

# RUNECAST RECEIVES THE 2023 NEW PRODUCT INNOVATION AWARD

---

*Identified as best in class in the European cloud-native  
application protection platform 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. Runecast excels in many of the criteria in the cloud-native application protection platform (CNAPP) space.

AWARD CRITERIA	
<i>New Product Attributes</i>	<i>Customer Impact</i>
Match to Needs	Price/Performance Value
Reliability	Customer Purchase Experience
Quality	Customer Ownership Experience
Positioning	Customer Service Experience
Design	Brand Equity

### Industry Challenges

Cloud computing is the new norm in the business landscape, offering a range of cloud models and services that simplify IT infrastructure and drive digital transformation. However, cloud migration entails a host of new attack vectors and cyber risks. The cloud environment’s complexity expands the attack surface, leaving organizations vulnerable to insecure cloud connections, misconfigurations, identity theft, unauthorized access, and attacks targeting cloud servers, workloads, applications, code, and APIs. Zero-day vulnerabilities, exploits, and sophisticated malware amplify the risks.

Open-cloud environments present lucrative opportunities for attackers to exploit traditional techniques like phishing, business email compromise, and zero-day vulnerabilities. Cloud servers, container images, and serverless applications frequently become the targets of such attacks, impacting industries like finance, healthcare, education, retail, technology, manufacturing, energy, real estate, and transportation.

Moreover, adopting modern cloud-native technologies—containers, Kubernetes, and serverless functions—introduces additional security challenges due to their inherent complexity and vulnerabilities. Each of these technologies can serve as a potential attack vector, increasing the

cloud environment's susceptibility to infiltration and compromise. While using open-source software in the development process offers benefits like source code access, cost savings, flexibility, and community support, it also introduces unique risks, such as container image vulnerabilities, code injection, credential loss, and compliance issues.

Finally, cloud adoption in Europe is growing in maturity, but its security practices and requirements are less mature, as on-prem and hybrid environments are more common, which

*“Runecast’s on-prem CNAPP runs in an entirely air-gapped environment with offline updates, which is a highly attractive proposition and an answer for companies operating in highly regulated industries, such as government, defense, banking, financial services and insurance, healthcare, and service providers. This is in contrast to its competitors who mainly offer CNAPP solutions with a SaaS-based deployment (particularly those without physical computing facilities in Europe) which makes it difficult for customers to comply with regulations like GDPR.”*

**- Anh Tien Vu**  
Industry Principal, Global Cybersecurity Practice

leads to a greater focus on vulnerability management. This necessitates continuous scanning of vulnerabilities and visibility into a software bill of materials (SBOM) to better understand the associated risks. European organizations increasingly pay attention to container security and shift-left practices, with a heavier emphasis on on-prem solutions due to the stringent compliance requirements. Most organizations

are aware of these solutions and practices in the case of cloud security frameworks and regulations. However, these are difficult to follow for both organizations and technology vendors that provide software-as-a-service (SaaS) services. As a result, enterprises need a more flexible approach to deal with said requirements by working with tech vendors and offering customized rules and policies, while tech vendors must strengthen their efforts to set up their physical presence or partner with local partners and provide services with custom rules and policies for regional customers.

### **Match to Needs**

Runecast provides organizations with cloud security solutions, including security capabilities to help organizations detect and respond to cloud security risks—vulnerabilities, compliance, runtime protection across different environments, including on-prem, cloud, or containers. Through AI-powered automation capabilities, Runecast helps organizations shift from a reactive approach to a proactive and far less time-consuming approach to handling cloud security risks. This reduces operational overhead by automating the discovery and prioritization of vulnerabilities, misconfigurations, hardware incompatibility, and non-compliance to maintain service availability and ensure compliance.

Runecast’s on-prem CNAPP runs in an entirely air-gapped environment with offline updates, which is a highly attractive proposition and an answer for companies operating in highly



regulated industries, such as government, defense, banking, financial services, and insurance (BFSI), healthcare, and service providers. This is in contrast to its competitors who mainly offer CNAPP solutions with a SaaS-based deployment (particularly those without physical computing facilities in Europe), which makes it difficult for customers to comply with regulations like GDPR. Since it is not limited to the on-prem CNAPP model, Runecast is able to offer cloud-first companies SaaS, making its solution extremely flexible. Digital companies can effectively manage security risks in the cloud environment thanks to Runecast's new product enhancements: a Runecast SaaS version, agentless vulnerability scanning for Amazon Elastic Compute Cloud (AWS EC2) Linux instances, and secure agentless scanning for VMware workloads.

More importantly, Runecast enables continuous compliance and risk-based vulnerability management through built-in granular historical comparison data, which can be a key selling point and differentiator that competitors do not offer. Besides compliance, this also enables significant efficiency and increased uptime for highly regulated verticals with mission-critical IT infrastructures. Runecast complies with the recent updates in automated compliance audits for TISAX (German automotive industry regulation) and DORA (European Digital Operational Resilience Act), which makes it one of the few vendors supporting the most industry/regulatory standards—a crucial requirement for companies in Europe.

### ***Positioning and Price/Performance Value***

Customers consider that Runecast's CNAPP solution is unique in the regional market thanks to its combination of innovative features and an extensive list of regulatory compliance profiles across hybrid environments. It addresses organizations' critical need to maintain compliance in complex IT landscapes, particularly in Europe's heavily regulated market. Additionally, Runecast offers ESXi specific configuration drift management as well as general best practices that allow IT teams to identify potential issues, enabling them to fix them before they can turn into service outages. This saves time and resources and minimizes potential disruptions during operation. Furthermore, Runecast's support for air-gapped environments caters to highly sensitive sectors like defense and intelligence agencies—a testament to the platform's adaptability to diverse customer needs.

While Runecast operates in a competitive market, the ability to facilitate customer cost savings is a solid differentiator, as companies are always under pressure for cost-cutting and optimizing their investment. In contrast, competitors often require hefty investment and spending. Runecast's cost-conscious solution helps IT procurement teams reduce expenses by consolidating tools, eliminating the need for overlapping solutions. With its ability to provide comprehensive insights across various domains, Runecast has maintained good customer retention and increased cross-sell and upsell revenue over the years.

Runecast's reputation for excellence is reflected in very positive public reviews. Customers frequently express satisfaction with the platform's performance and reliability, highlighting Runecast's commitment to listening closely to user feedback. For example, many customers

*"Runecast simplifies the customer purchase process, rendering it easy and accessible to customers of all sizes with its rapid onboarding process that includes running a trial, deploying, and running a first scan. This allows IT professionals to transition from the initial registration to obtaining their first scan results within approximately 15 minutes. Thanks to the Runecast platform's simplicity, the need for time-consuming and complex training disappears, making it a practical and efficient solution."*

**- Anh Tien Vu**  
**Industry Principal, Global Cybersecurity Practice**

review that Runecast offers a unified dashboard for granular visibility and transparency into the hybrid cloud environments, unique value with its K8s correlation and compliance checks, helping them save hundreds of hours on security compliance and reduce meantime to detect and remediation, which eventually help these organizations reduce overall IT and security operation costs.

Many customers claim that Runecast is the only solution for effective proactive issue prevention in mission-critical VMware cloud infrastructure, and no other tool in the

market can offer the same functionality and features as Runecast. This positive feedback further reinforces its positive positioning and high value in the market as a reliable and effective solution provider.

### **Customer Purchase, Ownership, and Service Experience**

Runecast simplifies the customer purchase process, rendering it easy and accessible to customers of all sizes with its rapid onboarding process that includes running a trial, deploying, and running a first scan. This allows IT professionals to transition from the initial registration to obtaining their first scan results within approximately 15 minutes. Thanks to the Runecast platform's simplicity, the need for time-consuming and complex training disappears, making it a practical and efficient solution.

In addition, with its "built by admins, for admins" approach, Runecast commits to helping IT professionals deal with daily challenges. It listens to their needs and makes resonating decisions when introducing new features or refining existing products, fully aligning with these professionals' needs. This enables Runecast to generate trust and loyalty in its customers.

More importantly, the company has made strides in revamping its UI to enhance user interaction and make its new features and products rapidly informed and accessible to customers. For example, the recent update of the UI that reduces load times for critical functionalities has significantly elevated user productivity, fostering loyalty and frequent platform engagement. The company's commitment to accessibility and transparent data presentation is another selling

point and differentiator due to the concerns over data privacy and transparency in Europe, which enables it to build trust and confidence among businesses.

Runecast provides a flexible and transparent pricing model for its customers, making it easy for them to decide on a purchase. With around 300 customers, Runecast can maintain a close and personal touch, offering an easy communication and close feedback mechanism, which its customers highly value, as the engagement helps identify and address any potential issues in an effective and fast manner.

Many customer testimonials underscore the value for money and the importance of Runecast's technology and support in their daily operations when managing security risks in the cloud environment. They see Runecast as the only solution providing comprehensive protection coverage and meeting their needs with a single tool, thus decreasing complexity and overheads. Runecast's platform provides exactly what they need with a simple and clear dashboard, enabling them to focus on what matters the most. This helps them save time and effort in daily operations—particularly in managing their security posture in the hybrid VMware, Cloud and container environment.

## Conclusion

---

Runecast's ability to provide a flexible deployment of its CNAPP in a fully air-gapped environment is one of its greatest selling points and differentiators in the region, as it helps companies in highly regulated industries deal with compliance requirements in an effective manner. With its strong focus on sustainable growth and commitment to user experience, Runecast maintains lean structures, remaining "small enough" to provide excellent customer service and support, enabling customers to deal with their challenges in cloud security operations in the most cost-effective manner. This allows the company to maintain solid growth over the year and, more importantly, the deepest customer confidence in the region.

For its strong overall performance, Runecast is recognized with Frost & Sullivan's 2023 European New Product Innovation Award in the CNAPP industry.

## What You Need to Know about the New Product Innovation Recognition

---

Frost & Sullivan's New Product Innovation Award recognizes the company that offers a new product or solution that uniquely addresses key customer challenges.

### Best Practices Award Analysis

For the New Product Innovation Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

#### *New Product Attributes*

**Match to Needs:** Customer needs directly influence and inspire product design and positioning.

**Reliability:** Product consistently meets or exceeds customer performance expectations

**Quality:** Product offers best-in-class quality with a full complement of features and functionality

**Positioning:** Product serves a unique, unmet need that competitors cannot easily replicate

**Design:** Product features an innovative design that enhances both visual appeal and ease of use

#### *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.](#)

### 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)

