kaspersky

2025 COMPETITIVE STRATEGY LEADER

Transforming Innovation Into High-Growth Performance and Competitiveness

RECOGNIZED FOR BEST PRACTICES IN THE META THREAT PREVENTION INDUSTRY

FROST & SULLIVAN

Table of Contents

Best Practices Criteria for World-class Performance 3

Kaspersky's Strategic Cybersecurity Leadership in the Middle East 3
Strategic Regional Integration 3
Advanced Threat Intelligence and Product Localization 4
Cyber Immunity and Kaspersky's Industry-Specific Solutions 4
Kaspersky Thin Client: Optimizing Secure Endpoint Strategy for Enterprises 4

Translating Vision to Impact: Kaspersky's Middle East Strategy 5
Embedding Security into Digital Ecosystems 5
Capacity Development and Talent Building 5
Advanced Technology and Platform Strength 6
Commitment to Transparency and Compliance 6
Research Leadership and Innovation 7
UAE Cyber Security Council and Kaspersky Unite to Boost Cyber Resilience 7
Kaspersky Launches Five Global Expertise Centers to Fortify Cybersecurity 7
Kaspersky's GReAT: Leading the Frontline Against Advanced Cyber Threats 8

Kaspersky's Stakeholder Integration in the Middle East 8
Government and Institutional Collaborations 8
Kaspersky Launched New Transparency Centers in Istanbul and Kigali 8
Public-Private Cooperation and Capacity Building 9
Community Outreach and Local Presence 9

Kaspersky's Brand Equity in the Middle East 10
Strategic Visibility and Industry Recognition 10
Thought Leadership and Ecosystem Engagement 10

Conclusion 10

What You Need to Know about the Competitive Strategy Leadership Recognition 11

Best Practices Recognition Analysis 11
Strategy Innovation 11
Customer Impact 11

Best Practices Recognition Analytics Methodology 12

Inspire the World to Support True Leaders 12

About Frost & Sullivan 13

The Growth Pipeline Generator™ 13

The Innovation Generator™ 13

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 Threat Prevention space.

RECOGNITION CRITERIA	
Strategy Innovation	*Customer Impact*
Strategy Effectiveness	Price/Performance Value
Strategy Execution	Customer Purchase Experience
Competitive Differentiation	Customer Ownership Experience
Executive Team Alignment	Customer Service Experience
Stakeholder Integration	Brand Equity

Kaspersky's Strategic Cybersecurity Leadership in the Middle East

In an era marked by escalating cyber threats, the Middle East faces a dynamic and complex cybersecurity landscape. The proliferation of artificial intelligence (AI)-driven malware, sophisticated ransomware attacks, and vulnerabilities in Internet of Things (IoT) devices have heightened the urgency for robust cybersecurity measures. Industries such as energy, manufacturing, and smart city infrastructures are particularly susceptible, necessitating proactive and tailored security solutions.

> *"Kaspersky's deep-rooted presence in the Middle East, especially with its Riyadh HQ, shows more than just expansion, it reflects genuine commitment. What stands out to me is their focus on tailored solutions and local threat intelligence. In a region where cyber risks are growing fast, this kind of personalized, on-the-ground approach is exactly what's needed."*
>
> ***- Sapan Agarwal***
> ***SVP, Frost & Sullivan***

Strategic Regional Integration

Recognizing the unique cybersecurity challenges of the Middle East, Kaspersky has strategically aligned its operations to address regional needs effectively. In 2024, the company received a Regional Headquarters (RHQ) license from Saudi Arabia's Ministry of Investment, establishing its Saudi Regional HQ in Riyadh. This move not only underscores Kaspersky's commitment to the region but also enables the company to provide localized services.

Kaspersky's Saudi Regional HQ serves as a hub for strategic development, threat research, and the delivery of region-specific services. This localized approach facilitates a deeper understanding of the regional

threat landscape and allows for the customization of cybersecurity solutions to meet the specific needs of Middle Eastern clients.

Advanced Threat Intelligence and Product Localization

At the 2025 Cyber Security Weekend for the Middle East, Turkiye, and Africa (META) region, Kaspersky unveiled critical insights into the evolving cybersecurity landscape. The company highlighted a significant uptick in AI-driven ransomware activities and the emergence of sophisticated advanced persistent threats (APTs) targeting the region. These findings underscore the importance of proactive threat intelligence and the need for region-specific cybersecurity strategies.

Kaspersky's commitment to product localization is evident in its release of region-specific threat reports and targeted intelligence briefs. By tailoring its global expertise to address local risks, Kaspersky empowers Middle Eastern enterprises and authorities to anticipate and mitigate cyber threats effectively.

Cyber Immunity and Kaspersky's Industry-Specific Solutions

Kaspersky has pioneered the concept of Cyber Immunity—a secure by Design approach for building IT systems with built-in, architectural-level protection against cyberattacks. At the core of this approach is KasperskyOS, the company's own microkernel operating system, developed to support industries that demand high levels of cybersecurity, reliability, and predictability.

These Cyber Immune technologies are particularly suited for sectors such as energy, manufacturing, and smart city systems, where safeguarding the industrial Internet of Things (IIoT) is essential. Beyond industrial applications, they also bring trusted protection to domains that rely on resilience and compliance, including the public sector, healthcare, finance and insurance, education, retail, and logistics. By delivering robust protection, Kaspersky empowers these industries to drive digital innovation without compromising on security.

Kaspersky Thin Client: Optimizing Secure Endpoint Strategy for Enterprises

Extending its Cyber Immunity strategy to the endpoint level, Kaspersky developed the Kaspersky Thin Client, a Cyber Immune operating system for thin clients, based on the KasperskyOS platform, and tailored for enterprise needs. Installed on fanless, durable hardware, Kaspersky Thin Client (KTC) supports rapid deployment and is well-suited for large, distributed environments.

KTC enables secure remote desktop and VDI access via Citrix, VMware, and Microsoft RDS, with support for USB and smartcard redirection. Its centralized management features simplify IT oversight across sectors such as finance, healthcare, government, education, and manufacturing.

By eliminating antivirus requirements and reducing total cost of ownership, Kaspersky Thin Client offers a scalable, security-first solution for modern enterprises.

Kaspersky's strategic initiatives in the Middle East exemplify a comprehensive approach to cybersecurity, combining regional integration, advanced threat intelligence, and industry-specific solutions. By aligning its offerings with the geopolitical and cybersecurity needs of the region, Kaspersky not only strengthens its foothold in the Gulf but also sets a precedent for proactive and localized cybersecurity strategies. As

cyber threats continue to evolve, such tailored approaches will be instrumental in safeguarding the digital frontiers of the Middle East.

Translating Vision to Impact: Kaspersky's Middle East Strategy

As digital transformation is accelerating, effective execution of cybersecurity strategies has become vital. The Middle East's heightened focus on national cybersecurity frameworks and regulatory alignment requires not just robust planning but precise and timely implementation. Kaspersky has distinguished itself by operationalizing its strategic vision through well-coordinated product rollouts, local partnerships, and capacity-building programs, cementing its executional prowess across the region.

Embedding Security into Digital Ecosystems

One of the most visible demonstrations of Kaspersky's execution success lies in its partnerships with leading telecom providers. By launching consumer security solutions with operators like e& (UAE), stc Kuwait, and Zain KSA, Vodafone Qatar, Kaspersky ensured widespread adoption and seamless integration of its products into the region's evolving digital infrastructure. These telecom collaborations enhanced customer accessibility and helped position Kaspersky as an intrinsic component of national digital growth.

This model of embedded cybersecurity not only expanded the company's user base but also demonstrated agility in distribution and adaptability to local digital consumption patterns, a clear testament to its strategic execution capability.

Further reflecting its readiness, Kaspersky secured public sector tenders in Bahrain and participated in institutional cybersecurity deployments in Qatar and Egypt. These initiatives not only fulfilled national-level mandates but also solidified the brand's reliability in delivering high-stakes security operations.

Capacity Development and Talent Building

A critical component of Kaspersky's execution success has been its commitment to nurturing local cybersecurity talent across the region. Through its Cyber Generation internship program in Saudi Arabia, the company has played a pivotal role in training and empowering Saudi nationals, ensuring that the next generation of cybersecurity professionals is homegrown. Additionally, its active partnerships with universities across the Gulf are tailored to identify, mentor, and advance local students, reinforcing national capabilities. This focus on developing a local workforce not only strengthens regional cyber resilience but also ensures the long-term sustainability and cultural relevance of Kaspersky's operations in the Middle East.

In parallel, Kaspersky expanded its presence by onboarding new PR agencies in Jordan and strengthening its distributor networks in Egypt, Bahrain, and Saudi Arabia. These moves enabled efficient market penetration and sharpened regional messaging, a tactical execution of outreach and brand positioning strategies.

Kaspersky's execution in the Middle East showcases how a global cybersecurity firm can translate strategy into action with precision. From telecom-integrated product rollouts and robust operational infrastructure to impactful workforce development and retail expansion, the company's initiatives reflect

a deep understanding of local dynamics. As cybersecurity becomes a national priority across the region, Kaspersky's performance stands as a model of effective and scalable strategy execution.

Kaspersky's Edge in the Middle East: Trust and Innovation

The evolving cybersecurity ecosystem in the Middle East presents increasing threats, requiring strong protection measures, transparency, and a drive for innovation. Kaspersky has strategically positioned itself to meet these demands, distinguishing its offerings through advanced technology, unwavering commitment to transparency, and pioneering research.

Advanced Technology and Platform Strength

Kaspersky's Next platform exemplifies its technological prowess, integrating multi-layered endpoint protection with Extended Detection and Response (XDR) and Endpoint Detection and Response (EDR) capabilities. This comprehensive approach is tailored for large enterprises operating in high-risk sectors, providing them with a unified security ecosystem together with Network Detection and Response (NDR), SIEM, and Threat Intelligence solutions. The platform is powered by AI technology. Kaspersky uses predictive algorithms, clustering, neural networks, statistical models and expert algorithms to boost detection speed and improve accuracy. These technologies help reduce the impact of cyber incidents and improve MTTD and MTTR.

Complementing this, Kaspersky Industrial CyberSecurity (KICS) is an XDR-class platform designed specifically to protect critical infrastructure across industries such as energy, manufacturing, oil & gas, transportation, and smart cities. It delivers security for both modern and legacy OT assets, automated systems, and industrial networks — without disrupting technological processes. By addressing the unique challenges of these industries, Kaspersky reinforces its commitment to safeguarding essential services against the evolving cyber threats. Combined with Kaspersky SIEM, it delivers unified IT/OT convergence defense, ensuring visibility, resilience, and operational continuity for essential services.

> *"Kaspersky's strategic alignment with regional priorities, through its Transparency Center in Riyadh, advanced corporate cybersecurity offerings for businesses of all sizes via Kaspersky Next, and tailored ICS solutions, reflects a deep understanding of the Middle East's cybersecurity needs. Its emphasis on transparency, innovation, and regulatory compliance positions the company as a reliable partner in enabling secure and resilient digital transformation across critical sectors."*
>
> ***- Sapan Agarwal***
> ***SVP, Frost & Sullivan***

Commitment to Transparency and Compliance

Trust is paramount in cybersecurity, and Kaspersky has taken significant steps to foster it. The establishment of a Transparency Center in Riyadh allows government stakeholders and partners to review the company's source code, software updates, and threat detection rules. This initiative aligns with regional aspirations for digital sovereignty and transparency.

Further enhancing its trust credentials, Kaspersky has relocated its data processing activities to Switzerland, ensuring compliance with stringent data protection standards. This move underscores

the company's dedication to adhering to local regulations, including those in the UAE and Qatar, thereby strengthening its appeal in trust-sensitive markets.

Research Leadership and Innovation

Kaspersky's proactive approach to threat intelligence sets it apart. The early identification of sophisticated threats like the Tria banking Trojan and the SparkCat malware, which utilizes optical character recognition to steal sensitive data from images, highlights the company's vigilance in monitoring emerging cyber threats.

At the Internet Governance Forum (IGF) 2024, Kaspersky introduced guidelines for the secure development and deployment of artificial intelligence (AI) systems. These guidelines provide organizations with cybersecurity requirements to consider when implementing AI technologies, addressing the pressing need for robust security frameworks as AI becomes integral to various industries.

UAE Cyber Security Council and Kaspersky Unite to Boost Cyber Resilience

At GITEX Global, the UAE Cyber Security Council (CSC UAE) and global cybersecurity firm Kaspersky signed a landmark Memorandum of Understanding (MoU) aimed at strengthening the nation’s cyber resilience. The agreement, signed by Dr. Mohamed Al Kuwaiti and Andrey Efremov, focuses on enhancing readiness across vital economic sectors through swift and effective threat intelligence sharing.

Key areas of collaboration include exchanging insights on malware trends, indicators of compromise, and vulnerabilities targeting critical infrastructure. The partnership also emphasizes capacity-building through specialized training programs, technical workshops, and public awareness initiatives, reinforcing the UAE’s commitment to a secure digital future.

Kaspersky Launches Five Global Expertise Centers to Fortify Cybersecurity

Kaspersky unites its global cybersecurity expertise into five Centers, which serve as the pillars of its leadership in multiple aspects of the cybersecurity domain. Each center is dedicated to the solution of highly relevant problems critical for modern users and businesses, combining advanced research, practical solutions, and rich, globally trusted intelligence.

Global Research & Analysis Team (GReAT) investigates the most sophisticated attacks, including APTs and cybercriminal campaigns, discovers zero-day exploits, develops novel research and forensic tools – while also sharing knowledge through expert.

Threat Research Center studies both mass malware infestations and targeted attacks, analyzes adversary tactics, techniques and procedures and builds cutting-edge protective technologies and actionable threat intelligence based on the acquired research results.

AI Technology Research pioneers development of AI-powered cybersecurity solutions using advanced algorithmics and GenAI to battle sophisticated threats, withstand AI-assisted cybercrime, and shapes global approaches to safe and responsible use of AI.

Security Services Center delivers hands-on expertise for customers through incident response, MDR, SOC consulting, digital footprint intelligence, and in-depth compromise and security assessments

ICS CERT researches cyberthreats targeting industrial systems, develops security standards and methodologies, and identifies zero-day vulnerabilities in automated environments

Together, these Centers embody the core of Kaspersky's global expertise. They not only transform advanced research into practical protection but also ensure that innovation and intelligence consistently drive the company's

Kaspersky's GReAT: Leading the Frontline Against Advanced Cyber Threats

Kaspersky's Global Research and Analysis Team (GReAT) serves as a vanguard against cuttingedge cyber threats. Comprised of elite analysts, reverse engineers, and threat hunters, GReAT specializes in uncovering advanced persistent threats (APTs) and high-level cybercriminal operations. Operating across regions, the team continuously monitors global threat activity, studies malware to develop countermeasures, and collaborates with law enforcement and industry peers to share vital intelligence. GReAT's notable achievements include exposing the Equation Group spyware campaign, dissecting the Stuxnet worm, and revealing the supplychain compromise Operation ShadowHammer. In 2024, GReAT highlighted the perils of fileless malware, pioneering behavior analysis-based and cloud-running detection techniques to safeguard organizations worldwide.

Kaspersky's competitive differentiation in the Middle East is anchored in its advanced technological solutions, unwavering commitment to transparency, and leadership in cybersecurity research. By aligning its offerings with regional needs and global best practices, Kaspersky not only addresses current cybersecurity challenges but also anticipates future threats, solidifying its position as a trusted partner in the region's digital transformation journey.

Kaspersky's Stakeholder Integration in the Middle East

In the Middle East's rapidly transforming digital landscape, cybersecurity resilience depends heavily on collaboration between governments, institutions, and local communities. Kaspersky has strategically embedded itself across these layers, ensuring that its services are not only technologically robust but also culturally and institutionally aligned.

Government and Institutional Collaborations

Kaspersky has taken proactive steps to co-create a secure digital infrastructure alongside public-sector stakeholders. Its Memoranda of Understanding (MoUs) with Oman's Cyber Defense Center and Digital DEWA's Moro Hub exemplify its alignment with national cyber agendas. These partnerships go beyond regulatory compliance, involving joint research, operational collaboration, and infrastructure hardening across sectors.

By aligning with national telecom operators and cybersecurity authorities, Kaspersky has become a trusted partner in national and institutional security frameworks.

Kaspersky Launched New Transparency Centers in Istanbul and Kigali

Kaspersky continues to bolster its Global Transparency Initiative with the recent opening of two new Transparency Centers, one in Istanbul, Turkey, and another in Kigali, Rwanda. These centers are part of a growing international network that supports independent code reviews, regulatory inspections,

and transparent data-handling practices, aiming to build greater trust in Kaspersky's cybersecurity products.

Istanbul: A Technical and Academic Hub

In 2024, Kaspersky opened its Istanbul Transparency Center at Boğaziçi University. This facility offers secure access to Kaspersky's source code, software updates, threat detection rules, and Software Bill of Materials (SBOM). In addition to technical briefings, the center serves as an educational platform through a formal collaboration with the university, fostering knowledge exchange on secure software development and cybersecurity best practices.

Kigali: First Center in Africa

Kaspersky launched its first African Transparency Center in Kigali, Rwanda. Tailored for regional enterprise customers, regulators, and partners, the center supports hands-on code review, engineering documentation access, and cybersecurity training under Kaspersky's Cyber Capacity Building Program.

Meta's Digital-Only Approach

In contrast, Meta's transparency efforts remain digital, with no physical centers announced. Its online Transparency Center, launched in 2021, focuses on policy disclosures and content moderation updates.

Public-Private Cooperation and Capacity Building

Kaspersky plays an active role in cybersecurity knowledge development through collaborations with academic institutions, international organizations, and corporate partners. Its work on AI safety through UN platforms, participation in regional cybersecurity summits, and education-driven programs under the Kaspersky Academy have reinforced its role as an enabler of talent development.

Additionally, red-team exercises for Zain KSA and consulting for telecom Security Operations Centers reflect a shared-responsibility model, where industry leaders collaborate with Kaspersky to elevate sector-wide cyber maturity.

Community Outreach and Local Presence

Recognizing the diverse needs across the region, Kaspersky has adopted a localized approach to engagement. Through strategic partnerships, region-specific service models, and culturally relevant educational resources, the company ensures its solutions align with the digital habits and expectations of local users. This tailored strategy reinforces its presence and relevance in the Middle East's digital ecosystem.

These efforts not only increase accessibility but also ensure regulatory alignment and deeper cultural relevance, reinforcing community trust in the brand.

Kaspersky's stakeholder integration approach in the Middle East blends strategic alliances, capacity building, and localized service delivery. By embedding cybersecurity within national systems, industry practices, and local communities, Kaspersky ensures that its role goes beyond protection, helping build a collaborative and resilient regional digital ecosystem.

Kaspersky's Brand Equity in the Middle East

In the dynamic cybersecurity setting of the Middle East, Kaspersky has established a strong brand presence through strategic visibility, thought leadership, and resilience amidst global challenges.

Strategic Visibility and Industry Recognition

Kaspersky's active participation in prominent regional events such as GISEC, Black Hat MEA, and GITEX has significantly enhanced its brand visibility. These platforms have allowed the company to showcase its cybersecurity solutions and engage with key industry stakeholders. The company's insights and contributions have been featured in regional media outlets, further establishing its presence in the market.

Complementing its event participation, Kaspersky has received accolades from independent testing organizations. In 2024, the company achieved top performance across all quarters in SE Labs' rigorous testing, earning a perfect 100% Total Accuracy Rating. Additionally, Kaspersky's consumer solutions received high ratings in AV-Comparatives' tests, underscoring the company's commitment to delivering reliable cybersecurity products.

Thought Leadership and Ecosystem Engagement

Kaspersky has demonstrated thought leadership by addressing emerging cybersecurity challenges. At the Internet Governance Forum (IGF) 2024, the company unveiled guidelines for the secure development and deployment of artificial intelligence (AI) systems, providing organizations with cybersecurity requirements to consider when implementing AI technologies. Furthermore, Kaspersky's research into AI-driven cyber threats highlights its proactive approach to identifying and mitigating advanced threats.

The company's commitment to knowledge sharing and capacity building is evident through its regional Corporate Social Responsibility (CSR) initiatives and collaborations with academic institutions. These efforts have reinforced Kaspersky's image as a partner invested in the region's cybersecurity ecosystem.

Conclusion

Kaspersky’s strategic alignment with the Middle East’s digital transformation highlights its leadership in cybersecurity through localized operations, advanced technologies, and strong stakeholder engagement. The company addresses evolving threats by integrating region-specific solutions, fostering talent, and promoting transparency while building trust. Its resilience, innovation, and active regional presence have solidified its role as a key cybersecurity partner. As the Middle East advances its digital agenda, Kaspersky stands out as a proactive, reliable force securing the region’s digital future.

With its strong overall performance, Kaspersky earns Frost & Sullivan’s 2025 META Company of the Year Recognition in the Threat Prevention industry.

What You Need to Know about the Competitive Strategy Leadership Recognition

Frost & Sullivan's Competitive Strategy Leadership 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 Competitive Strategy Leadership Recognition, Frost & Sullivan analysts independently evaluated the criteria listed below.

Strategy Innovation

Strategy Effectiveness: Effective strategy balances short-term performance needs with long-term aspirations and overall company vision

Strategy Execution: Company strategy utilizes best practices to support consistent and efficient processes

Competitive Differentiation: Solutions or products articulate and display unique competitive advantages

Executive Team Alignment: Executive team focuses on staying ahead of key competitors via a unified execution of its organization's mission, vision, and strategy

Stakeholder Integration: Company strategy reflects the needs or circumstances of all industry stakeholders, including competitors, customers, investors, and employees

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)