SCADAfence Recognized as the

2021

Entrepreneurial Company of the Year

Global Critical National Infrastructure
Cybersecurity Industry
Excellence in Best Practices

FROST & SULLIVAN

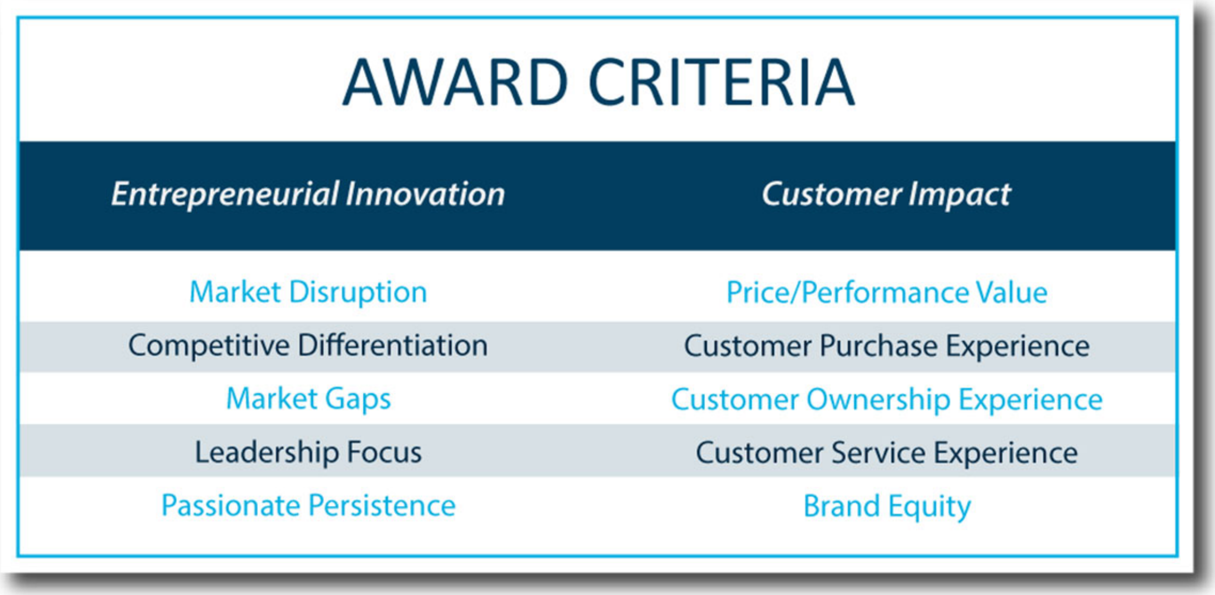
Strategic Imperatives

Frost & Sullivan identifies three key strategic imperatives that impact the security industry: geopolitical chaos, disruptive technologies, and innovative business models. Every company that is competing in the security space is obligated to address these imperatives proactively; failing to do so will almost certainly lead to stagnation or decline. Successful companies overcome the challenges posed by these imperatives and leverage them to drive innovation and growth. Frost & Sullivan's recognition of SCADAfence is a reflection of how well it is performing against the backdrop of these imperatives.

SI8	GEOPOLITICAL CHAOS	DISRUPTIVE TECHNOLOGIES	INNOVATIVE BUSINESS MODELS
Why	• The COVID-19 pandemic caused manufacturing operations that rely on multi-national supply chains to experience significant disruptions. • Project extensions are delaying contract fund allocation, which will affect contractors and subcontractors' bottom lines. • Commercial and passenger-centric industries will experience sharp declines in revenue due to the impact of COVID-19, whereas opportunities in the public sector will grow exponentially. • National security skirmishes between nations continue to cause piecemeal disruptions to security technology deals.	• Investment in digitization will increase to improve the intelligence cycle and address the current threat landscape, which includes ransomware, digital intrusion, and data theft. • Wearables, drones, and augmented reality will find application in crime scene mapping, automatic translation, border surveillance, search and rescue, and threat detection. • Demand will increase for artificial intelligence (AI)-enabled remote or cloud interactions to foster better communication and system support.	• Security forces are gradually transitioning from ownership to subscription-based business models. New business models (e.g., screening as a service, biometrics as a service, ISR as a service, and infrastructure as a service) are reducing the cost of ownership. • Increasing need for niche security solutions, rapid tech advancements, and budget pressures will drive the industry to explore innovative revenue models. • Customers want modular surveillance alternatives that allow for the contracting and scaling of long-term system design.
When	• Firms will need to pursue strategic partnerships between vendors with complementary solutions and local suppliers to improve global customer reach, without increasing their overhead costs. • After the pandemic, larger security companies will realign and acquire portfolios and businesses in growth areas (such as digital security) to expand their solution portfolios across end-user verticals. • Cloud access, zero-trust and multi-factor authentication, and security-as-a-service solutions will become imperative to business continuity in the next 1 to 5 years. • Security firms must understand the national security policies applicable to specific international customers because policy affects security technology.	• Firms must prioritize the development of data analytics and sensor networks' capabilities to provide increased value to customers. • Security companies will need to invest in contactless technologies, biometrics solutions used with AI technology, remote access and authentication, and multi-use analytics in the next 4 to 5 years. • Firms will need to differentiate technology offerings for vertical-specific solutions (i.e., analytics tailored to an airport or public safety function) among multiple end-user industries. • Actionable intelligence and multi-source data aggregation will gain prominence in the next 5 to 10 years, as will the desire to shift some security operations away from a physical location to a cloud-based, remote system.	• Competitive strategy, technology, and IP opportunities will push vendors to re-examine their solutions and road maps to account for market slowdowns. This will lead them to reposition existing offerings to meet new market demands in the next 2 to 3 years. • Achieving vertical market expansion and distribution channel optimization through strategic partnerships and acquisitions will become top priorities in the next 3 to 6 years. • Businesses will seek flexible business models to stay lean by minimizing capital expenditure while ensuring scalability and redundancy in critical operations processes. These models include leasing/renting and moving toward a security as a service (SECaaS) approach in the next 5 years.

Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each Award category before determining the final Award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. SCADAfence excels in many of the criteria in the CNI cybersecurity space.



AWARD CRITERIA

Entrepreneurial Innovation	*Customer Impact*
Market Disruption	Price/Performance Value
Competitive Differentiation	Customer Purchase Experience
Market Gaps	Customer Ownership Experience
Leadership Focus	Customer Service Experience
Passionate Persistence	Brand Equity

Revolutionary and Comprehensive OT and IoT Cybersecurity Solutions

Since the inception of the Internet of Things (IoT), organizations have come to recognize the benefits that the technology can bring to their daily business operations - such as convenience, decreased operational expenditures and downtime, and increased revenue, efficiency, and safety. Although IoT technologies have existed for more than a decade, critical national infrastructure (CNI) organizations (e.g., airports, manufacturing, maritime ports, oil and gas facilities, and utilities) have only begun implementing and enhancing their operations within the last several years. Frost & Sullivan's own research suggests that return on investment uncertainty and a lack of awareness or trust contribute to the industry's slow start to utilize the technology. Moreover, Frost & Sullivan notes that numerous challenges surrounding CNI cybersecurity hinder the technology's proliferation, as most of the operational technology (OT) used in industrial environments is more than five decades old and requires sophisticated cybersecurity solutions.

Due to their age, OT machines were not designed or manufactured with IoT capabilities in mind. As such, cybersecurity vendors and industrial organizations struggle to secure these complex ecosystems adequately. CNI organizations must deploy cybersecurity solutions specifically designed to protect Industrial IoT (IIoT) environments, as traditional information technology (IT) solutions cannot handle the complexity of securing OT equipment. Furthermore, IT and OT systems are often secured through disparate platforms and different vendors, creating protection gaps that cybercriminals can exploit.

Founded in 2014, SCADAfence brings innovation and best-in-class solutions to the CNI industry through its unique, comprehensive, and brand-agnostic OT and IoT cybersecurity platforms. The company's SCADAfence Platform passively and automatically discovers assets, manages inventory, and provides security teams with unmatched threat detection and risk management through real-time alerts, risk scoring, and actionable intelligence. Equipped with advanced analytics, artificial intelligence (AI), and machine learning (ML) capabilities, the company's SCADAfence Platform and SCADAfence IoT Security solutions continuously monitor a client's environment to detect unauthorized or abnormal device and network activities or misconfigurations. The solutions provide security operators with complete network visibility and real-time risk alerts, enabling them to remediate vulnerabilities quickly and efficiently before security events escalate. The company's solutions offer a remote access connection map that provides security teams with a comprehensive view of their organization's ecosystem that shows how devices connect to one another (e.g., follow and analyze the path of how a low-security IoT device can provide a cybercriminal access to highly-secured equipment). Moreover, SCADAfence's products integrate with virtual private network (more commonly known as VPN) gateways to enable activity tracking and policy enforcement across a client's entire environment. Notably, the highly scalable SCADAfence Platform and SCADAfence IoT Security solutions are agentless, i.e., they do not require any additional hardware to deploy and operate.

In addition to inadequately secured OT equipment and systems, IoT endpoints, such as those connected to building automation systems, can offer cybercriminals an avenue to breach an organization's ecosystem. For example, a hacker can infiltrate a smart thermostat and work through an organization's network to take over or shut down devices or systems. Some IoT and OT cybersecurity solutions will take such endpoints offline until security personnel can remediate security gap issues and then reactivate and reconnect them to the network. However, this process significantly reduces operational uptime, productivity, safety, security, and the organization's return on investment for those devices or systems. Furthermore, the security industry is experiencing a massive professional shortage, which further exacerbates such issues when personnel cannot repair, configure, and reintegrate these devices in a timely fashion (due to a backlog of other tasks they must address).

> *"Equipped with advanced analytics, AI, and ML capabilities, the company's SCADAfence Platform and SCADAfence IoT Security solutions continuously monitor a client's environment to detect unauthorized or abnormal device and network activities or misconfigurations. The solutions provide security operators with complete network visibility and real-time risk alerts, enabling them to remediate vulnerabilities quickly and efficiently before security events escalate."*
>
> ***- Tara Semon, Best Practices Research Team Leader***

SCADAfence's IoT Security platform automatically and immediately remediates such issues, removing a security team's need to resolve them manually while enabling the organization to maintain security resiliency continually. SCADAfence's IoT Security solution protects a client's IoT endpoints in a single platform, allowing the organization to view their complete cybersecurity status, reduce labor costs, and achieve a high return on investment for SCADAfence's platform and the devices and systems it protects.

Moreover, the company's platforms are brand-agnostic and agentless. As such, they do not require any additional hardware to integrate endpoints (regardless of brand, model, or firmware version), allowing SCADAfence to deploy its solution remotely, enabling the company and its clients to follow COVID-19 social distancing recommendations.

SCADAfence IoT Security supports devices and systems such as access control, IoT gateways, Internet protocol (IP) cameras and network video recorders, network-access storage, printers, smart sensors and televisions, and voice-over IP phones. Since the company's solutions are brand-agnostic, its platforms seamlessly integrate with a client's existing management systems, including firewalls, security operations centers, and security information and event management. Moreover, the platform automatically inventories all of a client's assets (significantly reducing the attack surface), provides in-depth endpoint data, and alerts security teams to abnormal (network or user) behaviors and malicious activities (e.g., malware). SCADAfence IoT offers real-time comprehensive and easy-to-understand actionable intelligence that allows security personnel to remediate vulnerabilities quickly and seamlessly, significantly reducing their need to interact physically with devices, saving time and operational expenditures, and increasing safety and security. Moreover, the platform detects known and zero-day vulnerabilities through the platform's AI and ML capabilities that learn a client's normal network behaviors and notifies security teams of any anomalous or suspicious activities.

> *"While the global COVID-19 pandemic has affected organizations across nearly every industry, causing decreased revenue due to various factors, such as social distancing and lockdowns, SCADAfence has remained unscathed. The company overcomes and dominates the challenges presented by COVID-19 through its comprehensive solutions, exceptional customer support, and robust partnerships with other leading cybersecurity technology vendors."*
>
> ***- Tara Semon, Best Practices Research Team Leader***

CNI environment security is vital for several reasons. An IIoT cybersecurity solution that cannot protect equipment from breaches provides cybercriminals with a remote and simple path to hack an organization's network to steal confidential information or take control of sensors and systems. Organizations must employ adequate cybersecurity solutions to protect the OT assets deployed at their sites. Moreover, organizations that do not secure their endpoints and systems can face steep consequences, such as hefty fines, job losses, and even loss of life, if a cybercriminal breaches their ecosystem. Companies must ensure they meet strict industry compliance regulations, e.g., the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), and the European Union's Directive on security of network and information systems (NIS Directive).

Moreover, compliance regulation authorities conduct periodic audits on an organization's ecosystem to ensure that they meet the mandates required for their respective industry. However, gathering the necessary information to prove that they secure their devices and systems to meet industry mandates requires manpower that most organizations simply do not have at their disposal. Even if they do possess the necessary workforce to support such feats, it would expose the cybersecurity process to human error. Thus, businesses must utilize automated solutions to collect the relevant data. The primary challenge with this approach is that most IoT and OT cybersecurity solutions cannot discover and inventory all of the devices and machinery on an organization's network. Furthermore, endpoints continually change their status, making them more challenging to detect. Many devices and systems fall under the radar and go unprotected, consequently burdening the organization's security team with the task of remediating network security gaps in addition to their already backlogged responsibilities.

SCADAfence's Governance Portal logs network activities and the security resiliency of endpoints and systems (patches, firewall statuses, policies, updates) to auto-populate a compliance audit report, making the audit process both seamless and accurate. The solution logs network activities such as user actions, their authorization level, and password strength; abnormal endpoint behaviors (e.g., when a sensor, such as a pressure or temperature gauge, reaches a certain threshold that could cause damage to property, harm employees, or shut down systems), and other unintentional or malicious events. SCADAfence's Governance Portal enables clients to maintain industry compliance with standards including the European Union's NIS Directive, IEC 62443, ISO 27001, NCSC CAF, NERC CIP, NIST 1800-23, and NIST CSF. Moreover, SCADAfence's portal enables security teams to pre-define and enforce company-specific security policies. The company's Governance Portal also creates site-specific reports, allowing security personnel to view and improve each site's security posture, which ultimately enables them to achieve holistic cybersecurity across the entire organization. Frost & Sullivan notes that SCADAfence's Governance Portal works with both IT and OT environments. It allows security teams to view risk trends (historical to current) to see how the organization's cybersecurity posture improves over time.

Meeting Customers' Needs through Operational Efficiency and a Customer-centric Approach

While the global COVID-19 pandemic has affected organizations across nearly every industry, causing decreased revenue due to various factors, such as social distancing and lockdowns, SCADAfence has remained unscathed. In fact, in Q2 2020, the company closed its fastest deal ever in only 31 days. In the age of COVID-19, many vendors struggle to spread market awareness, practice common marketing tactics, capture more market share, and build customer relationships as they cannot execute traditional strategies, such as attending tradeshows or traveling to a prospective client's site to conduct a proof-of-concept. SCADAfence overcomes and dominates the challenges presented by COVID-19 through its comprehensive solutions, exceptional customer support, and robust partnerships with other leading cybersecurity technology vendors. In addition to caring for their customers throughout the pandemic, SCADAfence also provided their employees with the necessary resources for their remote working environments, further prioritizing their employees' success.

Since the SCADAfence Platform and SCADAfence IoT Security are cloud-hosted, clients can access, monitor, and manage a single facility or multiple sites from anywhere in the world, which enables operators to secure the environment and endpoints (e.g., employer-issued or personal desktops, laptops, tablets, or smartphones) while working remotely. The SCADAfence Platform can also be deployed within an on-premise environment, due to the very nature of OT security environments. Likewise, SCADAfence can easily and remotely demonstrate the power of its solutions to potential clients by analyzing their environment's data to show the cybersecurity gaps they need to address and the value that SCADAfence's platforms can bring to their daily operations and organizational security. Moreover, the company's user-intuitive platforms display data in a format that anyone can understand, using bar graphs, color-coding, and priority level alerts. SCADAfence's solutions prevent "data overload" by cutting out irrelevant information to create role-specific cybersecurity risk reports for a client's different divisions and employees. For example, the data relevant for a floor supervisor is different from the information that a C-level executive needs.

SCADAfence partners with world-renowned brands including Barracuda, Check Point, Cisco, CyberArk, Forcepoint, Fortinet, IBM, Oracle, Palo Alto Networks, and RSA. The company also expanded its partnership with Rapid7 to become their strategic OT cybersecurity partner, joining Rapid7 in new customer pitches and campaigns to sell combined IT and OT cybersecurity solutions. Through its technology partnerships and internal research and development, SCADAfence delivers best-in-class vendor-agnostic solutions across multiple critical industries globally. The company serves clients globally, utilizing building management, CNI, and manufacturing equipment, devices, and systems. SCADAfence provides outstanding customer support through highly-trained channel partners and its internal dedicated customer service teams that work with clients throughout the entire relationship lifecycle.

SCADAfence develops and prioritizes its product roadmap based directly on customers' feedback, feature/capability needs, and customization demands. For example, the company added the user activity tracking feature to its platforms in response to more clients implementing work-from-home strategies due to the global COVID-19 pandemic. In addition, the company offers extended cybersecurity services to help clients protect their ecosystem regardless of their in-house security professional shortage. The company nicely offers a simple pricing model based on the number of devices a client needs secured and is available as a monthly subscription or a licensed product.

Frost & Sullivan analysts believe that SCADAfence's ability to secure both IoT and IIoT cybersecurity environments positions it to capture even more market share, as many other cybersecurity vendors simply do not offer solutions that can protect these two diverse environments. Demonstrating the company's versatility and customer satisfaction, clients praise SCADAfence for its technology and customer support:

> *"If it wasn't for SCADAfence, we would not have known of those remote access connections, since we thought we had our firewalls set up correctly, but SCADAfence was able to surface that traffic and then help us to keep the intruders out."*
>
> -Jeff R., Network Administrator for the City of Hutchinson, Kansas
>
> *"Working with SCADAfence, my goodness, they have been outstanding & they're awesome to work with. They are always working with us on how to use the tool better. There are very few vendors I've worked with that want to make sure you were really using their product; it wasn't just the sale. We're also helping them to further improve their products so we have a great two-way relationship."*
>
> - Jeff R., Network Administrator for the City of Hutchinson, Kansas

> *"With SCADAfence we got 120% of what was promised instead of 80% what was promised. That's rare in today's culture, where we got more than what was actually sold to us."*
>
> -Gene W., OT systems administrator at a United States Midwest Refinery
>
> *"If you're trying to fulfill the requirements of NERC CIP, with CIP-002 and CIP-003, you have to know who's on your network, how they're accessing your network, and what they're doing. SCADAfence is the only software that lets you build a custom policy, and then continuously monitors the compliance in real time, based on real data points."*
>
> -Gerald K., Plant Manager at the Garrison Energy Center

Further impressing Frost & Sullivan's research analysts, SCADAfence's clients' technology vendors praise SCADAfence and recognize the benefits and value that the company's solutions can bring to an organization:

> *"I'm frequently asked how much time an IT admin must allocate toward working with the SCADAfence platform, and I tell people about the City of Hutchinson's experience. Hutchinson's IT staff monitors over 4,000 assets in the platform, and it only takes them a few minutes each day to glance at the dashboard and handle new alerts. That's where the user interface and under-the-hood machine learning sets SCADAfence apart from other systems."*
>
> -Clint S., Sales Engineer, Logic, Inc.
>
> *"In addition to great detection, we also found that SCADAfence's alerting to be highly accurate. The alerts have been confirmed by our network engineers.[Furthermore], the only way you can prove that you're compliant with all of the NERC requirements is to show them the data in the SCADAfence Governance Platform. We no longer have to fill out compliance surveys, since the compliance reports and real-time alerts which SCADAfence provides us, ensure that we are compliant with the latest industry standards and that the power plant is running safely."*
>
> -Shawn L., Consulting Engineer at iV4, a ProArch Company

The company's most recent major deployment was in April 2021 for Murata, a Japanese electronic component manufacturer. The client selected SCADAfence to secure their 60 manufacturing facilities worldwide and facilitate their SmartFactory initiative. The company's innovative technology and customer-centric approach earn it customer trust and loyalty, cementing client relationships and positioning it for exponential growth. Serving as a testament to SCADAfence's innovative spirit and healthy growth potential, the company aims to develop smart metering (power and water) and smart city solutions in the near future by using its patented algorithms and advanced AI, ML, and analytics capabilities as the core for the new technology.

Conclusion

The critical national infrastructure (CNI) industry faces significant cybersecurity challenges that hinder an organization's operational technology (OT) ecosystem security, primarily the complexity of securing such equipment due to their age. Another major challenge is that OT cybersecurity solutions cannot detect and inventory all of the endpoints on an organization's network. Therefore, many devices and systems go unprotected, causing CNI companies to fall victim to cyberattacks and fail industry compliance audits. CNI organizations must deploy an OT cybersecurity solution that protects their environment and ensures they remain compliant with strict industry standards.

SCADAfence offers unparalleled endpoint detection, inventory management, threat detection, vulnerability management, and compliance governance solutions for OT and Internet of Things environments. The company's platforms relieve short-staffed and overwhelmed security professionals by automatically and accurately protecting a client's ecosystem through patented algorithms and advanced analytics, artificial intelligence, and machine learning capabilities. Moreover, SCADAfence offers extended cybersecurity services to help clients that do not have enough in-house cybersecurity professionals to protect their environment. The company provides exceptional customer support by building close client relationships and developing its product roadmap directly from customer feedback, needs, and requests, earning its clients' trust and loyalty. Moreover, the global COVID-19 pandemic devastated companies across nearly every industry; Frost & Sullivan applauds the way that SCADAfence has clearly thrived due to its innovative spirit, outstanding customer support, and robust partnerships with well-known brands.

With its game-changing platforms, customer-centric approach, and strong overall performance, SCADAfence earns the 2021 Frost & Sullivan Global Entrepreneurial Company of the Year Award.

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

Frost & Sullivan's Entrepreneurial Company of the Year Award recognizes the best up-and-coming, potentially disruptive market participant.

Best Practices Award Analysis

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

Entrepreneurial Innovation

Market Disruption: Innovative new solutions have a genuine potential to disrupt the market, render current solutions obsolete, and shake up competition

Competitive Differentiation: Strong competitive market differentiators created through a deep understanding of current and emerging competition

Market Gaps: Solution satisfies the needs and opportunities that exist between customers' desired outcomes and their current market solutions

Leadership Focus: Company focuses on building a leadership position in core markets and on creating stiff barriers to entry for new competitors

Passionate Persistence: Tenacity enables the pursuit and achievement of seemingly insurmountable industry obstacles

Customer Impact

Price/Performance Value: Products or services provide the best value for the price compared to similar market offerings

Customer Purchase Experience: Quality of the purchase experience assures customers that they are buying the optimal solution for addressing their unique needs and constraints

Customer Ownership Experience: Customers proudly own the company's product or service and have a positive experience throughout the life of the product or service

Customer Service Experience: Customer service is accessible, fast, stress-free, and high quality

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty

About Frost & Sullivan

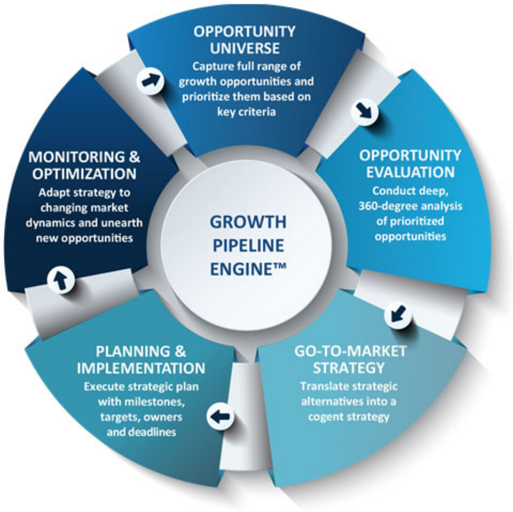
Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, 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 Engine™

Frost & Sullivan's proprietary model to systematically create on-going 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

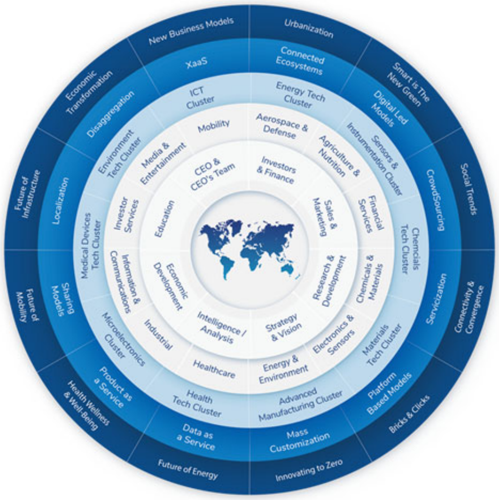

OPPORTUNITY UNIVERSE
Capture full range of growth opportunities and prioritize them based on key criteria
OPPORTUNITY EVALUATION
Conduct deep, 360-degree analysis of prioritized opportunities
GO-TO-MARKET STRATEGY
Translate strategic alternatives into a cogent strategy
PLANNING & IMPLEMENTATION
Execute 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 six analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives. Learn more.

Analytical Perspectives:

- ■ Mega Trend (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