FROST & SULLIVAN

BEST PRACTICES AWARDS

L7 DEFENSE

2020 GLOBAL FULLY AUTONOMOUS AI-BASED API SECURITY SOLUTION PRODUCT LEADERSHIP AWARD

Contents

Background and Company Performance

Industry Challenges

Enterprise infrastructure is changing dynamically as companies across industries implement digitization initiatives to modernize business functions. However, digital transformation generates volumes of sensitive data that businesses store across connected endpoints, in the cloud, and at data centers. Thus, the majority of the critical assets owned by organizations now take the form of information, such as confidential customer, payment, or company data collected through various connected devices. The critical nature of this data makes it quite attractive to hackers and cybercriminals. Businesses that experience security breaches can receive fines due to non-compliance according to their industry's data compliance standards, lose their customers' trust, or have more severe implications, such as the loss of sensitive or proprietary intellectual property.

However, for an organization to remain productive, it needs to have access to key enterprise assets and applications without having to follow complex procedures. Application program interfaces (APIs) are an integral part of the business processes of organizations across industries as they are pivotal to Web, mobile, software-as-a-service, Internet of Things, and microservices. For example, Uber Technologies Inc. (Uber) grew to a valuation of tens of billions of dollars in just a few years, surpassing the market cap of giants such as BMW by leveraging APIs. Uber essentially brings a plethora of APIs together that manage payments and user locations to provide its service.

Currently, the average large enterprise uses around 350 different APIs, and many organizations do not even have clarity regarding the number of APIs they utilize. Just as businesses leverage APIs, hackers target them to get access to user data in a more accurate way than conventional Web Internet services. Notably, the Open Web Application Security Project (OWASP) recognizes API security as a primary concern, and API breaches are predicted to be the most common attack vector in the coming years. Large players, such as Facebook, T-Mobile, Verizon, and Panera Bread, have all suffered from well-known API attacks. In 2018, hackers utilized Facebook's APIs to breach the data of 50 million user profiles.

Some organizations attempt to locate and resolve application vulnerability manually—overlooking many coding mistakes that are inevitable due to human error. Most application vulnerability solutions cannot detect more than 14% of vulnerabilities adequately, causing enterprises to utilize roughly three to five different scanners to cover 50% of vulnerabilities because these second-rate solutions often overlap in coverage. Even then, some vulnerabilities in code can still be missed due to lapsing coverage and lacking overall analysis of an application's complete operations. Each API's infrastructure is unique, and there is not a cookie-cutter security solution for all APIs, such as the case with adding a firewall to protect a whole network. Apart from restraints such as minimal automation, manual threat profiling, as well as manual policy creation and maintenance, the poor performance to cost ratio is also a limiting factor. Due to the complexity of APIs (as opposed to a website), API security solutions tend to be slow and costly and too dependent on manual programming and skill level.

However, investment in security solutions is on the rise. With more investment, large-scale enterprises are looking for innovative solutions that can work cohesively with their existing infrastructure to increase visibility into how exposed they are. In most cases, companies only discover vulnerabilities and compromised credentials after they have been exploited; therefore, thriving enterprises require tools that help them assess their risk and exposure to address issues proactively. Frost and Sullivan's independent research confirms that an application vulnerability solution provider that offers compliance-focused remediation for these challenges will have a distinct competitive advantage. To lead this market, API security vendors need to provide automated AI-based solutions featuring continuous, unsupervised machine learning technology. In particular, these offerings need to consider each API's unique requirements in real time, without managing endless configurations and analyzing a vast amount of false alarms.

Product Family Attributes and Business Impact of L7 Defense

Founded in 2015 and based in Israel, L7 Defense is a cybersecurity company that specializes in API security solutions. The company's Ammune™ AI-based machine learning technology autonomously and accurately protects inline from a wide range of API cyberattacks.

L7 Defense's Philosophy of Success: A Holistic AI-based Approach

L7 Defense takes a holistic API security approach by integrating its solution on all platforms and by discovering and protecting application APIs individually and automatically. The company offers deployment on-premise, cloud (e.g., Microsoft Azure, Amazon, Google, and hybrid cloud), integrated as part of a firewall or embedded in machines. L7 Defense provides API-DDOS defense that secures APIs against advanced multi-vector applicative DDoS attacks, API-BOT defense that protects against all OWASP top 20 automated threats, and API-WAF defense that protects against all OWASP top 10 API and Application risks. This new generation approach is unique in that it defends each API with a separate set of AI machines (API-DDoS, API-WAF, and API-BOT) that in turn deploy a unique AI-based policy automatically for the API. Achieving this type of resolution is critical for business success as opposed to the traditional approach of creating generalized policies that tend to form massive false positive alerts, damaging customer experience. Every API is a critical component of multiple applications; therefore, precise attack detection and mitigation are no longer a 'nice to have'—it has become a necessity. Due to constantly evolving threats and the breadth of API usage, manually defining security parameters is no longer an option. The L7 Defense solution provides holistic AI-based API-resolution security that enterprises can depend on within 0.5 hours without time-consuming policy and rule definition.

It Takes Machines to Battle Machines: Ammune™ Delivers Unprecedented Sophistication

With threat actors becoming advanced by using AI-enhanced attack tools, a superior level of sophistication is necessary to defend against them. The technology behind L7 Defense's security solution is the Ammune™ API security platform. Ammune™ is an inline advanced AI-based

machine learning solution that actively protects APIs from the most sophisticated attack types while hunting down "zero day" attacks, all while creating no interference to regular traffic. Ammune™ discovers and protects each API separately and automatically. It iteratively builds negative and positive profiles of any API that spots and stops emerging threats that would otherwise go unnoticed. API requests are evaluated for potential risk and compared to the assessed risk of the actual response generated by the application servers. A separate AI-based policy is automatically discovered for each API.

Frost & Sullivan found that a supervised learning model fails to provide an effective solution, primarily because the nature of network traffic data is unstable and changes dynamically. However, Ammune™ possesses a one-of-a-kind unsupervised learning model based on the biological "innate immune model" that monitors and analyzes data in real-time, identifies and stops even subtle, stealthy attacks and effectively mitigating these without prior knowledge of the attack pattern parameters. In essence, just as our bodies have an immune system that can defend against never before experienced unknown threats and mitigate them effectively, Ammune™ uses this capability to secure APIs.

Compared to other solutions available in the industry, Ammune™ differentiates itself by its approach to analyzing traffic. A traditional network traffic analysis tool uses a top-down approach, analyzing from the traffic level to the application level. The major drawback of this method is the significant amount of noise generated by the traffic. Ammune™, on the other hand, takes a bottom-up analysis line of action. The company's solution analyzes every API as separate units, and then these units are aggregated to create a unified landscape of incoming network traffic.

L7 Defense Delivers Advanced Industry-defining Advantages

L7 Defense's solution brings a spectrum of advanced industry-defining capabilities, such as:

Accuracy: Ammune™ consistently delivers the highly coveted 99.99% detection rate and 0.001% false positive rate.

Scalability: The deployment of L7 Defense's Plug & Play solution is easy to use and highly scalable across multiple machines. Ammune™ also offers a superior feature, enabling the installation of the solution on virtual machines and adding the capability to logically or virtually distribute the traffic among them. From an architectural perspective, this is a huge advantage. The solution has an inherent elastic scaling mechanism that can function seamlessly and effortlessly from gigabytes up to several terabytes of data traffic. At a machine level, the solution builds mitigation and monitoring features separately. Thus, monitoring can be carried out within a machine (e.g., post data decryption), generate signatures, and send data to the mitigation machine using a virtual secure bridge. Notably, by saving time and effort to perform inspections on the traffic during transmission, the solution radically reduces costs.

Flexibility: Ammune™ performs unsupervised, continuous self-learning without any required rule or signature definition.

Inline: Ammune™ delivers extremely fast and accurate response to threats without affecting network traffic speeds.

Automatic Monitoring: Ammune™ auto-discovers every API and continuously monitors it. It also adapts the baseline to reduce operational cost and save significantly on human capital and labor.

Zero Trust: As any request is suspicious, Ammune™ trusts no user - regardless of authentication or authorization checks.

Ease of Use: The solution is 'plug & play' and deploys immediately.

Conclusion

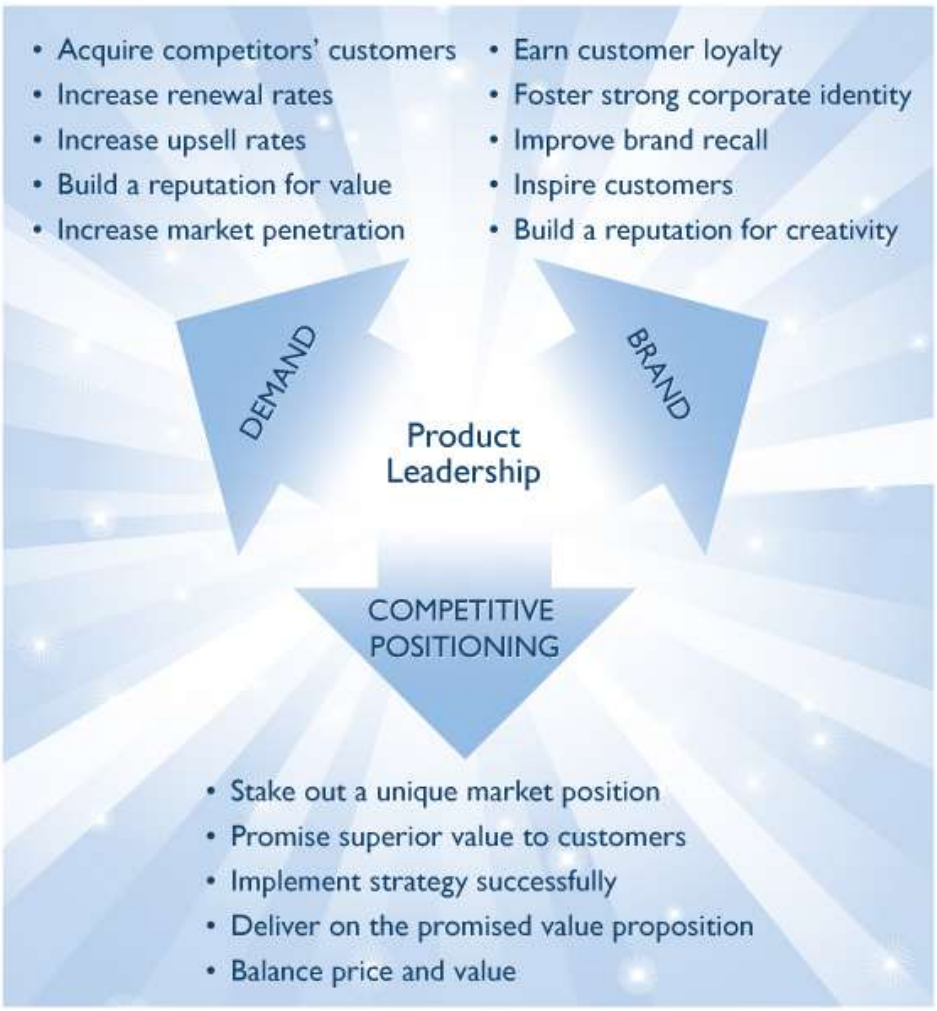
With digitization, more and more critical assets are getting connected to the Internet - intensifying the need to protect assets from cyberattacks. Due to the sheer volume and nature of application program interfaces (APIs) in use, organizations need a solution that automates API security. Most importantly, the Open Web Application Security Project (OWASP) recognizes API security as a primary concern and regards API breaches as the most common attack vector. However, some organizations attempt to locate and resolve application vulnerability manually - overlooking many coding mistakes that are inevitable due to human error. As cyberattacks become more sophisticated day by day, the average financial loss as a result of cyberattacks is alarmingly high and forces companies to adopt advanced cybersecurity solutions.

L7 Defense's autonomous inline AI-based machine learning API cybersecurity solution is disruptive to the other conventional solutions available in the current market. Frost & Sullivan identifies L7 Defense's algorithm as one of the company's standout features and recognizes that the solution has demonstrated reduced false positive and false negative rates in comparison to other competing products. Apart from its accuracy, other outstanding features of the Ammune™ technology include ease of deployment, flexibility, and scalability. With its continuous, unsupervised machine learning technology that considers each API's unique requirements in real time, without managing endless configurations and analyzing a vast amount of false alarms, L7 Defense automatic monitoring capability reduces costs dramatically.

With its unique approach to analyzing traffic, leveraged by its groundbreaking technology that delivers distinct competitive advantages, L7 Defense earns Frost & Sullivan's 2020 Global Product Leadership Award for its fully autonomous AI-based machine leaning API security solution.

Significance of Product Leadership

Ultimately, growth in any organization depends on customers purchasing from a company and then making the decision to return time and again. A comprehensive product line filled with high-quality, value-driven options is the key to building an engaged customer base. To achieve and maintain product excellence, an organization must strive to be best in class in three key areas: understanding demand, nurturing the brand, and differentiating from the competition.



Understanding Product Leadership

Demand forecasting, branding, and differentiating all play critical roles in finding growth opportunities for your product line. This three-fold focus, however, must be complemented by an equally rigorous focus on pursuing those opportunities to a best-in-class standard. Customer communication, customer feedback, pricing, and competitor actions must all be managed and monitored for ongoing success. If an organization can successfully parlay product excellence into positive business impact, market share will inevitably increase.

Key Benchmarking Criteria

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

Product Family Attributes

Criterion 1: Match to Needs
Criterion 2: Reliability and Quality
Criterion 3: Product/Service Value
Criterion 4: Positioning
Criterion 5: Design

Business Impact

Criterion 1: Financial Performance
Criterion 2: Customer Acquisition
Criterion 3: Operational Efficiency
Criterion 4: Growth Potential
Criterion 5: Human Capital

Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices

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

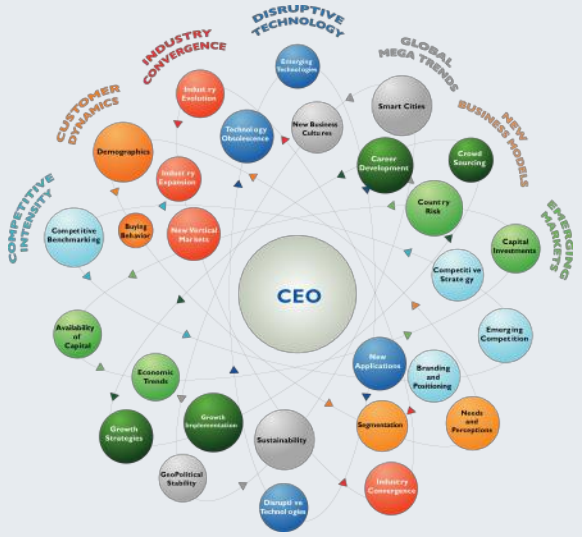
STEP		OBJECTIVE	KEY ACTIVITIES	OUTPUT
1	**Monitor, target, and screen**	Identify award recipient candidates from around the world	• Conduct in-depth industry research • Identify emerging industries • Scan multiple regions	Pipeline of candidates that potentially meet all best-practice criteria
2	**Perform 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 practices criteria • Rank all candidates	Matrix positioning of all candidates' performance relative to one another
3	**Invite thought leadership in best practices**	Perform in-depth examination of all candidates	• Confirm best practices criteria • Examine eligibility of all candidates • Identify any information gaps	Detailed profiles of all ranked candidates
4	**Initiate research director review**	Conduct an unbiased evaluation of all candidate profiles	• Brainstorm ranking options • Invite multiple perspectives on candidates' performance • Update candidate profiles	Final prioritization of all eligible candidates and companion best practices positioning paper
5	**Assemble panel of industry experts**	Present findings to an expert panel of industry thought leaders	• 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 practices award recipient	• Review analysis with panel • Build consensus • Select recipient	Decision on which company performs best against all best practices criteria
9	**Communicate recognition**	Inform award recipient of recognition	• Announce 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 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, resulting in errors of both omission and commission. Successful growth strategies are founded on a thorough understanding of market, technical, economic, financial, customer, best practices, and demographic analyses. The integration of these research disciplines into the 360-degree research methodology provides an evaluation platform for benchmarking industry participants and for identifying those performing at best-in-class levels.

360-DEGREE RESEARCH: SEEING ORDER IN THE CHAOS



About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, helps clients accelerate growth and achieve best-in-class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's growth team with disciplined research and best practices models to drive the generation, evaluation, and implementation of powerful growth strategies. Frost & Sullivan leverages nearly 60 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from 45 offices on 6 continents. To join Frost & Sullivan's Growth Partnership, visit http://www.frost.com.