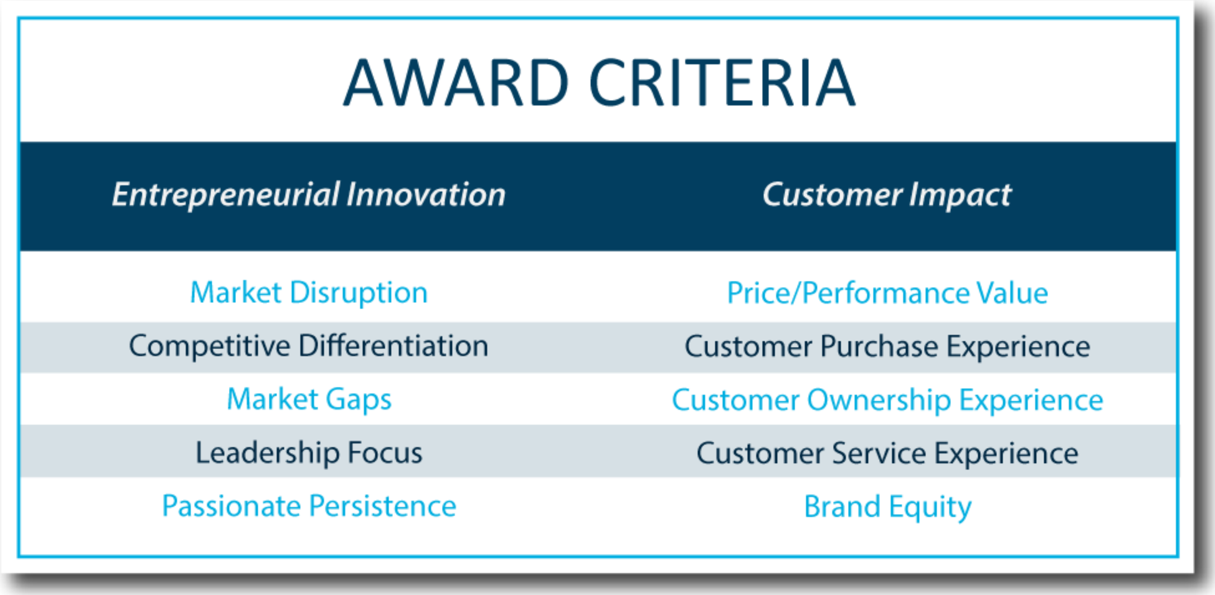
FROST & SULLIVAN

SECPOD RECEIVES THE 2023 ENTREPRENEURIAL COMPANY OF THE YEAR AWARD

Identified as best in class in the global vulnerability management industry

Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each award category before determining the final award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. SecPod excels in many of the criteria in the global vulnerability management market.



AWARD CRITERIA

Entrepreneurial Innovation	*Customer Impact*
Market Disruption	Price/Performance Value
Competitive Differentiation	Customer Purchase Experience
Market Gaps	Customer Ownership Experience
Leadership Focus	Customer Service Experience
Passionate Persistence	Brand Equity

Need for a Unified VM Tool

“Prevention is better than cure” – Desiderius Erasmus

The relevance of this famous saying in cybersecurity cannot be emphasized enough. However, according to the 2023 Frost & Sullivan Voice of the Enterprise Security Customer Survey, 30% of organizations are not confident that their security infrastructure can successfully prevent cyber-attacks. Small and medium enterprises are even less optimistic about their ability to prevent cyber-attacks, with 36% of organizations citing concern. Vulnerability Management (VM) tools can play a significant role in preventing cyber-attacks, but only 51% of organizations use them today, as per the aforementioned survey results.

New vulnerabilities are created at an alarming pace. In 2022, the US National Vulnerability Database recorded a 24.6% YoY increase in the number of vulnerabilities reported. In comparison, the rise in the reported vulnerabilities was just 9.8% in 2021 and 6.1% in 2020. Heightened awareness regarding the significance of vulnerabilities in data breaches, mature bug bounty programs, and the growing adoption of digital products and services are among the reasons for accelerated vulnerability growth in 2022.

Although new vulnerabilities emerge daily, most organizations perform a vulnerability scan just once a month, a quarter, or sometimes a year. In addition, VM processes in organizations often take a siloed approach. A typical organization invests in three to five different VM tools: one for identifying vulnerabilities, another for detecting threats, and a third for patch management. As a result, VM processes have become more complicated, and security teams seldom realize the value of VM implementation.

Finally, vulnerability scans take a significant amount of time to complete. Security analysts must parse through a 3,000-page post-scan report to identify risk factors. With limited contextual visibility and bandwidth, IT and security teams struggle to apply remediation patches.

Very few VM tools address all the use cases to implement end-to-end VM within an organization. A unified VM tool for vulnerability discovery, prioritization, and remediation is the need of the hour. Further, VM tools must harness automation to enable continuous assessment and reduce the workload of overwhelmed security teams.

The Evolution of SecPod

SecPod, founded in 2008 with offices in Bangalore and the US, has reinvented vulnerability management for fifteen years. SecPod focuses on preventing an attack by implementing cyber hygiene measures so that cyber adversaries find it more difficult to exploit the weaknesses within the organization.

> *"With its security intelligence repository as the base, SecPod started building its VM platform. After 7 to 8 years of intense product development, the company launched its full-fledged platform SanerNow in 2018. Today, SecPod has customers from about 25 countries covering all continents."*
>
> ***- Swetha Krishnamoorthi***
> ***Senior Industry Analyst,***
> ***Cybersecurity, Frost & Sullivan***

The company started as a contributor to some of the most important open-source projects in the vulnerability space, such as Nessus and OpenVAS. OpenVAS used the source code of Nessus as a foundation and developed capabilities on top of it.

SecPod helped to clean up the OpenVAS code into an executable project, which remains open source today. Over time, the company extended its services to other open-source projects in the cyber security space. Eventually, SecPod assisted prominent cybersecurity vendors in their security research and product engineering projects.

The company also contributed to developing the Security Control Automation Protocol (SCAP), driven by the US Department of Homeland Security. In 2010 and onwards, the company won several top contributor awards for its contributions to SCAP. These projects helped SecPod build a security intelligence database that it could license to other cybersecurity vendors.

With its security intelligence repository as a foundation, SecPod started building its VM platform. After 7 to 8 years of intense product development, the company launched its full-fledged platform, SanerNow, in 2018. Today, SecPod has customers across 25 countries and covering all continents. SecPod has consistently recorded double-digit average YoY growth rate of 35% since 2019.

The company has a loyal customer base that believes in the vision and value that SanerNow is communicating. SecPod has customers across a broad array of verticals, spanning financial services and manufacturing to IT services and healthcare.

SanerNow – A Comprehensive VM Tool

Many cyber-attacks happen because of unknown IT assets, unused computing, unwanted services and applications, and misconfigured devices. These are posture-specific issues that cyber adversaries can easily exploit to gain access to infrastructure.

SecPod's SanerNow platform provides continuous scanning to discover vulnerabilities in real-time. The normalize layer in the SanerNow platform gathers telemetry from every device and collectively applies statistical analysis and machine learning algorithms to find outliers. The security team can further investigate the device and determine if the deviation is an error. The normalize layer works even before discovering vulnerabilities because it is vital to standardize the IT infrastructure. Organizations can significantly reduce their risk exposures by using this solution.

After the IT infrastructure's normalization, SanerNow proceeds to vulnerability discovery with its detection layer. The detection layer uncovers multiple types of vulnerabilities, including software vulnerabilities, misconfigurations, missing security patches, and other security risk factors. After discovering the vulnerabilities, SanerNow prioritizes them based on attack potential.

> *"SanerNow's patch management capabilities stand out from the competition since it can patch all the discovered vulnerabilities and perform other system-hardening actions. Even if no direct remediation is available, SanerNow applies security controls that provide workarounds for the vulnerabilities."*
>
> ***- Swetha Krishnamoorthi***
> ***Senior Industry Analyst, Cybersecurity, Frost & Sullivan***

The remediation layer follows the detection and prioritizations. SanerNow automatically feeds the detected vulnerabilities into the remediation engine and provides mitigation options. Applying software patches might fix a significant percentage of these vulnerabilities. Similarly, SanerNow can identify misconfigurations, roll out required changes, and apply security controls that extend beyond patches. SanerNow's patch management capabilities stand out from the competition since it can patch all the discovered vulnerabilities and perform other system-hardening actions. Even if no direct remediation is available, SanerNow applies security controls that provide workarounds for the vulnerabilities.

Finally, SanerNow's reporting layer sheds light on remediation actions taken by security analysts and their impact on the organization's overall security posture.

Thus, SecPod offers an advanced VM platform that unifies and provides end-to-end coverage of all VM processes in an integrated manner.

Customer-focused Value Proposition

SecPod has seven products that come together to form a unified proposition.

1. **SanerNow AE:** Asset exposure module to give continuous visibility into the IT environment.
2. **SanerNow CPAM:** Continuous Posture Anomaly Management to uncover outliers and anomalies and mitigate them.
3. **SanerNow VM:** Vulnerability Management to detect software vulnerabilities and prioritize them.
4. **SanerNow CM:** Compliance management to detect misconfigurations and mitigate them.
5. **SanerNow RP**: Prioritize risk of vulnerabilities based on CISA's SSVC framework.
6. **SanerNow PM:** Patch Management to apply patches to risk exposures.

7. **SanerNow EM:** Endpoint management to apply security controls beyond patching to harden the devices.

The company allows its customers the flexibility to buy the entire platform or subscribe to individual modules. Thus, while customers often start with one module, they eventually expand the scope of usage to multiple modules, resulting in upsell opportunities for SecPod.

SanerNow is compatible with different endpoints, such as workstations, servers, network devices, and IoT. The platform is also compatible with operating systems such as Windows, Linux, and Mac. Security analysts can manage end-to-end VM from a single console and with a single agent. The platform is available natively on the cloud but works with on-premises resources.

SecPod primarily targets the medium-size to large enterprise segment, where security teams seek affordable, easy-to-deploy, and easy-to-use VM platforms. The company follows an annual subscription-based licensing model. Costs depend on the number of devices and modules. On average, organizations can purchase SecPod's end-to-end VM platform for $50 per device per year.

SanerNow offers rapid scanning, which enables security analysts to automate vulnerability discovery into a daily routine. SecPod leverages its experience as a security intelligence provider to deliver accurate scan results. Since some large cyber security vendors use the security intelligence repository, it is tested extensively. As a result, SecPod can provide one of the highest accuracy rates and lowest false positive rates in the VM market. Moreover, SanerNow can patch all of the discovered vulnerabilities and harden the systems with security controls beyond patching

The company continues to make significant innovations in the VM space. SecPod invested up to 70% of its revenue in R&D in 2022. In 2021, SecPod launched a network-based vulnerability scanner; in 2023, the company launched a posture anomaly product, an industry-first innovation. Also, in 2023, SecPod launched industry's first CISA SSVC based Risk Prioritization product.

Conclusion

The growing volume of vulnerabilities and shrinking bandwidth of security teams demand a unified and automated approach to VM. Multiple tools for the different stages of VM create complexity and add to already chaotic security operations. Moreover, such an approach creates siloes and restricts contextual visibility into risk.

SecPod's SanerNow seamlessly incorporates automation into the different layers of the platform. Security teams can run automated scans daily, apply rules, and schedule patches. The normalized layer is another example of its recent innovation, which uncovers hidden risk exposures. Additionally, SecPod has integrated remediation that goes beyond software patching to mitigate vulnerabilities of different kinds holistically.

SecPod's comprehensive end-to-end VM approach and continuous innovation have helped the company gain a loyal customer base and record sustained revenue growth. With its strong overall performance, SecPod earns Frost & Sullivan's 2023 Global Entrepreneurial Company of the Year Award in the vulnerability management market.

What You Need to Know about the Entrepreneurial Company of the Year Recognition

Frost & Sullivan's Entrepreneurial Company of the Year Award recognizes the best up-and-coming, potentially disruptive market participant.

Best Practices Award Analysis

For the Entrepreneurial Company of the Year Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Entrepreneurial Innovation

Market Disruption: Innovative new solutions have a genuine potential to disrupt the market, render current solutions obsolete, and shake up competition

Competitive Differentiation: Strong competitive market differentiators created through a deep understanding of current and emerging competition

Market Gaps: Solution satisfies the needs and opportunities that exist between customers' desired outcomes and their current market solutions

Leadership Focus: Company focuses on building a leadership position in core markets and on creating stiff barriers to entry for new competitors

Passionate Persistence: Tenacity enables the pursuit and achievement of seemingly insurmountable industry obstacles

Customer Impact

Price/Performance Value: Products or services provide the best value for the price compared to similar market offerings

Customer Purchase Experience: Quality of the purchase experience assures customers that they are buying the optimal solution for addressing their unique needs and constraints

Customer Ownership Experience: Customers proudly own the company's product or service and have a positive experience throughout the life of the product or service

Customer Service Experience: Customer service is accessible, fast, stress-free, and high quality

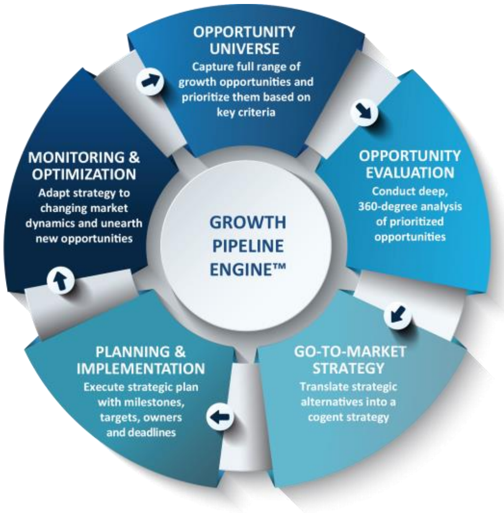
Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

The Growth Pipeline Engine™

Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.
Learn more.



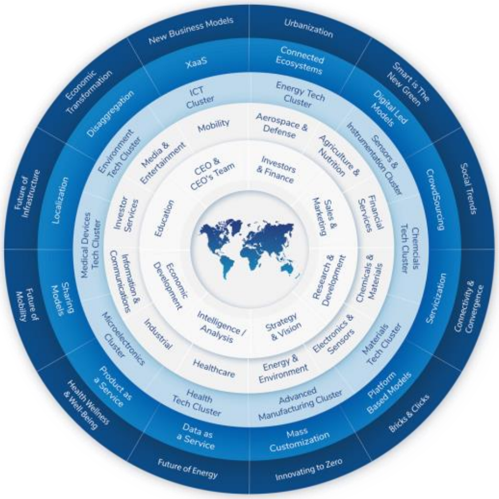
OPPORTUNITY UNIVERSE
Capture full range of growth opportunities and prioritize them based on key criteria
OPPORTUNITY EVALUATION
Conduct deep, 360-degree analysis of prioritized opportunities
GO-TO-MARKET STRATEGY
Translate strategic alternatives into a cogent strategy
PLANNING & IMPLEMENTATION
Execute strategic plan with milestones, targets, owners and deadlines
MONITORING & OPTIMIZATION
Adapt strategy to changing market dynamics and unearth new opportunities
GROWTH PIPELINE ENGINE™

Key Impacts:

- **Growth Pipeline:** *Continuous Flow of Growth Opportunities*
- **Growth Strategies:** *Proven Best Practices*
- **Innovation Culture:** *Optimized Customer Experience*
- **ROI & Margin:** *Implementation Excellence*
- **Transformational Growth:** *Industry Leadership*

The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.



Analytical Perspectives:

- Mega Trend (MT)
- Business Model (BM)
- Technology (TE)
- Industries (IN)
- Customer (CU)
- Geographies (GE)