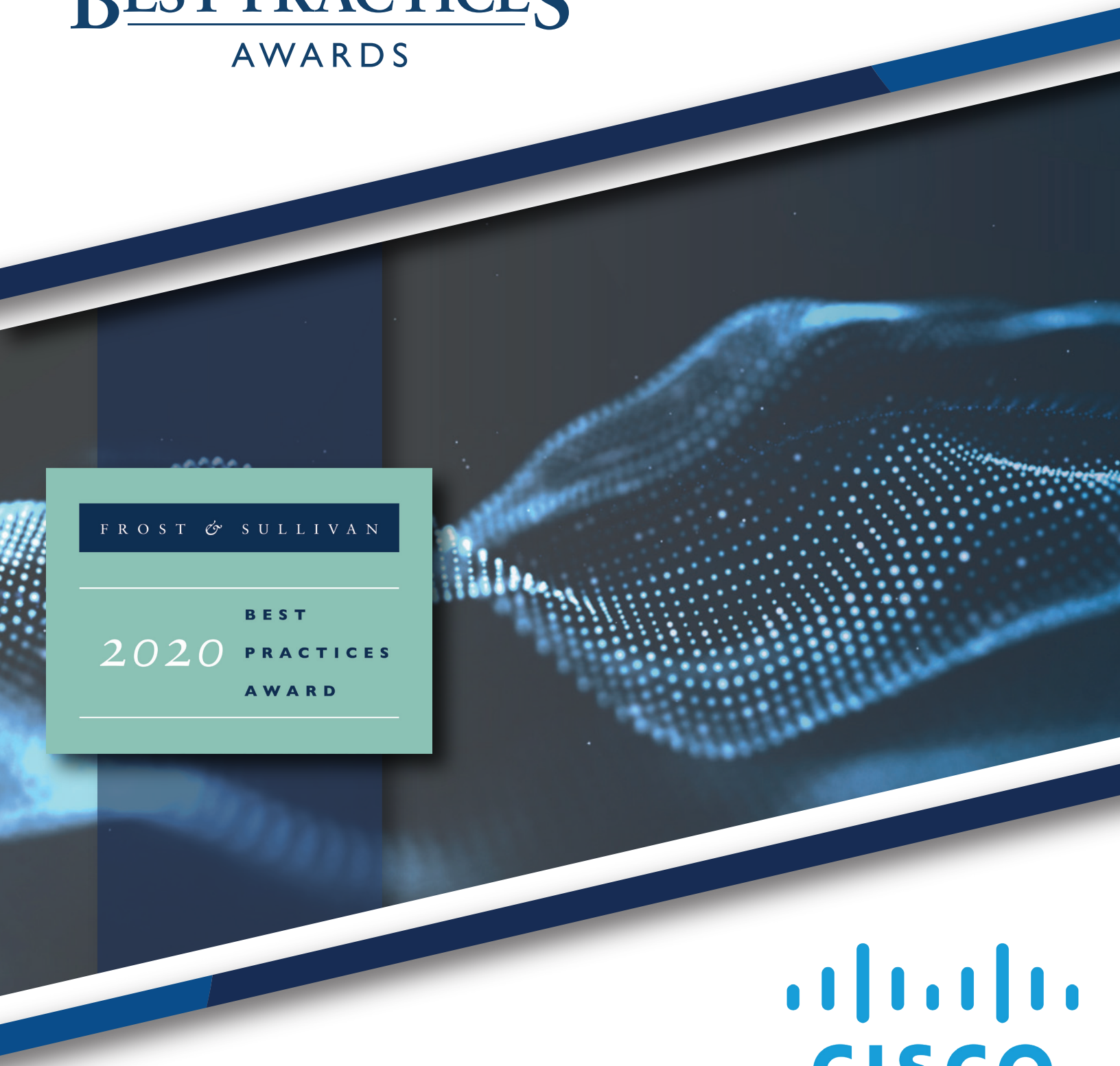
FROST & SULLIVAN

BEST PRACTICES AWARDS



CISCO

2020 GLOBAL INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY ENABLING TECHNOLOGY LEADERSHIP AWARD

Contents

Background and Company Performance

Industry Challenges

With the Internet of Things' (IoT) proliferation, and increased connectivity, organizations need to protect their ever-expanding ecosystems against cybercriminals and other malicious individuals, particularly in regards to those who have direct or easy access to the organization's most confidential data—e.g., employees through accidental or intentional means or cyber criminals stealing an organizations' sensitive data for monetary gain. The increasing threat landscape due to the IoT requires organizations to implement adequate cybersecurity solutions to protect their operations and confidential information. Industry 4.0 introduced Industrial IoT (IIoT), bringing operational technology (OT)—or Industrial Controls Systems (ICS)—into the realm, enabling organizations to automate their industrial, manufacturing, and critical infrastructure operations. OT devices are more difficult to protect as equipment can be up to 30 years old, thus manufactured decades before IoT capabilities emerged. Such sophisticated ICS machinery requires dedicated cybersecurity technologies to protect them as information technology (IT) solutions leave gaps in the OT environment.

In the energy and utilities industries alone, cyberattacks cost an average of $13.2 million per year.[1] These cyberattacks have gained government and end-user scrutiny, resulting in cybersecurity regulation enforcement—e.g., the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP). Cybersecurity adoption is accelerated by rising cyberattacks, evolving compliance regulations by governments, and increasing awareness among market participants. However, ICS cybersecurity complexity and unclear return on investment create ambiguity among organizations.

Due to the IIoT, the potential revenue opportunity in power generation alone will reach $2.87 billion by 2025 from $0.94 billion in 2018, growing at a compound annual growth rate of 17.4% between 2018 and 2025.[2] Moreover, 18 million industrial robots alone will be in operation by 2030.[3] In 2018, the ICS cybersecurity market revenue reached $1.51 billion, 20.1% more than the previous year.[4] Frost & Sullivan's research analysts expect the need for ICS cybersecurity solutions to continue growing to keep pace with the exploding growth of the industrial, manufacturing, and critical infrastructure markets.

The industrial cybersecurity market is at the high growth stage of its life cycle with rising awareness among end users and more ICS-based attacks globally. However, the shortage of security professionals further exacerbates the challenges above, requiring organizations to implement advanced, automated, and intelligent ICS cybersecurity technologies with pre-threat intelligence and anomaly detection being top priorities for organizations. ICS platforms equipped with artificial intelligence (AI) and machine learning (ML) capabilities will unburden security teams. Organizations need a comprehensive ICS cybersecurity solution that protects against malicious external attacks and insider threats and relieves security teams from conducting manual tasks that could be automated. Moreover, a vendor that can overcome these industry challenges and offer a vendor-agnostic platform to simplify and enhance ICS cybersecurity through a comprehensive platform will capture more market share and achieve market leadership.

Technology Leverage and Customer Impact of Cisco

Founded in 1984, San Jose, California-headquartered Cisco Systems, Inc. (Cisco) leverages decades of expertise in the networking and cybersecurity industries to provide a comprehensive platform to protect ICS ecosystems from the ever-evolving cybercriminal model. The company's Cyber Vision ICS cybersecurity technology, combined with its experience with industrial network equipment, cybersecurity, and industrial wireless technologies, positions Cisco to excel in the ICS cybersecurity industry. The company serves global ICS clients in the critical infrastructure, manufacturing, oil and gas, transportation, and utilities markets.

Game-changing ICS Cybersecurity Technology

Cisco obtained the Cyber Vision technology through its acquisition of Sentryo SAS, a French ICS cybersecurity provider. The acquisition allows Cisco to offer a holistic approach to ICS cybersecurity through the Cyber Vision platform and Cisco's ICS cybersecurity services. Equipped with advanced AI and ML capabilities, Cyber Vision automatically detects asset inventory as OT endpoints communicate with the network, and uses behavioral analytics to monitor network, device, and user activities. The platform sends operators real-time "abnormal activity" alerts—including for zero-day attacks—sorted by priority level and provides actionable insights, enabling them to mitigate cyber risks rapidly before the environment incurs damage.

OT cybersecurity solutions require organizations to deploy sensors across their industrial network to collect information and detect abnormal behaviors. Cisco has the unique capability of running this Cyber Vision feature within network switches, routers, and gateways. This makes the overall solution much simpler to deploy and dramatically reduces its total cost of ownership as the networking team doesn’t have to deploy, maintain, and manage a fleet of security appliances or build a separate network to carry the additional traffic created by these appliances to the central analytics platform.

Moreover, the platform breaks down the siloes between cybersecurity teams and systems, allowing seamless collaboration between IT and OT cybersecurity personnel via an integrated IT/OT security operations center platform to protect the organization's entire ecosystem against cyber vulnerabilities. It offers a unique “Universal OT Language” in the form of tags shown on the network map and asset inventory. These tags describe in plain text what the asset is doing and what the network flow is about, making it very easy for anyone to understand what is going on regardless of the OT protocol or the equipment vendor. The platform also offers mechanisms for control engineers to comment vulnerabilities, anomalies and events so that IT security experts have context and can act accordingly.

While IT and OT teams can work together better, the platform also prevents cyberattacks from spreading throughout a client's environment. It comes with premium signature files from Talos, the world's largest private threat intelligence organization and official developer of Snort rules to detect known and emerging threats such as malware intrusions or malicious traffic. Cyber Vision is also fully integrated with the rest of Cisco's security

portfolio, such as Cisco Identity Services Engine (ISE) to enable adaptive network segmentation by defining security policies according to asset types, group, and role as detected by Cyber Vision.

Cisco has integrated Cyber Vision with its wide suite of security products, such as Firepower firewalls, Stealthwatch network anomaly detection, or Cisco Threat Response, providing a seamless experience when investigating or remediating a threat within industrial networks. However, Cyber Vision has a rich API to also integrate with non-Cisco security solutions.

Moreover, Cyber Vision enables operators to gain a holistic view of their ecosystem to maintain their cybersecurity resiliency and ensure they meet strict industry compliance standards—e.g., NERC CIP and the National Institute of Standards and Technology (NIST) regulation—by implementing policies and procedures that enforce such mandates. Notably, the solution also generates detailed reports automatically, which aids customers with industry compliance audits.

Cyber Vision goes beyond traditional ICS cybersecurity solutions by giving operators detailed insights on their industrial processes, such as unexpected variable changes, program modifications, unnecessary communications that devour network bandwidth, or issues within the OT environment, such as available security patches not yet installed, and decommissioned assets or unauthorized devices connected to the network.

Cisco's communication flow mapping feature provides operators with a visual representation of how devices in the network connect to and affect one another. Impressing Frost & Sullivan's research analysts and offering clients with a high return on investment, the technology discovers hundreds of endpoints that a client did not know connected to their networks, such as employees' or contractors' personal cell phones, laptops, and tablets. Without knowledge of all the connected devices on their network, operators cannot secure the entire IT/OT environment, leaving security gaps that cyber criminals can easily exploit to steal information or execute a complete system takeover or shut down. For example, if an attacker gains control of an energy plant's machinery and shuts down power generation, chaos can ensue among plant workers, citizens, and the government. Moreover, such attacks can cause the organization to face significant financial fines, lose revenue, and incur additional operational costs, ultimately damaging their brand reputation.

Customer Services

Cisco provides Cyber Vision as a product as well as a range of services including advisory, implementation, optimization, and support. In order to help OT customers begin their cybersecurity journey, Cisco provides two different advisory options: 1) a consultative assessment, and 2) an in-depth proof of concept (POC). Both options are designed to help the OT user better understand their current ICS network, and the vulnerabilities that may exist. The consultative assessment uses the Cisco Cyber Vision technology as a tool to provide a comprehensive asset inventory, list of current vulnerabilities, and communication flow patterns so that customers can define their steps and budgets towards a secure industrial network. The POC provides the same, and adds in simulated threats to demonstrate the effectiveness of Cyber Vision. At the end of each engagement, a detailed

report is delivered, along with recommendations on how to improve the security posture. Moreover, this process takes only four to six-weeks, and can be conducted remotely.

Global COVID-19 Response Commitment

Cisco has displayed its leadership qualities in corporate social responsibility similar to its position in the technology space. Aligning with its core values, the company has stepped up during the Coronavirus (COVID-19) pandemic by generously committing $225 million in cash and products to response teams around the globe, including critical technology, education, government response agencies, and healthcare as well as the United Nations Foundation's COVID-19 Solidarity Response Fund. The company is assisting non-profit organizations globally by matching employee donations plus an extra $1 million. Additionally, Cisco is providing its Webex web conferencing platform free-of-charge to various government agencies, first responders, healthcare professionals, scientists, and others at the forefront of combating the virus. In addition to facilitating rapid and reliable communications, the company is also offering free security products for such COVID-19 response units.

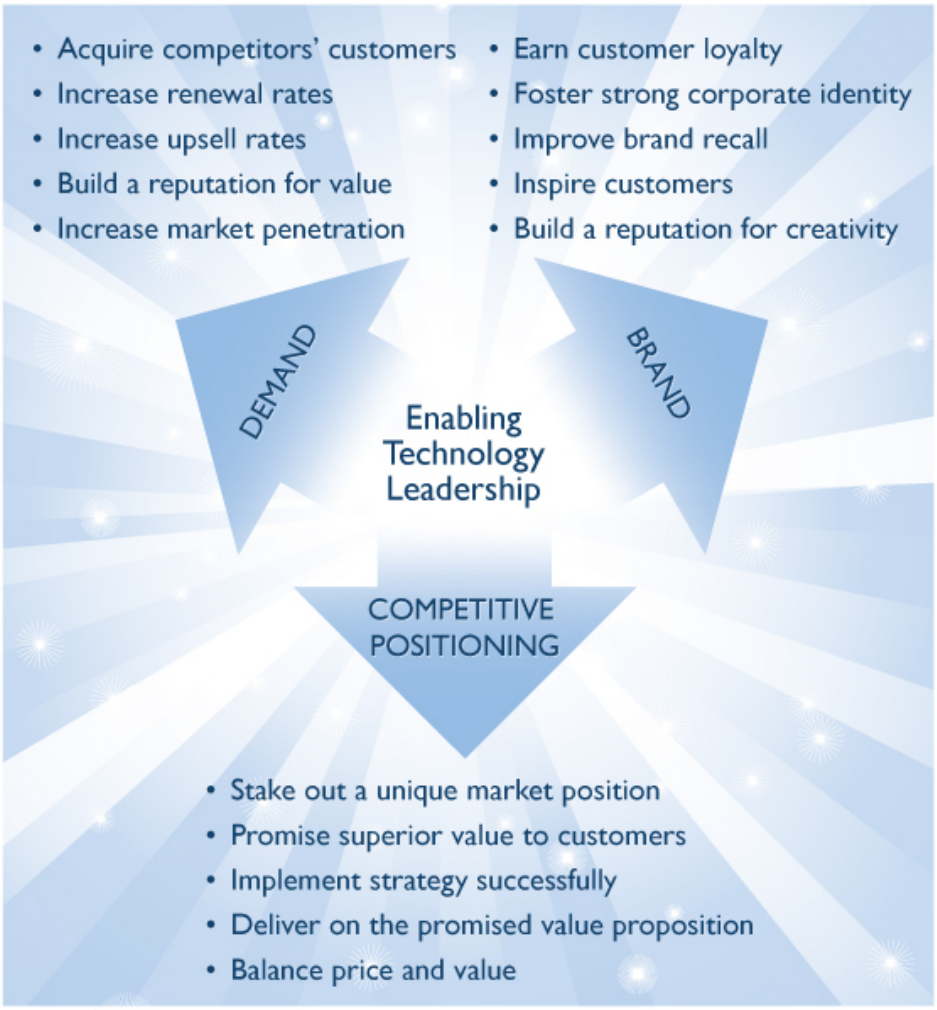
Conclusion

Industry 4.0 provides industrial organizations with myriad benefits once unachievable. However, these decades-old operational technologies were developed before the Internet of Things, and thus, require sophisticated cybersecurity solutions that can protect complex industrial control systems. Cisco's Cyber Vision platform breaks down the siloes between information technology and operational technology security solutions and teams, offering a comprehensive view of an organization's security posture and alerting operators of vulnerabilities and abnormal activities in their industrial environment. Cyber Vision enables operators to view the endpoints in the organization's environment through its communication flow mapping feature; often, clients discover that hundreds of more devices have access to their network than they realized. Frost & Sullivan commends Cisco for its in-depth customer support strategies and its global assistance in response to COVID-19.

For its industry-leading technology, customer-centric strategies, and strong overall performance, Cisco earns Frost & Sullivan's 2020 Global Enabling Technology Leadership Award in the industrial control systems cybersecurity industry.

Significance of Enabling Technology Leadership

Ultimately, growth in any organization depends on customers purchasing from a company and then making the decision to return time and again. In a sense, then, everything is truly about the customer. Making customers happy is the cornerstone of any successful, long-term growth strategy. To achieve these goals through enabling technology leadership, an organization must be best in class in three key areas: understanding demand, nurturing the brand, and differentiating from the competition.



Understanding Enabling Technology Leadership

Product quality (driven by innovative technology) is the foundation of delivering customer value. When complemented by an equally rigorous focus on the customer, companies can begin to differentiate themselves from the competition. From awareness, to consideration, to purchase, to follow-up support, organizations that demonstrate best practices deliver a unique and enjoyable experience that gives customers confidence in the company, its products, and its integrity.

Key Benchmarking Criteria

For the Enabling Technology Leadership Award, Frost & Sullivan analysts independently evaluated Technology Leverage and Customer Impact according to the criteria identified below.

Technology Leverage

Criterion 1: Commitment to Innovation
Criterion 2: Commitment to Creativity
Criterion 3: Stage Gate Efficiency
Criterion 4: Commercialization Success
Criterion 5: Application Diversity

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

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

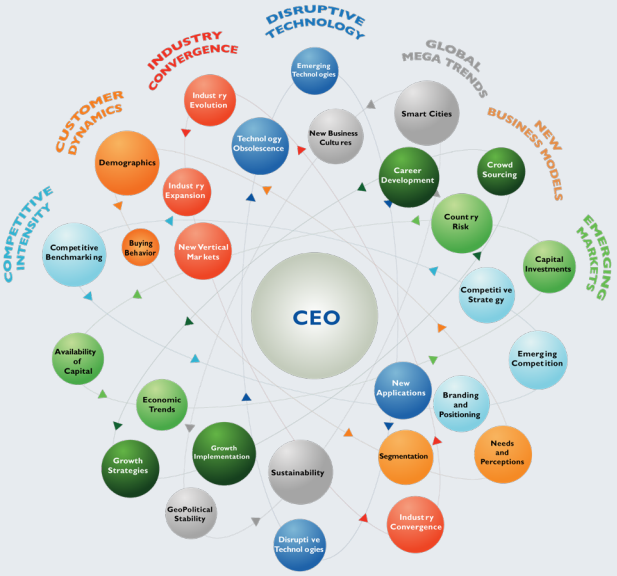
	STEP	OBJECTIVE	KEY ACTIVITIES	OUTPUT
1	**Monitor, target, and screen**	Identify Award recipient candidates from around the globe	• Conduct in-depth industry research • Identify emerging sectors • Scan multiple geographies	Pipeline of candidates who potentially meet all best-practice criteria
2	**Perform 360-degree research**	Perform comprehensive, 360-degree research on all candidates in the pipeline	• Interview thought leaders and industry practitioners • Assess candidates' fit with best-practice criteria • Rank all candidates	Matrix positioning of 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 • Examine eligibility of all candidates • 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 • Invite multiple perspectives on candidates' performance • 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 • Strengthen cases for candidate eligibility • 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 • Pressure-test fit with criteria • 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 • Write nominations • 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 • Build consensus • Select recipient	Decision on which company performs best against all best-practice criteria
9	**Communicate recognition**	Inform Award recipient of Award recognition	• Inspire the organization for continued success • 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 is able to share Award news with stakeholders and customers	• Coordinate media outreach • Design a marketing plan • Assess Award's role in future strategic planning	Widespread awareness of recipient's Award status among investors, media personnel, and employees

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 participants and for identifying those performing at best-in-class levels.

360-DEGREE RESEARCH: SEEING ORDER IN THE CHAOS



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 more than 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from 45 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.