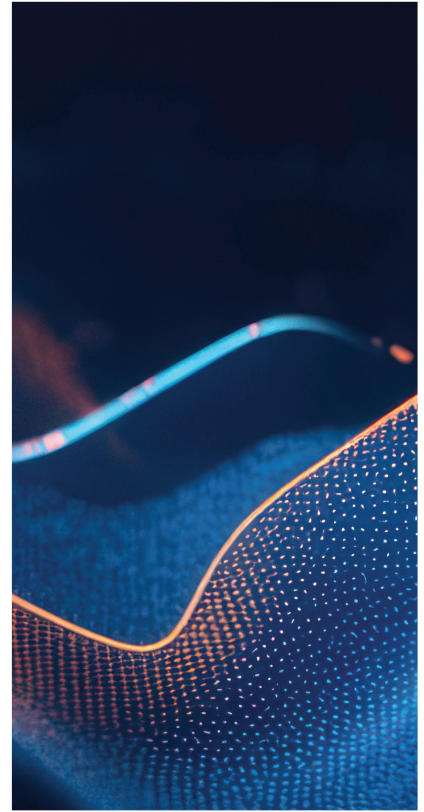
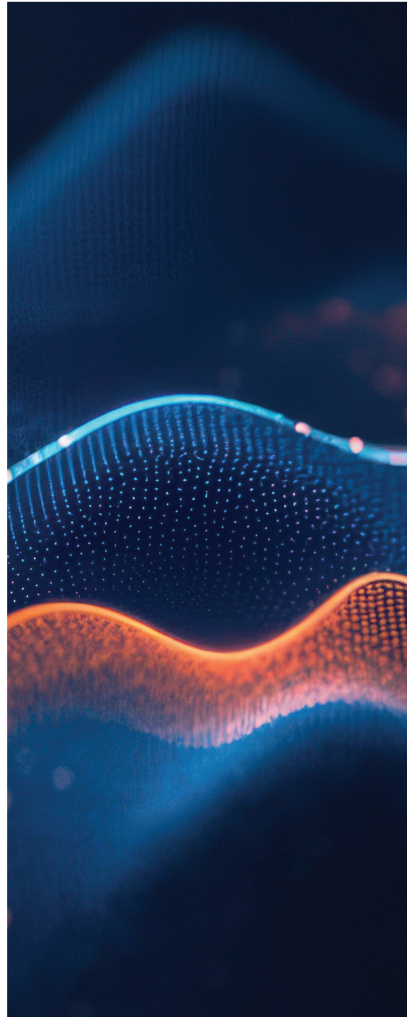


FROST & SULLIVAN
BEST PRACTICES



2026

CHINA

AI SECURITY

**TECHNOLOGY INNOVATION
LEADERSHIP**

Table of Contents

Best Practices Criteria for World-Class Performance	3
The Transformation of the AI Security Industry in China	3
Bridging the Gaps to Match China’s AI Security Needs	4
Ahead of the Curve: Unique Designs that Position NSFOCUS as an Innovator	6
Gaining Trust through Proven Outcomes and Enterprise Deployment Experiences.....	9
Conclusion	10
What You Need to Know about the Technology Innovation Leadership Recognition ...	11
Best Practices Recognition Analysis.....	11
Technology Leverage.....	11
Business 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. NSFOCUS excels in many of the criteria in the AI security space.

RECOGNITION CRITERIA	
<i>Business Impact</i>	<i>Technology Leverage</i>
Financial Performance	Commitment to Innovation
Customer Acquisition	Commitment to Creativity
Operational Efficiency	Stage Gate Efficiency
Growth Potential	Commercialization
Human Capital	Application Diversity

The Transformation of the AI Security Industry in China

Over the past few years, China’s enterprise AI landscape has undergone a structural transformation as large language models (LLMs), AI agents, intelligent applications, and AI-generated content have moved rapidly from experimentation to production environments. Organizations across financial services, government, energy, education, telecommunications, and large enterprises are increasingly embedding AI into customer service, internal knowledge management, software development, business operations, and decision-support workflows. This shift has expanded the enterprise attack surface beyond conventional applications, APIs, endpoints, networks, and cloud workloads to include prompts, models, AI agents, generated outputs, training data, inference pipelines, plug-ins, and unauthorized AI deployments.

The security implications are substantial. Traditional cybersecurity tools built to detect known malware, network intrusions, application-layer attacks, data leakage patterns, or endpoint compromise are ineffective in terms of helping organizations defend against novel threats caused by AI. They were not designed to understand semantic-level threats such as prompt injection, model manipulation, jailbreak attempts, malicious AI-generated content, AI output data leakages, unauthorized model access, or agentic workflow abuse. As a result, enterprises face a widening protection gap between AI adoption and AI-specific security control maturity.

This gap is especially relevant in China, where AI adoption is taking place under more stringent regulatory requirements. Organizations deploying generative AI and AI-generated content capabilities must consider

content safety, data protection, auditability, model governance, and security management requirements. For regulated sectors, such as banking, government, energy, and education, AI security is not only a technical requirement but also a compliance and operational resilience priority. Enterprises require security platforms that can discover AI assets, assess compliance exposure, inspect AI-specific interactions, prevent harmful or non-compliant outputs, protect sensitive information, and generate auditable evidence aligned with China's AI governance expectations.

“NSFOCUS’s approach reflects a clear shift from traditional security extension to AI-native protection. Instead of treating AI security as an add-on to its existing security products, such as WAF, DLP, or content filtering tools, NSFOCUS builds its Qingfengwei as a dedicated solution for AI security. It is structured around the distinct risk patterns of LLMs, AI agents, AI-generated content, and enterprise AI assets. It includes multiple independently deployable but coordinated components, such as AI-Scan for AI security and compliance assessment, AI-AFW for AI application-layer protection, AI-CONT for content safety, AI-DLP for data leakage prevention, and AI-UTM for AI asset discovery and unified threat management.”

- Anh Tien Vu
Industry Principal, Global
Cybersecurity Practice

The challenge is that most existing security products address only parts of this problem. Content moderation tools can assess generated outputs but often lack AI asset discovery, application-layer protection, data leakage prevention, or integrated response. Traditional WAF, DLP, and endpoint controls can provide baseline protection, but they cannot consistently interpret prompt semantics, model behavior, or AI-specific attack patterns. Cloud-native AI security tools from hyperscalers may provide value within cloud ecosystems but are less suitable for regulated Chinese enterprises that operate hybrid, on-premises, private cloud, edge, or domestic IT environments.

As enterprise AI adoption accelerates, organizations require a new class of AI-native security platform: one that moves beyond fragmented controls and provides full life cycle protection across assessment, discovery, runtime defense, content governance, data leakage prevention, automated response, audit, and continuous hardening. This market transition creates a clear opportunity for technology innovators that

combine AI-specific detection, regulatory alignment, domestic deployment flexibility, and enterprise-grade scalability into a unified architecture.

Bridging the Gaps to Match China's AI Security Needs

Founded in 2000, NSFOCUS is one of China's established cybersecurity vendors, with a broad portfolio spanning network security, application security, cloud security, threat intelligence, security operations, and managed security services. Building on this foundation, the company has expanded into AI security through its Qingfengwei AI Security Product Matrix, a comprehensive platform designed to protect enterprise AI deployments across the full security life cycle.

NSFOCUS's approach reflects a clear shift from traditional security extension to AI-native protection. Instead of treating AI security as an add-on to its existing security products, such as WAF, DLP, or content filtering tools, NSFOCUS builds its Qingfengwei as a dedicated solution for AI security. It is structured around the distinct risk patterns of LLMs, AI agents, AI-generated content, and enterprise AI assets. It

includes multiple independently deployable but coordinated components, such as AI-Scan for AI security and compliance assessment, AI-AFW for AI application-layer protection, AI-CONT for content safety, AI-DLP for data leakage prevention, and AI-UTM for AI asset discovery and unified threat management.

This integrated architecture gives NSFOCUS a differentiated position in China's AI security market, where most competing approaches remain either narrow, cloud-dependent, or insufficiently aligned with regulated-sector deployment realities. While domestic cybersecurity competitors have meaningful cybersecurity portfolios, their AI security capabilities are generally more limited in breadth, often centered on select functions such as content moderation, endpoint security, compliance assessment, or early-stage AI protection. These approaches can address isolated risks, but they do not fully solve the operational problem facing Chinese enterprises associated with AI asset discovery, AI compliance exposure assessment, semantic-level threat inspection, data leakage prevention, generated content control, and automated response through one unified platform.

In addition, many other cloud service providers also offer AI security capabilities, but their strengths are typically tied to their own cloud ecosystems. This creates a gap for regulated industries that operate across on-premises infrastructure, private cloud, hybrid cloud, edge environments, and domestic IT stacks. For banks, government agencies, energy organizations, and large universities, AI security cannot depend only on public-cloud-native controls. These customers need deployment flexibility, domestic compatibility, auditability, and consistent policy enforcement across mixed environments.

NSFOCUS's appliance, containerized, on-premises, and hybrid deployment options directly address this requirement, making the platform more suitable for China's sovereignty-sensitive and compliance-driven sectors. This architecture directly addresses several critical market gaps in China's AI security landscape.

- First, many organizations lack visibility into AI assets that are already deployed across business units, development teams, or shadow IT environments. Adoption of unauthorized AI tools, exposed model services, and unmanaged AI agents can create significant security and compliance risks to their business operations. NSFOCUS's AI-UTM is designed to help them discover AI assets through active scanning, passive monitoring, and asset mapping, enabling organizations to understand where AI is being used and how it is exposed.
- Second, AI-specific attacks increasingly occur at the semantic layer. Prompt injection, jailbreaks, malicious instructions, model output manipulation, and policy bypass attempts cannot be reliably detected through signature-based inspection alone. NSFOCUS's AI-AFW and AI-CONT capabilities apply AI-native analysis to detect and control prompt-level and content-level risks, helping organizations protect AI applications against misuse while supporting compliance with domestic content safety requirements.
- Third, AI introduces new forms of data leakage. Sensitive business information, personal data, source code, credentials, and regulated information can be exposed through prompts, generated outputs, model interactions, or AI agents connected to enterprise systems. NSFOCUS's AI-DLP extends data leakage prevention into AI interaction flows, helping enterprises reduce the risk of sensitive information being disclosed through AI-generated responses or unauthorized AI usage.

- Fourth, China's regulated sectors require deployment flexibility and domestic ecosystem compatibility. Many government, financial, energy, and education customers cannot rely solely on cloud-native AI security services. They need on-premises, private cloud, hybrid, and domestic IT-compatible deployments that align with procurement, sovereignty, operational resilience, and regulatory requirements. NSFOCUS's support for on-premises, hybrid, containerized, and domestic IT-compatible deployment gives it a significantly stronger fit for government, finance, energy, and education customers that cannot compromise on control, compliance, and operational resilience.

NSFOCUS's Qingfengwei does not merely compete as another AI security tool but bridges a China-specific market gap between AI adoption, AI regulation, and enterprise deployment reality. Its value lies in combining AI-native threat understanding with practical controls for asset discovery, content safety, data protection, automated response, and compliance-driven deployment. This combination is difficult for point-solution vendors, traditional security providers, and cloud-native AI security services to replicate quickly because it requires deep cybersecurity expertise, AI-domain model development, regulated-industry deployment experience, and local ecosystem compatibility in one platform.

Ahead of the Curve: Unique Designs that Position NSFOCUS as an Innovator

NSFOCUS has positioned itself as a technology innovator in China's AI security market through a full life cycle architecture that consolidates assessment, discovery, protection, governance, and response into one AI-native platform. While China's AI security market remains in the early stage, it has become a fast-

"NSFOCUS has positioned itself as a technology innovator in China's AI security market through a full life cycle architecture that consolidates assessment, discovery, protection, governance, and response into one AI-native platform. While China's AI security market remains in the early stage, it has become a fast-moving stage, requiring a holistic security approach to secure AI systems. Many vendors are attempting to extend their existing cybersecurity tools into AI security, but most approaches remain fragmented, focusing on select functions such as AI content review, compliance scanning, endpoint protection, traffic filtering, or cloud-native AI governance."

- Anh Tien Vu
Industry Principal, Global
Cybersecurity Practice

moving stage, requiring a holistic security approach to secure AI systems. Many vendors are attempting to extend their existing cybersecurity tools into AI security, but most approaches remain fragmented, focusing on select functions such as AI content review, compliance scanning, endpoint protection, traffic filtering, or cloud-native AI governance. These capabilities address parts of the problem, but they do not fully support the end-to-end requirements of enterprises deploying LLMs, AI agents, AI-generated content applications, and AI-enabled workflows across regulated environments. NSFOCUS's Qingfengwei platform moves further by combining AI asset discovery, semantic threat analysis, data protection, automated enforcement, AI-assisted security operations, and continuous hardening into one coordinated architecture. This allows the platform to provide comprehensive AI security capabilities to secure AI systems across environments.

This design also creates a higher innovation barrier than adding AI features to an existing security product.

Different from other domestic providers that develop their prompt filter, model assessment module, or content safety engine, NSFOCUS's approach requires security-domain model training, protocol-level security knowledge, AI-specific asset mapping, firewall-linked response, low-latency endpoint protection, and deployment experience in regulated Chinese environments. This not only helps Qingfengwei extend traditional cybersecurity into AI use cases, but it also builds an AI security control plane that connects discovery, protection, response, and governance across the enterprise AI life cycle.

One of NSFOCUS's key innovations is its Three-Phase Protection Framework: Radar Sweep, Real-Time Shield, and Continuous Hardening. This framework gives enterprises a practical operating model for AI security. Radar Sweep identifies AI assets, deployment exposure, model risks, and compliance gaps. Real-Time Shield protects AI applications, prompts, outputs, and data flows during active use, and Continuous Hardening supports ongoing remediation, policy improvement, and security posture enhancement as AI systems evolve. This integrated and holistic model is highly relevant for China's AI security market because enterprises require both detection and a robust governance and protection cycle that supports compliance, operations, and long-term AI risk management.

In addition, NSFOCUS's NSFGPT 14B security-domain large model helps further strengthen its innovation profile. Unlike general-purpose LLMs adapted for broad enterprise use cases, NSFGPT is purpose-built for cybersecurity scenarios, including security-domain reasoning, protocol parsing, threat analysis, work-order generation, and remediation support. The model can support more than 100 protocol parsing scenarios and deliver security-task performance comparable to larger general-purpose models, while reducing compute requirements. This creates an important product advantage compared to other solutions, enabling AI security operations to be more automated and context-aware without relying entirely on external general-purpose models that may not align with enterprise security, privacy, or domestic deployment requirements.

Another important differentiator is AI-UTM for AI asset discovery and automated response. As enterprises struggle with unauthorized AI deployments and unmanaged model services, AI asset visibility is becoming a foundational requirement. NSFOCUS's ability to identify AI agents and exposed AI deployments, then trigger automated firewall isolation or blocking within seconds, provides a stronger control model than manual asset review or periodic assessment. This capability is especially valuable in regulated industries, where unknown AI services can create compliance, data leakage, and operational risk.

NSFOCUS also advances the market through its LM-Security Plugin (NSF-ClawGuard), which provides lightweight endpoint-level AI protection with reported latency below 10 milliseconds. This makes it highly relevant to address new AI security challenges associated with solutions that are limited to network gateways or centralized inspection points. As employees increasingly interact with AI tools through endpoints, browsers, local agents, plug-ins, and internal applications, organizations need low-latency protections that can monitor inputs, detect risky commands, filter outputs, and track behavior without disrupting user experience.

Coupled with that, the company's AI agent penetration testing capability adds another forward-looking element. As AI agents introduce a new class of risk because they can call tools, execute workflows, access data, and interact with enterprise systems, testing these agentic behaviors is becoming important and requires different methods from traditional application or network penetration testing. By compressing

AI agent security testing from weeks to hours and improving operational efficiency, NSFOCUS addresses a market need that is likely to become more important as enterprises move from basic LLM usage to autonomous and semi-autonomous AI workflows.

These innovations are also difficult for competitors to mimic quickly. Building a comparable platform requires more than adding prompt inspection or content moderation to an existing security product. It requires security-domain model development, AI-specific asset discovery, automated enforcement workflows, endpoint-level AI interaction protection, regulated-sector deployment experience, domestic ecosystem compatibility, and continuous threat research. This gives NSFOCUS a strong position in China as the market matures and customers move from pilot projects toward production-scale AI governance and protection.

NSFOCUS has positioned itself as a technology innovator through the following aspects:

- **Comprehensive AI Security Product Matrix:** Unifying AI assessment, AI application firewalling, content safety, AI DLP, AI asset discovery, and continuous hardening into a coordinated platform rather than a set of disconnected tools.
- **Security-Domain Large Model:** Leveraging NSFGPT to enhance security analysis, protocol parsing, work-order automation, and remediation support in a way that is purpose-built for cybersecurity rather than generic AI assistance.
- **AI Asset Discovery and Automated Response:** Enabling enterprises to identify unauthorized AI assets and initiate automated responses within seconds, directly addressing shadow AI and unmanaged model exposure.
- **Semantic-Level Threat Protection:** Detecting AI-specific risks, such as prompt injection, harmful content, data leakage, jailbreak attempts, and misuse patterns, that legacy security tools were not designed to interpret.
- **China Regulation Alignment:** Supporting content safety, auditability, compliance assessment, domestic IT compatibility, and deployment flexibility for regulated sectors operating under China's AI governance environment.
- **Enterprise-Grade Performance and Scalability:** Demonstrating high-throughput deployments, large event processing capacity, and a distributed architecture suitable for large financial, education, government, and energy environments.

Gaining Trust through Proven Outcomes and Enterprise Deployment Experiences

NSFOCUS's technology differentiation is strengthened by documented enterprise outcomes across regulated and large-scale environments, reflecting its undeniable importance and influence in the Chinese AI security market. The ability to demonstrate real-world performance, operational efficiency, and compliance readiness is becoming a decisive factor, which positions NSFOCUS at the forefront of the AI security big wave.

Compared to AI security point solutions that focus mainly on assessment, content filtering, or model governance, NSFOCUS has demonstrated excellent operational deployment across complex environments. For example, in a bank deployment environment, NSFOCUS's platform can reduce alert noise by 98%, processing more than 200 log types from more than 20 security devices and helping security teams move from reactive alert handling toward more focused threat identification and response. This outcome is highly important for teams that struggle with alert fatigue. The ability to reduce noise and focus analyst attention on genuine threats helps strengthen its value proposition.

The platform's scalability also differentiates NSFOCUS from narrower AI security tools. NSFOCUS can support 130Gbps traffic handling, 1.2 million events per second, and a 60-node cluster architecture, allowing organizations to scale, especially in universities, banks, government clouds, and large enterprise networks where AI usage, generated content, application traffic, and user interactions can grow rapidly. This gives NSFOCUS a clear advantage compared to solutions that work only in controlled pilots or single-environment deployments, which may struggle to support production AI security at national, sectoral, or large-enterprise scale.

Furthermore, NSFOCUS's credibility and values are most evident in regulated sectors, with more than 80 financial-sector deployments and reference use cases across banking, government, education, and energy. This provides a clear advantage over competitors whose AI security offerings are still early-stage or less validated in production. In China's regulated industries, customer trust relies not only on technical claims but also on local support, domestic deployment experience, certification readiness, compatibility with domestic IT environments, and the ability to align security controls with procurement and compliance expectations.

Leveraging its strong business reputation and holistic product ecosystem, the company has become the fastest-growing AI security market participant, recording explosive growth of nearly 130% from 2024 to 2026, with a 60%+ conversion rate from AI-Scan customers to full-platform deployments, more than 95% customer retention, and shorter sales cycles. These have reflected the trust and high confidence of domestic organizations in its products and services and indicated that its AI security solutions are no longer treated as experimental tools but play an increasingly important role in domestic organizations' security strategies.

In addition, NSFOCUS's assessment-first model is particularly effective in China's AI security market. Many enterprises understand that AI introduces new risks, but they may not yet know where those risks exist, which AI assets are exposed, or how AI security should be prioritized. AI-Scan helps NSFOCUS create customer demand by identifying security and compliance gaps, while the broader Qingfengwei platform provides the response path through protection, data leakage prevention, asset discovery, and hardening.

This gives NSFOCUS a stronger commercialization model than vendors that lead with standalone tools but do not provide a clear maturity path from assessment to full operational protection.

Frost & Sullivan's analysis finds that NSFOCUS's Qingfengwei platform helps customers achieve several important outcomes:

- **Improved AI Asset Visibility:** Discovering unauthorized or unmanaged AI deployments that traditional security tools and general-purpose cloud security platforms often miss.
- **Reduced Alert Fatigue:** Achieving up to 98% alert noise reduction in documented banking operations, allowing teams to focus on genuine high-risk events instead of processing excessive AI security alerts.
- **Faster Detection and Response:** Supporting seconds-level detection and automated response workflows, including 3–8 second firewall isolation for certain AI asset risks.
- **Stronger Compliance Readiness:** Supporting assessment, audit, content safety, domestic IT compatibility, and regulatory alignment relevant to China's AI governance environment.
- **Lower Operational Complexity:** Consolidating multiple AI security functions into a unified platform, reducing the need for customers to integrate several point products from different vendors.
- **Better SecOps Productivity:** Using the NSFGPT security-domain model to assist with work-order generation, remediation suggestions, and analyst enablement.
- **Stronger Regulated Sector Fit:** Providing validated deployment experience across finance, government, education, and energy, where production proof, local compatibility, and compliance support are central to buying decisions.

Conclusion

NSFOCUS has built trust not only through product innovation but also through proven deployment outcomes. Its combination of measurable performance, regulated-sector references, domestic ecosystem compatibility, and customer expansion metrics gives it a stronger foundation than competitors relying mainly on partial AI security capabilities, cloud-bound controls, or early-stage market positioning. This reinforces NSFOCUS's claim to Technology Innovation Leadership in China's AI security industry.

With its strong overall performance, NSFOCUS earns Frost & Sullivan's 2026 Technology Innovation Leadership Recognition in the Chinese AI security industry.

What You Need to Know about the Technology Innovation Leadership Recognition

Frost & Sullivan's Technology Innovation Recognition identifies the company that has introduced the best underlying technology for achieving remarkable product and customer success while driving future business value.

Best Practices Recognition Analysis

For the Technology Innovation Leadership Recognition, Frost & Sullivan analysts independently evaluated the criteria listed below.

Technology Leverage

Commitment to Innovation: Continuous emerging technology adoption and creation enables new product development and enhances product performance

Commitment to Creativity: Company leverages technology advancements to push the limits of form and function in the pursuit of white space innovation

Stage Gate Efficiency: Technology adoption enhances the stage gate process for launching new products and solutions

Commercialization: Company displays a proven track record of taking new technologies to market with a high success rate

Application Diversity: Company develops and/or integrates technology that serves multiple applications and multiple environments

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

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)

