



2018 Global Advanced Malware Sandbox
Customer Value Leadership Award



2018
BEST PRACTICES
AWARDS

Contents

<i>Background and Company Performance</i>	3
<i>Industry Challenges</i>	3
<i>Customer Impact and Business Impact</i>	3
<i>Conclusion</i>	5
<i>Significance of Customer Value Leadership</i>	6
<i>Understanding Customer Value Leadership</i>	6
<i>Key Benchmarking Criteria</i>	7
<i>Customer Impact</i>	7
<i>Business Impact</i>	7
<i>Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices</i>	8
<i>The Intersection between 360-Degree Research and Best Practices Awards</i>	9
<i>Research Methodology</i>	9
<i>About Frost & Sullivan</i>	9

Background and Company Performance

Industry Challenges

Cyber threat risk is at an all-time high and shows no signs of abating. Nation-state agencies and criminal organizations are turning to cyber attacks as a means to sabotage or infiltrate distant and high profile targets. Cyber attacks offer advantages such as remoteness and anonymity, which attackers rely on as defense against attribution, retaliation, and prosecution.

These threat actors are increasingly relying on advanced malware for their attack campaigns, utilizing new evasion and obfuscation techniques, as well as zero-day vulnerabilities to bypass traditional network defenses. Malware such as WannaCry and Petya (classified as ransomware) wreaked havoc in 2017, disabling the radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant and causing millions in lost revenue and ransom payments.

The Advanced Malware Sandbox (AMS) was invented and designed to detect and block these types of advanced threats by identifying unknown and suspicious files, isolating and executing these in a virtualized environment, and monitoring and observing the file's behavior for any indicators of malicious programming. Based on this approach, AMS results deliver a high degree of detection accuracy and fidelity, as well as valuable insights into malware behavior. These capabilities have made the AMS a vital tool in any network security architecture.

However, IT and networking is changing rapidly. Businesses are expected to adopt new technologies and defend against emerging threats with little or no increase in budgets or staffing. Enterprises already report owning dozens of point products, each with unique management interfaces to learn and support processes to navigate.

As the AMS market becomes more competitive, vendors must deliver highly accurate products that are also integrated into a broader threat prevention ecosystem for greater security efficacy and ease-of-use. Essentially, enterprises require advanced security tools, including AMS solutions, which also deliver a high level of business value.

Customer Impact and Business Impact

Fortinet is a leading provider of Next Generation Firewalls (NGFWs) and Unified Threat Management (UTM) products. Fortinet also offers a broad portfolio of security solutions ranging from endpoint security, to intrusion prevention systems (IPS), filtering, web application firewall (WAF), and distributed denial-of-service (DDoS) mitigation.

Fortinet has emerged as an important emerging challenger in the AMS market. The company achieved strong growth rates in 2017, its success driven largely by a focus on product quality and integration within a broader framework that translates to enhanced

security efficacy and business value.

Focus on Product Quality

FortiSandbox is Fortinet's line of advanced malware sandbox solutions, available as physical or virtual appliances, hosted, or in the cloud. FortiSandbox can be deployed as a stand-alone product or as an integrated solution attached to a Fortinet security product or third-party solution. Fortinet also offers FortiSandbox on AWS public cloud environments (either bring-your-own-license or on-demand). As such, FortiSandbox offers a high degree of deployment flexibility.

FortiSandbox uses a combination of emulation and full dynamic sandbox-based analysis to detect unknown and new threats. Fortinet continues to add new capabilities to the FortiSandbox product, such as support for Mac OS and Android, analysis of encrypted threats and cloud-based threats. These expansions help customers to better defend their full range of network and computing environments.

FortiSandbox product quality is affirmed with its routine participation in third-party tests from NSS Labs earning Recommended awards for both 2017 Breach Detection Systems (BDS) tests with 99% detection rates and Breach Prevention Systems (BPS) tests with 99.6% block rates, and certification from ICSA Labs Advanced Threat Detection tests with 99%+ detection rates as well as low "total cost of ownership."

Interoperation with Broader Security Framework Yields Better Efficacy

FortiSandbox is one offering in Fortinet's extremely broad security portfolio. FortiSandbox draws on Fortinet's expertise in adjacent security technologies, such as IPS, antivirus, and web filtering, and uses these technologies as foundational security inspection layers in its FortiSandbox products.

FortiSandbox interoperates with the Fortinet Security Fabric, which provides intelligence sharing integrated with the full range of Fortinet security products including FortiGate (NGFW), FortiMail (SEG), FortiProxy (SWG), FortiSIEM (SIEM), FortiCASB (CASB), and FortiClient (EPP). This integration allows FortiSandbox to detect suspicious and unknown files across various entry points such as firewalls, secure web gateways, secure email gateways, and endpoint security. Once unknown malware is detected, FortiSandbox generates appropriate IOCs and shares in real-time with Fortinet and Fabric-Ready partner solutions to automate mitigation of the newly discovered threat. Optionally, the newly generated intelligence can be shared with FortiGuard Labs Global Threat Intelligence to create threat attribution as well as generate protections for the larger Fortinet community.

Additionally, FortiSandbox integrates with the FortiWeb Web Application Firewall (WAF) product. By comparison, no other AMS vendor offers a WAF product, and few competing AMS solutions integrate natively with WAF, which leaves an important attack vector vulnerable to delivery of advanced malware.

Similarly, the Fortinet Security Fabric provides zero-day integration with Fabric-Ready partners such as Carbon Black, Ziften, and SentinelOne. For example, Carbon Black and FortiSandbox working in conjunction can identify unknown malware from the network and then use the Carbon Black endpoint software to confirm and gather additional information such as location, scope and severity of the threat. Lastly, FortiSandbox offers third-party integration via JSON API as well as support for ICAP protocol. As part of a broader security framework (the Fortinet Security Fabric), FortiSandbox is able to deliver better protection, consistently, across all network environments and entry points.

Improved Security and Usability Enhances Business Value

While FortiSandbox offers value as a stand-alone product, the Fortinet Security Fabric imbues the solution with unique business value. The Security Fabric extends the advanced malware protections offered by the FortiSandbox across a broader and fuller set of network entry points. Fortinet Security Fabric is flexible and modular, and does not require a specific set of products to start—customers can use any already deployed Fortinet products as part of the Security Fabric and expand as needed.

FortiSandbox includes features to help reduce the security burden on IT organizations such as adjustable device priority and user profile management. Additionally, integration with Fortinet's Security Fabric provides centralized management. FortiSandbox centralized threat intelligence management is a vital capability that allows security professionals to understand the threat landscape more completely and with the contextual information necessary for rapid and accurate detection and response.

Conclusion

FortiSandbox helps to ensure consistent protection across the entire attack surface by coordinating Fortinet-protected network control points and endpoints including solutions from Fortinet's Fabric-Ready API Alliance Partners. The bi-directional integration of FortiSandbox provided through the Fortinet Security Fabric enables IT organizations to move past detection to prevention and protection from costly ransomware and other advanced persistent threats (APTs).

With its strong overall performance, Fortinet has earned Frost & Sullivan's 2018 Customer Value Leadership Award.

Significance of Customer Value Leadership

Ultimately, growth in any organization depends upon customers purchasing from a company and then making the decision to return time and again. Delighting customers is, therefore, the cornerstone of any successful growth strategy. To achieve these dual goals (growth and customer delight), an organization must be best-in-class in three key areas: understanding demand, nurturing the brand, and differentiating from the competition.



Understanding Customer Value Leadership

Customer Value Leadership is defined and measured by two macro-level categories: Customer Impact and Business Impact. These two sides work together to make customers feel valued and confident in their products' quality and long shelf life. This dual satisfaction translates into repeat purchases and a high lifetime of customer value.

Key Benchmarking Criteria

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

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.

Business Impact

Criterion 1: Financial Performance

Requirement: Overall financial performance is strong in terms of revenues, revenue growth, operating margin, and other key financial metrics.

Criterion 2: Customer Acquisition

Requirement: Customer-facing processes support the efficient and consistent acquisition of new customers, even as it enhances retention of current customers.

Criterion 3: Operational Efficiency

Requirement: Staff is able to perform assigned tasks productively, quickly, and to a high quality standard.

Criterion 4: Growth Potential

Requirements: Customer focus strengthens brand, reinforces customer loyalty, and enhances growth potential.

Criterion 5: Human Capital

Requirement: Company culture is characterized by a strong commitment to quality and customers, which in turn enhances employee morale and retention.

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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<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-practice 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-practice 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-practice criteria
9 Communicate recognition	Inform Award recipient of Award 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 future strategic planning 	Widespread awareness of recipient's Award status among investors, media personnel, and employees

The Intersection between 360-Degree Research and Best Practices Awards

Research Methodology

Frost & Sullivan's 360-degree research methodology represents the analytical rigor of our research process. It offers a 360-degree-view of industry challenges, trends, and issues by integrating all 7 of Frost & Sullivan's research methodologies. Too often companies make important growth decisions based on a narrow understanding of their environment, leading to errors of both omission and commission. Successful growth strategies are founded on a thorough understanding of market, technical, economic, financial, customer, best practices, and demographic analyses. The integration of these research disciplines into the 360-degree research methodology provides an evaluation platform for benchmarking industry participants and for identifying those performing at best-in-class levels.

360-DEGREE RESEARCH: SEEING ORDER IN THE CHAOS



About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best-in-class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages more than 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from 45 offices on six continents. To join our Growth Partnership, please visit <http://www.frost.com>.