FROST & SULLIVAN

2024 COMPANY OF THE YEAR

IN THE GLOBAL CONTAINER/KUBERNETES SECURITY INDUSTRY

sysdig

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. Sysdig excels in many of the criteria in the container/Kubernetes security space.

Industry Challenges

According to Frost & Sullivan's Cloud User Survey 2023, 31.7% of the organizations surveyed consider the cloud to be the most critical part of their digital transformation journey. This conviction has positioned the cloud as the top technology investment for these organizations over the next 12 months. The high level of trust in cloud adoption is rooted in the belief that it can enhance operational efficiency and customer experience, enabling organizations to achieve sustainable growth in the modern business landscape.

The widespread adoption of cloud technology by organizations worldwide has resulted in a major shift in how they build, operate, and manage both back-end infrastructure and front-end, customer-facing applications. As a result, many organizations have turned to cloud-native application development tools, such as infrastructure-as-code (IaC), serverless computing, continuous integration (CI)/continuous deployment (CD) platforms, and containers. However, the rising adoption of cloud and cloud-native application development tools, including containers and Kubernetes (K8s), has introduced multiple security challenges that organizations must address, particularly in terms of container and K8s security. Containerized environments are complex due to the dynamic nature of containers and the microservices architecture running across distributed clusters, which have heightened complexity levels and expanded the attack surface area for security teams to manage.

As the threat surface area widens, traditional security solutions are no longer effective because they are not designed to detect and mitigate attacks specifically targeting containerized applications and K8s clusters. Organizations now require solutions that provide comprehensive protection tailored to the unique characteristics of containers and containerized environments. This has led to a growing global demand for container and K8s security solutions specifically designed to tackle these challenges. Standard container/K8s security solutions offer several capabilities, including image and registry scanning, dependency checks, compliance verification, real-time monitoring for anomalous behaviors, unauthorized access prevention, and detection and mitigation of suspicious activities during runtime.

Addressing Unmet Needs

Founded in 2013, Sysdig is a San Francisco-based cybersecurity company that provides solutions to help organizations ensure the security and reliability of their containers, K8s, and cloud environments. The company is known for its cloud-native application protection (CNAPP) platform, Sysdig Secure, which provides end-to-end protection across the software lifecycle. Integrated into Sysdig Secure, its container/K8s security solution includes capabilities such as scanning vulnerabilities, secrets, and misconfigurations in images, CI/CD pipelines, registries, and hosts. Sysdig Secure also flags new common vulnerabilities and exposures (CVEs) and automatically prioritizes them using runtime contexts. Additionally, the platform utilizes out-of-the-box managed policies for quick detection and response to malicious activities within containers and K8s, enforces compliance controls using Open Policy Agent (OPA), unifies all Sysdig security-related features of an individual object, and facilitates incident response.

Container and K8s security solutions providers often specialize in specific areas such as container image scanning, network security, or runtime protection, excelling in one or two of these domains. Sysdig has successfully differentiated itself from competitors with an integrated approach that combines security and monitoring for cloud, container, and K8s environments within a single platform. While other vendors offer similar capabilities on their platforms, Sysdig stands out due to its deep integration with K8s and Prometheus, a well-known open-source monitoring and alerting tool. This integration provides customers with deep visibility into their infrastructure, services, and applications at an enterprise scale. This critical feature meets the needs of customers seeking container and K8s security solutions that offer comprehensive visibility across their containerized environments.

> *"Frost & Sullivan recognizes Sysdig for providing a comprehensive platform that helps organizations secure their entire application development and delivery process, from build to runtime. Sysdig's container and K8s security solutions offer capabilities that instill confidence in its customers, demonstrating the company's exceptional proficiency in addressing their needs and ensuring continuous protection for their containers and containerized environments."*
>
> ***- Daphne Dwiputriane, Research Associate***

Frost & Sullivan recognizes Sysdig for providing a comprehensive platform that helps organizations secure their entire application development and delivery process, from build to runtime. Sysdig's container and K8s security solutions offer capabilities that instill confidence in its customers, demonstrating the company's exceptional proficiency in addressing their needs and ensuring continuous protection for their containers and containerized environments.

Visionary Scenarios through Megatrends

Frost & Sullivan has identified cybersecurity as a megatrend that will exponentially grow in the next five years, transforming how organizations invest in information technology (IT) infrastructure, cloud-native applications, and security operations. As the use of containers continues to expand, investment in container/K8s security solutions is also expected to grow, particularly in solutions that provide comprehensive runtime protection.

The increasing demand for container and K8s security solutions with comprehensive runtime protection capability stems from the wider attack surface area that organizations encounter due container and K8s utilization. Runtime protection provides an additional layer of security by detecting and mitigating threats in real time within the production environment. Most vendors have incorporated runtime protection capabilities into their container/K8s security solutions, achieving varying levels of market success. Sysdig, however, has distinguished itself by using Falco. This open-source runtime security tool developed by Sysdig identifies and responds to suspicious behavior in containers and containerized environments. While other vendors also offer robust runtime protection capabilities, Falco is widely regarded as the industry-standard runtime security tool, particularly after its adoption into the Cloud Native Computing Foundation (CNCF) as an incubation project in 2018. As the first runtime security project accepted into the CNCF sandbox, Falco gained additional credibility and visibility among the open-source community, setting Sysdig apart in this area. As an open-source tool, Falco benefits from continuous contributions and improvements from the developer community, enabling it to quickly adapt to the latest security challenges.

Falco is not the only innovative product developed by Sysdig. Founded as an open-source project, the company has also created Sysdig OSS, the cloud-native standard tool for digital forensics and incident response (DFIR) and troubleshooting. Leveraging its experience in developing open-source projects, Sysdig has built its container and K8s security solution—integrated within its CNAPP platform—on an open-source stack that includes Falco and Sysdig OSS. This approach has established the platform as the open standard for runtime threat detection and response. Sysdig's dedication to creating and maintaining industry-standard open-source projects highlight its commitment to innovation, enabling it to successfully expand its customer base and become a preferred option for organizations globally, particularly those utilizing open-source tools in their environments.

Leadership Focus

Sysdig employs various strategies to solidify its leadership in the container and K8s security industry. The company showcases its commitment to its open-source roots by leveraging Falco and Sysdig OSS in its container/K8s security solutions. It actively maintains other notable open-source tools, such as Prometheus, a leading open-source monitoring solution, and Promcast, an open-source catalog for enterprise-level Prometheus monitoring. Additionally, the company is one of the most notable supporters of Wireshark, a highly regarded network protocol analyzer. Through its commitment to open source, Sysdig has successfully fostered an active and engaging community that continuously contributes to improving and validating the effectiveness of its solutions. By actively engaging the open-source

community for feedback, Sysdig enhances its container and K8s security solutions to effectively address the latest security challenges.

To maintain its leadership position in the container security space, Sysdig has made significant investments in its threat research team. These ongoing efforts have enabled the company to identify new threats and discover unknown vulnerabilities, particularly those targeting cloud and container environments. As a result, Sysdig can establish detection rules and update its machine learning models, empowering its customers to protect themselves against new threats.

Financial Performance

Based on Frost & Sullivan's estimates, Sysdig recorded a strong year-on-year (Y-o-Y) growth of 50.9% in the global container/K8s security space in 2023. The company has consistently maintained stable growth momentum over the years, solidifying its position as one of the leaders in the global container security industry. Additionally, Sysdig's container/K8s security solution has been widely adopted across various industries and organization of different sizes. This underscores Sysdig's ability to offer a versatile solution that effectively addresses the security challenges encountered in containers and containerized environments across diverse sectors and company scales. A recent testimonial from a customer highlighted that Sysdig's solution significantly simplified their operations following the migration of their entire technology stack to run as microservices on K8s. With Sysdig's container/K8s security solution, the customer now benefits from a centralized dashboard that enhances their understanding of activities within their environment and offers quick insights to address security issues before production.

> *"Falco is not the only innovative product developed by Sysdig. Founded as an open-source project, the company has also created Sysdig OSS, the cloud-native standard tool for digital forensics and incident response (DFIR) and troubleshooting. Leveraging its experience in developing open-source projects, Sysdig has built its container and K8s security solution—integrated within its CNAPP platform—on an open-source stack that includes Falco and Sysdig OSS. This approach has established the platform as the open standard for runtime threat detection and response."*
>
> ***- Daphne Dwiputriane, Research Associate***

Customer Purchase and Service Experience

Sysdig offers a simple and transparent pricing model for its customers. For container and K8s workloads, the company calculates prices based on agents. This simple pricing model allows customers to quickly understand pricing details, enabling them to estimate potential costs faster and more effectively. In contrast, many other container security vendors employ relatively complex pricing models for their container/K8s security solutions, which can deter potential customers due to the difficulty in understanding the price structure. Additionally, Sysdig offers its solutions on cloud marketplaces such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Azure, as well as through channel partners with licensing models, streamlining the purchasing process for customers.

Additionally, Sysdig offers a systematic and integrated proof of Value (PoV) process to assist customers in evaluating its products against their requirements and purchasing criteria, helping them maximize their investment value. The company extends its support post-purchase by providing training and enablement for customers through its customer success and technical account managers, ensuring effective utilization of its solutions. This approach helps Sysdig maintain high levels of customer satisfaction, exemplified by its top 60 customers who, on average, invest more than $1 million annually in recurring revenue with the company.

Conclusion

With organizations increasingly embracing cloud-native application development tools, the demand for container security solutions is set to grow exponentially. Organizations are recognizing the need for continuous protection of their containers and containerized environments. Sysdig stands out as a pioneer and leader in the global container/K8s security industry. Integrated within its comprehensive cloud security platform, Sysdig Secure, its container/K8s security solution provides extensive protection and visibility from build to runtime, helping organizations address security challenges. Sysdig's solution is powered by Falco, a leading runtime security tool, which provides a unique value proposition as the container/K8s security market increasingly emphasizes stronger runtime protection capabilities.

With its strong overall performance, Sysdig earns Frost & Sullivan's 2024 Company of the Year Award in the global container/K8s security industry.

© Frost & Sullivan 2024

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

Frost & Sullivan's Company of the Year Award is its top honor and recognizes the market participant that exemplifies visionary innovation, market-leading performance, and unmatched customer care.

Best Practices Award Analysis

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

Visionary Innovation & Performance

Addressing Unmet Needs: Customers' unmet or under-served needs are unearthed and addressed by a robust solution development process

Visionary Scenarios Through Mega Trends: Long-range, macro-level scenarios are incorporated into the innovation strategy through the use of Mega Trends, thereby enabling first-to-market solutions and new growth opportunities

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

Best Practices Implementation: Best-in-class implementation is characterized by processes, tools, or activities that generate a consistent and repeatable level of success

Financial Performance: Strong overall business performance is achieved in terms of revenue, revenue growth, operating margin, and other key financial metrics

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

© Frost & Sullivan 2024

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™

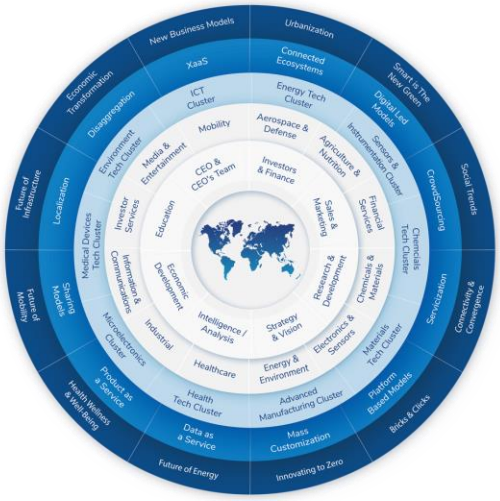
Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.
Learn more.

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)