FROST & SULLIVAN

BEST PRACTICES

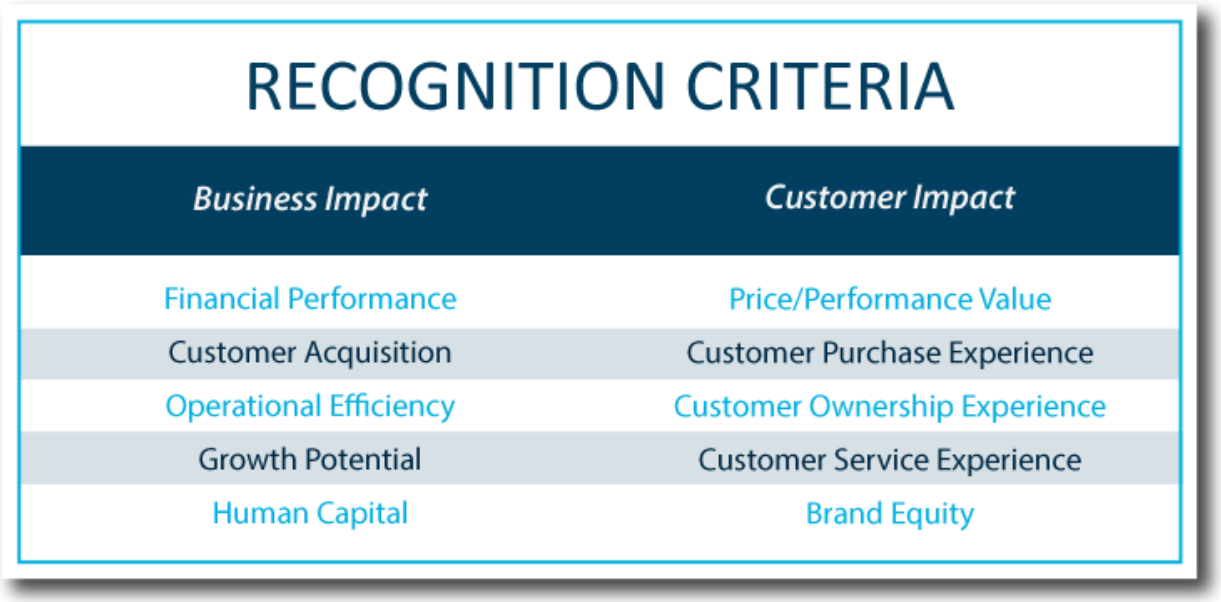
2026 ASIA-PACIFIC OT SECURITY CUSTOMER VALUE LEADERSHIP

kaspersky

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. Kaspersky excels in many of the criteria in the operational technology (OT) security space.



RECOGNITION CRITERIA	
Business Impact	*Customer Impact*
Financial Performance	Price/Performance Value
Customer Acquisition	Customer Purchase Experience
Operational Efficiency	Customer Ownership Experience
Growth Potential	Customer Service Experience
Human Capital	Brand Equity

Asia-Pacific OT Security Market

The OT cybersecurity market in Asia-Pacific is expanding rapidly as industrial organizations confront rising cyber risks, growing connectivity between IT and OT environments, and tightening operational resilience requirements. Demand is particularly strong in manufacturing, energy, utilities, and other critical infrastructure sectors where downtime, safety incidents, and compliance failures carry major business consequences. The market remains heterogeneous, with mature buyers in some countries and first-time OT security adopters in others, increasing the importance of solutions that can support both immediate risk reduction and longer-term IT-OT convergence.

In this environment, vendors combining OT-native protection, low-disruption deployment, broad visibility across industrial assets, and strong regional execution are best positioned to win. Kaspersky stands out in this space with a more comprehensive OT security vision encompassing endpoint, network, visibility, and management layers, while remaining practical for legacy and operationally sensitive industrial environments.

Delivering High-Impact Protection with Optimized Economic Value

Efficient security controls are paramount to ensure uninterrupted operational uptime. Kaspersky delivers a purpose-built, lightweight protection suite designed for industrial environments, characterized by low system resource consumption and minimal performance overhead, enabling secure operation across legacy Windows systems, industrial workstations, SCADA environments, and OT network assets like PLCs and Smart Machinery. Unlike many IT-centric solutions that introduce noticeable latency or require

frequent system interruptions, Kaspersky's architecture is optimized to operate with negligible impact on production performance.

This capability is a key differentiator in sectors such as manufacturing, where even minor disruptions can lead to significant production losses and financial impact, and national critical infrastructure where regulatory compliance and efficacy of advanced threat detection in mission-critical OT systems is crucial. Key features, including zero-reboot updates, precision alerting that avoids direct operational intervention, and portable scanning for air-gapped environments, translate into measurable operational benefits, such as reduced downtime risk and lower maintenance requirements.

From a total cost of ownership perspective, Kaspersky reduces the need for infrastructure upgrades, minimizes operational disruptions, and lowers ongoing administrative overhead. Compared with heavier, detection-centric OT security solutions that may require higher compute resources or intrusive remediation actions, Kaspersky's approach delivers a superior protection-to-disruption ratio. Customers therefore achieve robust OT security coverage while maintaining operational continuity, making the solution particularly compelling in cost-sensitive Asia-Pacific markets where both resilience and cost efficiency are critical.

Driving Customer Adoption Through Consultative Local Engagement

Kaspersky's customer acquisition strength in Asia-Pacific stems from its strategic engagement with industrial buyers leveraging an effective OT framework. In contrast to conventional IT security narratives, the company recognizes that demand often originates from the operational side of organizations, driven by priorities such as operational risk, compliance expectations, and the need to strengthen awareness of cyber threats in industrial settings. Kaspersky responds with a go-to-market model that closely aligns with these operational dynamics, combining OT-focused messaging, industry-specific use cases, and localized execution across major regional markets, including China, India, Vietnam, and Indonesia.

> *"Kaspersky delivers a purpose-built, lightweight protection suite designed for industrial environments, characterized by low system resource consumption and minimal performance overhead, enabling secure operation across legacy Windows systems, industrial workstations, SCADA environments, and OT network assets."*
>
> ***– Tetsuya Niihara***
> ***Director***

A distinct feature of Kaspersky's approach is its ability to translate complex OT security requirements into practical adoption pathways through its proprietary Kaspersky Industrial CyberSecurity (KICS) platform. KICS is unique because it combines endpoint protection for industrial systems, OT network anomaly detection, asset visibility, and centralized management within a unified architecture. Unlike many competitors that focus primarily on network monitoring or detection-only capabilities, Kaspersky integrates protection and visibility while maintaining low system overhead and compatibility with legacy environments, making it more deployable in actual industrial settings.

This technology is complemented by a structured partner ecosystem that includes industrial system integrators, automation vendors, and regional cybersecurity specialists with dedicated OT deployment capabilities. These partners are trained and certified in Kaspersky's OT deployment frameworks, enabling them to implement solutions in complex environments such as manufacturing plants and energy facilities.

This ecosystem is particularly strong in key Asia-Pacific markets, including China, where Kaspersky has established localized partnerships and presence across sectors such as manufacturing, energy, and public infrastructure.

Kaspersky's targeted industrial engagement strategy further lowers barriers to adoption by focusing on phased deployment models. For customers with limited OT cybersecurity maturity, deployments typically begin with passive asset discovery and monitoring, followed by incremental activation of protection and control features. In several Asia-Pacific manufacturing environments, this approach has enabled organizations to adopt OT security without disrupting production systems, accelerating time-to-value, and improving adoption confidence.

Supported by growing demand in industrial sectors such as manufacturing and energy, this combination of differentiated technology, localized partner execution, and structured adoption pathways has contributed to Kaspersky's continued expansion across Asia-Pacific, particularly in high-growth markets such as China and Southeast Asia.

For organizations expanding across borders or reassessing vendor choices amid evolving supply chain dynamics, Kaspersky's regional footprint and global cybersecurity credibility strengthen customer trust in the early stages of the procurement process. The company demonstrates particular strength in priority markets, including China, India, and Southeast Asia, where rapid industrial digitalization, increasing exposure to cyber threats, and expanding critical infrastructure create strong demand for OT cybersecurity solutions.

These markets are considered priority due to their high concentration of manufacturing, energy, and infrastructure assets, as well as growing regulatory focus on operational resilience. Kaspersky has established a solid presence across these sectors, particularly in manufacturing and energy, where industrial environments face increasing levels of cyber risk.

The company thrives in these regions by addressing critical vulnerabilities through its OT-specific capabilities while leveraging localized expertise and ecosystem partnerships. By combining local relevance with the scale and reputation of a global cybersecurity provider, Kaspersky positions itself as a trusted partner for industrial enterprises. This approach enhances confidence early in the buying cycle and supports customers seeking both operational familiarity and long-term vendor stability.

Capturing Opportunities in a Rapidly Evolving OT Security Market

OT cybersecurity is a high growth segment for Kaspersky globally, advancing at roughly twice the rate of its broader B2B portfolio. This remarkable growth is particularly evident in priority regions such as China, India, and Southeast Asia, where rapid industrial digitization, high exposure of manufacturing to cyber threats, and strict compliance expectations drive demand.

In addition to favorable market conditions, a central reason for the company's strong commercial momentum in OT cybersecurity is its strategic growth approach. While several vendors are moving toward product with universal capabilities, Kaspersky differentiates itself through a solutions framework that pairs its OT-native KICS platform with its broader IT security portfolio. KICS brings together OT and IIoT visibility, protection and management, while Kaspersky's IT security solutions (Kaspersky Next XDR Expert and Kaspersky SIEM) extend detection and correlation into enterprise environments. Together, these

deliver converged IT-OT security, supporting coordinated monitoring and response across domains and reducing the operational complexity often associated with managing multiple disconnected tools.

This distinction is particularly compelling in a market where many competing solutions remain detection-centric or primarily focused on OT visibility, lacking deeper cross-domain integration. As industrial cyber risks increasingly involve lateral movement between IT and OT environments, customers place greater value on platforms that can correlate events across systems and provide a consolidated view of risk.

> *"Kaspersky demonstrates customer ownership excellence through a platform strategy built around completeness rather than isolated point capabilities. A unified approach is central to this value proposition, integrating endpoint protection, anomaly detection, secure remote access, asset visibility, and centralized management. This coherent operational model is especially valuable in industrial environments where low asset awareness and disconnected tools can slow response times, reduce efficiency, and leave security teams with an incomplete view of risks."*
>
> ***– Tetsuya Niihara***
> ***Director***

For example, in a large manufacturing deployment in Asia-Pacific, Kaspersky enabled centralized monitoring of both IT and OT assets, allowing the customer to identify anomalous activity originating in the IT network and propagating toward production systems. By correlating data across environments within a unified platform, the customer was able to respond more quickly and avoid potential operational disruption. This illustrates how Kaspersky's integrated approach provides tangible advantages in managing complex industrial threat scenarios.

Kaspersky is adept at anticipating segments experiencing rapidly growing demand in the Asia-Pacific. It has a strong manufacturing foothold in fast-growing sectors such as batteries, automotive, microelectronics, and public sector-related industrial environments. With a localized ecosystem in China and a growing regional presence, the company leverages multiple pathways to sustain expansion, including deepening penetration in high-growth industrial verticals, expanding localized partner ecosystems, and scaling cross-domain IT-OT security deployments by integrating KICS with its IT security portfolio. These pathways are further supported by increasing demand for integrated cybersecurity solutions capable of addressing both legacy OT environments and modern interconnected systems. Frost & Sullivan finds that Kaspersky's capability to meet both immediate OT protection needs and support the broader transition toward IT-OT convergence positions it strongly for continued gains as the market matures.

Advancing Long-Term Value Through Adaptive Security Platform Evolution

Kaspersky demonstrates customer ownership excellence through a platform strategy built around completeness rather than isolated point capabilities. A unified approach is core to this value proposition, integrating endpoint protection, anomaly detection, secure remote access, asset visibility, and centralized management. This coherent operational model is especially valuable in industrial environments where low asset awareness and disconnected tools can slow response times, reduce efficiency, and leave security teams with an incomplete view of risks.

Kaspersky's KICS platform, introduced as its unified and comprehensive OT security solution, enables customers to move beyond siloed security operations toward a more cohesive IT-OT security posture. As

industrial organizations mature, their needs often evolve from initial OT security controls to broader IT-OT convergence. Kaspersky is well-positioned to support this transition by combining KICS with its corporate security solutions such as Kaspersky Next XDR Expert and Kaspersky SIEM, which together provide unified asset inventory, correlated data across IT and OT environments and consolidated oversight through the Open Single Management Platform. This approach reduces operational complexity, minimizes tool fragmentation, and improves long-term value realization.

For example, Kaspersky implemented KICS together with solutions for the corporate environment to unify visibility across the IT and OT assets of a large manufacturing facility, apply similar security policy level to both environments, enabling the customer to correlate alerts between enterprise systems and production networks, and initiate safe coordinated response measures lowering the MTTR. This allowed security teams to identify potential lateral threat movement earlier and respond more efficiently without disrupting operations. Such implementations demonstrate how Kaspersky's unified platform approach delivers practical benefits, including improved situational awareness, faster response times, and more efficient security operations across complex industrial environments.

Kaspersky's solution strategy promotes long-term adoption in environments that cannot be modernized all at once. Customers can secure legacy assets, air-gapped systems, and modern industrial infrastructure within a broader, more future-ready framework rather than repeatedly replacing tools as their requirements change. This capacity to protect today's operational estate while forging a path toward enhanced cyber resilience is a major contributor to the brand's customer ownership value.

Ensuring Operational Continuity with Responsive and Expert-Led Support

With an in-depth understanding of the operational realities of industrial environments, Kaspersky's service quality is measured not only by its response speed but also by its ability to maintain uptime and avoid unnecessary intervention. Many OT customers are acutely sensitive to disruption, particularly in production settings where downtime, latency, or forced system changes can lead to significant repercussions. As such, the security vendor's support must be technically proficient and operationally disciplined.

Kaspersky excels in this area through its robust OT-aware support and service model, which complements its technological design and enhances the overall customer service experience. Capabilities such as non-disruptive updating, alert-led protection, portable scanning for restricted environments, and support for secure remote connections enable customers to maintain strong protection without interrupting critical operations.

This service model is further reinforced by consistently high service availability, rapid incident response times, and structured escalation processes that ensure the timely resolution of complex issues. Customers benefit from predictable support performance, with reduced incident response timelines and improved resolution efficiency, particularly in mission-critical industrial settings. In addition, customer feedback and engagement programs indicate strong satisfaction with the company's ability to provide timely, technically proficient support tailored to OT environments.

These attributes are especially important in industrial contexts, where downtime must be minimized and conventional remediation approaches are often too disruptive or slow. By combining operationally aware

service delivery with measurable support performance, Kaspersky strengthens its ability to provide reliable, high-quality customer service across complex OT environments.

Furthermore, Kaspersky meets the growing demand for OT professional services, including OT security operation center (SOC) support and consultancy, particularly among large manufacturers. This demand strengthens its customer service profile by extending the relationship from product support into broader advisory and operational enablement partnerships. For customers, this value transcends swift assistance; it is the access to deep expertise and an extensive partner ecosystem that enables their evolution from basic OT security deployment toward a more integrated, resilient security operating model.

Building Trust Through Proven Expertise and Global Cybersecurity Leadership

Kaspersky strengthens its brand equity in the Asia-Pacific OT cybersecurity sector by combining global cybersecurity credibility with demonstrable industrial relevance and a strong focus on trust and transparency. Customers value not only the company's reputation in threat intelligence and advanced threat research, but also its ability to translate this expertise into effective OT-specific protection in real-world industrial environments. In the OT domain, brand strength is increasingly shaped by operational compatibility and trustworthiness, particularly in markets with complex and evolving regulatory landscapes.

A key differentiator is Kaspersky's proactive approach to transparency and compliance. Through its Global Transparency Initiative, the company has established transparency centers and data processing infrastructure across multiple regions, enabling independent verification of its technologies and strengthening customer confidence. This initiative, combined with adherence to regional data protection and cybersecurity requirements across Asia-Pacific markets, reinforces Kaspersky's credibility in environments where regulatory scrutiny and sovereignty concerns are critical.

In addition, Kaspersky's ability to deliver integrated protection across IT, OT, and IIoT environments further enhances its positioning as a strategic partner. By aligning technical capability with transparency, regulatory awareness, and industrial applicability, Kaspersky builds sustained trust and brand preference among organizations operating in highly regulated and mission-critical sectors.

Kaspersky's vast global presence, localized market execution, and extensive ecosystem support in key Asia-Pacific countries further reinforce its brand strength. In markets where buyers demand both local security insights and the expertise of a leading global vendor, Kaspersky occupies a prominent presence. The company's blend of research credibility, industrial specialization, and regional execution enhances customer trust and supports its enduring brand preference within the Asia-Pacific OT cybersecurity landscape.

Conclusion

Kaspersky excels in the Asia-Pacific OT cybersecurity market for the completeness of its vision and robust compatibility with industrial environments. Rather than approaching OT security as merely a threat detection issue, the company brings together endpoint protection, anomaly detection, asset visibility, secure remote access, and unified management across IT, OT, and IIoT environments. This broad coverage is particularly relevant as industrial organizations face increased cross-domain threats and seek stronger coordination between operational and enterprise security teams.

Its purpose-built, lightweight deployment, non-disruptive operations, support for legacy and air-gapped environments, and strategic go-to-market model combine localization with expertise in industrial domains. These characteristics make Kaspersky a compelling value proposition for Asia-Pacific customers seeking to improve cyber resilience without compromising uptime, performance, or operational continuity. The company's ability to support both immediate OT security requirements and the future transition toward IT-OT convergence gives it a clear edge in a fast-evolving cybersecurity market.

For its robust commercial momentum, regional execution capabilities, and trusted global cybersecurity credentials, Kaspersky earns Frost & Sullivan's 2026 Asia-Pacific Customer Value Leadership Recognition in the OT security industry.

What You Need to Know about the Customer Value Leadership Recognition

Frost & Sullivan's Customer Value Leadership Recognition identifies the company that offers products or services customers find superior for the overall price, performance, and quality.

Best Practices Recognition Analysis

For the Customer Value Leadership Recognition, Frost & Sullivan analysts independently evaluated the criteria listed below.

Business Impact

Financial Performance: Strong overall business performance is achieved in terms of revenue, revenue growth, operating margin, and other key financial metrics

Customer Acquisition: Customer-facing processes support efficient and consistent new customer acquisition while enhancing customer retention

Operational Efficiency: Company staff performs assigned tasks productively, quickly, and to a high-quality standard

Growth Potential: Growth is fostered by a strong customer focus that strengthens the brand and reinforces customer loyalty

Human Capital: Leveraging innovative technology characterizes the company culture, which enhances employee morale and retention

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)