FROST & SULLIVAN

NIKSUN®

2017 Global Network Security Forensics Enabling Technology Leadership Award

Background and Company Performance

Industry Challenges

"Defense in depth" is the term used to define the contemporary cyber defensive posture taken by enterprise networks. A network is the confluence of end users, data, access points (virtual, cloud, Web, and/or on-premises network hardware), and applications. In cyber security, defense in depth means the layering of multiple cyber defenses that correspond to each discrete network mechanism (*i.e.* endpoint defenses for end users, network firewalls to defend the core network, data loss prevention (DLP) to monitor the status of data, etc.).

Defense in depth creates friction for potential attackers. Additionally, a smartly aligned defense in depth strategy might create any number of redundancies—for example, if malware bypasses an antivirus system, perhaps its presence can be observed if an alteration or a theft of a file is attempted (file integrity management).

Unfortunately, intrusions into networks are not so easily detected. Malware intrusions vary from simplistic to highly sophisticated. Malware can attempt extraction immediately, or can lay in wait as in zero day threats. According to the 2017 IBM and Ponemon Institute Cost of Breach Study, the mean-time-to-detect a breach fell to 191 days in 2016. A breach is often discovered when an irate customer complains about identity theft or a company is visited by an external party like the FBI.

Fortunately, many of the tactics that are necessary to unify a defense in depth strategy can be leveraged in network security forensics.[1] Network security platforms are a class of tools that relies on partial packet capture with metadata or use full packet capture (PCAP) to trigger an investigation. These platforms are used to correlate users and events, and the platform is also capable of full fidelity session replay.

Technology Leverage and Customer Impact

When an investigation occurs, the forensic analyst will need to know where the security incident occurred, what was the consequence, if there was exfiltration, and where the attacker left the network. To do this, the forensic analyst will need information about network flow data and context about the end users and applications. An advantage to using a PCAP tool is its ability to see every bit within the packets. Often malicious code will leave the same footprint within the payload of infected packets.

[1] Network security forensics is a specific term introduced by Frost & Sullivan in the 2015 report Network Security Forensics Global Market - How Much Forensics Do You Need?, November 2015.

Contents

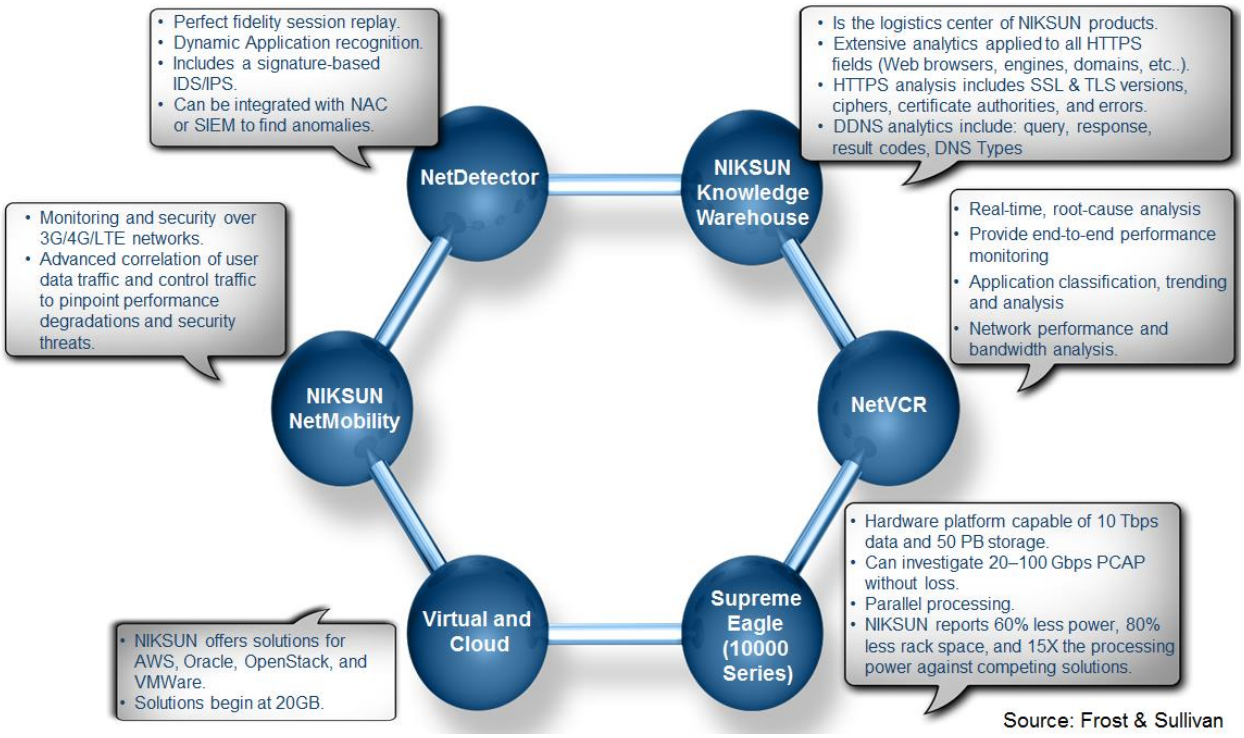
Many companies choose to use partial packet extraction with metadata collection (NIKSUN appliances are capable of both). Two important advantages are gained using partial packet capture. The first is a significant cost realization mostly through decreased storage needs. In general, the metadata technique provided about 80% of the data at 10% of the cost of PCAP. Secondly, while PCAP does in fact record every packet, the raw data is almost impossible to enrich. The trick is to enrich data for indexing, storage, and search at line-rate at the time of processing.

Commitment to Innovation

The strength of NIKSUN products is its focus on real-time big data analytics, forensics-based cyber security, and network and application monitoring as interrelated concerns of a single solution set.

Before the larger technical discussion is joined, perhaps the best course of action is to introduce the major platforms and capabilities of major NIKSUN products. The table below is not comprehensive as there are NIKSUN platforms are extensible providing coverage for the branch office and edge networks, but the technology principles are reasonably well outlined.

Figure 1 Visibility Provided by NIKSUN Products



NIKSUN products perform full packet capture and immediately generate "metadata" (in layman's terms, "data about collected data") to provide full and actionable visibility into a user's network. At this point, NIKSUN platforms store and index extracted full packet

capture, metadata content, and alarms/events about both security and performance incidents in the same NIKSUN Knowledge Warehouse for quick querying and granular root-cause investigation. High line-rates and extensibility within platforms are easily achieved because NIKSUN's architecture does not require an extra aggregation layer.

Alarms are triggered immediately upon an event and made actionable with just one click, filters are used to zoom in on the data, traffic, flow or time period the analyst wants to see. Forensic analysts are not bound to just setting recording filters for compliance and security—these can be used for a variety of reasons, like establishing statistical baselines or trending.

NIKSUN's NikOS Everest platform provides multi-layer and multi-protocol and protocol inspection analysis. NikOS Everest offers a large selection of out-of-the-box dashboard reports and the ability for users to create and customize their own and share. Scroll bars are used to zoom in to one second granularity or out to days, weeks or months of history. Importantly, the scroll bars can be applied to each appliance. For instance, one appliance can initiate full packet capture, and perhaps another appliance only monitors packet headers. Context sensitive hot links quickly move users to other dashboards, which are automatically updated as new traffic is captured. Packet broker and bounce diagrams are integrated as well as Role Based Access Controls (RBAC) and built-in training.

For network security forensics, NIKSUN has solutions that scale from 100 Mbps to above 100 Gbps with lossless packet handling. A full suite of NIKSUN's solution has been tested to handle 10 Tbps of data and 50 PB of storage.

Application Diversity

One would think that NIKSUN appliances, with its ability to index data at high line rates and its visibility over multiple environments, would lend itself to elegant solutions for vertical markets. In fact, refining NIKSUN platforms for specific industries is relatively easy.

In retail stores, companies are subject to Payment Card Industry Data Security Standard (PCI DSS) regulations. In software, PCI compliance reporting is available in real time by customers' servers and clients or by third parties, even for independent authorities. Users can identify clear text credit cards or SSN and receive extensive alerts on traffic anomalies, content, signatures, attachments, and validation firewall rule changes by observing traffic.

Additionally, in retail, payment card terminals are endpoint devices that are attached to a central network (or at least to credit institutions that approve transactions). In the December 2013, the Target breach was initiated when hackers went through software-control system that moderated HVAC units and then moved laterally to access the payment card terminals. NIKSUN offers Puma which is a handheld network recording

device capable of 1Gbps Ethernet, and the IntelliSeries 300 which includes solid-state storage. Puma can be used with NetDetector or NetVCR and is attached to a TAP or SPAN port. The form and function of the IntelliSeries 300 is similar to the Puma, except this device includes solid-state storage. Note, either the Puma or IntelliSeries 300 can be attached to payment card terminals for recording and incident detection (worth noting, either device would have detected the breach that afflicted Target).

NIKSUN NetTradeWatch offers multicast data monitoring, delay measurements, and transaction analytics that give a user full visibility into financial network environments. NetTradeWatch is an end-to-end solution that enables performance monitoring from market data inputs to real-time execution with the ability to zoom in on packet level details of interest. It provides out-of-the-box functionality and easy-to-customize dashboards and reports.

Even better than specific products for vertical markets, the NetVCR feature gives operations and network security teams the ability to customize to their respective needs. For network performance: operations, planning, accounting and application teams can use recorded data to identify and gauge trends and patterns. An application or operations team can set alarms based upon baseline, preset parameters—NetVCR performance alarms distinguish between short term, intermittent and sustained changes within the network.

Price/Performance Value

Assessing a price/performance in many ways can be a subjective judgment. Additionally, this Best Practice references multiple products and companion software. Perhaps the best deep-dive for pricing would be with Supreme Eagle with Enterprise software license pricing.

The Supreme Eagle has a six-server footprint where comparable server functions would use a 30-server array (source: SC Magazine Review: October 2015.) Supreme Eagle pricing depends on its configuration and enterprise software licenses include NetVCR, NetDetector, NetDetectorLive, and NetOmni. Enterprise software provides visibility, analytics to detect anomalies in behavior or network performance gaps, and a top-down holistic view of all NIKSUN appliances from a centralized view, regardless of physical or network spans. The comprehensive enterprise software suite ranges from $100,000 - $200, 000, and maintenance packages can also be purchased.

While the upfront costs for Supreme Eagle are significant, the cost is consistent with the capability and capacity of the platform. Three direct savings are realized.

- **Savings from a consolidation of tools.** The combination of NetVCR and NetDetector make an application performance monitoring system obsolete. Perhaps integrations with firewalls, intrusion detection and intrusion prevention system

(IDS/IPS), and security information and event management (SIEM) tools sharper or even minimize the need for these platforms. Supreme Eagle can store 50 PB of data, and this means that the cost of external storage systems or hard drive discs is avoided.

- **Hardware costs.** Again, this calculation could be gnarly if the cost of storage, and rack space is thoroughly considered.[2] A useful calculation might be to determine the cost of housing, powering, and cooling 24 servers (a six-server set versus a 30-server array). A typical datacenter designed to host roughly 50,000 servers will require 11,600,000 Megawatts for critical load capacity, cooling, and an acceptable PUE which is the ratio of total amount of energy used by a computer data center facility to the energy delivered to computing equipment. Electrical costs vary, however, general assumptions of $0.07 per/kwh and $9 per Watt at critical load capacity seem reasonable. If the model is carried through to include server and network amortization, we get to $1,450 as an annual cost to host a server in datacenter. The savings realized would be $34,800 annually.

- **Soft costs, which are not-so-soft costs.** Ultimately, NIKSUN products are designed to investigate network and application performance issues and to reduce the mean-time-to-detect and the mean-time-to-respond to network intrusions. The time that analysts spend investigating incidents are real costs; some of the metrics were explained in the previous footnote. These costs are not easy to quantify, but generally forensic analysts average $100,000 a year in wages. However, the man-hour costs are dwarfed by the loss of assets, intellectual property and personally identifiable information (PII) from certain breaches.

Customer Ownership Experience

Each network security tool has its own idiosyncrasies. However, a forensic investigation must uncover the type of attack (malware, stolen credential, etc.), how the attacker got in, what was targeted, and what damage has been done. Triage is the mundane process of putting together end users with their network histories (Websites visited, applications run, place in the network). Mundane or otherwise, in a closed-loop process, triage takes roughly 70% of the time consumed in investigation assuming an investigation is successful at all.

[2] However, in the spirit of not short-changing NIKSUN, one client case study was illuminating. An undisclosed client reported Supreme Eagle demonstrated a 505% increase in efficiency. The breakdown is as follows: NIKSUN's Supreme Eagle reduced the average time to analyze normal incidents from three hours to 20 minutes (a 900% improvement), the affirmative conclusion rate on normal issues went from 25% to 65% (a 260% improvement), the number of incidents about which no conclusion could be drawn from 75% to 35% (a 215% improvement), the average time to analyze complex issues with a team of four went from 10 hours to four hours (a 250% improvement), the affirmative conclusion rate on complex issues from 5% to 45% (a 900% improvement), and their zero day capture rate up from 0% to 20%. Supreme Eagle also manifested as 1/10th of the required rack space.

NIKSUN has several features that make the work of analysts safer and easier.

- **HTML5 interface.** NIKSUN products use a Web based HTML5 browser. The search function is initiated using plain English (similar to a Google function). The search function is quick in the UI, but remember that data is wrote onto the NIKSUN Knowledge Warehouse instead of onto a data collection layer for quick retrieval; recording, indexing, and querying is gathered in the same process.

- **Full fidelity session replay.** NetDetector has Quick Mode and Full Mode session reconstruction options. Additionally, a DNS reconstruction of events, malware, and attachments is possible to investigate DNS spoofing or DNS DoS attacks. If an analyst traces the steps of an infected end user, the analyst will see the exact same Web page the end user visited. However, the objects in the search are quarantined in a sandbox so while a session is being initiated, the investigator is not also infecting the network.

- **Better visibility.** Towards visibility, all NIKSUN products use a Dynamic Application Recognition (DAR) plug-in framework which is optimized for the fast processing and securing of large amounts of data. This is differentiated from using a port- or TCP-based visibility method and enables custom application definitions for customer use. One of the key tactics that hackers use is to move activities to commonly used infrastructure such as web services, which always appear on the same TCP/IP protocol port. DAR is able to determine what the underlying application is.

- **Comprehensive metadata fields.** NIKSUN Knowledge Warehouse has drop-down menus where security teams can pull down relevant packet flows on-demand as requested by an analyst. The packet HTTPS analysis includes SSL and TLS versions, ciphers, certificate authorities, errors, and organizations. DNS analytics include query, response, result codes, and DNS types such as Name, Cname, NS, MX, and IPv4 vs. IPv6. Additionally, extendable GeoIP and GeoTCP monitoring/performance is offered by city, branch office, application, social media, service provider and any IP range(s). As a reminder, filters can be created within metadata fields to alarm a security team of suspicious behavior *before* a threat detonates.

Brand Equity

NIKSUN has earned a reputation as a system-level solution provider. In hardware, parallel processing speeds up the analytics engine, and powerful processing reduces the need for additional machinery. Data collection, indexing, and storage are treated as a continuous event. NIKSUN helps SecOps teams investigate anomalies in both network performance and potential security incidents.

NIKSUN has significant presence in government agencies, with Fortune 500 companies, and is the chosen provider of full packet capture for the U.S. Department of Defense (DoD) and Defense Information Systems Agency (DISA).

Conceptually, NIKSUN appliances perform data collection of raw data at very high rates, and the raw data is extracted as metadata and is cross-indexed for fast and accurate searching.

Conclusion

Since its inception in 1997, NIKSUN has been a hardware solutions provider working on issues in cyber security, application monitoring, and network performance markets. Many competing cyber security platforms treat network performance, network anomalies, and application monitoring as discrete platforms. Consequently, a SecOps team would have to combine several network security and performance technologies to do what NIKSUN platforms can do natively.

With its strong overall performance, NIKSUN has earned Frost & Sullivan's 2017 Enabling Technology Leadership Award for Network Security Forensics.

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.

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

Customer Impact

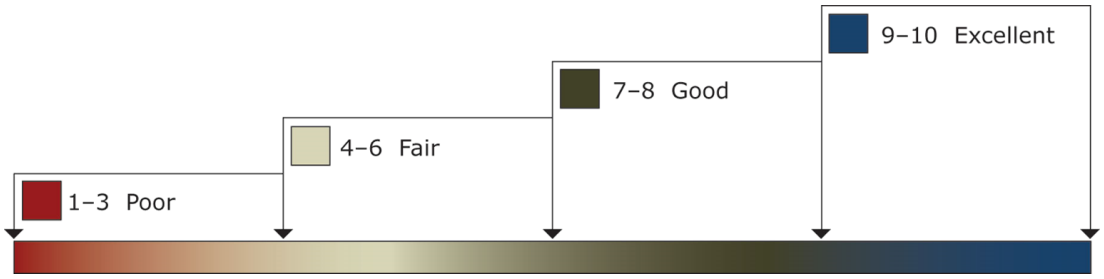
Criterion 1: Price/Performance Value
Criterion 2: Customer Purchase Experience
Criterion 3: Customer Ownership Experience
Criterion 4: Customer Service Experience
Criterion 5: Brand Equity

Best Practices Award Analysis for NIKSUN

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**
NIKSUN	**9.8**	**9.6**	**9.7**
Competitor 2	8.0	6.0	7.0
Competitor 3	5.4	7.2	6.3

Technology Leverage

Criterion 1: Commitment to Innovation

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

Criterion 2: Commitment to Creativity

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

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

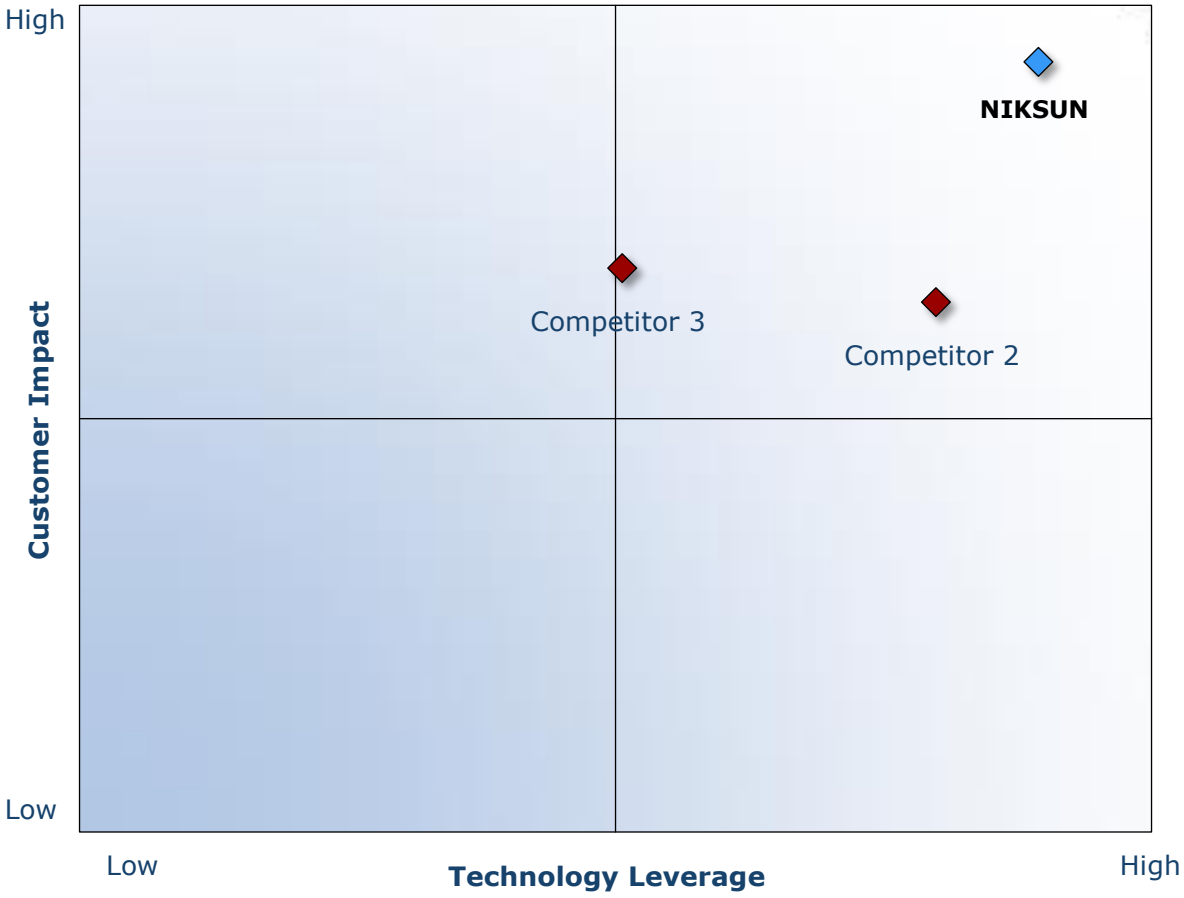
Requirement: Customer service is accessible, fast, stress-free, and of high quality.

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

© Frost & Sullivan 2017

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.