FROST & SULLIVAN

Fortified
HEALTH SECURITY

2018 North American Healthcare IoT Cybersecurity Company of the Year Award

FROST & SULLIVAN

2018 BEST PRACTICES AWARD

NORTH AMERICAN
HEALTHCARE IOT CYBERSECURITY
COMPANY OF THE YEAR AWARD

2018
BEST PRACTICES
AWARDS

Contents

Background and Company Performance

Industry Challenges

The Internet of Things (IoT) is increasingly permeating every aspect of consumer and enterprise activities. With the growth of microelectronics, ubiquitous connectivity, and cognition (predictive computing), IoT is poised for rapid growth. Frost & Sullivan expects the total number of IoT devices to grow from approximately 12.44 billion devices in 2016 to over 45.41 billion devices in 2023, at a global compound annual growth rate (CAGR) of 20.3%.

Security is essential for reliable operations of IoT. Whether malicious or accidental, malfunctioning or 'compromised' IoT devices can pose a significant risk to consumers, businesses, and societies. In fact, Frost & Sullivan research indicates that more than 70% of organizations today believe security is a top consideration in IoT purchase decisions. These outfits expect security will emerge as the top consideration for more than 90% of customers by the year 2020. IoT devices typically have limited processing capacity and memory. Therefore, IoT must be secured by using efficient technologies that are purpose-built for the machine environment.

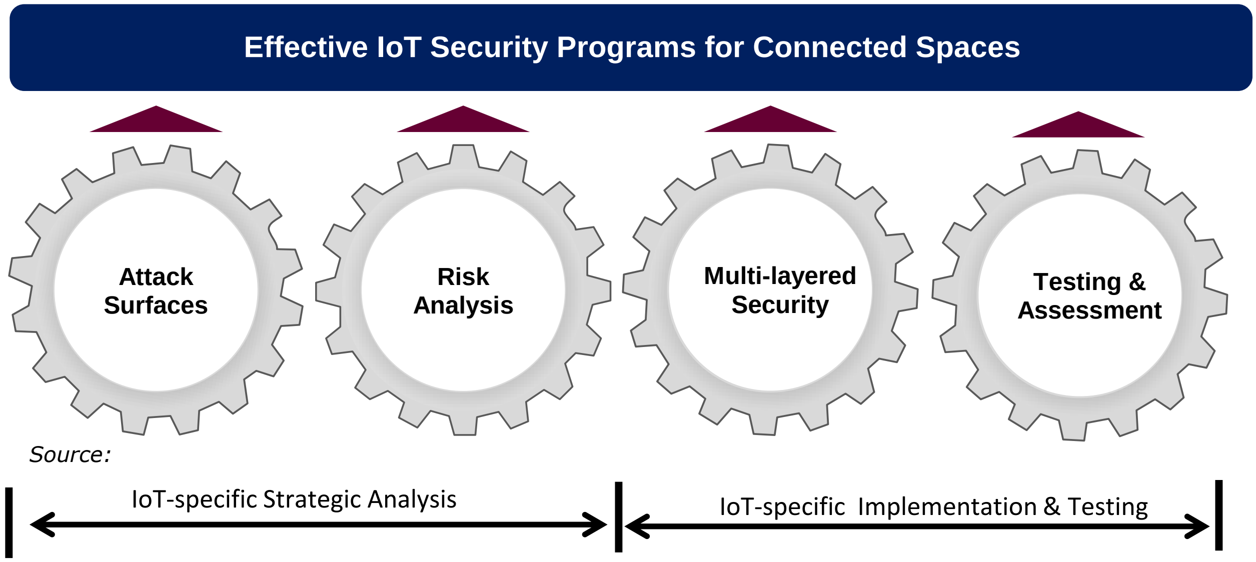
Cybersecurity Requirements for IoT

IoT creates new security challenges that currently are not being adequately addressed by traditional IT security technologies and approaches. While the basic concepts of protection remain the same (digital certificates, hardware-based trust, and data encryption), a range of unique security challenges have emerged with IoT deployments including:

- Addressing memory and processor limitations;
- Managing the large volume of IoT devices; and
- Handling data velocity and volumes.

Many open-source security options are available for IoT; however, Frost & Sullivan believes that open-source implementations cannot consistently deliver scalable and effective protection for IoT deployments, unless they are optimized for IoT.

Exhibit shows the key pillars of an effective IoT cybersecurity strategy.


Effective IoT Security Programs for Connected Spaces
Attack Surfaces
Risk Analysis
Multi-layered Security
Testing & Assessment
IoT-specific Strategic Analysis
IoT-specific Implementation & Testing

Source: Frost & Sullivan

Simplifying IoT Security through Managed Services

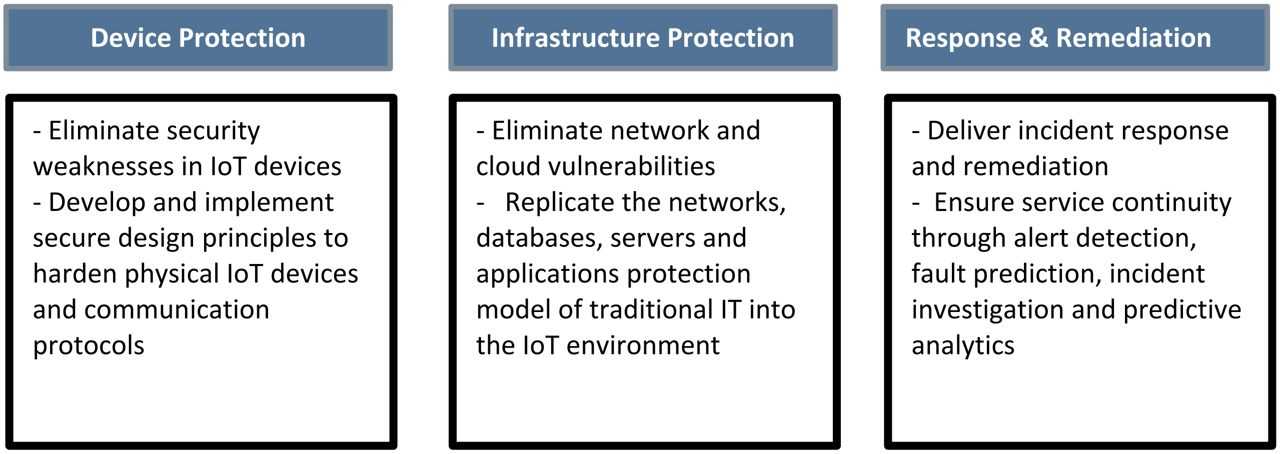
The managed security services (MSS) market for IT services is growing at an attractive pace and is already a multi-billion dollar opportunity worldwide. The MSS model has resonated well with enterprises due to the following reasons:

- Increased demands for threat detection, response and remediation for emerging security threats;
- Increased requirements for compliance, reporting, and analytics in intelligent automation environments;
- Limited budgets (and lack of expertise) for resources to address security requirements; and
- Exceptional service-level quality and customer care offered by leading MSS providers.

Frost & Sullivan believes that many of these drivers are applicable in IoT as well. With the proliferation of hyper connectivity in both enterprise and consumer domains, MSS and hybrid MSS models will be increasingly important for IoT security. Ideally, MSS solution providers should help protect IoT deployments by:

- Protecting IoT devices by eliminating security weaknesses in IoT devices;
- Protecting IoT infrastructure by monitoring for and eliminating network and cloud vulnerabilities; and
- Delivering effective incident response and remediation services.

Exhibit shows the key market needs for MSS in IoT.



Device Protection

- Eliminate security weaknesses in IoT devices
- Develop and implement secure design principles to harden physical IoT devices and communication protocols

Infrastructure Protection

- Eliminate network and cloud vulnerabilities
- Replicate the networks, databases, servers and applications protection model of traditional IT into the IoT environment

Response & Remediation

- Deliver incident response and remediation
- Ensure service continuity through alert detection, fault prediction, incident investigation and predictive analytics

Source: Frost & Sullivan

Cybersecurity for the Healthcare Industry

The healthcare industry continues to be disrupted by the ongoing digital revolution. From the massive sets of sensitive digital information created and stored by electronic health records (EHR), to remote patient and provider access to medical records, virtually every aspect of healthcare facility operations is shifting to 'digital-first' operations. In particular, the push towards the intelligent integration of third-party applications, medical devices, and IoT endpoints with legacy healthcare infrastructure has exposed healthcare facilities to cybersecurity vulnerabilities.

Cybersecurity attacks in the healthcare vertical can lead to theft of sensitive patient data, supply chain interruptions, the theft of intellectual property, disruptions in patient care, and even device malfunction that could harm patients. According to the Healthcare Industry Cybersecurity Task Force's report on *"Improving Cybersecurity in the Healthcare Industry"*, healthcare cybersecurity remains in critical condition, with the current industry hampered by:

- A severe lack of security talent;
- The continued existence of legacy equipment;
- Premature/over-connectivity; and
- An epidemic of known vulnerabilities that can impact patient care.

Other key industry challenges in the space include managing the useful life of connected medical devices, processing the high volume and velocity of connected devices data, and defining the roles of healthcare facility IT and clinical engineering teams for connected medical devices security. The complicated structure of the U.S. healthcare industry, coupled with numerous Federal and state laws and regulations, often creates barriers to innovation. Moreover, a significant percentage of healthcare organizations operate on low business margins and don't have the ability to hire full-time cybersecurity specialists or to invest in technologies for threat detection and response. Therefore, a MSS offering is often an attractive proposition to help healthcare industry participants secure their connected IT and IoT assets and networks.

Exhibit shows the key market needs of healthcare IoT cybersecurity.

Agentless Security	Accurate Inventory	Managed Services
- Agentless security in healthcare facilities - Healthcare facilities cannot afford disruptions in connected machine operations due to third-party security agents on connected endpoints	- Accurate inventory of connected endpoints - Accurate identification of connected medical devices or endpoints and software configurations is essential for establishing a security baseline against which to monitor abnormalities	- Outsourcing focused on security needs - While IT outsourcing is used in healthcare environments, outsourcing for connected device security is currently not a focus and must be a consideration

Source: Frost & Sullivan

Visionary Innovation & Performance and Customer Impact

Fortified Health Security (Fortified) is a cybersecurity firm exclusively focused on serving the healthcare market. With clients in 35 states, a near 100% client renewal rate, and more than 100,000 devices scanned monthly, Fortified has emerged as a leading full service provider of healthcare cybersecurity solutions. The key success factors for Fortified in connected medical devices cybersecurity are presented below.

Core Offerings

Fortified firmly believes that security must be comprehensive in nature, and that point solutions create gaps in security that can be exploited. Its product line strategy is focused on addressing the full spectrum of cybersecurity requirements of healthcare facilities; with an emphasis on delivering easy to use managed cybersecurity services. Fortified's core offerings for healthcare cybersecurity include:

1) HIPAA Risk Analysis, Vulnerability and Threat Assessment
2) Security Information and Event Management (SIEM)
3) Penetration Testing
4) Connected Medical Device and IoT Security Program
5) Data Loss Prevention (DLP)
6) Business Associate Lifecycle Management
7) HITRUST Assessment
8) Virtual Information Security Program (VISP)

A comprehensive product line, along with Fortified's extensive industry experience continues to help Fortified strengthen healthcare organizations' security programs by assessing risks, implementing safeguards to protect sensitive information, and assisting with compliance on state and federal regulations.

Next Generation Implementations

In an environment challenged by lack of internal expertise and regulatory clarity on cybersecurity, Fortified enables healthcare organizations to manage cybersecurity risks from a strategic, operational and tactical perspective. For example, healthcare organizations struggle to operationalize the high volume connected medical device data in order to generate meaningful insights. With the fully-managed Connected Medical Device and IoT Security Program, Fortified enables healthcare organizations to leverage advanced, connected devices with a high level of confidence that their deployments will be secure and any anomalies will be identified in a timely manner.

Similarly, with VISP, Fortified offers “Expertise on Demand” to healthcare organizations that either don’t have a CISO or would like additional expertise to help assess and manage their cybersecurity posture. With offerings such as HIPAA Risk Analysis and Vulnerability Threat Management, Fortified has taken what has historically been a time and material consulting arrangement around risk analysis, and created a multi-year program which includes monthly scans to drive equipment patching programs and deliver value on an ongoing basis.

In order to better manage third party vendor relationships and their associated risks, Fortified offers an innovative Business Associate Lifecycle Management business process outsourcing program that evaluates third-party products and services used in healthcare facilities to better secure against and mitigate data breaches. These innovative programs and implementations are key reasons why Fortified continues to generate high levels of customer satisfaction from its services.

Healthcare IoT Cybersecurity

Fortified’s continued growth demonstrates that there is a clear need for cybersecurity solutions that can address the technical, operational, and regulatory requirements in the healthcare market in a unified, programmatic manner.   With proactive support, remediation planning, and risk prioritization to strengthen security processes over time, healthcare facilities with a proliferation of connected medical devices are encouraged to consider Fortified for their cybersecurity and regulatory compliance needs. IoT deployments inherently involve a complex and interconnected systems of device and network based technologies that have to be constantly upgraded to address the security threats in healthcare environments. Therefore, innovative offerings such as Fortified’s Connected Medical Device and IoT Security program, coupled with services such as Risk Analysis and Vulnerability Assessment, and Business Associate Lifecycle Management have emerged to deliver effective end-to end security.

Competitive Assessment

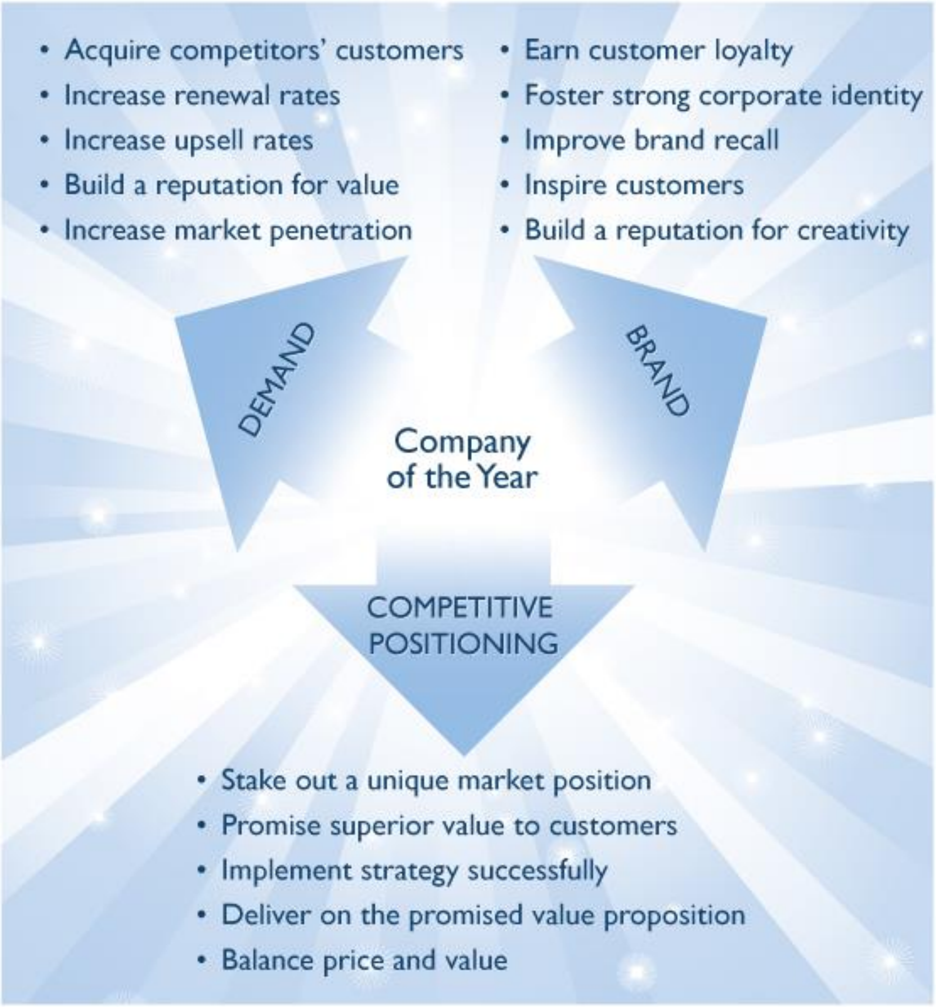
Fortified competes against some well-established companies that offer healthcare cybersecurity solutions. Regardless, Frost & Sullivan believes that Fortified will continue to demonstrate strong growth momentum consistent with the increased deployment of connected products and IoT in healthcare. Managed security services, the ability to generate tangible improvements in patient care, and extensive experience in the healthcare industry have helped the company improve its competitive position in North America. The company's strong focus on continuous process improvement has enabled it to drive out errors and optimize operations and service delivery models to levels higher than competitors. The ability to offer an unparalleled level of flexibility and agility for a wide variety of use cases is a strategic advantage for Fortified. Frost & Sullivan firmly believes that the unique Connected Medical Device Security Program will help Fortified strengthen its position as the preferred provider of healthcare cybersecurity in North America.

Conclusion

Digital Transformation is not a destination, but an evolution from analog, people-dependent business operations, to data-enabled processes. The integration of digital technologies in the healthcare industry is essential to help deliver effective care. However, as digitization expands, cybersecurity risks will increasingly surface in healthcare facilities. Through its impressive portfolio of healthcare cybersecurity solutions, Fortified can help healthcare facilities effectively address their cybersecurity needs. With its strong overall performance, Fortified Health Security has earned Frost & Sullivan's 2018 Company of the Year Award.

Significance of Company of the Year

To win the Company of the Year Award (i.e., to be recognized as a leader not only in your industry, but among your non-industry peers as well) requires a company to demonstrate excellence in growth, innovation, and leadership. This kind of excellence typically translates into superior performance in three key areas: demand generation, brand development, and competitive positioning. These areas serve as the foundation of a company's future success and prepare it to deliver on the two criteria that define the Company of the Year Award (Visionary Innovation & Performance and Customer Impact).


• Acquire competitors' customers
• Increase renewal rates
• Increase upsell rates
• Build a reputation for value
• Increase market penetration
• Earn customer loyalty
• Foster strong corporate identity
• Improve brand recall
• Inspire customers
• Build a reputation for creativity
DEMAND
BRAND
Company of the Year
COMPETITIVE POSITIONING
• Stake out a unique market position
• Promise superior value to customers
• Implement strategy successfully
• Deliver on the promised value proposition
• Balance price and value

Understanding Company of the Year

As discussed above, driving demand, brand strength, and competitive differentiation all play a critical role in delivering unique value to customers. This three-fold focus, however, must ideally be complemented by an equally rigorous focus on Visionary Innovation & Performance to enhance Customer Impact.

Key Benchmarking Criteria

For the Company of the Year Award, Frost & Sullivan analysts independently evaluated two key factors—Visionary Innovation & Performance and Customer Impact—according to the criteria identified below.

Visionary Innovation & Performance

Criterion 1: Addressing Unmet Needs
Criterion 2: Visionary Scenarios through Mega Trends
Criterion 3: Implementation Best Practices
Criterion 4: Blue Ocean Strategy
Criterion 5: Financial Performance

Customer Impact

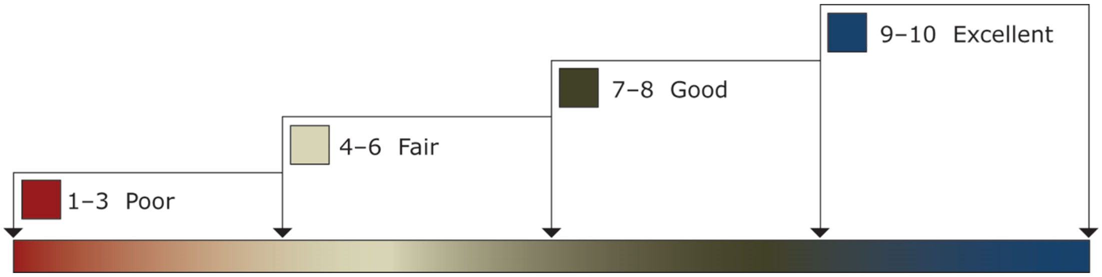
Criterion 1: Price/Performance Value
Criterion 2: Customer Purchase Experience
Criterion 3: Customer Ownership Experience
Criterion 4: Customer Service Experience
Criterion 5: Brand Equity

Best Practices Award Analysis for Fortified Health Security

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 Visionary Innovation & Performance and Customer Impact (i.e., these are 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, we have chosen to refer to the other key participants as Competitor 2 and Competitor 3.

Measurement of 1–10 (1 = poor; 10 = excellent)			
Company of the Year	Visionary Innovation & Performance	Customer Impact	**Average Rating**
Fortified Health Security	**9.5**	**9.5**	**9.5**
Competitor 2	8.5	8.5	8.5
Competitor 3	8.0	8.0	8.0

Visionary Innovation & Performance

Criterion 1: Addressing Unmet Needs

Requirement: Implementing a robust process to continuously unearth customers' unmet or under-served needs, and creating the products or solutions to address them effectively

Criterion 2: Visionary Scenarios through Mega Trends

Requirement: Incorporating long-range, macro-level scenarios into the innovation strategy, thereby enabling "first-to-market" growth opportunity solutions

Criterion 3: Implementation of Best Practices

Requirement: Best-in-class strategy implementation characterized by processes, tools, or activities that generate a consistent and repeatable level of success.

Criterion 4: Blue Ocean Strategy

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

Criterion 5: Financial Performance

Requirement: Strong overall business performance in terms of revenues, revenue growth, operating margin, and other key financial metrics

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 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

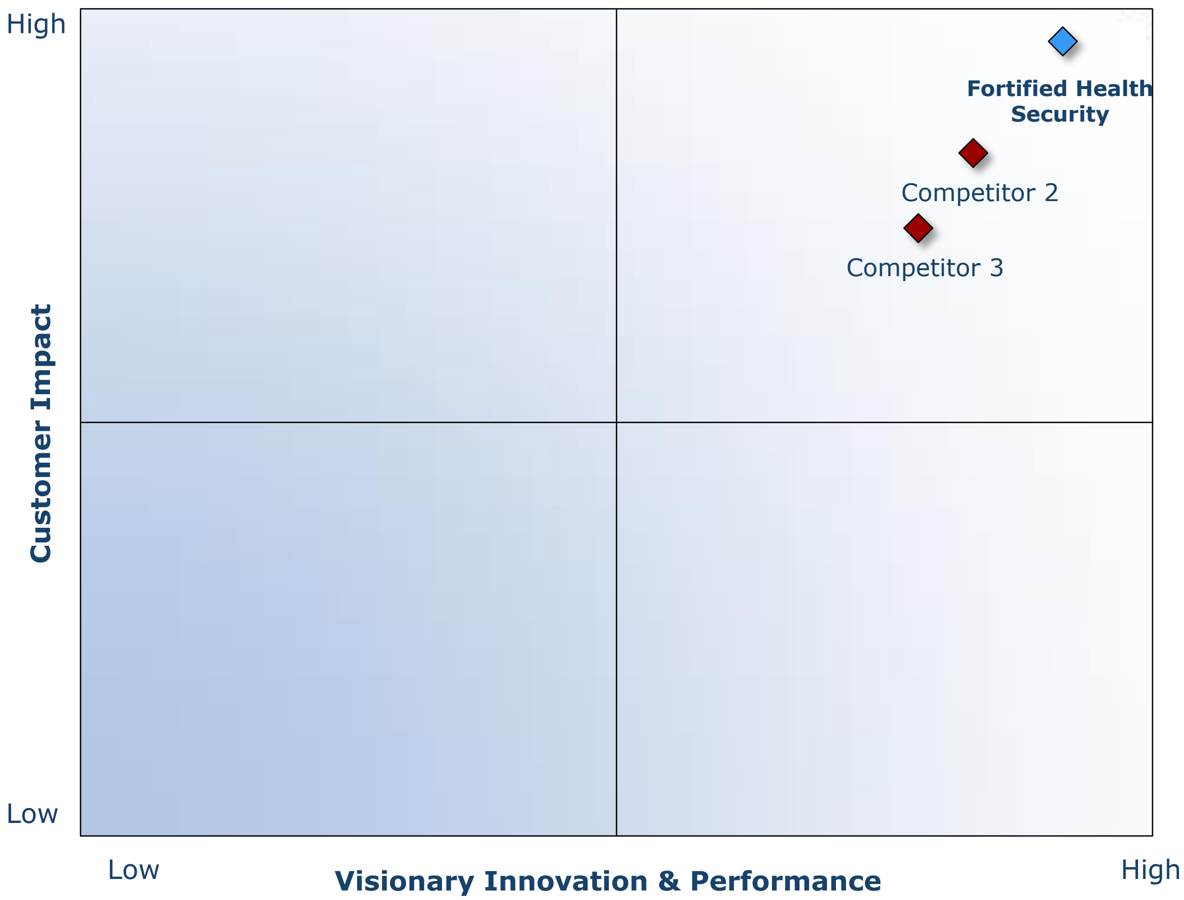
Requirement: Customer service is accessible, fast, stress-free, and of high quality.

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

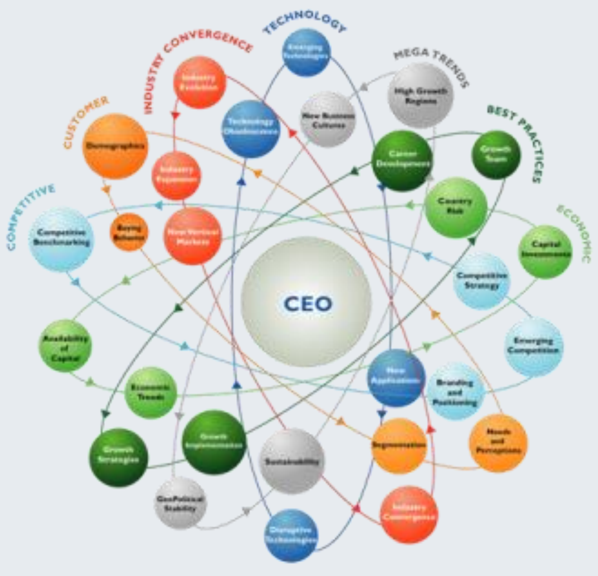
STEP		OBJECTIVE	KEY ACTIVITIES	OUTPUT
1	**Monitor, target, and screen**	Identify Award recipient candidates from around the globe	• Conduct in-depth industry research • Identify emerging sectors • Scan multiple geographies	Pipeline of candidates who potentially meet all best-practice criteria
2	**Perform 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 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 • 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 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.