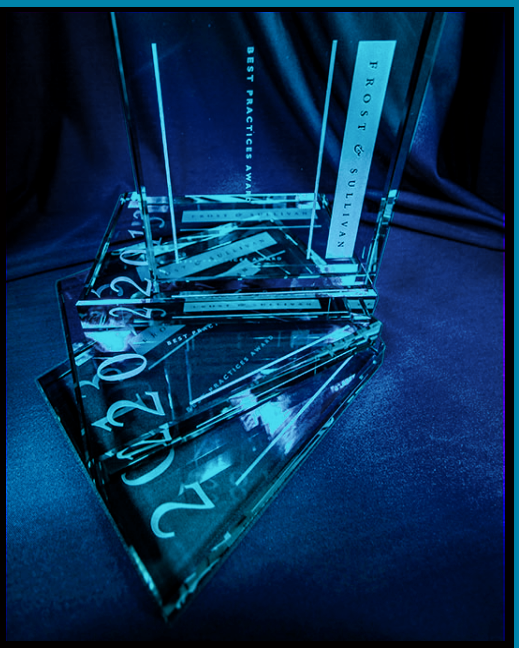
FROST & SULLIVAN

RSA®

2016 Global Network Security Forensics Enabling Technology Leadership Award



FROST & SULLIVAN

2016 BEST PRACTICES AWARD

GLOBAL
NETWORK SECURITY FORENSICS
ENABLING TECHNOLOGY LEADERSHIP AWARD

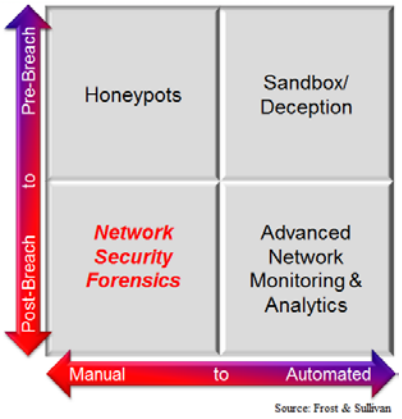
2016
BEST PRACTICES
AWARDS

Contents

Background and Company Performance

Industry Challenges

The network security team at Frost and Sullivan views Advanced Persistent Threat (APT) defense as not a singular technology, but rather as a collection of technologies used in concert. Network security forensics is the requisite technology used when a suspected security breach has occurred.



The difference between a security incident and a breach is subtle and may be a matter of semantics, but is necessary to establish to explain the capabilities of network security forensics tools. A security incident occurs anytime a detective system creates an alert. The majority of security incidents are not an indication of a breach, but of course this can't be confirmed without an investigation. An alarm could be raised when an end user is using or consuming an unusual amount of bandwidth, an endpoint device is connecting to a server outside of its normal region, or a server reconfiguration is taking place outside of normal practices, as well as many other indicators of compromise. Rightly these incidents are cause for investigation but in fact may turn out to be benign.

A validated security breach requires three conditions to be met:

- A breach is the establishment of an unapproved presence (potentially malicious) within a proprietary network.
- The end user's system or credential, or aspects of the enterprise network has been exploited, which often leads to data exfiltration outside of the enterprise.
- A forensics investigation has to be initiated to run the issue to ground. A network security forensics investigation occurs when an exploit becomes known to an IT/Security team as a result of a material and malicious change somewhere on the enterprise network.

Today, the tools that are often used to protect networks are often the same tools used to determine what happened in a breach. This is problematic for these preventive focused network security platforms. One example of the problem is if malware[1] did defeat the preventive security system, the vendors offering the forensics tool are asking security teams to use the same tools that ostensibly "failed" in the first place. However, more

[1] Part of the problem with the term "breach" is the term is broadly used in network security. Breach is almost synonymous with malware and phishing attacks. In fact, breaches can occur without the use of malware when servers are being reconfigured, passwords and credentials are stolen, or a theft of physical equipment happens. In these cases, the breach situation is not caused by a failing in a preventive security tool; nonetheless, the breach must be detected, understood, and remediated.

mature security organizations understand the limitation of prevention and are increasingly focusing on systems and processes to improve their detection and response capabilities.

RSA Security Analytics is cited in this award for its ability to support investigations leveraging network flow data, full packet capture (PCAP), logs, and endpoint data as well as information from other security platforms and external threat intelligence sources providing world class network security forensics. In addition, but not the focus of this particular award, RSA Security Analytics provides Advanced Network Monitoring & Analytics capabilities as well as part of an integrated threat detection and response solution.

Technology Leverage and Customer Impact

RSA has long been a leader in network security technology. RSA offers products and services for authentication, identity management & governance, data protection, advanced security operations, network and endpoint monitoring and analytics, and for the management of governance, risk and compliance. The RSA Security Analytics product is delivered via the combination of a scalable server, storage, and security data collection architecture providing advanced detective analytics, forensic investigations, reporting, incident management, and threat intelligence correlation via an integrated platform.

Commitment to Innovation

The RSA Security Analytics platform is comprised of two primary elements: the capture infrastructure and the analysis, investigation, and data retention infrastructure. See RSA Security Analytics for more details on this. This distributed architecture provides Security Analytics several important capabilities:

- **Platform versatility, scalability, and flexibility.** The capture and analytics infrastructure of Decoders, Concentrators, Analytic Servers, Event Stream Analysis (ESA) Servers, and Archivers can be deployed using just a handful of appliances or via many dozens of systems in highly distributed, global deployment – scaled up or down to meet the performance needs of the organization. In addition RSA Security Analytics can be deployed virtually in part or in whole.
- **Unified analytics.** The ESA server provides detective analytics leveraging metadata from logs/events, network packets, NetFlow, endpoint data, threat intelligence, and other context data. The ESA server can apply both traditional correlations as well more sophisticated data science based techniques to detect and alert on security anomalies.
- **Real-time capture data enrichment.** RSA uses a proprietary ingestion technology to simultaneously tag and enrich data for threat indicators while parsing the raw data into metadata for further detective analytics as well as to support forensic and investigative uses. In a forensics investigation the use of this metadata without losing connection to the raw data is critical to finding the "root cause" of the event. The collection of the raw data for extended periods also enables Security Analytics to recreate full sessions (Web browsing, FTP, email etc.) so that the investigating security analysts can literally "see" what happened.

- **Golden image and whitelisting.** If Security Analytics and ECAT (RSA's endpoint detection and response tool) are used concurrently, all new file insertions into the network (via Security Analytics) and onto monitored endpoints (via ECAT) can be analyzed statically as well as dynamically. If a file is found to be secure, it can be added to ECAT's and Security Analytics's whitelists and be trusted from that point forward.

Cyber security platforms such as vulnerability management (VM), firewalls and intrusion detection and prevention systems (IDS/IPS) generally depend upon file signatures to detect malware and other security relevant activity. Security Analytics does not depend on signatures; it uses multiple analytic techniques that are focused on detecting anomalous behavior at both lower (such as at the protocol level) and higher levels (such as at the Web domain level) of the IT stack. RSA ECAT, a closely integrated technology with RSA Security Analytics, also provides a signature-less threat detection system that uses agents on endpoints (servers & clients) to look for anomalous behavior & malware across the enterprise at both the user and kernel level of the host.

Commitment to Creativity

Frost & Sullivan insists on at least partial, but preferably full packet capture or PCAP as a qualification to be considered as a network security forensics platform. The selection of this attribute excludes tools or tool sets that rely only on NetFlow as the data source for forensics investigations.

In one camp, a new class of network forensics tools is being developed that rely on the extraction of packet headers only, combined with metadata correlation. This approach is attractive from a storage perspective as packet headers consume between 1–10% of the storage space as do full PCAP based systems.

Good→Better→Best Network Security Forensics Practices

Searching Security Events→Packet Headers with Context→PCAP with Metadata

Endpoint Visibility→L2-L7 Traffic Visibility→Real-time Indexing and Correlation

Signature-based Detection→Integration with 3rd Party Platforms→External Threat Services

Anomaly Detection→Statistical Thresholds→Behavioral Analytics Detection

Source: Frost & Sullivan

However, the efficacy of full packet capture is difficult to argue against as this approach provides incident detection, metadata management and context, as well as full session reconstruction on their platforms. Key advantages to organizations using network security forensics with full packet capture technologies include full traffic visibility (including east-west traffic), more complete metadata, full packet analysis which may be necessary to see where bad code is embedded in the malware or when protocols are malformed (see graphic to the left).

When deep security monitoring capabilities and performance are the key criteria, vendors offering network security forensics with full packet capture, such as RSA, increasingly win the business.

Application Diversity

Perhaps the most underappreciated aspect of a good network forensics tool is the man-hours that can be saved. Frost & Sullivan believes that 50—70% of the time to investigate a security incident is in triage. In journalism, the emphasis is on the 4 Ws (who, what, where, and when). The four Ws can be used in security operations, but with two added caveats. The first caveat is that by definition a network security event is triggered when a breach is likely to have occurred; time is really of the essence. Secondly, the most effective correlations and analytics use more than just one security event to estimate the importance of the security incident. An attack may be designed to exploit a specific OS, application, user group, or file type and often will exploit many systems and points of entry at the same time. Investigations cannot be limited to one specific area of a network or system; rather, a threat is best contained to the degree that the infection/exfiltration is discovered on all systems that are affected. With today's more targeted attacks, attackers often have multiple points of entry into the organization. If you don't find them all you haven't sufficiently mitigated the threat.

RSA Security Analytics is ahead of the curve in creating advantages for security investigation teams:

- **Native incident management.** A security incident is centrally managed and thus can be investigated by several analysts concurrently or in sequence.
- **Metadata.** The RSA Security Analytics generates, analyzes, and makes available for investigations of more than 175 metadata fields. Metadata is automatically enriched with threat intelligence. No matter what the source of data, logs, events, Netflow, packet capture, or other, the same metadata model is used. This avoids the problem of data silos thus helping security analysts to more easily connect the dots during an investigation.
- **Session replay.** RSA Security Analytics can replay whole suspect sessions (Web, FTP, email, etc.) as well as provide a view of exactly what was exfiltrated in a potential attack. Furthermore, short, intermediate, and long time period searches, reports, and analytics can be conducted as well
- **Data science.** RSA Security Analytics uses data science and machine learning to better detect threats and guide the priority of forensic investigations.

Brand Equity

The origin of RSA is in 1979—the RSA acronym stands for the Rivest-Shamir-Adleman cryptosystem that is used in public key encryption systems even today. RSA has a strong historical affiliation with state-of-the-art technology.

The current RSA incident detection and network forensics platform, RSA Security Analytics with RSA ECAT for the endpoint, is a combination and evolution of several well-reputed predecessor products. In April 2011, RSA acquired NetWitness. NetWitness provided RSA with packet decoding, network visibility, and an investigation platform.

EMC, RSA's parent company, had worked with Silicium Software for several years to provide endpoint detection and investigation capabilities for EMC's CIRC. In September

2012, RSA acquired Silicium Software and its key ECAT endpoint threat detection and response technology. To provide a genuinely unique security platform, RSA has integrated Security Analytics and ECAT to provide a unified network and endpoint monitoring and investigation solution.

The RSA Security Analytics platform receives fresh threat intelligence information and other content continuously through its RSA Live service, which is included with the product. The RSA Live content delivery service dynamically updates the components of Security Analytics with threat information as it is discovered by RSA Research teams as well as those of 3rd parties. This makes this threat intelligence actionable immediately as part of the Security Analytics system.

Conclusion

Network security is not just for the detection of malware; it involves the detection and investigation of security incidents using multiple forms of telemetry as well as multiple forms of analytics. With Security Analytics, RSA is able to bring a comprehensive set of technologies to incident detection and network security forensics. Metadata generation and full packet capture gives Security Analytics depth and real-time visibility to determine the security posture of the enterprise as inbound and outbound communications are traversing its network.

With its strong overall performance, RSA with RSA Security Analytics has earned Frost & Sullivan's 2016 Network Security Forensics Enabling Technology Leadership Award.

Significance of Enabling Technology Leadership

Ultimately, growth in any organization depends upon customers purchasing from your 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 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

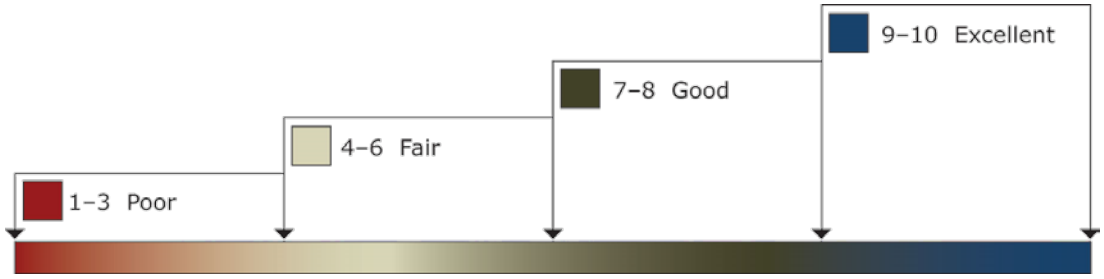
Criterion 1: Price/Performance Value
Criterion 2: Customer Purchase Experience
Criterion 3: Customer Ownership Experience
Criterion 4: Customer Service Experience
Criterion 5: Brand Equity

Best Practice Award Analysis for RSA, The Security Division of EMC

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., the overarching categories for all 10 benchmarking criteria; the definitions for each criteria 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 players as Competitor 2 and Competitor 3.

DECISION SUPPORT SCORECARD FOR ENABLING TECHNOLOGY LEADERSHIP AWARD

Measurement of 1–10 (1 = poor; 10 = excellent)			
Enabling Technology Leadership	Technology Leverage	Customer Impact	**Average Rating**
RSA	**9.5**	**9.9**	**9.7**
Competitor 2	8.0	6.0	7.0
Competitor 3	5.8	7.0	6.4

Technology Leverage

Criterion 1: Commitment to Innovation

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

Criterion 2: Commitment to Creativity

Requirement: Technology is 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 like 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

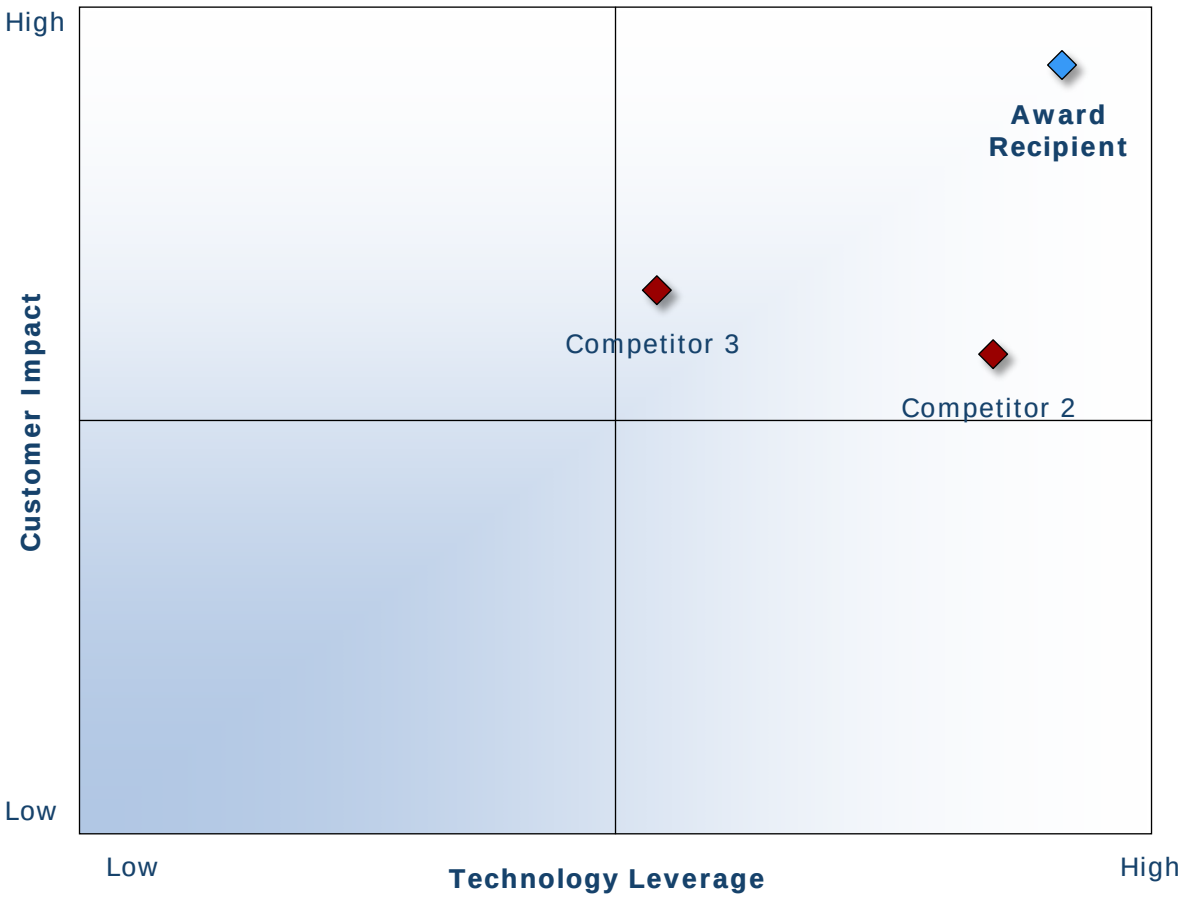
Criterion 5: Brand Equity

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 can 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.

DECISION SUPPORT MATRIX FOR ENABLING TECHNOLOGY LEADERSHIP AWARD



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 players and for identifying those performing at best-in-class levels.

360-DEGREE RESEARCH: SEEING ORDER IN THE CHAOS

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, 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 almost 50 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from 31 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.