FROST & SULLIVAN

BEST PRACTICES

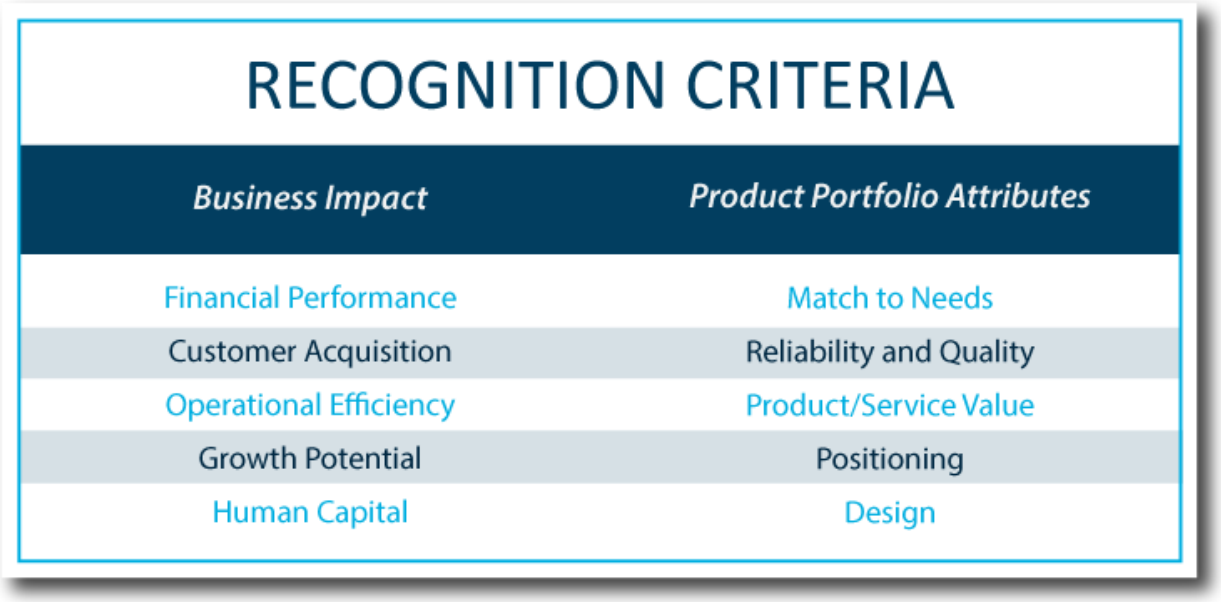
2026 ASIA-PACIFIC CONVERGED IT AND OT SECURITY PRODUCT LEADERSHIP

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 converged IT and OT security space.



The Transformation of the Converged IT and OT Security Industry

The Asia-Pacific (APAC) converged information technology (IT) and operational technology (OT) security landscape is undergoing rapid transformation, driven by aggressive digitalization across industrial critical infrastructure, such as manufacturing, energy, and mining. As organizations increasingly integrate operational technology with enterprise IT systems to enable real-time data flows, automation, and artificial intelligence (AI)-driven decision-making, the traditional boundaries between the factory floor and corporate networks are dissolving. While this converged cyber-physical systems unlocks significant efficiency and innovation gains, it simultaneously introduces a dramatically expanded attack surface where cyber incidents have digital, financial, and physical consequences.

This shift exposes a range of structural and systemic challenges unique to the APAC region. Industrial environments often rely on legacy systems that are not designed for connectivity, making them difficult to secure without disrupting operations. At the same time, organizations must navigate fragmented infrastructure, limited visibility across IT and OT domains, and a shortage of specialized cybersecurity skills capable of managing cyber-physical risks. A sharp rise in targeted attacks on industrial control systems compounds these challenges, increasing ransomware and malware activity across state-critical sectors such as energy, manufacturing, and mining.

Furthering the industry's complexity, enterprises must balance conflicting priorities between operational continuity and security enforcement, as downtime in OT environments directly impacts safety, revenue, and production quality. The convergence also demands new governance models, cross-functional

collaboration between IT and OT teams, and scalable security architectures capable of addressing modern digital threats and entrenched legacy vulnerabilities. Collectively, these challenges underscore the urgent need for purpose-built, unified cybersecurity solutions that can secure interconnected industrial ecosystems while enabling organizations across APAC to fully realize the benefits of digital transformation.

Founded in 1997 and headquartered in Moscow, Russia, Kaspersky is a global cybersecurity company recognized for its deep threat intelligence capabilities and purpose-built approach to securing complex digital and industrial environments. The company stands out for its OT-native architecture and unified IT/OT security platform, enabling organizations to protect critical infrastructure while ensuring operational continuity and efficiency. Through advanced AI-driven capabilities, integrated threat intelligence, and a strong focus on cyber-physical systems, Kaspersky is leading the evolution of secure, resilient, and scalable industrial cybersecurity globally.

Engineered for Industry Reality, Positioned to Lead Secured IT/OT Convergence

Kaspersky's product leadership in the converged IT/OT security market is grounded in a fundamentally differentiated design philosophy, one that starts with industrial realities rather than adapting enterprise IT paradigms. Unlike many competitors that have extended IT security solutions into operational technology environments, the company builds its industrial cybersecurity portfolio natively for OT systems, reflecting over a decade of focused development and deep domain expertise. This OT-first architecture ensures security mechanisms align with the operational priorities of industrial enterprises, where uptime, process continuity, and system stability outweigh aggressive remediation actions.

> *"Beyond compatibility, Kaspersky delivers comprehensive coverage across the industrial stack through KICS, which provides endpoint protection for industrial hosts, deep packet inspection and anomaly detection for industrial networks, and advanced asset discovery—giving a complete picture of the operational environment. The Open Single Management Platform then ingests this OT telemetry and asset information, unifying it with IT security data to give organizations a single, cross-domain view. This full-stack visibility strengthens threat detection and enhances operational awareness, enabling organizations to identify anomalous behaviors across both IT and OT assets."*
>
> ***- Rajarshi Dhar***
> ***Associate Director, Security Advisory Practice***

At the core of this design is Kaspersky's ability to deliver true IT/OT convergence through a unified, platform-driven approach. The Kaspersky Industrial CyberSecurity (KICS) suite integrates endpoint protection, network monitoring, anomaly detection, and asset visibility into a native extended detection and response (XDR) framework. Combined with Kaspersky IT solutions, such as Next XDR Expert or SIEM—this unified architecture spans IT and OT domains, correlating telemetry from endpoints, industrial networks, and control systems thereby allowing organizations to detect and respond to threats that traverse traditionally siloed environments. By combining node-level and network-level intelligence within a single OT XDR system, the company directly addresses the growing enterprise need for holistic visibility across cyber-physical systems.

Central to Kaspersky convergence capability is the Open Single Management Platform (OSMP), Kaspersky's IT-side platform, which consolidates functions such as endpoint protection response, security information and event management, and XDR into a unified control system. By ingesting OT telemetry

and asset data from KICS alongside this enterprise security information, OSMP enables centralized asset management and cross-environment threat correlation spanning both IT and OT. From an operational standpoint, this eliminates the fragmentation that typically burdens security teams managing separate IT and OT tools. It also enables a "single security operations center (SOC)" model, where security operations teams monitor, investigate, and respond to incidents across the entire infrastructure from one console, significantly reducing complexity and cost of constant maintenance of multiple integrations while enhancing responsiveness.

Kaspersky's product design also demonstrates a strong alignment with the unique constraints of industrial environments. The solutions operate with a low system footprint and high compatibility, supporting legacy operating systems, proprietary industrial protocols, and heterogeneous automation environments. By enabling passive monitoring, supporting outdated platforms, and maintaining stability even during security operations, the company ensures that its solutions can be deployed without disrupting production processes, a key adoption barrier that many competitors struggle to overcome.

Beyond compatibility, Kaspersky delivers comprehensive coverage across the industrial stack through KICS, which provides endpoint protection for industrial hosts, deep packet inspection and anomaly detection for industrial networks, and advanced asset discovery—giving a complete picture of the operational environment. The Open Single Management Platform then ingests this OT telemetry and asset information, unifying it with IT security data to give organizations a single, cross-domain view. This full-stack visibility strengthens threat detection and enhances operational awareness, enabling organizations to identify anomalous behaviors across both IT and OT assets.

A defining feature of Kaspersky's positioning is its deep integration of AI and threat intelligence into the product architecture. Drawing from its global threat research capabilities and dedicated advanced technology centers, the company embeds AI-driven anomaly detection, behavioral analytics, and automated incident summarization directly into its solutions. This is exemplified by the Kaspersky Investigation and Response Assistant (KIRA), the company's first GenAI-powered assistant, integrated into the Kaspersky products. KIRA empowers analysts by translating plain-language requests into structured threat-hunting queries, generating concise incident summaries that explain the initial attack vector and the attacker's actions and deobfuscating command lines. These capabilities improve detection accuracy and significantly enhance security operations efficiency by reducing false positives, accelerating incident response, and lowering analyst workload. In industrial environments, where specialized security talent is scarce, this AI-driven augmentation becomes a critical value driver.

Kaspersky further strengthens its positioning through an open and scalable platform design. With extensive third-party integrations and modular deployment options, the platform can be adopted incrementally, supporting organizations at early stages of cybersecurity maturity and advanced enterprises seeking full-scale security operations integration. This flexibility, combined with its channel-driven delivery model and strong partner ecosystem in APAC, ensures that the solution is effectively localized and scaled across diverse markets and industry verticals.

Real-world deployments underscore the effectiveness of this design and positioning strategy. In complex industrial environments, Kaspersky's solutions enable secure IT/OT convergence, improved visibility across infrastructure, and ensured continuous protection without compromising system performance.

Organizations benefit from reduced operational disruptions, improved efficiency, and stronger resilience against cyber threats and human error, demonstrating that the platform's design principles translate directly into measurable business outcomes.

Delivering Industrial-Grade Resilience with Measurable Business Value

Kaspersky's consistent ability to deliver high reliability and quality across complex, mission-critical environments, while simultaneously generating measurable operational and business value for its customers further enhances its leadership position. At the foundation of the company's reliability is its deep-rooted threat intelligence and research heritage. Kaspersky maintains continuous visibility into evolving cyber threats targeting IT and industrial environments. It directly embeds this intelligence into its cybersecurity platform, enabling real-time detection, early warning capabilities, and proactive threat mitigation. By combining global threat insights with industrial-specific context, the company ensures that its solutions are reactive and anticipatory, significantly enhancing the quality and effectiveness of protection for critical infrastructure operators. This protection quality is consistently validated by independent authorities: over the past decade, Kaspersky products have participated in 1,122 independent tests and reviews, earning 861 first-place results and 965 top-three finishes.

The robustness of Kaspersky's product design is further reflected in its industrial-grade engineering standards. The company built its KICS platform to maintain operational continuity, even in highly sensitive environments where downtime can result in significant financial or safety risks. In example, the entire Kaspersky OT XDR Platform (KICS) holds an IEC 62443 certification since 2020, specifically for the ISA/IEC 62443-4-1 standard. This certification guarantees that Kaspersky's product development lifecycle for its industrial cybersecurity platforms adheres to rigorous industrial-grade security-by-design principles. Its architecture prioritizes stability, using lightweight agents, passive monitoring techniques, and safe-response mechanisms to avoid disrupting industrial processes. This approach ensures that security operations do not interfere with production systems, creating a balance between rigorous protection and operational reliability, a critical differentiator in the OT security landscape.

Kaspersky tests solutions against various industrial control systems and certified by automation vendors, ensuring seamless integration across diverse and heterogeneous environments. This compatibility extends to legacy systems and proprietary technologies, enabling consistent performance even in complex infrastructures that combine modern and outdated components. As a result, customers benefit from a solution that can be deployed with minimal friction while maintaining consistent and predictable performance outcomes.

A key indicator of reliability and value is Kaspersky's proven performance in real-world industrial deployments. In large-scale production environments, the platform demonstrates the ability to provide continuous protection across IT and OT domains, eliminate issues such as virus propagation within network, storages, and ensure uninterrupted operation of virtualized environments and containers. Simultaneously, it enhances overall infrastructure resilience by reducing exposure to external threats and

human-induced risks. These outcomes directly translate into greater operational stability and reduced risk of costly disruptions.

Kaspersky's platform delivers significant value through improved efficiency in security operations. By integrating endpoint, network, and asset-level visibility within a unified XDR framework, the solution empowers faster detection, streamlined investigation, and coordinated response across the entire infrastructure. AI-driven capabilities further enhance this efficiency by reducing false positives, accelerating incident analysis, and supporting faster decision-making. In operational terms, this leads to measurable improvements in key metrics such as mean-time to detect and respond, critical for maintaining security posture in high-risk environments.

Beyond technical performance, Kaspersky drives tangible economic value for its customers. The centralized management model reduces the need for multiple standalone security tools, lowering total cost of ownership while simplifying system administration. Furthermore, improved threat detection and prevention capabilities reduce the likelihood of costly incidents, while optimized performance and minimal system overhead contribute to lower operational expenditure. In documented use cases, organizations have realized strong returns on investment through reduced maintenance costs, improved system uptime, and more efficient use of IT and security resources.[1]

Another dimension of Kaspersky's value proposition lies in its ability to enhance transparency and visibility across industrial environments. Through unified asset management and centralized monitoring, organizations gain a comprehensive view of their infrastructure, including IT and OT components. This visibility strengthens security and supports broader operational objectives, such as regulatory compliance, risk management, and strategic decision-making. By transforming fragmented data into actionable intelligence, the company enables organizations to move from reactive security postures to proactive, insight-driven operations.

Kaspersky's commitment to quality extends beyond product functionality to encompass long-term customer trust and performance assurance. The company emphasizes transparency, continuous improvement, and adherence to international standards and regulatory requirements, ensuring that its solutions remain effective and relevant in a rapidly evolving threat landscape. This focus on sustained performance and accountability reinforces customer confidence and supports long-term partnerships, particularly in critical infrastructure sectors where reliability is non-negotiable.

Transforming Security Operations through Intelligence, Automation, and Human Augmentation

Kaspersky's leadership in converged IT/OT security extends beyond product capabilities into the operational domain, where efficiency, scalability, and human enablement are critical success factors. In industrial cybersecurity, operational complexity often arises from fragmented tools, siloed teams, and a shortage of specialized talent. The company addresses these challenges through a platform-centric model that simplifies security operations while augmenting human capabilities, enabling organizations to achieve higher levels of efficiency without proportionally increasing resource burden.

[1] Provided by Kaspersky during interview.

The platform's ability to aggregate and cross-correlate telemetry from IT and OT environments further enhances efficiency. By combining data from endpoints, industrial networks, and control systems into a centralized analytics engine, Kaspersky enables faster and more accurate threat detection. This cross-domain visibility allows SOCs to identify attack patterns that span across environments, reducing investigation time and enabling more coordinated and effective responses.

Kaspersky also significantly improves operational efficiency through automation and orchestration capabilities embedded within its platform. Predefined workflows, playbooks, and automated response mechanisms reduce the need for manual intervention in routine tasks, enabling faster incident handling and consistent execution of security processes. Features such as centralized incident management, automated investigation graphs, and orchestration tools allow organizations to standardize their response strategies, minimizing variability and improving overall operational discipline.

> *"Kaspersky's design philosophy also considers the operational realities of industrial environments, where security measures must not interfere with production processes. By employing lightweight agents, passive monitoring techniques, and non-intrusive controls, the platform minimizes performance impact while maintaining high levels of protection. This ensures that operational efficiency is preserved within the security function and across the broader industrial ecosystem, supporting uninterrupted production and business continuity."*
>
> ***- Rajarshi Dhar***
> ***Associate Director, Security Advisory Practice***

AI also plays a pivotal role in enhancing operational efficiency and human productivity. Kaspersky's AI-driven capabilities, ranging from anomaly detection and behavioral analytics to automated alert summarization and query generation, reduce the cognitive load on security analysts. Tools such as the Kaspersky Investigation and Response Assistant enable analysts to quickly interpret incidents, generate queries, and understand attack sequences without extensive manual effort. This accelerates decision-making and allows less experienced personnel to perform complex analysis tasks, effectively bridging the cybersecurity skills gap.

In practical deployments, organizations leveraging Kaspersky's integrated platform report reductions in false positives, faster incident response times, and improved overall efficiency in security operations. By automating data correlation and leveraging AI to prioritize and contextualize alerts, the platform enables teams to focus on high-value activities rather than being overwhelmed by alert fatigue.

The company's strong emphasis on human capital development compliments its approach to operational efficiency. Recognizing that technology alone cannot address the complexities of cybersecurity, Kaspersky invests in training, knowledge transfer, and capability building for its customers and partners, enhancing the proficiency of client's internal teams to ensure effective utilization of the platform's capabilities.

Furthermore, Kaspersky's extensive partner ecosystem plays a crucial role in scaling operational efficiency across the APAC region. With a fully channel-driven model and a network of certified partners categorized by expertise and capability, the company ensures that customers have access to skilled resources for implementation, support, and ongoing optimization. This ecosystem accelerates deployment timelines and provides localized expertise, enabling organizations to address region-specific challenges more effectively.

Another dimension of efficiency is the platform's ability to adapt to organizations at different stages of cybersecurity maturity. Kaspersky offers scalable solutions that cater to emerging enterprises and advanced security operations teams. For less mature organizations, simplified and cloud-based offerings provide an accessible entry point with lower complexity, while more advanced enterprises can leverage the full capabilities of the unified platform. This flexibility ensures that organizations can optimize their operational models as they evolve, without requiring disruptive changes to their security architecture.

Importantly, Kaspersky's design philosophy also considers the operational realities of industrial environments, where security measures must not interfere with production processes. By employing lightweight agents, passive monitoring techniques, and non-intrusive controls, the platform minimizes performance impact while maintaining high levels of protection. This ensures that operational efficiency is preserved within the security function and across the broader industrial ecosystem, supporting uninterrupted production and business continuity.

Scaling Market Leadership through Accelerated Growth and Strategic Expansion

Kaspersky's product leadership in the converged IT/OT security market is reinforced by strong financial momentum, a clearly defined growth trajectory, and a scalable customer acquisition model particularly across high-growth industrial sectors in the APAC region. These elements collectively demonstrate current market success and the ability to sustain and expand its leadership position in an increasingly critical cybersecurity domain.

A key indicator of Kaspersky's financial strength lies in the rapid growth of its industrial cybersecurity portfolio. The company demonstrates strong performance within its business-to-business (B2B) segment, with industrial cybersecurity emerging as one of the fastest-growing components of its overall business. Notably, KICS has achieved accelerated growth rates, driven by increasing global demand for protecting critical infrastructure and enabling secure digital transformation. This growth is further validated by the platform's strong compound annual growth trajectory within the OT cybersecurity segment, significantly outpacing broader market averages and highlighting the company's ability to capitalize on emerging industry needs.

Kaspersky's growth potential is particularly pronounced in the APAC region, where industrial digitization, energy transition, and infrastructure modernization drive demand for converged IT/OT security solutions. The company identifies key high-growth sectors, including new energy, manufacturing, automotive, and electronics, where cybersecurity requirements are intensifying due to increased connectivity and operational complexity. Among these, the new energy sector has emerged as a particularly strong growth driver, reflecting broader regional trends toward sustainability and electrification. This targeted industry alignment positions Kaspersky to capture sustained demand as these sectors continue to scale and evolve.

A robust pipeline of industrial cybersecurity projects strengthens its future growth visibility. Kaspersky indicates strong momentum in upcoming deployments, with expectations of significant business expansion over the next two years, including the potential to double its IT/OT security-related business annually. This forward-looking growth outlook is supported by increasing customer awareness of cyber-physical risks, regulatory pressures, and the need for unified security architectures, factors that collectively expand the addressable market for the company's solutions.

From a customer acquisition perspective, Kaspersky employs a highly scalable, channel-driven model that enables rapid market penetration across geographically diverse regions such as APAC. The company's channel-led approach for B2B customers leverages a structured and tiered partner ecosystem, including distributors and certified partners categorized by expertise and performance. This model enhances reach while also ensuring that customers benefit from localized expertise and implementation support, which is particularly important in complex industrial environments. With over 30 active partners in APAC alone, Kaspersky has built a strong foundation for sustained customer acquisition and expansion.[2]

This partner-led strategy is complemented by a focus on large industrial enterprises and critical infrastructure operators, which represent high-value, long-term customers. By targeting organizations with complex IT/OT environments and significant cybersecurity requirements, Kaspersky drives deeper engagements, larger deal sizes, and long-term relationships. These customers often expand their use of the company's solutions over time, moving from initial deployments to broader, integrated security architectures, thereby increasing lifetime value and reinforcing customer retention.

Additionally, Kaspersky's ability to support greenfield and brownfield environments enhances its customer acquisition potential. Its compatibility with legacy systems and flexible deployment options allows it to engage with a wide range of organizations, including those with outdated infrastructure or limited cybersecurity maturity. This inclusivity broadens the addressable market and enables the company to capture demand across various stages of digital transformation, from early adopters to highly advanced enterprises.

With thousands of customers globally and deployments across multiple industries, Kaspersky benefits from strong brand recognition and trust. Its ability to demonstrate successful use cases across diverse geographies reinforces its credibility and facilitates new customer acquisition, particularly in markets where cybersecurity adoption is accelerating.

Importantly, Kaspersky's growth strategy is closely aligned with long-term industry trends, including the convergence of IT and OT, the rise of cyber-physical systems, and the increasing role of AI in security operations. By investing in next-generation capabilities, such as AI-enabled detection, advanced XDR platforms, and cyber-physical security innovations, the company positions itself to capture future demand and maintain its competitive edge. Its roadmap for next-generation AI-driven cybersecurity platforms further underscores its commitment to innovation-led growth.

[2] Provided by Kaspersky during interview.

Conclusion

Kaspersky's leadership in converged information technology (IT) and operational technology (OT) security is anchored in a rare combination of purpose-built industrial design, unified platform architecture, and proven ability to deliver measurable operational and business value at scale. Its OT-native approach, strengthened by deep threat intelligence and artificial intelligence-driven capabilities, enables organizations to secure complex cyber-physical environments without compromising performance, reliability, or uptime. By seamlessly integrating IT and OT security operations through a single platform, the company simplifies complexity and drives significant gains in efficiency, visibility, and decision-making effectiveness. Backed by strong market momentum, a rapidly expanding industrial customer base, and a scalable, partner-led go-to-market strategy, Kaspersky is well positioned to capitalize on the accelerating demand for converged security across Asia-Pacific (APAC). Together, these capabilities establish the company as a clear leader, delivering not just advanced cybersecurity solutions, but a future-ready foundation for resilient, intelligent, and secure industrial operations.

With its strong overall performance, Kaspersky earns Frost & Sullivan's 2026 APAC Product Leadership Recognition in the converged IT and OT security industry.

What You Need to Know about the Product Leadership Recognition

Frost & Sullivan's Product Leadership Recognition identifies the company that offers a product or solution with attributes that deliver the best quality, reliability, and performance in the industry.

Best Practices Recognition Analysis

For the Product 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

Product Portfolio Attributes

Match to Needs: Customer needs directly influence and inspire the product portfolio's design and positioning

Reliability and Quality: Products consistently meet or exceed customer expectations for performance and length of service

Product/Service Value: Products or services offer the best value for the price compared to similar market offerings

Positioning: Product serves a unique, unmet need that competitors cannot easily replicate

Design: Product features an innovative design that enhances both visual appeal and ease of use

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)