FROST & SULLIVAN

LogRhythm®

2017 Global SIEM Enabling Technology Leadership Award

FROST & SULLIVAN

2017 BEST PRACTICES AWARD

GLOBAL SIEM
ENABLING TECHNOLOGY LEADERSHIP AWARD

Contents

Background and Company Performance

Industry Challenges

Security information and event management (SIEM) engines have a storied legacy in cybersecurity. Traditionally, the SIEM engine has three specific functions and these functions remain relevant today:

1. SIEM is used to prove compliant practices (noting that there are numerous industry compliance standards).
2. SIEM is used as a way to formalize storage. Data is normalized and logged for recall.
3. The SIEM engine initiates the first part of a forensics investigation. In the event that a breach is uncovered, the SIEM is used to access all related directory groups, OS, applications, or other applicable similarities to determine how far a breach has spread.

However, there is a popular colloquialism passed along by network security professionals, “There are only two types of networks: those that have been breached and those that are about to be.”

The cynicism may be exaggerated, but network security teams do need to have an investigatory technology that occurs after the network security perimeter. The revelation has been that a SIEM which ingests flow data from network security appliances, network-based sensors, log sources, and data straight from end-user devices, contains a vault of valuable information. Why not use the rich data proactively in incident detection and response?

Technology Leverage and Customer Impact

A novelty act might be a juggler that throws and catches an orange, a bowling ball, and a chainsaw. Similarly, a SIEM engine ingests disparate data sources, but the challenge is to normalize data in such a way that a security analyst can effectively search the data, and build out correlations. Additionally, SIEM is often integrated with other cyber security tools. For example, if the SIEM sees a rules violation, it can inform the firewall to block similar signatures. For another, the SIEM can also communicate bidirectionally with network access control (NAC) to determine if an end-user class (C-level executives for example) is being targeted and then the NAC can quarantine those end users until an investigation takes place or remediation is initiated and completed.

SIEM and other cyber security technologies are in a transitional phase. Security professionals recognize the need to automate as many processes as possible, but at the same time are reticent to give up full control of the investigative process. At the same time there are time constraints, storage considerations, and usability concerns. More simply put, the best SIEM have to integrate machine learning, external threat feeds, user behavioral analytics, and establish statistical baselines.

The fruition of data collection/machine learning/user and entity behavioral analytics is to improve mean-time-to-detect, and mean-time-to-respond to threats. The security analyst is a vital part of this process, therefore SIEM has to be intuitively easy to use; it has to drive well. LogRhythm Platform 7.2 systematically addresses many of these concerns.

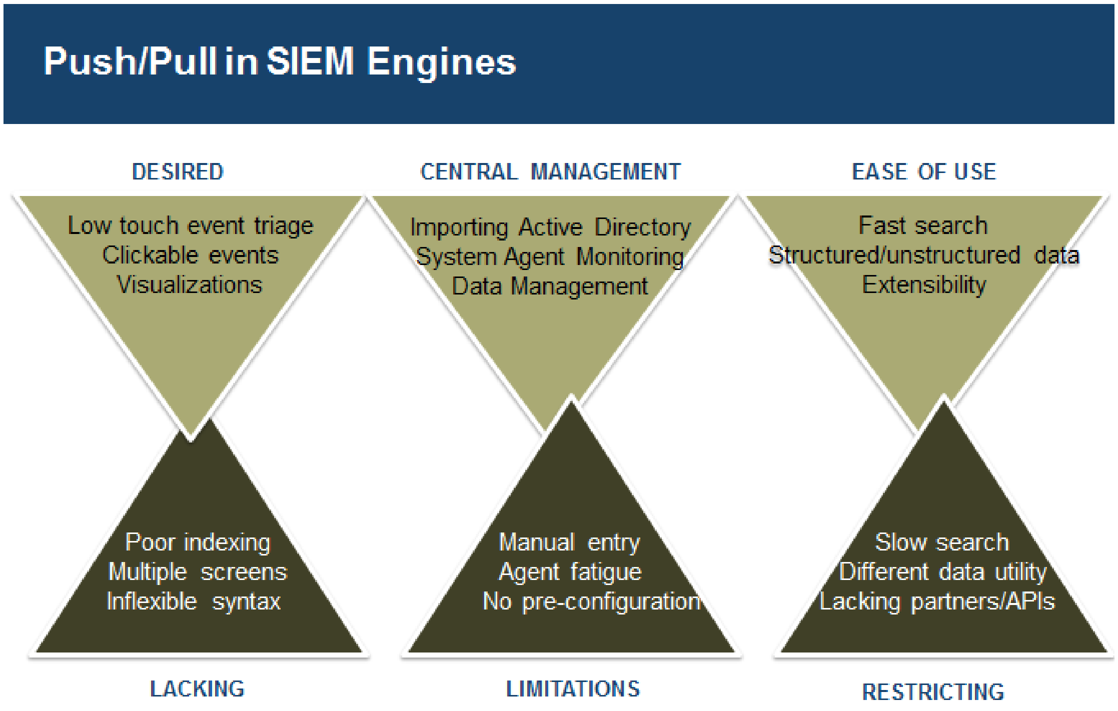
In truth, SIEM is increasingly used from beginning-to-end in the threat management lifecycle. LogRhythm improves on the traditional SIEM functions. The LogRhythm Threat Lifecycle Management Platform addresses the larger framework used to bring in data, provide search and automated analytics, and then fold in a formal incident response. This Best Practice recognizes LogRhythm's support for analyst work, including transitioning through lifecycle phases from forensic data, discovery, and qualification of events, through to search, and the steps necessary for remediation.

Commitment to Creativity

LogRhythm's origin is as a built-from-the-ground-up SIEM; rather than as the product of the acquisition and integration of disparate technologies. This distinction is subtle as other SIEM providers have also made a continuous effort to improve their platforms. However, overall performance has been a cornerstone to LogRhythm products. For instance, at different times when SIEM engines were chasing faster ingestion rates LogRhythm worked on usability or on data normalization. LogRhythm built a SIEM that was practical for mid markets but also robust enough for enterprise networks.

The effectiveness of SIEM is the successful execution of several small things done in integrated fashion at line-rate. The illustration below is a conceptualization of the best SIEM approaches compared to industry practices that could be improved.

Figure 1. The Conflict between Good and Suboptimal SIEM Engines



Source: Frost & Sullivan.

Eac
h

specific SIEM function can be reviewed ad nauseam, but there are big ideas that can be reviewed here. In simple terms, a SIEM is a data reservoir. The effectiveness of the SIEM is the smart management approaches that help to shape how IT/security analysts turn data into actionable knowledge.

- **Normalizing and data enrichment.** The data that comes into the SIEM from multiple sources is diverse. Data comes in at different speeds, from appliances, devices, infrastructure equipment, external threat feeds (optionally), and other data sources. Without a common taxonomy simple recall of data becomes problematic, and automated correlative analysis becomes almost impossible.

  Data enrichment is the process of indexing and storing data at the time of collection, and then pre-treating data for contextual awareness when an investigation begins. Off the bat, LogRhythm normalizes data centrally at the data processing layer as opposed to the collection layer, allowing normalization logic to be updated and propagated in a consistent manner. LogRhythm SIEM maintains a consistent three-tier log/event classification structure across all log data. This provides a user-friendly organization of all logs and enables quick search and reporting adoption. LogRhythm prepares data with its Machine Data Intelligence (MDI) Fabric directly after collection, powering analytics.

  The LogRhythm can parse and normalize machine data from over 830 sources, generating metadata that is specifically structured to enable security analytics. The MDI fields schema was recently expanded by 20 fields including: CVE, hash, detailed process information, domain names, and HTTP attributes. The MDI fabric also offers updated support for AWS, Box, Office365, Azure, Salesforce, and Tenable Nessus Cloud.

- **Central management.** LogRhythm offers agents that perform both log collection as well as independent monitoring including file integrity monitoring. The System Monitor Agent supports centralized and batch agent deployments. Active Directory Group Based Authorization allows customers to leverage their Active Directory infrastructure to automatically provision and manage LogRhythm user accounts. The dashboard and associated controls are designed so administration of LogRhythm components can be managed centrally, via policies, and supported through batch operations. Additionally, these tools are designed for local or global administration. In addition to dashboards and procedures, LogRhythm assists with training.

- **Data management and reporting.** An end user can wholly configure a SIEM, but that defeats the purpose. With LogRhythm, Data Management Profiles deliver standardized configuration options for various data management modes based on best practices for customer requirements, simplifying the deployment process. Once in a SIEM, data management is ongoing. However, administrators have no need to re-create scenarios during search or when generating reports. LogRhythm provides data management by entity to allow re-use of reports, alarm rules, and AI Engine rules without re-creating per entity.

Commitment to Innovation

Unlike many industries, network security tools providers do not have the luxury of resting on their laurels. In 2016 and into 2017, LogRhythm made many innovations to its already elite SIEM.

- **Improved operating effectiveness.** SIEM is a potentially complicated tool to use; but LogRhythm made strides toward helping enterprises with its total cost of ownership. On a platform level, Log Rhythm increased simultaneous user support by 60% in single node and better than 500% in multi-node. Infrastructure updates, including new appliances, increased indexing and storage capacity by a factor of two. Administrative improvements include enhanced auto-log sources acceptance, UNIX agent auto-update, scaled UIs, and Web deployment and systems monitoring through widgets. LogRhythm added 20 new Web UI visualizations and analyst workflow enhancements including easy access to external threat feeds.
- **Improved endpoint monitoring.** SIEM engines are perceived to be data-in engines, but in reality, SIEM can have visibility over multiple surfaces. LogRhythm augmented its endpoint monitoring capabilities by adding data capture types, and providing plug-ins that enable SOCs to respond to malicious behavior by invoking investigatory actions and countermeasures on the endpoint.
- **Extended the embedded Security Automation and Orchestration (SAO) function.** Enhancements were made to SOA workflow with improved case management and internal knowledge management. Widgets were created to record and monitor MTTD/MTTR responses. Creating alerts and detecting problems is one thing; but formal incident response is just as important. In LogRhythm 7.2, there are now 20 automated actions in its SmartResponse platform including Cisco, Fortigate, Anue, and Infoblox devices supported out of the box.
- **Emphasis was given to better "qualify" events.** LogRhythm SIEM 7.2 was designed to better ingest and normalize the results from multiple threat feeds in connection with observed activities. By itself this feature is helpful, but LogRhythm goes further by corroborating activity connected with threat intelligence data with additional suspicious activities across endpoints and user activities to better realize and prioritize truly concerning activity and suppress false positives.
- **Continued leadership in holistic threat detection.** LogRhythm has a strong user and entity behavior analytics (UEBA) engine. LogRhythm leverages UEBA in its user Threat Detection Module which aligns scenario-based analytics to the cyber kill chain taxonomy and with updates from customer field experiences.

Customer Purchase Experience

Network security products have to match the architectures of how networks are constructed. What was once "flat" network architecture is now heterogeneous networking with a combination of on-premises, private cloud, and public cloud networks.

LogRhythm has five different purchasing options: as an appliance, as software, enterprise licensing, cloud, and programs designed specifically for managed security service providers (MSSP).

LogRhythm has products for SMB businesses as well as for enterprises. LogRhythm offers the Enterprise Licensing Program (ELP) for enterprises. Enterprises are likely to have multiple locations, but LogRhythm pricing is a consumption model based on messages per second (MPS) used, not on the number of appliances installed. To help customers get their LogRhythm appliance up to speed, LogRhythm has a simple install and upgrade experience shared across appliance or software deployments. Mentioned earlier, Active Directory Group Based Authorization, Data Management Profiles, and the System Monitoring Agent are not only time saving tools, these applications cut down on the number of errors made in standing up and maintaining a SIEM.

Customer Ownership Experience

This citation has been bullish about the LogRhythm approaches to on-boarding end users through Active Directory, the delivery of threat detection and compliance content through Knowledge Base, and device management and recognition. In the LogRhythm SIEM, the early work matters . . . however, it only matters if the data has been shaped for investigation—which it has.

Search is at the absolute heart of SIEM. The search process has to be fast, and associate the right data. LogRhythm wisely uses the Elasticsearch backend which gives the analyst agility across massive data sets. The dashboards are clean, intuitive, and utilitarian—any event that is shown on the LogRhythm dashboard is a clickable event, enabling rapid drill-down.

“Precision search” is a vitally important facet of the search function provided by LogRhythm. A structured search might co-join different search instructions like “Windows OS,” and some IP address range in a formal investigation. For unstructured search, the analyst uses flexible search syntax to scan machine data. However, the most important and elegant feature is that from the perspective of the analyst, they can work with both structured and unstructured data simultaneously. On the dashboard the solution is particularly elegant as analysts can isolate a set of structured data sets (C-level executives, machine types) and create searches against unknown variables (software, malware types, etc.).

Lastly, at some point search becomes case management. Customizable widgets and dashboards facilitate the search function. As each new analytics criterion is selected, a "breadcrumb" is created to create an intuitive display of all search and filter criteria. Breadcrumbs can be removed and investigated independently. (Note: users who prefer a command-line approach can augment search with the Lucene query language to perform complex searches).

The last strength of the LogRhythm SIEM is the transition from investigation to response.In 2017, the trend is toward automated response, although many customers still prefer manual attestation and processes. LogRhythm’s SmartResponse automation framework enables the automated execution of targeted actions. LogRhythm provides as many as many as three levels of authorization before an action is taken. SmartResponse is a differentiator; shown below are a few other features:

- **SmartResponse plug-ins.** In 2016, LogRhythm created plug-ins with nine other security service providers. One plug-in with Cisco Identity Service Engine (ISE) will trigger a quarantine based on the offending host's MAC Address, IP Address, or Session ID.
- **Incident response.** Automated playbooks support rapid incident response and countermeasures.
- **Automated playbooks by use case.** Playbooks can be developed to shape a response for compliance with specific regulations. Additionally, playbooks can be developed against specific threats. One example is that LogRhythm could detect a ransomware attack (like CryptoLocker) by identifying systematic file modifications or if a user is encrypting files on a proxy honeypot server. Actions can be applied to the file server, file management system, or audit logs.

Brand Equity

The body of this citation explained what is good about the platform, but another nice aspect of LogRhythm is that the platform is extensible. LogRhythm has an extensive partnership network (see Technology Partners | LogRhythm). Partnerships may include two-way integrations using standards-based data collection methodologies; public and private partner APIs, LogRhythm's API, and integration with LogRhythm AI Engine Rules and LogRhythm SmartResponse plug-ins. New partnerships are being developed to help clients with integrations like Internet of Things (IoT), identity solutions, and supervisory control and data acquisition (SCADA).

LogRhythm is a privately-held company that built its products from the ground up. At the same time, LogRhythm built its relationships from the ground up. What were once essential soft values like customer relations and technical support has been an important element in the continued growth of LogRhythm as a major SIEM vendor.

Conclusion

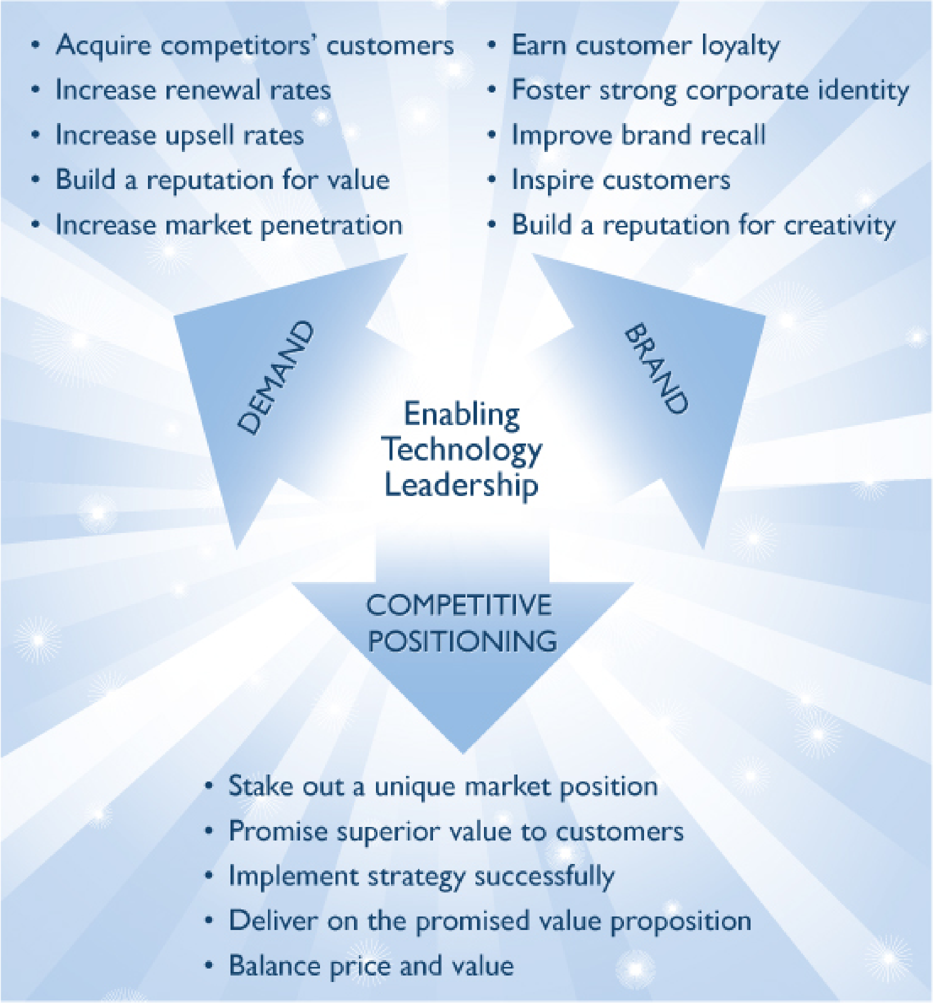
Frost & Sullivan estimates the global SIEM as a roughly $1.8 billion market in terms of revenues attained through appliances and services. For LogRhythm, the company has enjoyed a steady, but certain ascent. Frost & Sullivan has charted the global SIEM market since 2010, and Frost & Sullivan believes that LogRhythm has had double-digit revenue growth in every year. Not only is the growth rate significant, LogRhythm has outpaced the overall global SIEM in terms of year-over-year growth in each of those years.

LogRhythm's success is the not only the result of doing many individual small things well; it is the result of putting the pieces together in a continuous, unified platform.

With its strong overall performance, LogRhythm has earned Frost & Sullivan's 2017 Enabling Technology Leadership Award.

Significance of Enabling Technology Leadership

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


• 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
Enabling Technology Leadership
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 Enabling Technology Leadership

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

Key Benchmarking Criteria

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

Technology Leverage

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

Customer Impact

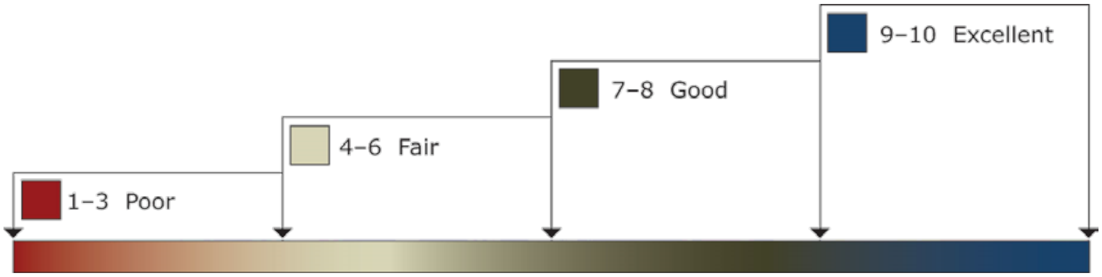
Criterion 1: Price/Performance Value
Criterion 2: Customer Purchase Experience
Criterion 3: Customer Ownership Experience
Criterion 4: Customer Service Experience
Criterion 5: Brand Equity

Best Practices Award Analysis for LogRhythm

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 Technology Leverage 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)			
Enabling Technology Leadership	Technology Leverage	Customer Impact	**Average Rating**
LogRhythm	**9.2**	**9.6**	**9.4**
Competitor 2	8.4	7.0	7.7
Competitor 3	7.2	7.2	7.2

Technology Leverage

Criterion 1: Commitment to Creativity

Requirement: Technology leveraged to push the limits of form and function in the pursuit of "white space" innovation

Criterion 2: Commitment to Innovation

Requirement: Conscious, ongoing adoption of emerging technologies that enables new product development and enhances product performance

Criterion 3: Stage Gate Efficiency

Requirement: Adoption of technology to enhance the stage gate process for launching new products and solutions

Criterion 4: Commercialization Success

Requirement: A proven track record of taking new technologies to market with a high rate of success

Criterion 5: Application Diversity

Requirement: The development and/or integration of technologies that serve multiple applications and can be embraced in multiple environments

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

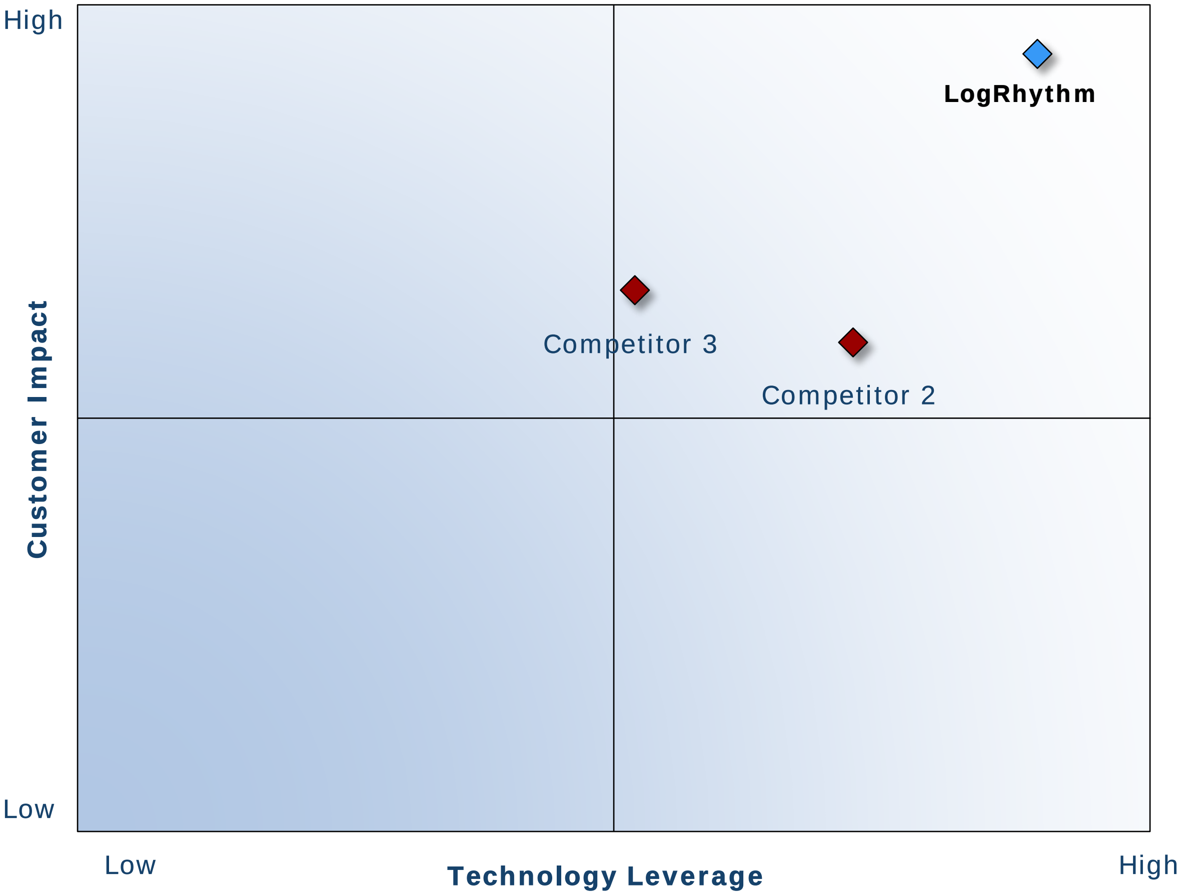
Requirement: Customer service is accessible, fast, stress-free, and of high quality.

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

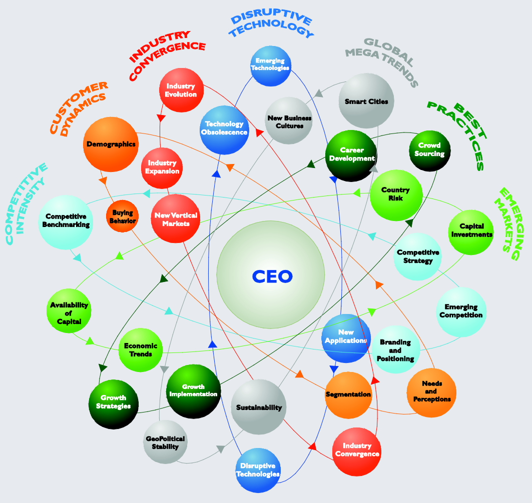
Frost & Sullivan analysts follow a 10-step process to evaluate Award candidates and assess their fit with select best practice criteria. The reputation and integrity of the Awards are based on close adherence to this process.

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 recipient	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 is able to share Award news with stakeholders and customers	• Coordinate media outreach • Design a marketing plan • Assess Award's role in future strategic planning	Widespread awareness of recipient's Award status among investors, media personnel, and employees

The Intersection between 360-Degree Research and Best Practices Awards

Research Methodology

360-DEGREE RESEARCH: SEEING ORDER IN THE CHAOS



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.

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.