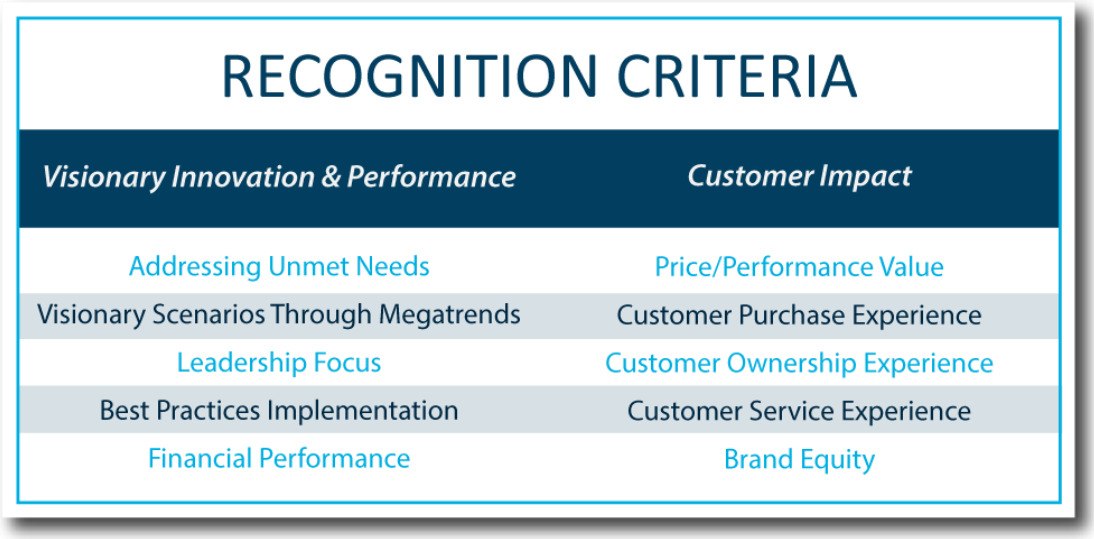
COMPANY OF THE YEAR

Singtel

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.



The Transformation of the Cybersecurity Services Industry

Organizations in Singapore continue to advance their digital transformation agendas, with widespread adoption of cloud computing, software-as-a-service platforms, and connected technologies embedded into core operations. This shift reflects the country's highly digitalized economy, where enterprises rely on scalable, always-on infrastructure to support growth and innovation. However, these technologies also expand the attack surface, exposing organizations to a broader and more complex threat landscape. As digital environments grow, businesses face increasing volumes of sophisticated and targeted cyber threats that challenge traditional security approaches.

These dynamics place significant strain on internal security teams, which must manage rising alert volumes while maintaining continuous monitoring and meeting evolving regulatory expectations. At the same time, limited availability of experienced cybersecurity professionals constrain organizations' ability to scale in-house capabilities. As a result, enterprises are reassessing how they allocate cybersecurity resources, prioritizing efficiency and resilience. Many organizations are turning to external service models to access specialized expertise and 24/7 monitoring capabilities, enabling them to strengthen security postures without significantly increasing internal costs or operational complexity.

As traditional security solutions fail to address modern threats effectively, organizations shift toward managed security services (MSS) and professional security services (PSS) to strengthen their defenses. MSS providers deliver 24/7 monitoring, threat detection, and incident response, enabling organizations to offload resource-intensive tasks while maintaining a strong security posture. This model offers access to skilled professionals and comprehensive solutions without the burden of expanding internal teams. Consequently, the MSS and PSS market in Asia-Pacific (APAC) continues to grow, with a projected

compound annual growth rate of 10.7% from 2022 to 2027, reflecting sustained demand for outsourced cybersecurity capabilities.[1]

Leading providers, such as Singtel, illustrate how the industry evolves to meet these needs. The company leverages its regional presence and regulatory licensing under Singapore's Cybersecurity Act to deliver integrated MSS and PSS offerings, including real-time monitoring, managed threat detection and response, cloud security, and incident management. It also supports clients through consulting, cyber architecture design, and digital forensics, while expanding into managed secure service edge solutions to protect cloud access and remote work environments. With strong regional growth, the company demonstrates how providers capitalize on digital transformation trends to deliver scalable, end-to-end cybersecurity services that align with evolving enterprise demands.[2]

Powering Secure Digital Futures

Singtel stands at the forefront of Asia's communications technology landscape by positioning cybersecurity as an inseparable component of the network rather than a standalone function. The company differentiates itself through its ability to converge connectivity, security, and intelligence into a unified operational model that transforms fragmented security stacks into a single, policy-driven, intelligence-led framework. By embedding security directly into the network fabric, Singtel enables enterprises to enforce policies consistently, strengthen visibility across environments, and respond to threats more effectively across users, devices, applications, and cloud infrastructures. This integrated approach allows organizations to address cybersecurity challenges comprehensively while aligning protection strategies with broader operational and business objectives. Unlike traditional cybersecurity providers, Singtel combines telecom-grade infrastructure, network intelligence, and managed cybersecurity capabilities within a single operational ecosystem. This enables the company to secure traffic flows, identities, applications, and edge environments at scale while delivering the resilience, visibility, and performance expected from mission-critical communications infrastructure

> *"Frost & Sullivan recognizes Singtel for its ability to deliver integrated, network-centric cybersecurity solutions that combine technological innovation, strong regional expertise, and a customer-focused approach to address the evolving security needs of modern enterprises."*
>
> ***- Natalia Casanovas***
> ***Best Practices Research Analyst***

This integration allows customers to secure their digital operations end-to-end while maintaining seamless connectivity across systems, users, and environments. By embedding security directly into network infrastructure, the company creates a differentiated value proposition that strengthens resilience and simplifies cybersecurity management for organizations navigating complex Information Technology ecosystems.

Singtel has built a strong reputation as a trusted cybersecurity partner, particularly among large enterprises in Singapore and across the region. Its established local presence, combined with extensive domain expertise, allows the company to deliver tailored, context-aware solutions that global competitors

[1] *Asia-Pacific (APAC) Managed and Professional Security Services*. Frost & Sullivan. (2023, December 22).
[2] Ibid.

often struggle to replicate. Organizations benefit from Singtel's ability to provide consistent support, deep market understanding, and fully integrated services that address operational and strategic security requirements.

Guided by a clear purpose to harness technology for positive impact, Singtel aligns its business strategy with innovation, sustainability, and customer-centricity. Through its Singtel28 strategy, the company focuses on strengthening core operations, scaling growth engines, and advancing digital infrastructure and services. By consolidating fragmented networking and security operations into a unified service model, Singtel helps enterprises reduce operational complexity, improve policy consistency, accelerate incident response, and strengthen cyber resilience across hybrid and multi-cloud environments

Frost & Sullivan recognizes Singtel for its ability to deliver integrated, network-centric cybersecurity solutions that combine technological innovation, strong regional expertise, and a customer-focused approach to address the evolving security needs of modern enterprises.

Securing the Unseen

Organizations in Singapore face increasing difficulty keeping pace with the growing complexity of their digital environments. As enterprises adopt hybrid networks, multi-cloud architectures, and Internet of Things (IoT) deployments, traditional security models no longer provide consistent visibility or control across systems. These limitations create fragmented security postures, making it difficult for businesses to monitor assets effectively and respond to threats in a coordinated manner. Singtel addresses these challenges by designing solutions that unify connectivity, security, and intelligence within a single operational framework. This approach enables enterprises to move away from disjointed security strategies and establish more cohesive protection across their digital environments, improving visibility, control, and overall resilience.

Singtel identified a critical unmet need in the market: the inability of organizations to manage diverse infrastructure environments that span multiple vendors, geographies, and technologies. Many enterprises operate with a mix of local connectivity providers, cloud platforms, and legacy systems, which creates blind spots in monitoring and threat detection. The company addresses this challenge through its multi-vendor managed services model and CUBE platform, which provide real-time visibility into network performance and security posture through a single interface. This approach eliminates silos between IT and security teams, enabling faster decision making and more coordinated responses across complex environments. By integrating best-of-breed technologies within a unified policy and operational framework, Singtel enables customers to maintain consistent control, manage risks more effectively, and simplify operations across heterogeneous infrastructures.

The company also addresses the growing complexity of IoT and edge ecosystems. Enterprises increasingly deploy connected devices across campuses, logistics networks, and industrial environments, yet they lack effective methods to secure these endpoints. Singtel integrates device-level identity and network-based authentication into its cybersecurity framework, ensuring that even agentless devices remain protected. This innovation strengthens security coverage in areas where traditional endpoint solutions cannot operate.

In addition, Singtel recognizes that enterprises face operational strain due to limited cybersecurity expertise. Internal teams often struggle to manage alert volumes and respond to incidents in real time. By offering flexible managed and co-managed security models, the company supports organizations with augmenting internal capabilities while maintaining control over sensitive environments. This adaptability ensures that customers receive tailored support aligned with their operational maturity.

Through these initiatives, Singtel closes critical gaps in visibility, scalability, and expertise, enabling organizations to navigate increasingly complex threat landscapes with confidence.

Engineering the Future

Singtel builds its cybersecurity strategy around the convergence of key megatrends, including cloud adoption, 5G expansion, artificial intelligence (AI) integration, and the proliferation of IoT devices. The company anticipates how these trends reshape enterprise environments and proactively develops solutions that align with future operational demands. Its "connected intelligence" vision reflects a forward-looking approach that integrates networking, security, and analytics into a unified ecosystem.

The rise of 5G and edge computing introduces new use cases such as autonomous systems, smart infrastructure, and real-time analytics. Singtel leverages its ownership of network infrastructure to embed security directly into these environments, enabling secure connectivity at the edge. Its integration of cellular-based identity and security policies ensures that devices remain protected even when they operate outside traditional network perimeters.

AI plays a central role in Singtel's long-term vision and operational strategy. The company applies AI across the cybersecurity operations lifecycle, spanning telemetry correlation, anomaly detection, automated triage, orchestration, and remediation. By integrating AI-driven operational intelligence into its service delivery framework, Singtel reduces mean time to detect and respond (MTTD/MTTR), minimizes alert fatigue, and enables security teams to focus on high-impact threats and strategic risk management. The company also proactively develops governance and security guardrails for AI-driven and agentic environments, recognizing that autonomous systems will become foundational to next-generation enterprise operations. Through its AI Studio platform, the company enables customers to extract actionable insights from network and security data, bridging the gap between raw telemetry and decision-making. This capability positions enterprises to transition from reactive security models to predictive and adaptive frameworks.

Singtel also anticipates the growing importance of securing AI-driven environments. As organizations adopt agent-based workflows and automated decision systems, new vulnerabilities emerge. The company actively explores guardrails and protection mechanisms for AI agents, ensuring that automation enhances security rather than introducing new risks. This proactive stance demonstrates a deep understanding of how emerging technologies redefine cybersecurity requirements.

By aligning its strategy with global megatrends, Singtel equips organizations to operate securely in a future defined by hyperconnectivity, automation, and intelligent systems.

Driving Excellence

Singtel's leadership team drives a clear and consistent vision centered on integration, innovation, and customer-centricity. The company moves beyond traditional telecommunications by positioning itself as a comprehensive digital services provider that combines connectivity with advanced cybersecurity capabilities. This strategic direction allows Singtel to differentiate itself in a highly competitive market.

Leadership places strong emphasis on unifying networking and security functions, recognizing that enterprises increasingly demand integrated solutions. At the core of Singtel's strategy is the Singtel CUBΣ platform, a unified digital orchestration and intelligence layer that converges networking, cybersecurity, observability, and analytics into a single operational environment. By eliminating silos between IT, network, and security domains, the platform enables enterprises to orchestrate policies consistently, automate workflows, gain real-time operational visibility, and accelerate threat response across distributed infrastructures

The organization also prioritizes innovation through strategic partnerships. Collaborations with leading technology providers enable Singtel to incorporate best-in-class solutions into its ecosystem while maintaining flexibility for customers. These partnerships support continuous enhancement of capabilities across SD-WAN, secure service edge, and managed security services.

> *"Through disciplined execution and continuous optimization, Singtel establishes a robust operational framework that delivers consistent, high-quality cybersecurity services across diverse environments. Frost & Sullivan applauds the company for executing a best-practice-driven strategy that combines automation, operational discipline, and innovation to deliver consistent, scalable, and high-impact cybersecurity services."*
>
> ***- Vivien Pua***
> ***Senior Industry Analyst***

Internally, Singtel fosters a culture of continuous improvement and accountability. Teams focus on developing automation frameworks, refining service delivery models, and enhancing customer engagement processes. Leadership encourages experimentation with emerging technologies, such as AI and digital twins, ensuring that innovation translates into tangible value for customers.

Singtel's leadership approach balances long-term vision with practical execution, enabling the company to adapt quickly to evolving market demands while maintaining a strong focus on customer outcomes.

Precision in Practice

Singtel translates its strategic vision into execution through a strong focus on best practices across service delivery, automation, and operational management. The company builds its solutions around standardized frameworks that ensure consistency, reliability, and scalability. Its orchestration engine, which supports a significant portion of service deployments, reduces provisioning time and minimizes human error.

Automation plays a central role in Singtel's operations. The company leverages AI-driven AIOps capabilities to analyze large volumes of telemetry data, identify patterns, and automate actions across the entire incident lifecycle, from detection and triage to response and remediation. This approach

reduces mean time to detect and respond (MTTD/MTTR), minimizes operational overhead, and enables security teams to focus on high-impact threats rather than routine alerts. By automating repetitive processes and accelerating coordinated threat responses, Singtel enhances both operational efficiency and overall cybersecurity effectiveness. This approach reduces alert fatigue, improves response times, and allows security teams to focus on high-priority threats. By training models on real operational data, Singtel enhances the accuracy and relevance of its automation processes.

Singtel also implements best practices in multi-vendor management. Through its intelligent fabric and overlay network capabilities, the company provides unified monitoring and control across diverse infrastructures. This model enables enterprises to maintain performance and security standards regardless of underlying connectivity providers. The ability to integrate application programming interfaces with partner systems further streamlines incident management and reduces resolution times.

Customer engagement processes reflect a structured and flexible approach. Singtel offers fully managed and co-managed service models, allowing organizations to choose the level of control that suits their needs. This flexibility ensures that customers can scale services according to business requirements while maintaining alignment with internal governance policies.

Through disciplined execution and continuous optimization, Singtel establishes a robust operational framework that delivers consistent, high-quality cybersecurity services across diverse environments. Frost & Sullivan applauds the company for executing a best-practice-driven strategy that combines automation, operational discipline, and innovation to deliver consistent, scalable, and high-impact cybersecurity services.

Trust at Scale

Singtel builds strong customer relationships by delivering seamless, end-to-end experiences across the entire lifecycle, from purchase to ongoing operations. Its integrated portfolio simplifies procurement by combining connectivity, security, and digital services into a unified offering. Customers benefit from a single provider that manages complex environments while ensuring consistent service quality.

The company enhances the ownership experience through centralized platforms that provide visibility into network performance, security posture, and service usage. Features such as real-time analytics, automated ticketing, and interactive dashboards empower customers to make informed decisions and respond quickly to operational challenges. This level of transparency strengthens trust and fosters long-term engagement.

Singtel's customer service model emphasizes responsiveness and reliability. Dedicated support teams operate with defined service-level commitments that exceed industry benchmarks, ensuring timely resolution of issues. The company structures its operations with specialized teams for network and security functions, enabling more effective handling of complex incidents.

Brand equity remains a key strength for Singtel, particularly in Singapore and across APAC. The company's reputation as a trusted partner stems from its deep domain expertise, strong local presence, and consistent delivery of high-quality services. Large enterprises rely on Singtel for mission-critical operations, reinforcing its position as a market leader in cybersecurity and digital services.

By combining operational excellence with customer-centric innovation, Singtel strengthens its brand and delivers experiences that drive loyalty, trust, and sustained business value.

Conclusion

Singtel continues to redefine the cybersecurity services landscape by aligning technological innovation with real-world enterprise needs. The company integrates connectivity, security, and intelligence into a unified framework that addresses growing complexity across hybrid, multi-cloud, and IoT-driven environments. Through its investments in AI-driven operations, multi-vendor management, and secure edge capabilities, Singtel equips organizations with the tools to anticipate threats, streamline operations, and scale securely. As enterprises transition toward AI-native, hyperconnected operating environments, Singtel is positioning cybersecurity as an embedded, intelligence-driven capability that underpins digital trust, operational resilience, and business innovation. Through the convergence of connectivity, security, AI, and cloud orchestration, the company continues to shape the future of secure digital infrastructure across the region

Singtel's consistent focus on execution, customer experience, and forward-looking innovation reinforces its leadership in the Singapore cybersecurity market. By delivering measurable value through flexible service models, strong operational frameworks, and deep regional expertise, the company builds lasting trust with its customers. Its differentiated approach, anchored in integration, automation, and intelligence, enables enterprises to move beyond reactive security toward resilient, future-ready operations. Frost & Sullivan recognizes Singtel for setting a benchmark in cybersecurity services through its visionary strategy, robust execution, and unwavering commitment to customer success.

With its strong overall performance, Singtel earns Frost & Sullivan's 2026 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 megatrends 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 fueled 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)