FROST & SULLIVAN

BEST PRACTICES

AWARDS

CYBER MDX

2020 NORTH AMERICAN MEDICAL DEVICES AND ASSETS SECURITY TECHNOLOGY INNOVATION LEADERSHIP AWARD

Contents

Background and Company Performance

Industry Challenges

In an increasingly connected digital ecosystem, the quality and functionality of healthcare devices are at more risk from data breaches. As such, cybersecurity is becoming a critical requirement for all healthcare stakeholders to secure medical devices and clinical assets on the Internet of Medical Things (IoMT).

A 2019 cybersecurity survey conducted by Irdeto[1], a Swedish software company, reveals that 82% of healthcare providers, including hospitals and clinical services providers, have registered cyberattacks on their medical devices and assets in the past one year, putting patient safety and data at risk. Conventional agent-based security solutions lack granular visibility and domain knowledge to protect the medical network at each device level. Biomedical teams are also facing difficulties in understanding network workflows of each device and type. Lack of interdepartmental collaboration between biomedical engineers, IT, and information security professionals at hospitals hampers the security management process further.

Healthcare providers are dependent on medical devices for clinical workflows and lifesaving treatments. However, unlike other IT assets, IoMT devices lack full protection due to complex communications protocols specific to the healthcare industry. The majority of medical device vulnerabilities go undetected owing to insufficient cybersecurity controls, risk assessment, context-aware flow monitoring, and access control policies and compliance for supporting device integration. With a multi-vendor device ecosystem, providers lack strong in-house research expertise for clinical and medical vulnerabilities, resulting in devices without suitable security measures[1].

Traditional security tools fail to identify threats because they have not considered security vulnerabilities at the initial design phase and react to threats only after a device has been breached, lacking proactive prevention measures throughout the device lifecycle. Security lapses in IoMT can shut down hospital operations, potentially risking patient safety, financial losses, and reputational damages. Frost & Sullivan notes that security deployments for medical devices and clinical assets can benefit further from the addition of AI-based contextual monitoring solutions. These solutions would detect, prevent, and mitigate risks through a proactive approach with full visibility of the entire medical devices and assets network.

Technology Leverage and Business Impact

Demonstrates Commitment to Innovation, Application Diversity, and Visionary Innovation

Founded in 2017 and headquartered in the US, New York City, CyberMDX developed its cyber intelligence platform to enable secure connectivity for medical devices and clinical assets. Through the platform's real-time threat monitoring and prevention capabilities, the

[1] 82% of Healthcare Providers Using IoT Devices Have Encountered a Cyberattack, Calculated HIPAA, September 13, 2019, accessed from https://www.calhipaa.com/82-of-healthcare-providers-using-iot-devices-have-encountered-a-cyberattack/

company addresses the growing security challenges of healthcare stakeholders in protecting networked medical devices in IoMT, strengthening hospital network security.

The CyberMDX platform uses artificial intelligence (AI) to provide real-time security insights into medical devices and assets. This makes threat monitoring and prevention more accessible to hospital IT, security, and biomedical teams while facilitating continuous network endpoint discovery, including sensors and switches. The platform offers comprehensive risk assessment and AI-based actionable responses for any anomaly detected in the hospital network of connected devices.

Frost & Sullivan is impressed with CyberMDX's leadership in addressing healthcare security concerns by setting up a proactive prevention mechanism. The platform automatically discovers and maps medical devices and follows a novel approach to detect, identify, assess, and prevent malicious activity across connected IT, medical, and IoT devices. It ensures automatic isolation or quarantine of affected devices until it neutralizes the threat by enabling micro-segmentation policies to protect other devices and data.

The vendor developed its platform to meet the demands of next-generation medical cybersecurity in IoT environments at scale. Unlike competitors, it leverages a powerful combination of deep industry expertise, vulnerability research, and proprietary AI technology to offer comprehensive visibility of medical devices and critical assets without human intervention. The major differentiating factor for CyberMDX's platform compared to competitive offerings in the market is that it delivers context-aware device profiling tailored to clinical networks and protocols, integrating it with healthcare risk assessment and remediation capabilities with proactive prevention. This lowers the overall risk for medical assets and networks.

CyberMDX has made it possible for hospitals and other healthcare stakeholders to ensure the security of their devices through superior visibility, without compromising the performance and functionality of devices and assets. Conventional agent-based security solutions lack scalability as many medical devices are incompatible with third-party software and hardware, limiting the IoMT security mechanism. CyberMDX's open application programming interface (API) allows easy integration with third-party software and hardware, ensuring enhanced security throughout the IoMT environment.

Frost & Sullivan sees tremendous value in CyberMDX's platform because it offers deep and contextual visibility, enabling healthcare stakeholders to manage and mitigate risks, prevent threats, provide incident response, and perform lifecycle management. Through live inventory mapping and risk profiling, the platform provides a holistic dashboard view of the entire network of connected healthcare assets, allowing actionable device utilization and strategic insights.

Uses Dedicated Research and Cyber Analytics Team to Secure Medical Assets while Maximizing Performance

CyberMDX designed its IoMT cybersecurity platform to support high-scale secure device deployment, providing in-depth risk reporting of medical devices, and ensuring business-enhancing operational continuity and data safety.

CyberMDX assists in the Health Insurance Portability and Accountability Act (HIPAA) compliance by implementing various strategies, covering multisystem data collection through the United States Food and Drug Administration (US FDA) database integration, automatic documentation, and reporting. Unlike competitors' products, the platform integrates with existing security infrastructure of vulnerability scanners, firewalls, and workflow managers for better classification of devices with network flow visualization and risk grouping. Through deep device network visibility and domain expertise, the security staff receives automatic alerts for anomalies in devices and assets such as misconfigurations, connectivity issues, and recalls. Based on the network positioning and vulnerabilities identified, it assigns every device a risk score, enabling healthcare staff to respond to high-risk devices and prioritize their security actions.

CyberMDx provides a holistic, multilevel view of the security posture and risk faced by medical and hospital staff. Unlike competitors, the platform enables collaboration between internal hospital departments for security grouping, reassignment of device shielding, and auto-generated policy recommendations. In addition, the AI-powered analytics dashboard ensures proactive prevention, device optimization and utilization, digital maintenance monitoring, and visibility into the functioning of medical assets. This enables data-driven workflow and collaboration between hospital security, IT, clinical engineering, and compliance teams. During the challenging COVID-19 pandemic period, CyberMDX is helping healthcare stakeholders to ramp up identification, tracking, device onboarding, security policy planning, suspicious activity detection, and reporting of critical medical devices' utilization.

CyberMDX empowers hospitals to bring full visibility of medical devices and other unmanaged devices, into their SOC awareness by integrating with software security solutions from McAfee, IBM, Splunk, and ArcSight, set policies, attacks and set responses. Through the software licensing model, the vendor has successfully demonstrated its platform offerings for global healthcare customers like the Metro Health Hospital in Ann Arbor, Michigan, an HDO operating across 30 facilities, and protecting millions of medical devices across hundreds of facilities. It adds value to network access control (NAC) services from companies such as Cisco, Forescout, Aruba and Fortinet, and firewall (FW) services from companies such as Cisco, Palo Alto Networks, Check Point and Fortinet, by automating device profiling and grouping as well as providing a segmentation / micro-segmentation policies that minimize and control the residual risk. The classification and policies information from CyberMDX is shared with the NAC/FW solution for the actual security enforcement. The automation allows boosting a process which was otherwise high in resources and prone to human errors.

Frost & Sullivan believes that addressing security issues from the medical device design and deployment phase, like CyberMDx, has initiated a new industry best practice for healthcare stakeholders, providing a 360-degree view of security across the entire device lifecycle. With AI-based network analytics, hospitals can enhance their functioning assets and inventory through data on device-level hardware, software, and configurations.

The company's entire staff is focused on healthcare delivery organizations and comprises multidisciplinary experts, including veterans from elite Israeli cyber intelligence units, medical devices experts, and academic and research leaders in AI. CyberMDX has a dedicated research team focused on monitoring and reporting of vulnerabilities across the segment They work with medical device organizations and regulatory bodies in the responsible disclosure of security vulnerabilities. Additionally, it employs a group of cyber analysts who collect information about possible attack paths to understand attacker motives, means, and methods in an effort to ensure customer environments are protected and implementations are smooth and successful.

Employing people with diverse skillsets allows CyberMDX to develop high-quality connected healthcare and IoMT security solutions, providing a unique competitive advantage. The team collaborates with medical device manufacturers and regulatory bodies such as the Certified Information Systems Auditor (CISA), ECRI Institute, MITRE Corporation, and US FDA to detect and eliminate security vulnerabilities at an early stage before cyberattackers can exploit it.

Frost & Sullivan commends the research team's efforts in identifying multiple vulnerabilities in medical devices such as the infusion pump for anesthesia and respiratory machines, alerting authorities about the threats to implement proactive measures. CyberMDX recorded a 550% revenue growth in 2019 compared to 2018. In April 2020, the company received a US$20 million investment, led by its strategic partner Sham (Relyens Group), along with Pitango Venture Capital and Qure Ventures. With this funding, the company plans to enhance its IoMT security portfolio and deploy its offering in new geographies and markets.

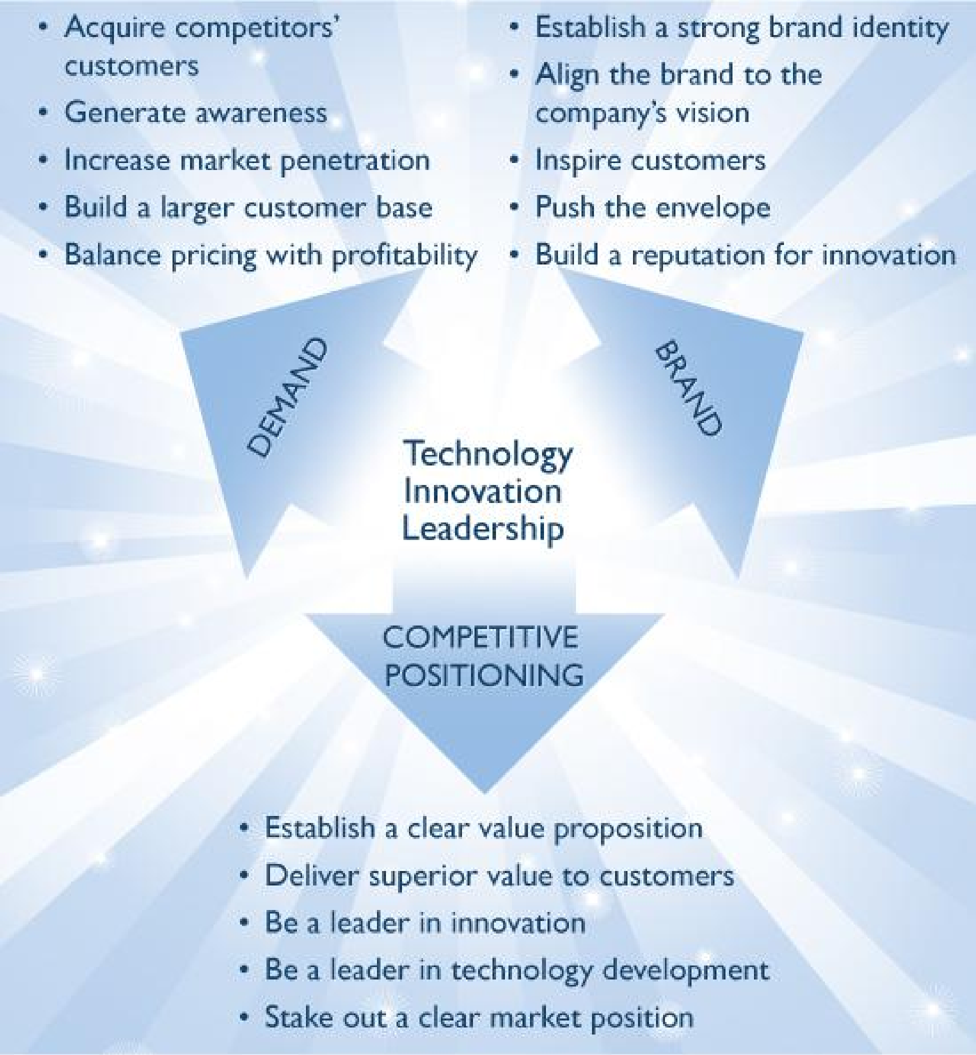
Conclusion

The holistic and proactive prevention approach to healthcare data security in IoMT is fast becoming the standard for healthcare providers worldwide. CyberMDX uses an innovative AI-based technology to streamline IoMT devices' security, ensuring superior visibility, proactive prevention, compatibility with other software and solutions, and comprehensive risk assessment without requiring human intervention across the entire device lifecycle and network workflow.

CyberMDX demonstrates thought leadership, technical excellence, and a unique customization ability to strengthen healthcare security through its platform. It also empowers the continuous discovery of medical devices and intelligent micro-segmentation policies and responses during cyberattacks. Through these achievements, CyberMDX has earned Frost & Sullivan's 2020 Technology Innovation Leadership Award.

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
DEMAND
BRAND
Technology Innovation Leadership
COMPETITIVE POSITIONING
• 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

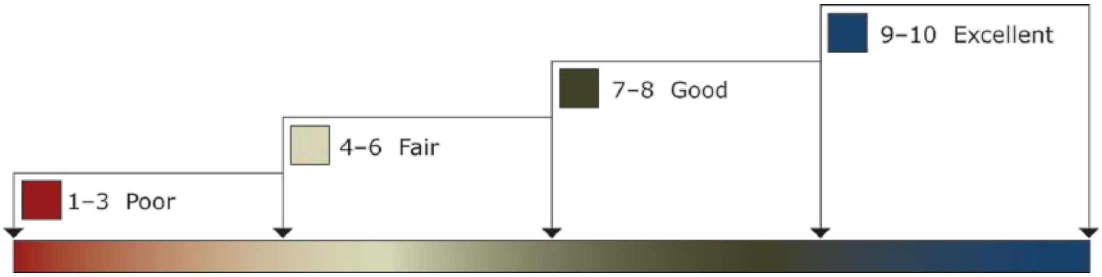
Criterion 1: Financial Performance
Criterion 2: Customer Acquisition
Criterion 3: Operational Efficiency
Criterion 4: Growth Potential
Criterion 5: Human Capital

Best Practices Award Analysis for CyberMDX

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**
CyberMDX	**9.5**	**9.2**	**9.3**
Competitor 1	8.5	8	8.2
Competitor 2	8	8	8

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

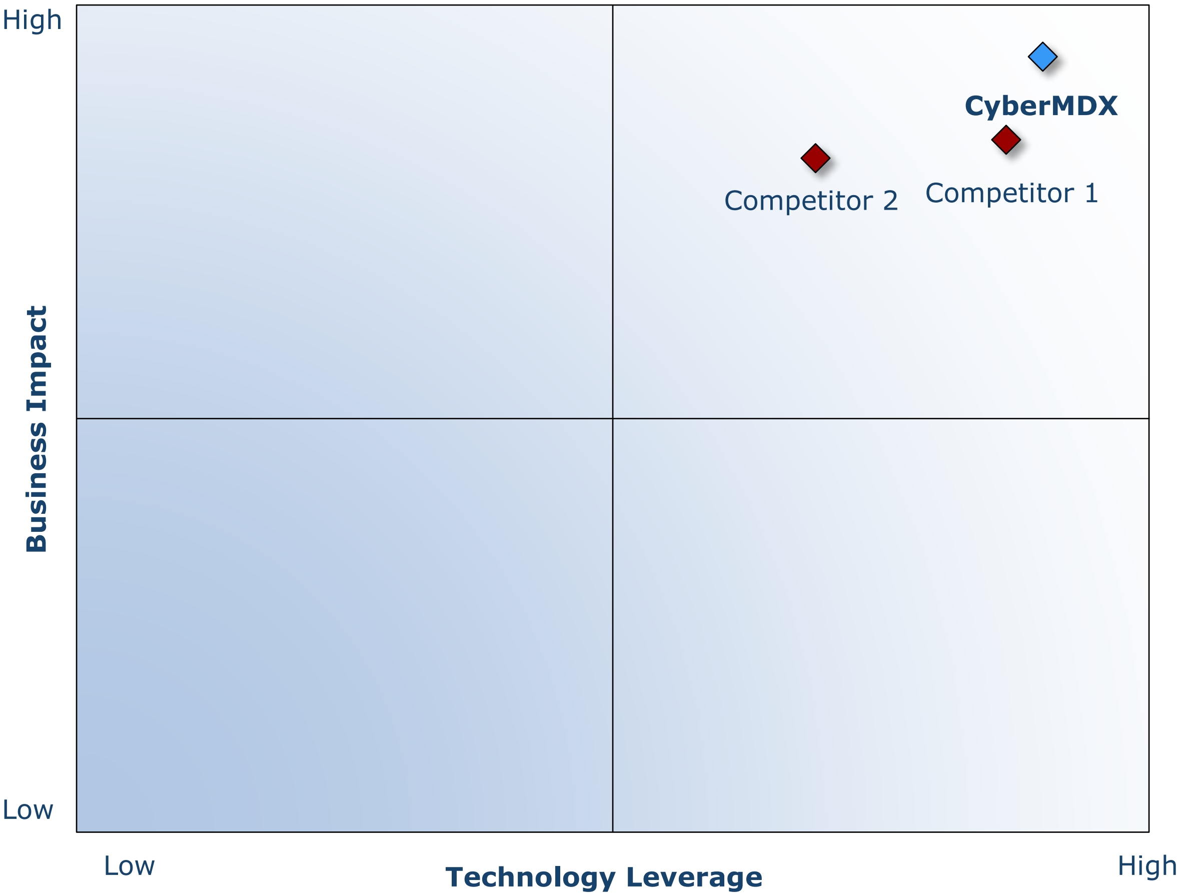
Requirements: Technology focus strengthens brand, reinforces customer loyalty, and enhances growth potential.

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.

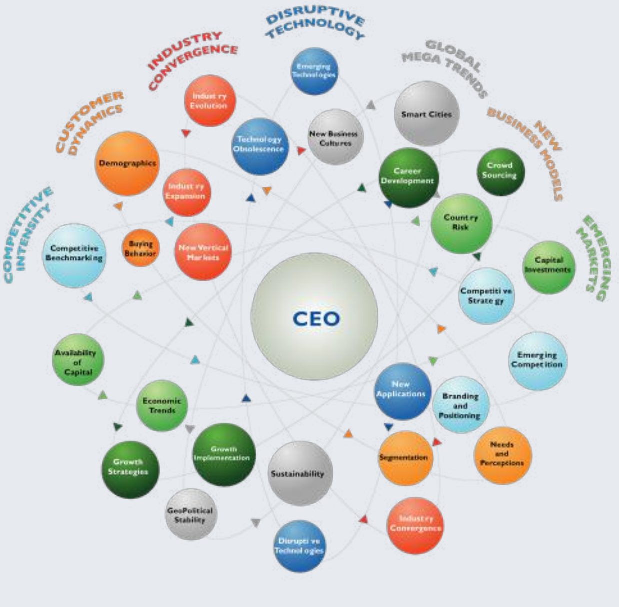
STEP		OBJECTIVE	KEY ACTIVITIES	OUTPUT
1	**Monitor, target, and screen**	Identify award recipient candidates from around the world	• Conduct in-depth industry research • Identify emerging industries • Scan multiple regions	Pipeline of candidates that potentially meet all best practices criteria
2	**Perform 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.