FROST & SULLIVAN

BEST PRACTICES

AWARDS

deepinstinct™

BEFORE YOU KNOW IT

2020 EUROPEAN & ISRAELI THREAT PREVENTION TECHNOLOGY INNOVATION LEADERSHIP AWARD

Contents

Background and Company Performance

Industry Challenges

Enterprise IT infrastructure is far more complex today than only a few years ago, with cloud adoption on the rise and business practices, such as bring-your-own-device (BYOD), gaining prominence. The attack surface for modern enterprises, therefore, is much larger and more susceptible to cyberattacks. Adding to the problem is that cybersecurity tools and solutions have arguably been unable to keep up with the pace of transformation in the enterprise IT segment.

Deep Instinct is a prevention first security company built on the belief that every organization deserves security solutions that do everything it can to prevent a successful attack first and foremost. If prevention does not occur, Deep Instinct is committed to delivering solutions that make the detection, investigation, and response to the suspected threat as simple and efficient as possible. Using a dedicated deep learning framework, Deep Instinct delivers a solution that prevents attacks before they can begin. This preemptive approach dramatically reduces the workload on security teams, while simultaneously improving the security posture, making all the other security controls in the security stack more effective. Deep Instinct customers can see a significant reduction in the cost associated with attacks, of up to 90%, enabling security teams to take on more strategic projects without increasing their budget.

Technological advancements in recent years have had a game-changing effect on the global cybersecurity landscape. Cyber criminals have access to a wide gamut of sophisticated tools that allow them to stay ahead of security solutions and circumvent enterprise security controls. With over 350,000 malware generated daily, current security tools are unable to keep pace; therefore, breaches are becoming more common every day. The inherent problem lies in the approach that most security solutions follow, which is reactive and only comes into action when a threat or malware is detected within the boundaries of the enterprise network. With malware samples dynamically changing their signature almost in real time, enterprises using a reactive approach often sustain heavy damages in the period between their systems being infected and the threat being neutralized. Even advanced threat hunting and antivirus solutions using machine learning have the inherent flaw of focusing only on previously discovered threats, leading to a scenario where many threats remain in the system and damage the enterprise environment freely before being discovered and neutralized. Security approaches need to evolve from being reactive to preventive.

Further aggravating the problem is that enterprises' security frameworks are highly fragmented. For example, security teams often use a combination of 30 to 40 different tools and solutions, including endpoint protection, network protection, threat hunting, and threat intelligence. While each solution can effectively protect a limited segment of the overall IT infrastructure, IT teams are finding it difficult to maintain and keep track of a large number of alerts and remediation tasks allotted to them. In the absence of intelligent automation and a unified enterprise threat management solution across devices, environments, and operating systems, IT teams that are already stretched thin are proving ineffective and are inadequately armed to deal with sophisticated threats.

With the current cybersecurity landscape, cybersecurity solutions are needed that utilize a more proactive and preventive approach toward threat management, and more companies need to bring cohesiveness among the different components of their security solutions.

Technology Leverage and Business Impact

Industry Impact

Deep Instinct, a deep-learning cybersecurity solution provider, has built a platform that can identify and stop undiscovered threats before they affect the enterprise environment. The company has applied end-to-end deep learning to protect endpoint devices, including

desktops, smartphones, and even virtual machines, with support for all major operating systems, including Windows, Chrome OS, Android, macOS, and iOS. The key to Deep Instinct's solution, however, is its approach toward cybersecurity, where instead of finding or hunting for an existing threat in the enterprise environment, the platform thwarts both known and previously undiscovered attacks.

The inability to detect, mitigate, and neutralize cyberattacks in real time is emerging as one of the key deficiencies of current enterprise security solutions, and many hackers have successfully exploited this faulty nature of enterprise security controls to mount devastating zero-day attacks. Compared to competitors with security solutions that often fail to detect alarming attacks, Deep Instinct has proved its capabilities by protecting clients from attacks that are unknown to the cybersecurity community. An impressive example of this is the case of Maze Ransomware campaign that was first seen in the wild in May 2019. By May 2020, a new and sophisticated variant had appeared that was being used in a series of targeted and devastating attacks, but alarmingly was missed by some prominent cybersecurity tools that picked up the threat only when it was publicized on public forums. In contrast, Deep Instinct's 19-month old deep-learning model successfully detected and prevented the Maze Ransomware attack from executing. Essentially, even endpoints that had remained offline for 19 months were protected from ransomware that was non-existent when the deep-learning brain was configured.

This deep-learning model is updated twice a year based on the training performed at the Deep Instinct labs, inculcating the learning from hundreds of millions of files gathered from a large number of sources. In addition, the company has successfully maintained a high detection rate based on its approach of moving away from a feature extraction-based methodology used by competing machine learning solutions. Instead, Deep Learning employs the use of raw data from a file, which allows for deeper and more insightful analysis. Notably, feature extraction-based solutions are limited by the knowledge and experience of security experts and can only analyze a fraction of the available data.

Frost & Sullivan research indicates that Deep Instinct has been one of the most ground-breaking companies to harness the full potential of deep learning and then design a future-proof cybersecurity solution that can combat the most sophisticated threats being devised today.

Product Impact

Cybersecurity is becoming more complex each day, and the landscape has changed drastically on the criminal side. While cybercrime was an activity of lone hackers or dispersed groups of criminals some years back, increased digitalization and the potential to accrue huge amounts of money or cause extreme disruptions have brought organized criminals and nation states into the fold. With the list of adversaries and the extent of their capabilities growing, current cybersecurity tools are unable to ensure 100% prevention or even detection of cyberattacks. Enterprises, therefore, must ensure that apart from deploying robust breach-prevention measures, they must be able to control the damage in an event of a breach.

Deep Instinct, cognizant of such a dynamic landscape of cyberthreats, designed its platform to protect users at each stage of the fight against cyberattacks. The platform works as an endpoint security solution, with an agent installed on each device, including personal computers (PCs), smartphones, servers, and virtual desktop infrastructure (VDI). To have a minimal impact on the user experience, the agent is designed to occupy less than 150 megabytes (MB) on the device storage and use less than 1% of the CPU. On the administrative side, Deep Instinct provides security teams with a robust management console deployed either on the cloud or on-premises, which they can use to maintain granular control of and visibility on devices in the environment.

Deep Instinct’s platform security takes a multi-layered approach, covering distinct steps and measures throughout the following three stages: pre-execution, on-execution, and post-execution. The platform’s primary focus is on the pre-execution stage, where it can predict and prevent a threat before it has been executed in the enterprise environment. The platform takes less than 20 milliseconds to detect and prevent a threat, after which another 50 milliseconds are attributed to analyzing, classifying and investigating the root cause and source. In addition, the platform can deal with both malicious files and file-less attacks, with the ability to analyze a large variety of files, including but not limited to executables, PDFs, office files, images, fonts, scripts and powershells. The platform provides a script control feature that allows administrators to control which endpoints can and cannot execute scripts, thereby allowing enterprises to reduce their exposure to PowerShell- and Java script-based file-less threats.

In the on-execution layer, Deep Instinct’s platform protects users if a threat circumvents the prevention layer. The platform is configured to detect a threat through behavioral analysis and can identify any unnatural behavior and respond to it automatically if it is found to be malicious. The company is actively working toward developing an automated threat hunting and response tool that can allow users to actively scan and identify any threats in their devices. Moreover, Deep Instinct provides administrators with a detailed post-execution analysis and remediation capability so that they can carry out granular investigations on the cause and process the chain of an attack, allowing them to plan the remediation process. The platform provides users with several tools, such as sandboxes, whitelisting, blacklisting and device isolation, to carry out the remediation process efficiently.

Commercialization Success

Since its inception in 2015, Deep Instinct has redefined how the security community views general endpoint security and threat management practices. At a time when the industry is questioning the long-established approach toward cybersecurity, Deep Instinct has been spearheading the move toward preventive security.

Deep Instinct's strong focus on innovation and its proven effectiveness in preventing cyberattacks have earned the trust of a number of clients worldwide. The company's platform has been adopted by clients across several industry verticals, such as healthcare, education, finance, and IT; however, one of the most notable testaments for the company comes from its partnership with HP, announced in 2019. Under this partnership, HP has leveraged Deep Learning's solution as an unmanaged anti-malware tool, named HP SureSense, for all laptops shipped to enterprise customers. As one of the market leaders in the enterprise endpoint market, HP has already shipped millions of laptops with Deep Instinct's solution preloaded for clients worldwide.

In 2017, Deep Instinct entered into a partnership with NVIDIA Corporation, the global leader in the graphics processing unit (GPU) market and a strategic investor in Deep Instinct, to pursue the efficient use of GPUs in cybersecurity. GPUs are currently the only effective processing chip that has the power to enable the training of the deep neural network. Working directly with NVIDIA has contributed significantly to Deep Instinct's knowledge base in this area.

Human Capital and Financial Performance

Deep Instinct was founded by CEO Guy Caspi, CTO Nadav Maman, and CSO Dr. Eli David to leverage deep learning to combat some of the most sophisticated cyberthreats. The company has since expanded, with a more than 150-member team across numerous locations in the United States, the United Kingdom, Japan and Israel.

In addition, the company has garnered a total funding of about $100 million from a number of strategic investors, including LG Innovation Ventures, NVIDIA GPU Ventures, HP, Samsung Venture Investment, and Millennium Technology Value Partners. The company has secured such an impressive group of investors because of its innovative approach toward cybersecurity, combined with its strong financial performance since its founding. In 2019, the company achieved growth in its annual recurring revenue of over 400% and increased its customer base by 300% in the same year.

Conclusion

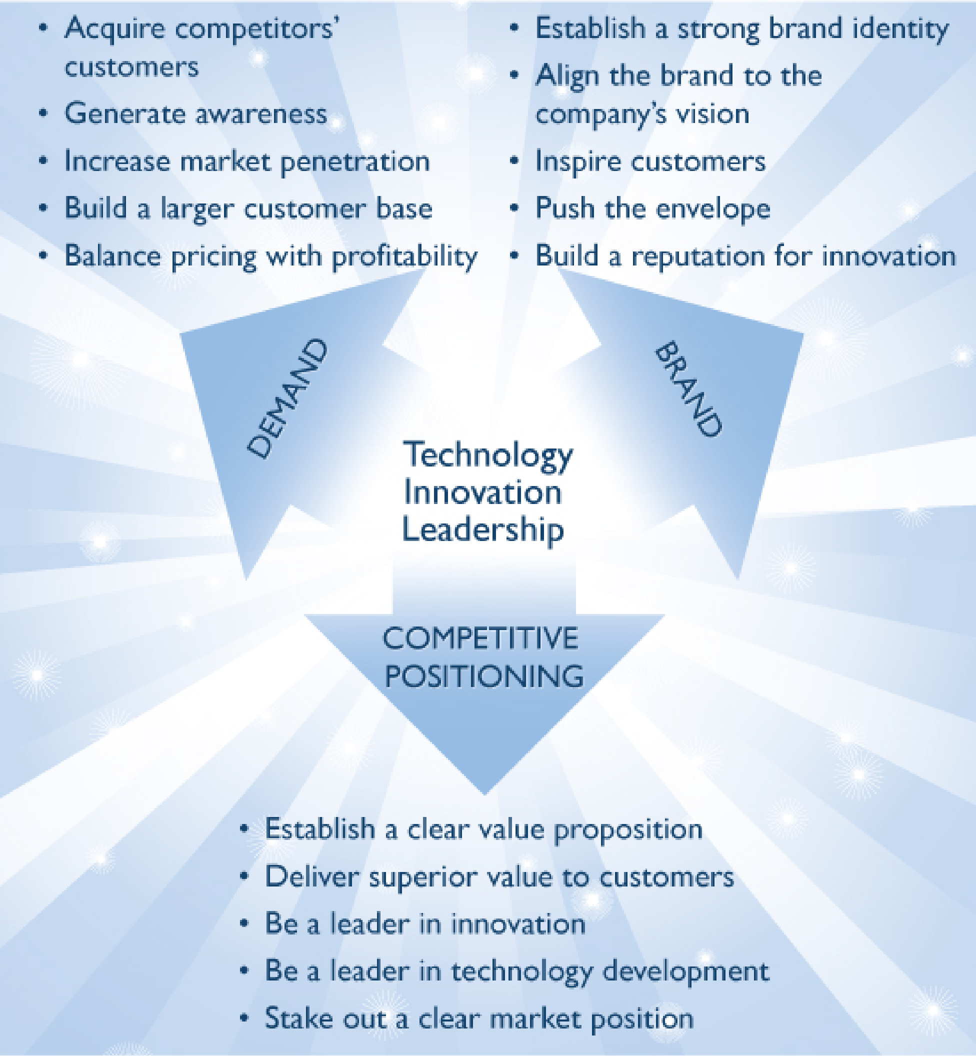
The cybersecurity landscape is changing rapidly, and cybercriminals are becoming more sophisticated. Cybersecurity solution providers' reactive approach has proved to be highly ineffective in dealing with machine-generated malware and attacks.

In a highly dynamic market, Deep Instinct has spearheaded the adoption of a preventive cybersecurity approach that successfully thwarts previously unknown attacks from entering the enterprise environment. The company's end-to-end deep learning platform helps clients to prevent threats, both file-based and fileless, dramatically minimizing the number of breaches successfully penetrating the organization. This has numerous benefits to managing a cohesive cyber defense strategy; firstly security controls are not flooded with events and become easier to manage, secondly, false positives are reduced and require less investigation, and most importantly, keeping the enterprise in a continually trusted state has finally become an achievable reality.

With its strong overall performance, Deep Instinct has earned Frost & Sullivan's 2020 Technology Innovation Leadership Award in the threat prevention industry in Europe and Israel.

Significance of Technology Innovation Leadership

Technology-rich companies with strong commercialization strategies benefit from the demand for high-quality, technologically innovative products that help shape the brand, resulting in a strong, differentiated market position.



- Acquire competitors' customers
- Generate awareness
- Increase market penetration
- Build a larger customer base
- Balance pricing with profitability

- Establish a strong brand identity
- Align the brand to the company's vision
- Inspire customers
- Push the envelope
- Build a reputation for innovation

- Establish a clear value proposition
- Deliver superior value to customers
- Be a leader in innovation
- Be a leader in technology development
- Stake out a clear market position

Understanding Technology Innovation Leadership

Technology innovation leadership recognizes companies that lead the development and successful introduction of high-tech solutions to customers' most pressing needs, altering the industry or business landscape in the process. These companies shape the future of technology and its uses. Ultimately, success is measured by the degree to which a technology is leveraged and the impact it has on growing the business.

Key Benchmarking Criteria

For the Technology Innovation Leadership Award, Frost & Sullivan analysts independently evaluated 2 key factors (Technology Leverage and Business Impact) according to the criteria identified below.

Technology Leverage

Criterion 1: Commitment to Innovation
Criterion 2: Commitment to Creativity
Criterion 3: Technology Incubation
Criterion 4: Commercialization Success
Criterion 5: Application Diversity

Business Impact

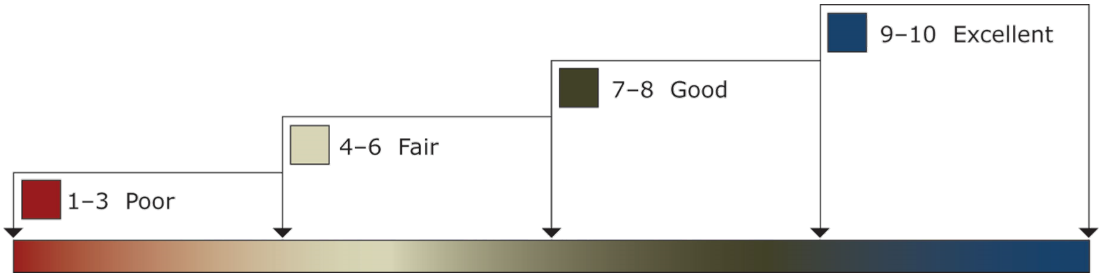
Criterion 1: Financial Performance
Criterion 2: Customer Acquisition
Criterion 3: Operational Efficiency
Criterion 4: Growth Potential
Criterion 5: Human Capital

Best Practices Award Analysis for Deep Instinct

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 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 considers Technology Leverage and Business Impact (i.e., the overarching categories for all 10 benchmarking criteria; the definitions for each criterion 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, Frost & Sullivan has chosen to refer to the other key participants as Competitor 1 and Competitor 2.

Measurement of 1–10 (1 = poor; 10 = excellent)			
Technology Innovation Leadership	Technology Leverage	Business Impact	**Average Rating**
Deep Instinct	**9**	**9**	**9**
Competitor 1	7	6	6.5
Competitor 2	5	5	5

Technology Leverage

Criterion 1: Commitment to Innovation

Requirement: Conscious, ongoing development of an organization’s culture that supports the pursuit of groundbreaking ideas through the leverage of technology.

Criterion 2: Commitment to Creativity

Requirement: Employees rewarded for pushing the limits of form and function by integrating the latest technologies to enhance products.

Criterion 3: Technology Incubation

Requirement: A structured process with adequate investment to incubate new technologies developed internally or through strategic partnerships.

Criterion 4: Commercialization Success

Requirement: A proven track record of commercializing new technologies by enabling new products and/or through licensing strategies.

Criterion 5: Application Diversity

Requirement: The development of technologies that serve multiple products, multiple applications, and multiple user environments.

Business Impact

Criterion 1: Financial Performance

Requirement: Overall financial performance is strong in terms of revenue, revenue growth, operating margin, and other key financial metrics.

Criterion 2: Customer Acquisition

Requirement: Overall technology strength enables acquisition of new customers, even as it enhances retention of current customers.

Criterion 3: Operational Efficiency

Requirement: Staff is able to perform assigned tasks productively, quickly, and to a high quality standard.

Criterion 4: Growth Potential

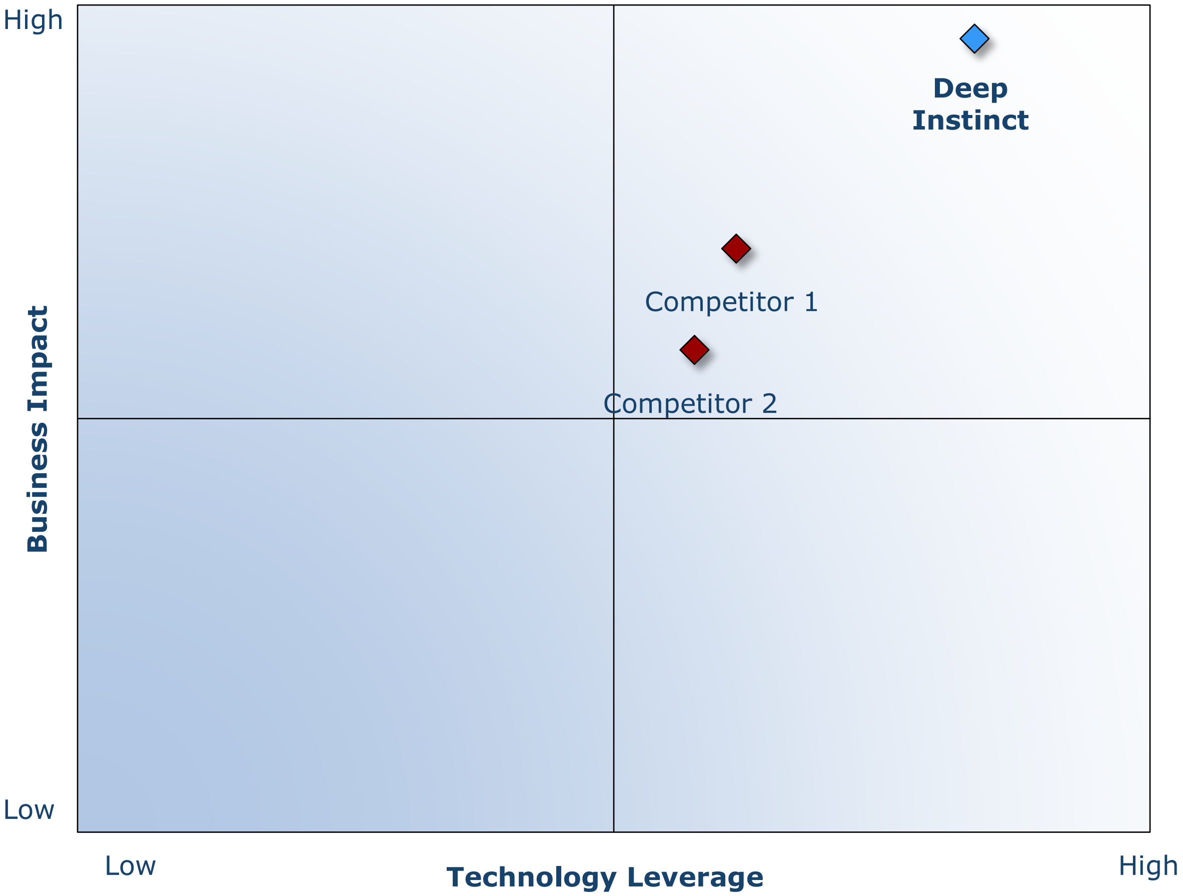
Requirements: Technology focus strengthens brand, reinforces customer loyalty, and enhances growth potential.

Criterion 5: Human Capital

Requirement: Company culture is characterized by a strong commitment to customer impact through technology leverage, which enhances employee morale and retention.

Decision Support Matrix

Once all companies have been evaluated according to the Decision Support Scorecard, analysts 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.



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 practices criteria. The reputation and integrity of the awards are based on close adherence to this process.

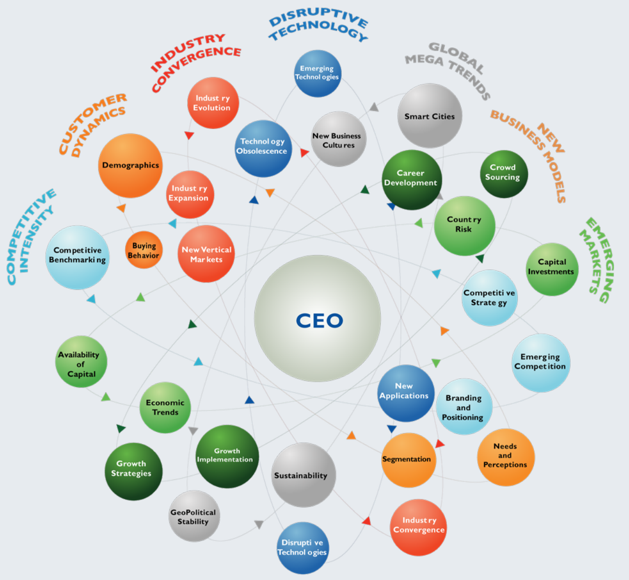
STEP		OBJECTIVE	KEY ACTIVITIES	OUTPUT
1	**Monitor, target, and screen**	Identify award recipient candidates from around the world	• Conduct in-depth industry research • Identify emerging industries • Scan multiple regions	Pipeline of candidates that potentially meet all best practices criteria
2	**Perform 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 practices 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 practices 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 practices 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 practices award recipient	• Review analysis with panel • Build consensus • Select recipient	Decision on which company performs best against all best practices criteria
9	**Communicate recognition**	Inform award recipient of recognition	• Announce award to the CEO • 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 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 the 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, resulting in 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



About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, helps clients 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 nearly 60 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from 45 offices on 6 continents. To join Frost & Sullivan's Growth Partnership, visit http://www.frost.com.