

F R O S T & S U L L I V A N

FROST & SULLIVAN BEST PRACTICES AWARD

THREAT INTELLIGENCE PLATFORM- NORTH AMERICA

Technology Innovation 2019

THREATQUOTIENT 

FROST & SULLIVAN

2019

BEST
PRACTICES
AWARD

Contents

Background and Company Performance	3
<i>Industry Challenges.....</i>	<i>3</i>
<i>Technology Attributes and Future Business Value</i>	<i>3</i>
<i>Conclusion</i>	<i>6</i>
Significance of Technology Innovation	7
Understanding Technology Innovation	7
<i>Key Benchmarking Criteria</i>	<i>8</i>
Best Practices Award Analysis for ThreatQuotient	8
<i>Decision Support Scorecard</i>	<i>8</i>
<i>Technology Attributes.....</i>	<i>9</i>
<i>Future Business Value.....</i>	<i>9</i>
<i>Decision Support Matrix</i>	<i>10</i>
Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices	11
The Intersection between 360-Degree Research and Best Practices Awards	12
<i>Research Methodology.....</i>	<i>12</i>
About Frost & Sullivan	12

Background and Company Performance

Industry Challenges

Cybercriminals are becoming increasingly sophisticated and using various advanced techniques to attack and spread malicious activities. To safeguard against cyberattacks, enterprises are setting up in-house threat operations teams comprised of security operations centers (SOCs), incident response (IR) capabilities, and threat intelligence. Routinely, these security teams analyze the internal and external threat environment to detect any malicious threat activities that can disrupt customer business operations. Analyses span data collected from internal systems and multiple data feeds from commercial sources, the open source community, industry, and their existing security vendors. However, most enterprises lack the resources and intelligent technology needed to efficiently analyze the constantly increasing volume of gathered data. Without proper analysis, security teams will generate false results and fail in detecting all potential threats.

Frost & Sullivan believes that today's enterprises require a streamlined, efficient threat intelligence platform that will position their threat operations teams to understand and quickly act upon the highest priority threats they face.

Technology Attributes and Future Business Value

Industry and Product Impact

ThreatQuotient is a US-based threat intelligence platform provider that arms security operations teams with the tools needed to efficiently prioritize anticipated threats and become more proactive in addressing them. ThreatQuotient's threat intelligence platform, ThreatQ, is designed to collect information from more than 200 sources, both external and internal, and serves as the central repository for an enterprise's threat intel. The repository facilitates collaboration, better decision making, and accelerated detection and response to all kinds of threats. Further, the ThreatQuotient platform provides intelligence to understand, prioritize, and take more timely action on the most relevant threats enterprises face.

Frost & Sullivan recognizes that ThreatQ is the industry's first flexible and customizable intelligence-scoring platform that allows customers to dynamically change scoring parameters. The platform has the ability to capture feedback and empowers teams to identify and anticipate threats to reduce risk now and in the future. Moreover, the ThreatQ platform easily integrates with the customer's existing technologies and tools. The easy integration feature of ThreatQ allows it to quickly self-adjust its threat library depending upon customer requirements. This makes the solution highly effective and responsive to customers' rapidly changing business requirements.

ThreatQ's unique self-adjust threat library capability makes it the perfect fit for a diverse set of customers. For instance, a US-based global financial services firm needed a threat intelligence platform to aggregate all external and internal threat and event data in one place to help it assess risks and take action. Distributed threat data in different places and ad hoc analysis and action by siloed teams proved time-consuming, disjointed, and inefficient. The firm selected ThreatQuotient and uses the ThreatQ platform to empower its

security teams and tools to work harmoniously and detect specific incidents, resulting in actions taken in a matter of hours, which used to take days. The flexibility and openness of the platform through customized connectors made it highly configurable to work with whatever processes, data, and tools the customer had within the organization, without any re-architecting required.

Visionary Innovation

ThreatQuotient's vision is to empower customers' security operations team with the desired threat intelligence platform that is armed with the right data to understand, detect, and respond to threats. When deciding between dozens of vendors whose products do not talk to one another, customers face a disjointed big data problem due to large, disparate data sets. This lack of data coordination has resulted in inefficient and ineffective security operations. In contrast, ThreatQuotient has innovated its ThreatQ platform with distinct capabilities to integrate various technologies, provide customer-specific scoring, and automate threat investigations and responses.

Through its breadth and depth of integrations, ThreatQ collects data from various sources (both internal and external) of customers through fully supported, robust API and SDK. Customers have significant flexibility in which data sources they choose to integrate and how they want to integrate them. Moreover, ThreatQ can be easily adapted to work with many different customer environments while still acting as a standardized central repository for curated, custom-scored threat intelligence.

Utilizing all this data, ThreatQ provides a customizable algorithm to generate a score based on the customer's specified requirements. ThreatQ's intelligence scoring algorithm generates a consolidated aggregate of many individually scored customer-selected parameters. Because ThreatQ allows customers to weigh the impact of so many individual intelligence parameters, it enables them to determine how granular and sophisticated they would like their scoring to be. Having multiple data points provides a more precise scoring algorithm, highlighting high priority items while removing false positives and noise that can make up well over ninety percent of the data.

ThreatQ platform's intelligence scoring algorithm takes the following parameters into consideration while prioritizing threats:

- **Source:** Source of an indicator is a fundamental evaluation of the relevance and priority of malicious activity. All indicators must have a source — internal (ticketing system, sandbox, etc.) or external. ThreatQ aggregates multiple sources into one central location and transforms them into a simplified format.
- **Indicator of Compromise (IOC) Type:** The IOC type maps back to how a customer can leverage indicators for detecting or blocking. Different indicators have different lifecycles; IOC helps security teams to identify and leverage specific indicators depending on the customer requirements.
- **Attributes:** An indicator's attributes are core components of its threat score because they help create a granular picture of the type of threat and the context in which it is

relevant to a customer. The indicator attributes are classified into three categories: indicator identification, attack detailing, and adversary action.

- **Adversary Attribution:** An indicator's association with adversary groups is another method available for calculating indicator risk levels. The customized scoring methodology across multiple adversaries empowers clients with a granular ability to help score the risk of indicators.

Once data is scored and the customer has a curated set of relevant, prioritized items that data can be used to support decision-making and resulting actions, both automatically and through human intervention. ThreatQ enables the security teams through its ThreatQ Investigations module, an innovative visualization, collaboration, and documentation capability. ThreatQ Investigations accelerates analysis and a shared understanding of the threat, enabling the right responses to be determined and acted upon faster than previously possible. Investigation leads, SoC managers, incident handlers, and other key parties can observe the analysis unfolding in real-time. This enables them to control the chaos typically seen in security operations.

Frost & Sullivan appreciates the ability of ThreatQ and ThreatQ Investigations to support the multiple use cases including alert triage, threat hunting, vulnerability management, and threat intelligence management. ThreatQ Investigations is a unique offering from ThreatQuotient that provides real-time visualization, collaboration, and documentation capability to customers' security teams. Frost & Sullivan notes ThreatQ enjoys an edge over the competition as it is the only solution in the threat intelligence space that enables siloed security teams to work collaboratively and block threats effectively.

Human Capital

ThreatQuotient has an excellent team of leaders and technical experts who bring strong experience in developing cybersecurity solutions.

John Czupak is the president and CEO of ThreatQuotient and is responsible for the company's global expansion strategy and financial growth plans. Prior to ThreatQuotient, Mr. Czupak worked at Sourcefire, Inc. (acquired by Cisco in 2013) where he joined as a senior VP of International & Business Development in 2002 and left as general manager in 2014.

Tom Ashoff is the SVP of Engineering at ThreatQuotient who leverages his 20+ years of strong expertise in building cybersecurity products. Prior to joining ThreatQuotient, Mr. Ashoff worked at Sourcefire Inc. He has more than 20 years of experience in driving the software and hardware strategy for an integrated network security product portfolio covering next-generation firewall, VPN, intrusion detection/prevention, and threat management.

Leon Ward is the VP of Product Management who has 15+ years of technical experience in the information and network security space. At ThreatQuotient, Mr. Ward drives the ThreatQ product development and innovation roadmap aimed at improving the efficiency of analysts,

security teams, and threat operations. Prior to ThreatQuotient, Mr. Ward worked at Cisco as group product manager of Security Innovation.

Frost & Sullivan recognizes that ThreatQuotient's exceptional team of experts has laid a solid foundation for the company to set a benchmark with their innovative, customizable threat intelligence platform.

Financing and Customer Acquisition

ThreatQuotient has successfully attracted funding from notable venture capitalists in the cybersecurity industry. The company has secured a total of \$47.5 million to date. Some of its key investors include New Enterprise Associates (NEA), Adams Street Partners, Cisco Investments, and NTT DOCOMO Ventures, Inc., and growth capital partner Silicon Valley Bank.

The funding has helped ThreatQuotient accelerate its growth and acquire customers through geographic expansion, product development, and sales and marketing both in the United States and globally. The company continues to invest funds in R&D to address the cybersecurity industry's increasing demand for an integrated threat intelligence platform that streamlines operations and management.

Frost & Sullivan appreciates ThreatQuotient's efforts to chart new territory as an innovator in the threat intelligence platform space where in just 6 years since inception, it has established itself as a major player. In fact, ThreatQuotient was named one of the top 16 most innovative companies by SINET (Security Innovation Network) in 2017.

Conclusion

Frost & Sullivan appreciates ThreatQuotient's unique ability of providing real-time visualization and a collaborative investigation approach to its customers' security teams, which no other competitor is offering in the threat intelligence space. Further, the platform's outstanding features of customized scoring and prioritized threats empower its customers' security teams to effectively block and protect enterprises from all manner of increasingly sophisticated threats.

For its strong overall performance, ThreatQuotient has earned the 2019 Frost & Sullivan Technology Innovation Award.

Significance of Technology Innovation

Ultimately, growth in any organization depends on finding new ways to excite the market and maintaining a long-term commitment to innovation. At its core, technology innovation, or any other type of innovation, can only be sustained with leadership in 3 key areas: understanding demand, nurturing the brand, and differentiating from the competition.



Understanding Technology Innovation

Technology innovation begins with a spark of creativity that is systematically pursued, developed, and commercialized. That spark can result from a successful partnership, a productive in-house innovation group, or a bright-minded individual. Regardless of the source, the success of any new technology is ultimately determined by its innovativeness and its impact on the business as a whole.

Key Benchmarking Criteria

For the Technology Innovation Award, Frost & Sullivan analysts independently evaluated 2 key factors—Technology Attributes and Future Business Value—according to the criteria identified below.

Technology Attributes

- Criterion 1: Industry Impact
- Criterion 2: Product Impact
- Criterion 3: Scalability
- Criterion 4: Visionary Innovation
- Criterion 5: Application Diversity

Future Business Value

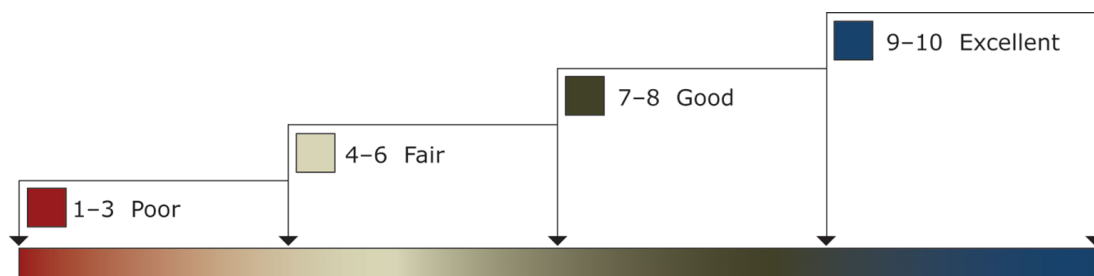
- Criterion 1: Financial Performance
- Criterion 2: Customer Acquisition
- Criterion 3: Technology Licensing
- Criterion 4: Brand Loyalty
- Criterion 5: Human Capital

Best Practices Award Analysis for ThreatQuotient

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 Attributes and Future Business Value (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.

<i>Measurement of 1–10 (1 = poor; 10 = excellent)</i>			
Technology Innovation	Technology Attributes	Future Business Value	Average Rating
ThreatQuotient	9	9.5	9.25
Competitor 1	8	7	7.5
Competitor 2	7	6.5	6.75

Technology Attributes

Criterion 1: Industry Impact

Requirement: Technology enables the pursuit of groundbreaking ideas, contributing to the betterment of the entire industry.

Criterion 2: Product Impact

Requirement: Specific technology helps enhance features and functionalities of the entire product line for the company.

Criterion 3: Scalability

Requirement: Technology is scalable, enabling new generations of products over time, with increasing levels of quality and functionality.

Criterion 4: Visionary Innovation

Requirement: Specific new technology represents true innovation based on a deep understanding of future needs and applications.

Criterion 5: Application Diversity

Requirement: New technology serves multiple products, multiple applications, and multiple user environments.

Future Business Value

Criterion 1: Financial Performance

Requirement: Potential is high for strong financial performance in terms of revenue, operating margins, and other relevant financial metrics.

Criterion 2: Customer Acquisition

Requirement: Specific technology enables acquisition of new customers, even as it enhances value to current customers.

Criterion 3: Technology Licensing

Requirement: New technology displays great potential to be licensed across many verticals and applications, thereby driving incremental revenue streams.

Criterion 4: Brand Loyalty

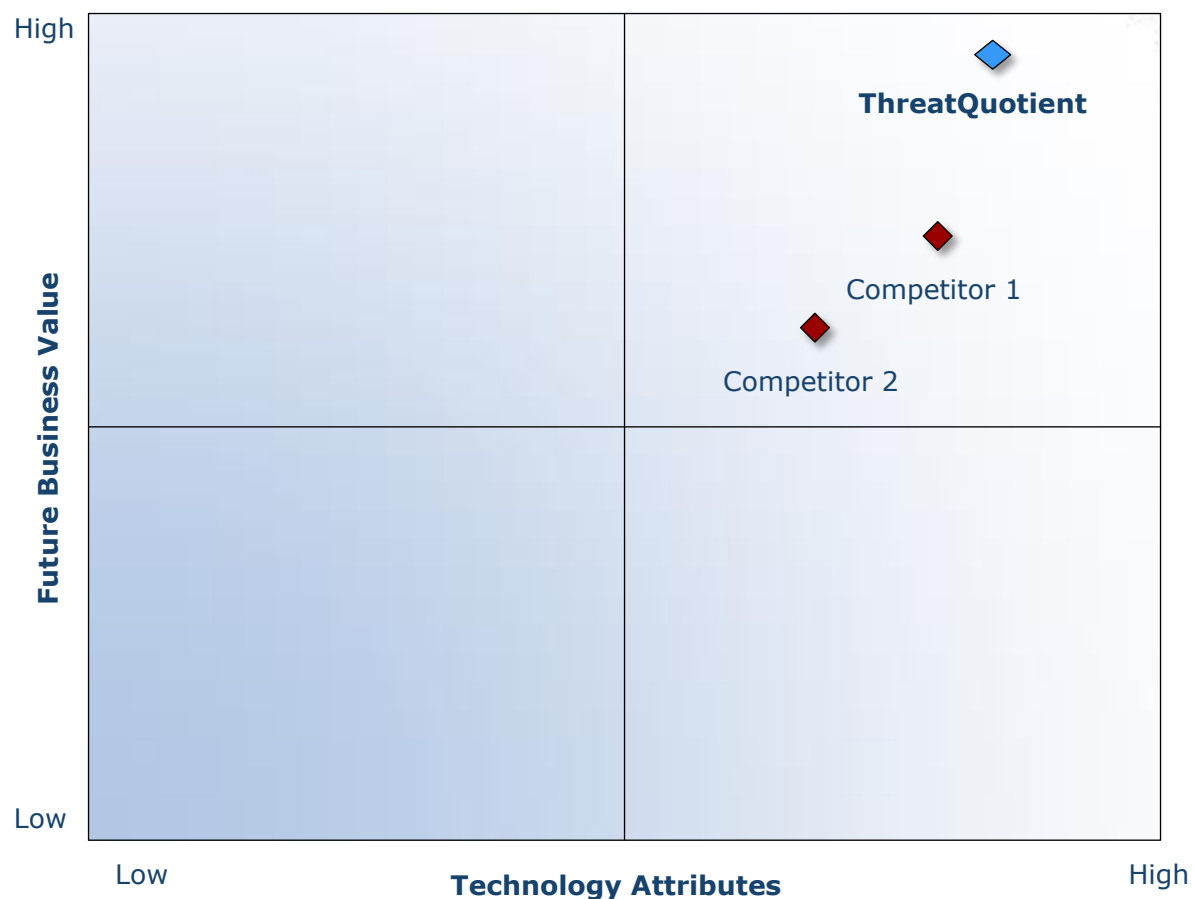
Requirement: New technology enhances the company's brand, creating and/or nurturing brand loyalty.

Criterion 5: Human Capital

Requirement: Customer impact is enhanced through the leverage of specific technology, translating into positive impact on 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 is able to share award news with stakeholders and customers	<ul style="list-style-type: none"> 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 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, 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-practices 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>.