upwind

2025 COMPANY OF THE YEAR

Driving impact across the customer value chain

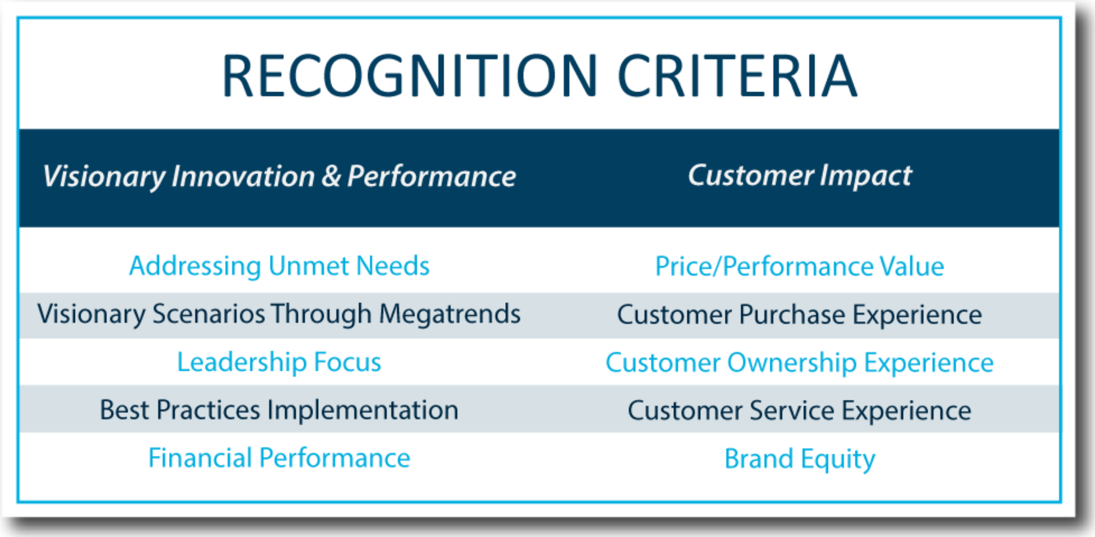
RECOGNIZED FOR BEST PRACTICES IN THE GLOBAL CLOUD-NATIVE APPLICATION DETECTION & RESPONSE (CNADR) INDUSTRY

FROST & SULLIVAN

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. Upwind excels in many of the criteria in the CNADR space.



RECOGNITION CRITERIA

Visionary Innovation & Performance	Customer Impact
Addressing Unmet Needs	Price/Performance Value
Visionary Scenarios Through Megatrends	Customer Purchase Experience
Leadership Focus	Customer Ownership Experience
Best Practices Implementation	Customer Service Experience
Financial Performance	Brand Equity

The Transformation of the CNADR Industry

Traditionally, SecOps/SOC teams have been centered around key threat management-associated tasks, including threat monitoring, incident response, threat intelligence analysis, and security vulnerability management. Often, they deal with conventional threats, mainly in on-premises environments, using traditional security and security monitoring tools, such as SIEM, UEBA, and XDR.

However, with the surge in the adoption of cloud and cloud-native application services, these conventional threat management strategies have become inadequate due to the dynamic, complex, distributed, ephemeral, and scalable nature of these cloud technologies. SecOps teams do not have comprehensive and real-time visibility into the threat landscape of their cloud assets, particularly cloud resources, such as containers and serverless functions that can be spun up and down rapidly, creating a constantly changing attack surface and making it challenging for SecOps teams to detect and respond to threats effectively.

The multi-layered architecture of cloud-native applications, involving containers, microservices, and underlying infrastructure, complicates both threat detection and incident response. Attacks can move across these layers, starting at the application level, exploiting API or unknown vulnerabilities, and moving laterally through the container layer to the cloud infrastructure.

Many organizations use CNAPP and AppSec tools to solve cloud and application security issues. CNAPP and AppSec testing tools are embedded into DevOps workflows and offer visibility into cloud infrastructure and CI/CD pipelines, automating the detection of vulnerabilities and compliance issues, from code to cloud.

While delivering great value for compliance, vulnerability, and misconfiguration management, CNAPPs lack robust capabilities for real-time detection and response to active threats. They bring limited value to SOC teams, with excessive false positives, no real-time threat detection, and an inability to provide runtime visibility or adequate contextualization. Similarly, AST tools fail to capture how applications behave in production under real-world conditions and often generate a high number of false positives due to the lack of runtime context, whereas traditional runtime tools suffer from static rule-based detection, fragmented visibility, and operational inefficiencies, leaving SecOps teams struggling to address sophisticated, multi-layered threats in dynamic cloud environments.

As a result, organizations are increasingly focusing on modern runtime security to protect their cloud and cloud-native applications from threats. CDR and ADR can provide a better approach to runtime security, filling these gaps by delivering continuous monitoring, behavioral analysis, and actionable insights tailored to both cloud infrastructure and application layers, significantly enhancing SOC efficiency and threat response capabilities.

CDR can provide real-time visibility into ephemeral workloads, multi-cloud environments, and identity-based risks that CNAPPs often fail to provide due to their reliance on periodic scans and limited runtime awareness. ADR tackles the deficiencies of traditional AppSec and runtime solutions by focusing on application-layer threats that WAFs, RASP, and runtime reachability miss, detecting zero-day exploits, API abuse, and supply chain risks in real time, thereby overcoming the static, signature-based limitations of legacy tools and providing SecOps with precise, low-noise alerts that reduce manual triage efforts.

Though both CDR and ADR can bring greater benefits and value to SecOps, relying on standalone CDR and ADR may introduce some challenges and cause security fragmentation as each tool has a specific focus. The use of standalone tools can cause SecOps teams to struggle to correlate events across layers, leading to incomplete threat visibility and delayed responses. CDR and ADR can detect the attack when it occurs in the relevant layer, but without integration, SecOps teams may not have full visibility into the attack chain. For example, CDR might identify a spike in API calls or data exfiltration, but these are typically signs of an attack that has already succeeded in exploiting a vulnerability.

Moreover, installing agents for each solution adds significant complexity and overhead, straining system resources and SecOps teams. This agent sprawl increases operational costs, introduces performance bottlenecks, and complicates management, especially in dynamic cloud-native environments where workloads are ephemeral and scaling is frequent.

To address these challenges, a unified cloud/app runtime security solution is required for modern SecOps to tackle threats in the cloud-native environment. Frost & Sullivan envisions a CNADR platform that integrates the capabilities of CDR, ADR, and other runtime-focused functionalities, such as API security, CWPP, and EDR, to deliver comprehensive threat visibility, detection, and response capabilities across cloud infrastructure, applications, and workloads.

By integrating CDR and ADR, CNADR reduces the need for multiple agents, minimizing system overheads and simplifying security operations. CNADR can correlate an infrastructure event, such as an unauthorized

API call with an application anomaly, to provide context that standalone tools (CDR, EDR, or ADR) do not provide. Through this unified approach, CNADR not only reduces alert fatigue but also aligns with the dynamic, multi-dimensional nature of cloud-native threats, empowering SecOps teams to detect and respond faster and more effectively.

Addressing Unmet Needs Leveraging Industry Evolution

Founded in 2022 and headquartered in Israel, Upwind is a new start-up specializing in runtime-powered CNAPP solutions designed to meet the growing need for unified cloud security solutions, helping organizations deal with the security challenges associated with product segmentation and siloed approaches to risk and threat management in the cloud environment.

Upwind has redefined the CNAPP market by fully integrating runtime intelligence across its platform, offering a consolidated solution that unifies ADR, CDR, CSPM, CWPP, and application security. This unified platform is powered by real-time runtime intelligence. It goes beyond basic visibility to provide unified application and cloud infrastructure runtime visibility, giving security teams rich context to solve configuration, data, and code issues holistically. Unlike traditional CNAPP solutions that often rely on static snapshots, Upwind uses a lightweight, high-performance eBPF sensor (consuming minimal resources [1%–3% CPU]) to help organizations achieve full-stack runtime-powered cloud security rapidly.

> *"Upwind has redefined the CNAPP market by fully integrating runtime intelligence across its platform, offering a consolidated solution that unifies ADR, CDR, CSPM, CWPP, and application security. This unified platform is powered by real-time runtime intelligence. It goes beyond basic visibility to provide unified application and cloud infrastructure runtime visibility, giving security teams rich context to solve configuration, data, and code issues holistically."*
>
> ***- Anh Tien Vu,***
> ***Industry Principal, Global Cybersecurity Practice***

By bridging traditionally separate domains, Upwind offers a single source of truth for cloud risk, dynamically connecting APIs, applications, configurations, identities, workloads, and data flows with runtime context. This visionary approach empowers organizations to see and secure their entire cloud stack in context, a game changer in the cloud/application runtime security industry. The company integrates infrastructure and application security for seamless synergies that address challenges in cloud/application detection and response. Upwind's unified platform not only reduces complexity and tool sprawl but also solidifies its position as the frontrunner in CNADR innovation.

By delivering the following capabilities, Upwind's platform can meet needs that other traditional solutions fail to meet:

Runtime Intelligence and Proactive Defense

By leveraging a high-performance eBPF-based sensor that monitors cloud workloads deep at the kernel level, Upwind can provide unprecedented real-time visibility into process, network, and system behavior with minimal performance impact. This method allows organizations to achieve rich telemetry without sacrificing performance and stability, which are crucial for customers operating at a massive scale. By using the same unified sensor to maintain full-stack visibility, this method does not require the installation of any new agents, avoiding additional complexity when customers extend protection from the cloud infrastructure into the application layer. This enables proactive detection of anomalies and multi-stage attack patterns across the cloud stack, which often evades traditional static rules.

Unified Attack Storylines Through Full-stack Correlation

A standout feature of Upwind's platform is its ability to correlate disparate security signals into a unified attack storyline. Upwind integrates data from cloud misconfiguration scanners, container runtime events, Kubernetes audit logs, identity actions, and more into a single timeline of an incident. This end-to-end visibility allows security teams to immediately understand the who, what, how, and when of any threat scenario across their cloud stack, drastically reducing triage and investigation time by correlating runtime detections with audit logs. By correlating cloud control-plane events with workload-level signals, Upwind provides a complete story of attacks, from an initial misconfiguration or code vulnerability all the way to runtime exploitation and lateral movement, allowing analysts to connect the dots quickly and respond decisively to complex, multi-vector threats.

AI-driven Cloud Baselines

Upwind has also improved its detection engine with AI/ML-driven Cloud Baselines that monitor cloud behaviors over time to build activity profiles and detect anomalies that indicate emerging multi-stage attacks, which move beyond known signatures, enabling proactive identification of sophisticated threats and allowing organizations to intervene before attacks escalate. It can correlate insights from cloud misconfiguration and runtime container detection with cloud audit logs to reduce false positives and speed up investigations, providing security teams with unified visibility of the entire attack storyline—from the initial cloud misconfiguration to the workload compromise, drastically reducing alert fatigue.

From Runtime Threats Back to Code Remediation

More importantly, Upwind bridges the gap between runtime security and development. The platform can trace runtime vulnerabilities and threats back to their origin in code, container images, or misconfigured pipeline processes. The company links real-time risk data to the developers, repositories, and CI/CD pipelines. This enables the identification of the application build or code commit from which it originated, as well as the author of that change, once a malicious process in a container or an exploited vulnerability is detected. In this way, security teams can alert the relevant developer with context to fix the problem at its source before the next deployment. In addition, its built-in, real-time API security is a major differentiator. Leveraging its eBPF sensor, Upwind automatically discovers APIs, builds an API catalog, monitors traffic for sensitive data flows, and tests APIs against OWASP Top 10 CWEs.

Transforming SecOps and Business Outcomes

Upwind's visionary technology has been proven by the real-world outcomes it delivers for customers as it grows its business. CISOs and security teams have benefited from its runtime-powered unified CNAPP platform that helps them achieve significant improvements in efficiency, effectiveness risk posture, and threat management in the cloud environment.

By consolidating formerly siloed tools into a comprehensive platform, Upwind drastically simplifies operations for security teams, helping them save time, centralize cloud security strategy and efforts, and improve response and remediation workflows. This also enables organizations to stay compliant and automate workflows so teams can focus on rapid remediation.

Upwind also eliminates redundant tools and manual correlation work and frees up scarce analyst time and energy, allowing them to operate more proactively without the need to chase noisy alerts or juggle multiple consoles. This consolidation not only cuts costs but also eliminates the blind spots and integration challenges that come with disparate products. This approach helps the company stand out from traditional cloud security vendors that either provide separate tools or tools that are stitched together from acquired technologies, causing tool sprawl and fragmentation and leading to the inefficiency of risk and threat management in the cloud environment.

For SOC/SecOps teams, Upwind's unified, context-rich approach directly translates to faster and more effective threat response. The platform correlates runtime insights and audit logs across the cloud stack, including cloud infrastructure, workload, CI/CD pipelines, and network activities, offering holistic visibility and accelerating the investigation process. Security engineers can instantly see an attack's full storyline and scope, allowing them to understand and respond to cloud threats with unprecedented speed and confidence.

> *"Upwind was the fastest-growing CNADR company in 2024, witnessing an explosive revenue growth of more than 4,000% YoY and continuing to maintain momentum in 2025. The company has gradually become a significant contender and a leading participant in the emerging CNADR industry due to its comprehensive and unique capabilities that correlate risk and runtime data across cloud stack layers."*
>
> ***- Anh Tien Vu,***
> ***Industry Principal, Global Cybersecurity Practice***

Many organizations have made Upwind's platform their central hub for SecOps, breaking down silos between cloud, application, and DevOps stakeholders, driving better focus and collaboration between teams, and facilitating faster decision-making and more resilient cloud environments. For example, by providing detailed threat context, including pinpointing root causes and affected assets, spanning CI/CD pipeline data, process trees, and network topology, Upwind can help security teams increase their incident response speed. It also helps them improve the mean time to detect and remediate incidents, significantly reducing risk exposure.

In addition, organizations benefit from Upwind's strong customer-centric practices. The company works closely with clients to continuously enhance its products, demonstrating a strong commitment to technological innovation, customer support, and product updates to cater to customer needs. This results in high levels of customer satisfaction and trust, enabling Upwind to gain more popularity among customers looking to work with a trusted partner to strengthen their cloud security strategies.

Leadership Focus Through Explosive Growth and Platform Expansion

Upwind was the fastest-growing CNADR company in 2024, witnessing an explosive revenue growth of more than 4,000% YoY and continuing to maintain momentum in 2025. The company has gradually become a significant contender and a leading participant in the emerging CNADR industry due to its comprehensive and unique capabilities that correlate risk and runtime data across cloud stack layers.

Upwind's solutions resonate well with organizations seeking comprehensive cloud and application security, detection, and response capabilities that reduce alert fatigue and improve SecOps and cloud threat hunting efficiency. The company's core business comes from mid-to-large enterprises in key sectors such as BFSI, technology, and eCommerce/retail across North America, where it is executing an aggressive sales strategy. At the same time, Upwind is seeing growing interest from EMEA enterprises and a developing presence in Asia-Pacific, largely through its channel partners.

Particularly, new customer acquisition has been steadily rising, up 40% in Q1 2025, reflecting a strong product-market fit. This momentum is further supported by a meaningful increase in average deal size, driven by larger multi-year contracts and deeper adoption across enterprise accounts. In addition, Upwind's platform usage has surged over time, with core adoption metrics growing more than 200% quarter over quarter for several consecutive quarters, highlighting its strong customer engagement and sustainable growth. The number of new platform evaluations (POCs) has also increased significantly, demonstrating the accelerating market interest and pipeline growth into 2025.

To expand its platform and business presence and leadership, in 2025, Upwind made a strategic move by acquiring Nyx Security, a start-up specializing in application-layer threat detection. This acquisition further strengthens Upwind's ADR capabilities, allowing function-level monitoring of code execution in real time, to further expand its unified CNADR platform. More importantly, this advanced ADR is delivered without adding any new agents as it leverages the same Upwind runtime sensor, preserving the platform's simplicity and allowing it to deliver a truly unified view of threats across both cloud infrastructure and the applications running on top of it. This acquisition demonstrates the company's forward-thinking innovation and commitment to unified cloud security. It also solidifies its leadership position in the CNADR industry by unifying live runtime visibility across infrastructure and application layers, delivering holistic protection in one powerful solution.

Conclusion

Upwind's visionary approach, rapid innovation, and strong customer-centric approach have set it apart as a rising star in cloud security. The company has redefined what CNAPP can achieve through the unified CNADR capabilities on its runtime-powered cloud security platform that protects cloud infrastructure and applications, helping SecOps teams detect and respond to cloud threats effectively. By leveraging runtime intelligence and machine learning, as well as focusing on customer needs, Upwind is gaining tremendous popularity, enabling it to become the fastest-growing CNADR company. With its strong overall performance, Upwind earns Frost & Sullivan's 2025 Global Company of the Year Recognition in the CNDAR industry.

What You Need to Know about the Company of the Year Recognition

Frost & Sullivan's Company of the Year Recognition is its top honor and recognizes the market participant that exemplifies visionary innovation, market-leading performance, and unmatched customer care.

Best Practices Recognition Analysis

For the Company of the Year Recognition, Frost & Sullivan analysts independently evaluated the criteria listed below.

Visionary Innovation & Performance

Addressing Unmet Needs: Customers' unmet or under-served needs are unearthed and addressed to create growth opportunities across the entire value chain

Visionary Scenarios Through Megatrends: Long-range scenarios are incorporated into the innovation strategy by leveraging mega trends and cutting-edge technologies, thereby accelerating the transformational growth journey

Leadership Focus: The company focuses on building a leadership position in core markets to create stiff barriers to entry for new competitors and enhance its future growth potential

Best Practices Implementation: Best-in-class implementation is characterized by processes, tools, or activities that generate consistent, repeatable, and scalable success

Financial Performance: Strong overall business performance is achieved by striking the optimal balance between investing in revenue growth and maximizing operating margin

Customer Impact

Price/Performance Value: Products or services offer the best ROI and superior value compared to similar market offerings

Customer Purchase Experience: Purchase experience with minimal friction and high transparency assures customers that they are buying the optimal solution to address both their needs and constraints

Customer Ownership Excellence: Products and solutions evolve continuously in sync with the customers' own growth journeys, engendering pride of ownership and enhanced customer experience

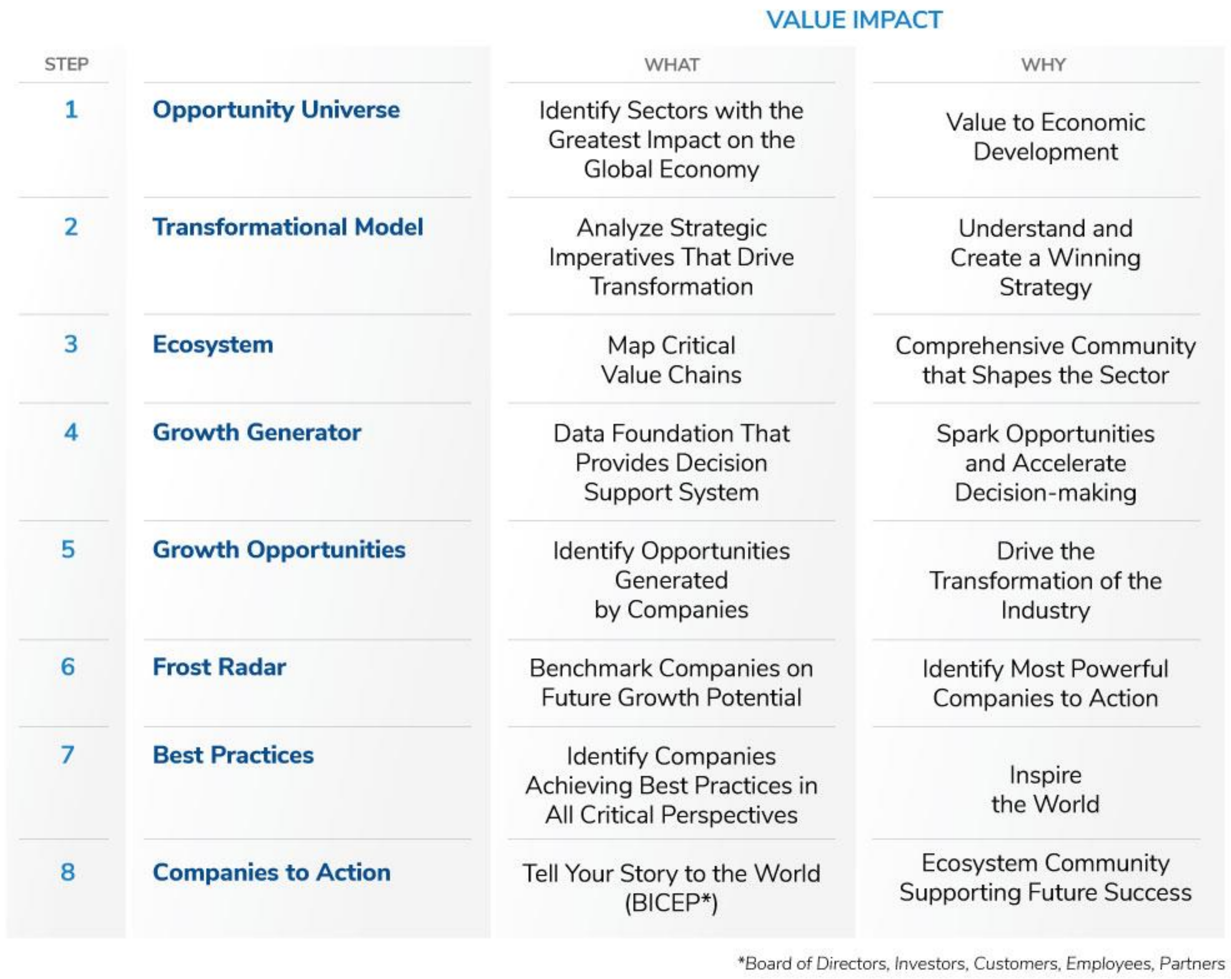
Customer Service Experience: Customer service is readily accessible and stress-free, and delivered with high quality, high availability, and fast response time

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty, which is regularly measured and confirmed through a high Net Promoter Score®

Best Practices Recognition Analytics Methodology

Inspire the World to Support True Leaders

This long-term process spans 12 months, beginning with the prioritization of the sector. It involves a rigorous approach that includes comprehensive scanning and analytics to identify key best practice trends. A dedicated team of analysts, advisors, coaches, and experts collaborates closely, ensuring thorough review and input. The goal is to maximize the company’s long-term value by leveraging unique perspectives to support each Best Practice Recognition and identify meaningful transformation and impact.



		VALUE IMPACT	
STEP		WHAT	WHY
1	**Opportunity Universe**	Identify Sectors with the Greatest Impact on the Global Economy	Value to Economic Development
2	**Transformational Model**	Analyze Strategic Imperatives That Drive Transformation	Understand and Create a Winning Strategy
3	**Ecosystem**	Map Critical Value Chains	Comprehensive Community that Shapes the Sector
4	**Growth Generator**	Data Foundation That Provides Decision Support System	Spark Opportunities and Accelerate Decision-making
5	**Growth Opportunities**	Identify Opportunities Generated by Companies	Drive the Transformation of the Industry
6	**Frost Radar**	Benchmark Companies on Future Growth Potential	Identify Most Powerful Companies to Action
7	**Best Practices**	Identify Companies Achieving Best Practices in All Critical Perspectives	Inspire the World
8	**Companies to Action**	Tell Your Story to the World (BICEP*)	Ecosystem Community Supporting Future Success

*Board of Directors, Investors, Customers, Employees, Partners

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

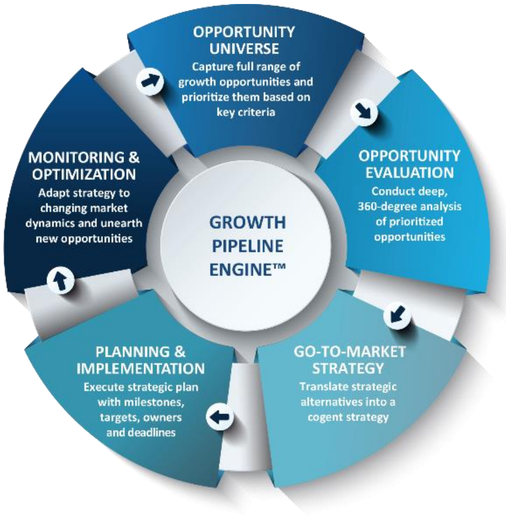
The Growth Pipeline Generator™

Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is 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*



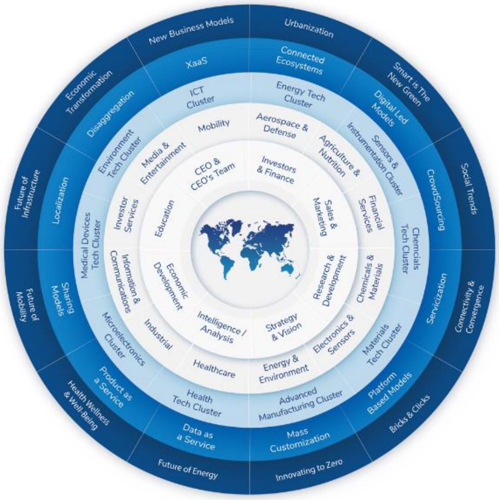
OPPORTUNITY UNIVERSE
Capture full range of growth opportunities and prioritize them based on key criteria
OPPORTUNITY EVALUATION
Conduct deep, 360-degree analysis of prioritized opportunities
GO-TO-MARKET STRATEGY
Translate strategic alternatives into a cogent strategy
PLANNING & IMPLEMENTATION
Execute strategic plan with milestones, targets, owners and deadlines
MONITORING & OPTIMIZATION
Adapt strategy to changing market dynamics and unearth new opportunities
GROWTH PIPELINE ENGINE™

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)



New Business Models
Urbanization
Smart is The New Green
Social Trends
Connectivity & Convergence
Bricks & Clicks
Innovating to Zero
Future of Energy
Health Wellness & Well-Being
Future of Mobility
Future of Infrastructure
Economic Transformation
XaaS
Connected Ecosystems
Digital Led Models
CrowdSourcing
Servicization
Platform Based Models
Mass Customization
Data as a Service
Product as a Service
Sharing Models
Localization
Disaggregation
ICT Cluster
Energy Tech Cluster
Sensors & Instrumentation Cluster
Chemcials Tech Cluster
Materials Tech Cluster
Advanced Manufacturing Cluster
Health Tech Cluster
Microelectronics Cluster
Medical Devices Tech Cluster
Environment Tech Cluster
Mobility
Aerospace & Defense
Agriculture & Nutrition
Financial Services
Chemicals & Materials
Electronics & Sensors
Energy & Environment
Healthcare
Industrial
Information & Communications
Investor Services
Media & Entertainment
CEO & CEO's Team
Investors & Finance
Sales & Marketing
Research & Development
Strategy & Vision
Intelligence / Analysis
Economic Development
Education