FROST & SULLIVAN

2019 Global Automated Penetration-testing Customer Value Leadership Award

2019
BEST PRACTICES
AWARDS

Contents

Background and Company Performance

Industry Challenges

Cybersecurity professionals have to contend with a flood of cyber challenges, such as malware, denial of services, and ransomware, while making sure that a business's data is kept safe. This data is often the most valuable and sensitive asset of a company. However, businesses struggle to keep pace with the ever-evolving hacking models and techniques, giving many Chief Information Security Officers (CISOs) and their teams the ability to only react to breaches rather than proactively prevent hackers from accessing their systems and networks.

Frost & Sullivan estimates vulnerability management (VM) vendors sold $836.7 million in VM appliances and related services in 2017, representing an improvement of 20.3% over 2016. The revenue for 2017 was higher than anticipated. While the rate of growth began to decline in 2018, it will remain in the double digits through 2020 and reach a market value of $1.45 billion by 2022[1].

Faced with a multitude of cybersecurity challenges, CISOs rely on a variety of solutions from numerous providers, such as firewall and antivirus programs. Furthermore, to evaluate the resilience of their most valuable data assets, businesses occasionally enlist the help of a so-called red team, made up of individuals known as white hat hackers who use their collective skills to test the company's cybersecurity defenses in a process known as penetration testing (pen testing). This process does not interfere with the daily operation or harm the system.

While useful, there are a number of drawbacks associated with white hat hackers. First and foremost, they are expensive and invoke a lengthy undertaking, therefore limiting a comprehensive assessment to occurring only once or twice per year due to budgetary constraints. Moreover, due to the cost of such projects, CISOs might need to focus on a specific area of the network infrastructure, leaving some domains untouched and potentially at risk for intrusions. Even the most skillful white hat hackers are still vulnerable to human error, which can lead to overlooked security flaws during a manual pen test. As such, their final recommendations are not always accurate and comprehensive.

With the appearance of new technology, such as automated penetration testing, the drawbacks of VM tools have become more apparent. While VM can identify potential vulnerabilities, penetration testing takes the process one step further and actually establishes that a specific vulnerability is an entry point hackers can use to gain access to crucial information. By taking the additional step, pen testers are able to present their

[1] Vulnerability Management (VM) Market Analysis, Global, Forecast to 2022 (Jul. 2018)

clients with a shorter and more workable list of de facto exploitable vulnerabilities within their environment.

Frost & Sullivan believes that these challenges have been address by Pcysys, which has introduced a cost-effective automated penetration testing solution that frees CISOs of the budgetary and technical restraints of the current pen testing techniques.

Customer Impact and Business Impact

Established in 2015, Israel-based Pcysys—an acronym for Proactive Cyber Systems—channels the extensive cybersecurity experience of its founding team to solve the concerns associated with manual pen testing. In doing so, it is able to give corporations the ability to continually assess and improve their cybersecurity resilience. To achieve this goal, Pcysys developed an automated penetration testing platform called PenTera™ that addresses issues linked with manual pen-testing—namely, its excessive costs and labor intensity.

Consistent, Continuous, and Current Penetration Testing

The main problem with manual penetration testing is the human factor; no matter the level of expertise or ethical dispositions of white hat hackers, there is only so much they could do during a day. With the power of algorithmic pen testing, the PenTera platform can supersede a human pen tester's capacity multiple times. It can validate large computer networks simultaneously and repeatedly review all pen testing stages: discovery, vulnerability analysis, and exploitation. The enhanced capabilities of an automated system give CISOs the option of conducting specialized, targeted scenarios that focus on specific network segments and applications as well as validating previously discovered and mitigated vulnerabilities.

Furthermore, Pcysys's proprietary algorithm-based pen testing solution is consistent because it does not depend on a manual pen tester's mood or precision, eliminating human error and increasing productivity.

The consistency and cost efficiency of Pcysys's pen tests enable a CISO to run a test as often as deemed necessary. More importantly, this allows the CISO to view results over time because the pen test is undertaken in the same manner each time. For example, a CISO can set a security posture target for their company and track those results over time through Pcysys's scoring feature. A score is a powerful tool for CISOs when calculating budget requirements, and it allows the executive board that allocates the budget to see the returns of its cybersecurity investments.

Today, clients internally process penetration test results. However, Pcysys envisions a future where it standardizes penetration testing—outlining what needs to be validated and the testing frequency—with tracked and comparable results over time. This will help establish guidelines regarding procedures, industry sectors, and validation frequencies for

the currently unstandardized pen testing industry. It will also establish index tracking for the test scores of various industries, which will enable companies to benchmark results in comparison to similar businesses.

Agentless and Seamless

The PenTera solution is agentless, installed locally, and operated by the CISO's own team. The proof-of-concept trial takes typically 24 hours to conduct, and there is no need for the company to install additional software before the trial begins. Once completed, the results are displayed in an easy-to-view graphical presentation with an auto-generated penetration testing report. The display illuminates the results and outlines how it was achieved; thereby, giving the CISO a comprehensive view of the company's network infrastructure, potential security loopholes, and recommendations on how to improve its cybersecurity score. The proposals are not limited to software upgrades, commonly known as patching, but also include firewall and network configuration and access privilege suggestions, as these determine who in the organization has the right to make changes to the network infrastructure.

The ease, speed, and low cost at which PenTera operates means that an organization's internal cybersecurity staff can re-run a pen test after making changes to the business's network infrastructure. This creates a standardized quality assurance cycle-type process for cybersecurity management. This is a concept that was previously non-existent due to the cost of manual pen testing.

In addition to being fully automated, PenTera enables businesses to comply with the European Union's (EU) powerful General Data Protection Regulation (GDPR). The GDPR stipulates how companies doing business within the EU store and protect personal information. Fines for non-compliance can amount to 4% of an organization's annual revenue.

Industry Agnostic Technology

Pcysys's current client base includes financial institutions, government organizations, retailers, and healthcare providers in the United States, Canada, the United Kingdom, Italy, Switzerland, Portugal, Israel, and more. Because Pcysys's technology is industry-agnostic and cybersecurity is a major concern for any modern business, potential clients can be found in any vertical that must protect consumer data, such as medical records or credit card information. Additionally, the client will likely be able to better utilize their IT security team, which is often understaffed.

Conclusion

Businesses struggle to keep pace with the ever-evolving hacking models and techniques, leaving many CISOs and their teams merely reacting to breaches rather than proactively preventing hackers from accessing their systems and networks, exhausting information technology professionals and reducing productivity. Penetration testing allows businesses to test systems and networks without harming daily operations and threats of nefarious hacking, but as a manual process, it is typically expensive, time consuming, and not comprehensive. Pcysys's automated pen testing platform, PenTera, provides CISOs and cybersecurity professionals with unprecedented insights from repeatable and cost-effective pen tests. PenTera's consistency eliminates the uncertainty the human pen test, resulting in tracked and comparable information that is gathered over time and can guide businesses as they strive to reach their cybersecurity goals.

For its strong overall performance, Pcysys earns Frost & Sullivan's 2019 Global Customer Value Leadership Award in the Automated Penetration Testing market for its PenTera platform.

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
Criterion 2: Customer Purchase Experience
Criterion 3: Customer Ownership Experience
Criterion 4: Customer Service Experience
Criterion 5: Brand Equity

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 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	• 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 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.