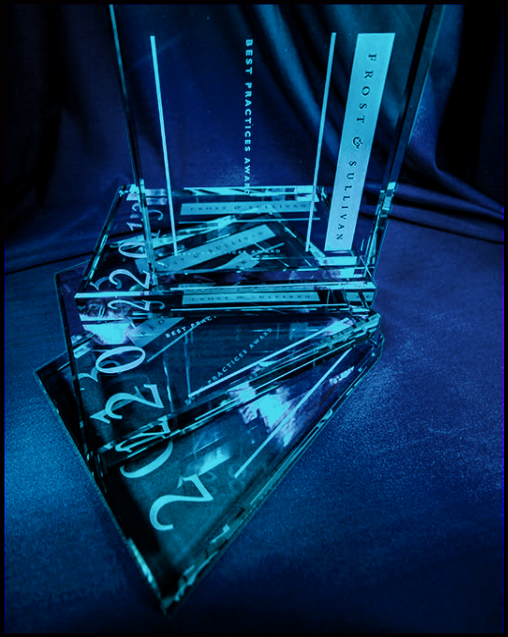
FROST & SULLIVAN

NexDefense

# 2016 North American Industrial Cybersecurity Monitoring Software Entrepreneurial Company of the Year Award



FROST & SULLIVAN

2016 BEST PRACTICES AWARD

NORTH AMERICAN INDUSTRIAL CYBERSECURITY MONITORING SOFTWARE ENTREPRENEURIAL COMPANY OF THE YEAR AWARD

2016
BEST PRACTICES
AWARDS

# Contents

# Background and Company Performance

## *Industry Challenges*

Many of the industrial control systems (ICS) in use today are built with legacy products not resilient enough to weather modern security attacks. This is because most automation product and networks in the past were originally designed for isolated, closed-loop communications without any external connectivity nor a need to route data outside of the system. Since these systems lacked Internet Protocol (IP)-enabled devices, control product security hardening, encryption, authentication, and other security protections were just not necessary in these aging systems, many of which still continue to operate nearly as-is on a 24x7x365 schedule.

Today however, the Industrial Internet of Things (IIoT) is sweeping across discrete and process industries alike, bringing with it the Cloud, Big Data, and Analytics; all of which have brought considerable value when it comes to asset performance, operations, energy efficiency and productivity. The downside to the connectivity required for these technologies and services is that it increases a system’s potential attack-surface and susceptibility to threats. Because the IIoT environment generates massive amounts of data, intricate security layers are needed to protect the data being sharing across various devices, systems and networks. Today's solution providers are therefore tasked with developing systems that are compatible with these legacy ICS installations. The alternative would be to push a more expensive and time consuming "rip-and-replace" solution that won't sit well with companies looking to keep costs down and not interrupt regular operations with new system deployments.

End-to-end ICS cybersecurity for data in transit can be achieved through various methods including physical security, secure authentication and authorization, encrypted communication channels, intelligent firewalls, deep packet inspection filtering, automated intrusion detection, and perimeter-monitoring solutions. These cybersecurity controls and technical solutions need to accommodate the intricacies of other industrial devices or networking technologies so that security is also ensured for the array of open industrial communication protocols already established like BACnet, DNP3, EtherNet/IP, Foundation Fieldbus HSE, IEC61850, ModbusTCP, OPC, Profinet and other lesser known open and proprietary industrial Internet protocols. Unlike the business enterprise and Information Technology world, the ICS world is more complicated because of the wide variety of standard practices and legacy ICS systems that have been deployed that often continue to operate tirelessly for years to decades. For controls engineers and operators, visibility into these systems typically consists of watching the status of the overall process, obtaining specific device health and status details, and checking the quality and integrity of the resulting products and services the systems produce. However, the ability to monitor the network and check the system and its data packets that enable control, configuration and data collection without affecting network safety, integrity and performance at the application layer is crucial in the ICS arena. This is especially true given the complexity of the network infrastructure needed in today's contemporary systems.

With the industry becoming a mix of IT and Operational Technology (OT) networks, implementation of IIoT is complicated and the price for these solutions increases in proportion to the integration complexities of various devices, systems and software applications. However, ICS cybersecurity monitoring software is extremely important because historically it has been absent from most every control system installation; yet when used, it can enable crucial situational awareness that will distinguish between good and bad (vulnerable) data packets and provide actionable intelligence that can help keep systems safe while also guiding engineers and technicians to make more informed decisions.

## *Entrepreneurial Innovation and Customer Impact*

**Price/Performance Value**

Numerous attacks that targeted ICSs in the past using specially crafted malware (i.e. Stuxnet, Duqu, Flame, Shamoon, BlackEnergy) have profoundly impacted the evolving 'threat landscape' and exposed, in some cases even exploited security vulnerabilities both known and unknown in many ICS environments. As many organizations face significant challenges in implementing an effective ICS cybersecurity risk management program, increasing business necessity and demands for implementing IIoT technologies on the plant floor becomes unavoidable. The perceived return on investment from enabling IIoT and connecting new devices (that provide new levels of control and information) can be extremely compelling; However, oftentimes these decisions are not counterbalanced with an understanding or appreciation for the risks and complexity such connectivity brings. For example, in 2014 a blast furnace at a German steel mill was reported to have suffered massive damage following a phishing email that enabled hackers to gain access to the plant's office network and move through the IT systems to reach production systems. It's plausible that the resulting damage to the blast furnace equipment may have been averted altogether had there been appropriate technical and non-technical security controls in place so as not to overlook early indications of unusual, abnormal communications activities in that system.

The high cost incurred from an attack, and its aftermath, more than justifies the need to build a solid ICS system that will give businesses a deep situational awareness on asset inventories, configuration changes and abnormalities. Loss of life, in addition to disruption, damage and destruction of products and services are all potential impacts from a successul attack in the event that preemptive, early-warning signs or indicators of compromize are missed or outright ignored.

NexDefense's Integrity™ industrial network anomaly detection software, is a passive monitoring solution that tracks and closely examines potential threats in the communication connections and patterns of ICS to notify users, in real-time, prior to an attack/breach; the software solution fingerprints what is connected and communicating to allow its user to create a baseline of expected, normal and acceptable network operation. Integrity™ detects abnormal events and activity even at lowest communication levels in industrial Ethernet systems, addressing the abovementioned issues and notifying those responsible for maintaining an ICS of the time and details associated with events that may give rise to safety and security concerns. It can also simultaneously deliver detailed alert data to other automated security controls used to help protect a given system. Because many ICS environments evolve slowly and contain multiple legacy devices from a variety of manufacturers, NexDefense designed Integrity™ with the ability to distinguish between connected devices, communication ports and protocols, packet payloads with control commands, and the interactions and abnormal conditions that may indicate trouble or malicious activites within a system.

The Integrity™ solution can help organizations align and comply with contemporary guidelines, best-practices and standards. For instance, it can help those firms seeking to comply with voluntary cybersecurity frameworks and guidelines like the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), the NIST SP 800-82 R2: Guide to Industrial Control System (ICS) Security, or industrry standards like the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) and international standards including the ISA/IEC 62443 series. Integrity™ is designed to be a permanent part of a cybersecurity solution for ICS to monitor, log and analyze relevant network events in real time (or offline via packet capture analysis) so that users can protect already-operating systems in real-time or replay data-traffic patterns in post-event troubleshooting and forensics activities, enabling them to better understand normal versus abnormal events and adjust their security protocol configurations as needed.

**Customer Experience**

The Integrity™ solution grew out of a proof-of-concept project and collaboration between the Department of Energy, Battelle Energy Alliance and Idaho National Lab (INL). In 2013 NexDefense acquired exclusive rights to the concept and preliminary work. It has since commercialized the concept into today’s patent-pending Integrity™ software solution, tailoring it and making it suitable for addressing the growing cyber security needs of all critical infrastructure and manufacturing sectors. To ensure its compatibility with legacy systems and its ability to deliver superior security, the Integrity™ solution has been beta-tested by more than 70 organizations. Integrity™ is engineered to ensure it has full visibility to device activities and communication patterns, abnormal events and unusual activities to ensure there are no blind spots in ICS networks and to detect over 60 protocols via deep packet inspection making it a best-in-class solution.

Beyond its Integrity™ software solution, NexDefense also started a “Fellowship” program to raise awareness and educate automation professionals, potential customers and employees on contemporary ICS security issues. As IIoT technologies become more widely spread and implemented, this type of program will help raise awareness and open the door for public discussions regarding security issues to help foster innovation in the industry. This approach also helps to counteract the severe shortage of skilled/training workers in ICS security space. This kind of interactive mind sharing enriches customer knowledge and experience and helps them better understand and appreciate the intricacies of their systems and industrial security needs.

As a good example of the excellent 'customer experience' that NexDefense has achieved, Scitor Corp., a Science Applications International Corp. (SAIC) Company, deployed Integrity™ software to assess and secure its customers' ICS installations. Because Scitor already participated in the software beta program, it was well aware that Integrity™ was the ideal choice for its ICS cybersecurity framework. Scitor felt that the main value in Integrity™ was related to the real-time visibility on anomalies in ICS networks and the ability to gain actionable intelligence, enabling users to maintain operations and augment security, all without interrupting operations.

### Competitive Differentiation

Frost & Sullivan anticipates NexDefense to achieve a leadership position in the industrial cybersecurity monitoring software market in the coming years. As many security vendors try to approach the industrial market via their broader solutions, NexDefense's Integrity™ solution approaches the market through the operational technology (OT) side of things. Integrity™ is also unique because, unlike competing systems, it allows operators to visualize in a 3D environment specific device connections, interactions and security event data in an intuitive and visually informative manner. This intuitive visualization interface offers expanded data analysis, event views and anomaly reports giving users both a deep and broad look into their unique security landscape. In short, the Integrity™ product solution enables customers to streamline workflows, reduce liabilities and better-ensure the integrity of their ICS while expanding into IIoT technologies.

### Brand Equity

The initial proof-of-concept for Integrity™ is a result of extensive collaboration between the United States Department of Energy, the Battelle Energy Alliance and cybersecurity experts from the Idaho National Laboratory (INL). As a NexDefense product, Integrity™ is deployed in select US Government applications while also being used during ICS security assessments, incident response activities and cyber security training programs such as those provided by the Department of Homeland Security and its ICS-CERT group.  The comprehensive background of industrial expertise from NexDefense's board and employees, along with their "Fellows" program, create a resonance in the market amid the NERC CIP V6 compliance mandates that take effect post July 1, 2016[1]. As the industrial cybersecurity software market is evolving and expected to have a strong growth rate in

[1] https://ics.sans.org/blog/2016/02/28/ready-set-stop-ferc-postpones-cip-version-5

the coming years, Frost & Sullivan believes that the NexDefense Integrity™ solution will have a big impact in this space. Plus, since this evolving market is based on trust and relationships, NexDefense's team of recognized industry veterans adds further strength to the company's brand equity.

**Passionate Persistence**

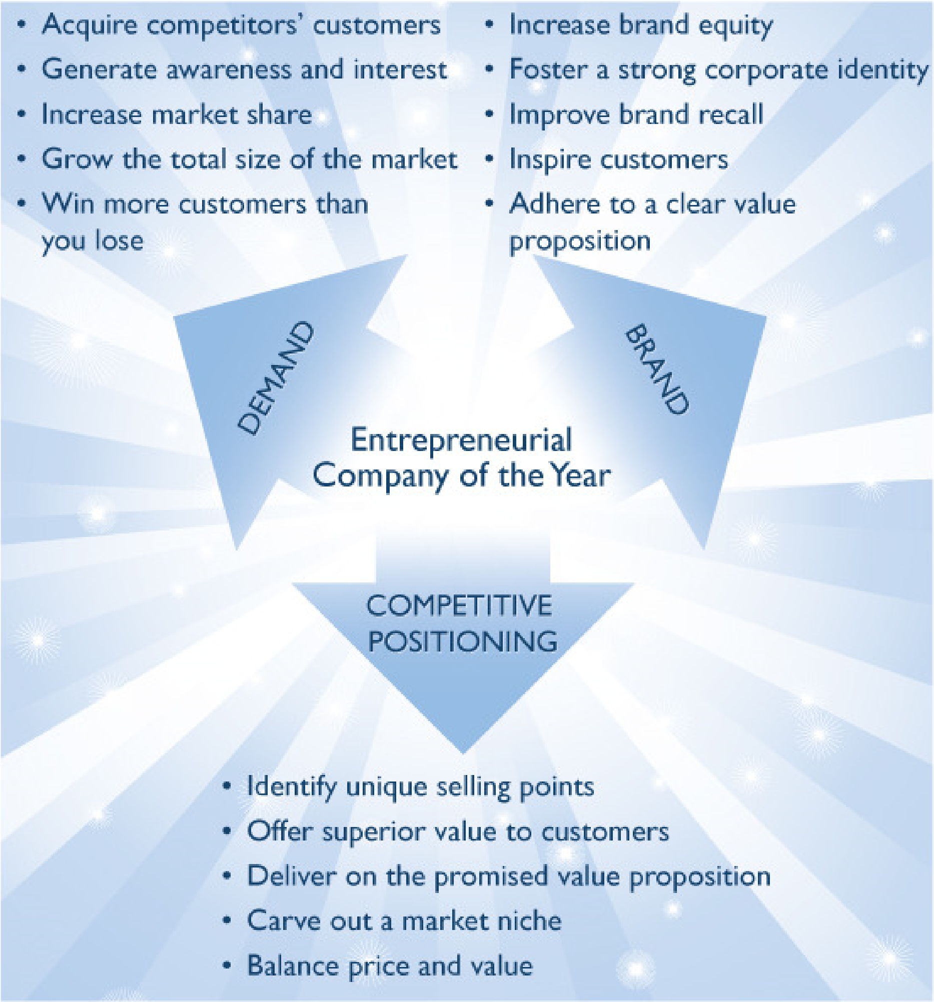
Because of strong growth in the IIoT market and ICS cybersecurity compliance mandates from regulatory authorities and sector-specific agencies, NexDefense is gaining a lot of traction for Integrity™ with always-on products and always-available networks. The company completed an investment seeding round in November 2014 and raised a total of $5.62 million to date. The top industry veterans in NexDefense executive team have a deep belief in the NexDefense's product strategy that helps to tangibly combat the increasing cybersecurity threats to critical infrastructure. As an emerging company in the industrial cybersecurity space, NexDefense is building a confluence of IT and OT security experts and advisors who are committed to develop a robust industrial cybersecurity monitoring software despite tough competition from various market participants.

## Conclusion

Frost & Sullivan's independent research shows NexDefense's Integrity™ software to be the ideal security solution for ICS's. Because of its passive situational awareness features that include device idenitification and traceability, network anomaly detection, expanded data analysis, views and reports, user-defined customization, tracking change management and issuance of real-time alerts, Integrity™ stands above all others in the evolving ICS cybersecurity monitoring software market. Thanks to its strong team, solid product strategy, and timely launch in the market, NexDefense is recognized with Frost & Sullivan's 2016 Entrepreneurial Company of the Year Award in the Industrial Cybersecurity Monitoring Software market.

## Significance of Entrepreneurial Leadership

Ultimately, growth in any organization depends upon customers purchasing from your company, and then making the decision to return time and again. In a sense, then, everything is truly about the customer—and making those customers happy is the cornerstone of any long-term successful innovation or growth strategy. To achieve these dual goals (customer engagement and growth), an organization must be best-in-class in three key areas: understanding demand, nurturing the brand, differentiating from the competition. This three-fold approach to successful entrepreneurship is explored further below.



- Acquire competitors' customers
- Generate awareness and interest
- Increase market share
- Grow the total size of the market
- Win more customers than you lose

- Increase brand equity
- Foster a strong corporate identity
- Improve brand recall
- Inspire customers
- Adhere to a clear value proposition

- Identify unique selling points
- Offer superior value to customers
- Deliver on the promised value proposition
- Carve out a market niche
- Balance price and value

## Understanding Entrepreneurial Leadership

Demand forecasting, branding, and differentiation are part of an entrepreneurial company's larger journey toward forming deep relationships with customers and permanently altering the market with their actions. These two concepts—entrepreneurial innovation and customer impact—are therefore the cornerstones of this award, as discussed further in the next section.

## *Key Benchmarking Criteria*

For the Entrepreneurial Company of the Year Award, we evaluated two key factors—Entrepreneurial Innovation and Customer Impact—according to the criteria identified below.

### Entrepreneurial Innovation

Criterion 1: Market Disruption
Criterion 2: Competitive Differentiation
Criterion 3: Market Gaps
Criterion 4: Blue Ocean Strategy
Criterion 5: Passionate Persistence

### Customer Impact

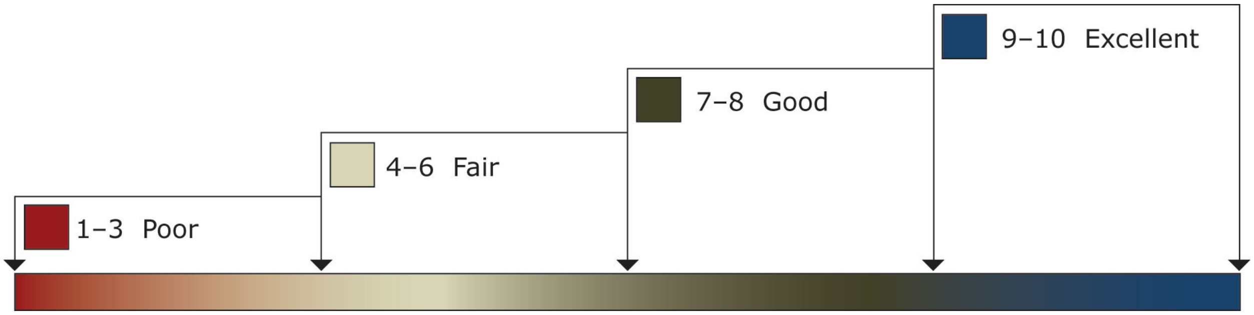
Criterion 1: Price/Performance Value
Criterion 2: Customer Purchase Experience
Criterion 3: Customer Ownership Experience
Criterion 4: Customer Service Experience
Criterion 5: Brand Equity

## Best Practice Award Analysis for NexDefense

## *Decision Support Scorecard*

To support its evaluation of best practices across multiple business performance categories, Frost & Sullivan employs a customized Decision Support Scorecard. This tool allows our research and consulting teams to objectively analyze performance, according to the key benchmarking criteria listed in the previous section, and to assign ratings on that basis. The tool follows a 10-point scale that allows for nuances in performance evaluation; ratings guidelines are illustrated below.

RATINGS GUIDELINES



The Decision Support Scorecard is organized by Entrepreneurial Innovation and Customer Impact (i.e., the overarching categories for all 10 benchmarking criteria; the definitions for each criteria are provided beneath the scorecard). The research team confirms the veracity of this weighted scorecard through sensitivity analysis, which confirms that small changes to the ratings for a specific criterion do not lead to a significant change in the overall relative rankings of the companies.

The results of this analysis are shown below. To remain unbiased and to protect the interests of all organizations reviewed, we have chosen to refer to the other key players in as Company 2 and Company 3.

| *Measurement of 1–10 (1 = poor; 10 = excellent)* | | | |
|---|---|---|---|
| Entrepreneurial Company of the Year | Entrepreneurial Innovation | Customer Impact | Average Rating |
| | | | |
| **NexDefense** | **9.0** | **9.0** | **9.0** |
| Competitor 2 | 7.0 | 7.0 | 7.0 |
| Competitor 3 | 7.0 | 5.0 | 6.0 |

## *Entrepreneurial Innovation*

### Criterion 1: Market Disruption

Requirement: Innovative new solutions that have a genuine potential to disrupt the market, obsoleting current solutions and shaking up competition

### Criterion 2: Competitive Differentiation

Requirement: Deep understanding of both current and emerging competition to create and communicate strong competitive differentiators in the market

### Criterion 3: Market Gaps

Requirement: A clear understanding of customers' desired outcomes, the products that currently help them achieve those outcomes, and where key gaps may exist

### Criterion 4: Blue Ocean Strategy

Requirement: Strategic focus in creating a leadership position in a potentially "uncontested" market space, manifested by stiff barriers to entry for competitors

### Criterion 5: Passionate Persistence

Requirement: A deep belief in the "rightness" of an idea, and a commitment to pursuing it despite seemingly insurmountable obstacles

## *Customer Impact*

### Criterion 1: Price/Performance Value

Requirement: Products or services offer the best value for the price, compared to similar offerings in the market

### Criterion 2: Customer Purchase Experience

Requirement: Customers feel like they are buying the most optimal solution that addresses both their unique needs and their unique constraints

### Criterion 3: Customer Ownership Experience

Requirement: Customers are proud to own the company's product or service, and have a positive experience throughout the life of the product or service

**Criterion 4: Customer Service Experience**

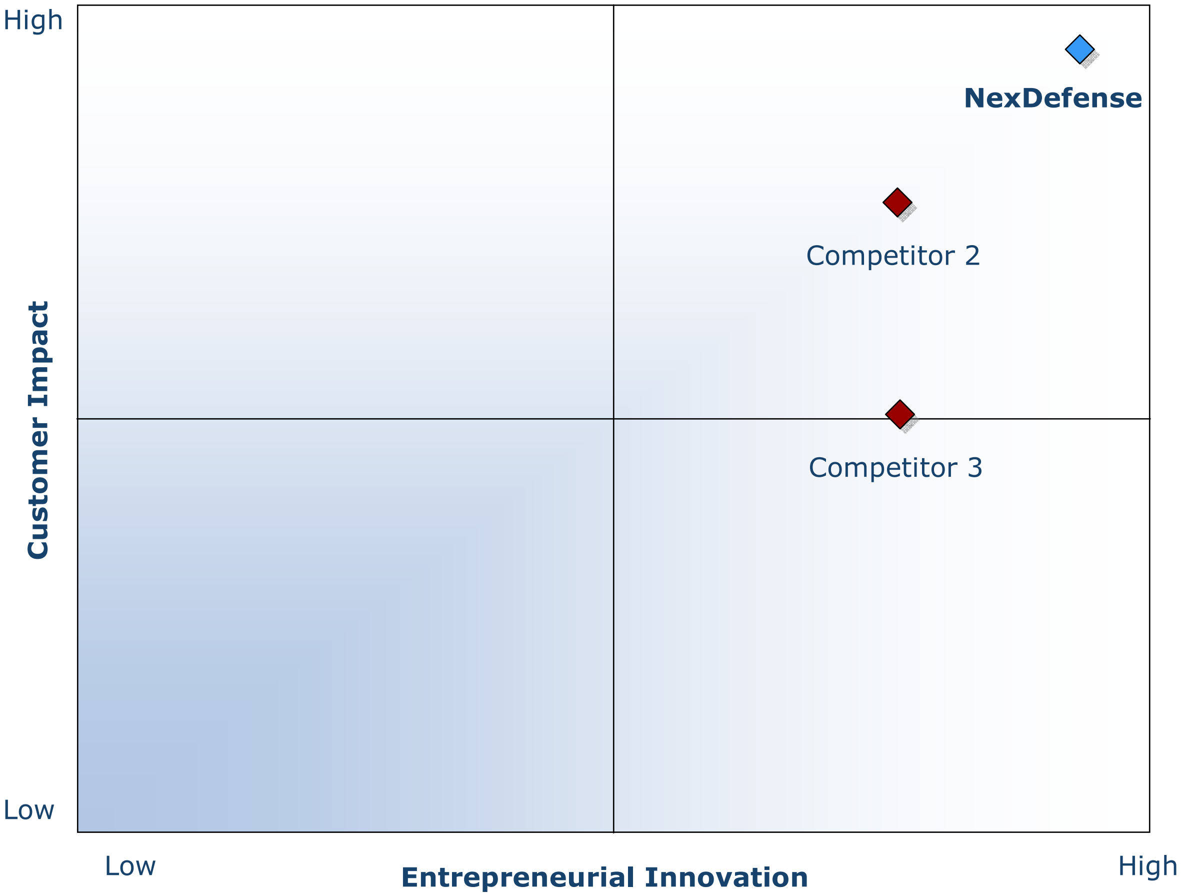
Requirement: Customer service is accessible, fast, stress-free, and of high quality

**Criterion 5: Brand Equity**

Requirement: Customers have a positive view of the brand and exhibit high brand loyalty

## *Decision Support Matrix*

Once all companies have been evaluated according to the Decision Support Scorecard, analysts can then position the candidates on the matrix shown below, enabling them to visualize which companies are truly breakthrough and which ones are not yet operating at best-in-class levels.

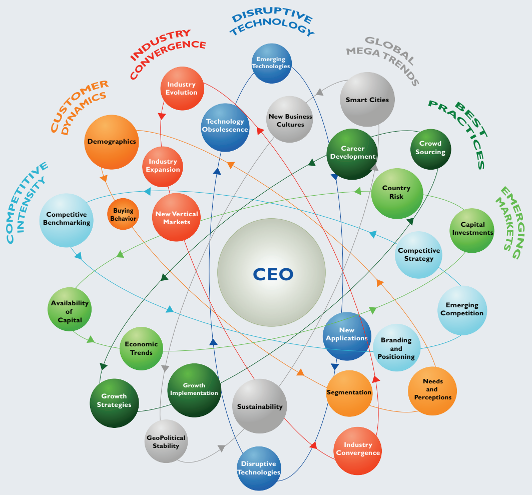


# The Intersection between 360-Degree Research and Best Practices Awards

## *Research Methodology*

Frost & Sullivan’s 360-degree research methodology represents the analytical rigor of our research process. It offers a 360-degree-view of industry challenges, trends, and issues by integrating all 7 of Frost & Sullivan's research methodologies. Too often, companies make important growth decisions based on a narrow understanding of their environment, leading to errors of both omission and commission. Successful growth strategies are founded on a thorough understanding of market, technical, economic, financial, customer, best practices, and demographic analyses. The integration of these research disciplines into the 360-degree research methodology provides an evaluation platform for benchmarking industry players and for identifying those performing at best-in-class levels.

360-DEGREE RESEARCH: SEEING ORDER IN THE CHAOS



## Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices

Frost & Sullivan Awards follow a 10-step process to evaluate Award candidates and assess their fit to best practice criteria. The reputation and integrity of the Awards are based on close adherence to this process.

| STEP | | OBJECTIVE | KEY ACTIVITIES | OUTPUT |
|---|---|---|---|---|
| 1 | **Monitor, target, and screen** | Identify award recipient candidates from around the globe | • Conduct in-depth industry research<br>• Identify emerging sectors<br>• Scan multiple geographies | Pipeline of candidates who potentially meet all best-practice criteria |
| 2 | **Perform 360-degree research** | Perform comprehensive, 360-degree research on all candidates in the pipeline | • Interview thought leaders and industry practitioners<br>• Assess candidates' fit with best-practice criteria<br>• Rank all candidates | Matrix positioning all candidates' performance relative to one another |
| 3 | **Invite thought leadership in best practices** | Perform in-depth examination of all candidates | • Confirm best-practice criteria<br>• Examine eligibility of all candidates<br>• Identify any information gaps | Detailed profiles of all ranked candidates |
| 4 | **Initiate research director review** | Conduct an unbiased evaluation of all candidate profiles | • Brainstorm ranking options<br>• Invite multiple perspectives on candidates' performance<br>• Update candidate profiles | Final prioritization of all eligible candidates and companion best-practice positioning paper |
| 5 | **Assemble panel of industry experts** | Present findings to an expert panel of industry thought leaders | • Share findings<br>• Strengthen cases for candidate eligibility<br>• Prioritize candidates | Refined list of prioritized award candidates |
| 6 | **Conduct global industry review** | Build consensus on award candidates' eligibility | • Hold global team meeting to review all candidates<br>• Pressure-test fit with criteria<br>• Confirm inclusion of all eligible candidates | Final list of eligible award candidates, representing success stories worldwide |
| 7 | **Perform quality check** | Develop official award consideration materials | • Perform final performance benchmarking activities<br>• Write nominations<br>• Perform quality review | High-quality, accurate, and creative presentation of nominees' successes |
| 8 | **Reconnect with panel of industry experts** | Finalize the selection of the best-practice award recipient | • Review analysis with panel<br>• Build consensus<br>• Select winner | Decision on which company performs best against all best-practice criteria |
| 9 | **Communicate recognition** | Inform award recipient of award recognition | • Present award to the CEO<br>• Inspire the organization for continued success<br>• Celebrate the recipient's performance | Announcement of award and plan for how recipient can use the award to enhance the brand |
| 10 | **Take strategic action** | Upon licensing, company may share award news with stakeholders and customers | • Coordinate media outreach<br>• Design a marketing plan<br>• Assess award's role in future strategic planning | Widespread awareness of recipient's award status among investors, media personnel, and employees |

## About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best in class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages almost 50 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from 31 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.