FROST & SULLIVAN

SYSDIG

2022 COMPANY OF THE YEAR

GLOBAL
CONTAINER SECURITY 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. Sysdig excels in many of the criteria in the container security space.

Addressing Unmet Needs

Businesses worldwide are increasingly embracing digital transformation and realizing the need for flexible cloud infrastructure and strategies to meet urgent business goals, such as improved customer experience and innovation. In Frost & Sullivan's 2021 global survey on cloud usage, 74% of businesses considered the cloud the most critical to digital transformation.

With the growth of cloud adoption, accelerated by the COVID-19 pandemic, organizations must change how they build, operate, and manage back-end infrastructure and front-end, customer-facing applications. Many have turned to cloud-native application development tools to facilitate cloud migration and digital transformation, such as infrastructure-as-code (IaC), serverless computing, function-as-a-service, containers, and continuous integration (CI)/continuous deployment (CD) platforms. The framework and approach for application are also changing as organizations transition from traditional, monolithic application development to the microservice and containerized architecture and more open-source dependencies and libraries.

However, the rising adoption of the cloud and cloud-native application development tools introduces more complexities, expanded attack surfaces, and security challenges to the business environment. The growing dependence on the containerized approach and open-source dependencies and libraries has created concerns about container and Kubernetes security, which is essential to the shift-left security model among global businesses.

Because container and Kubernetes security is vital to the cloud application development stage, industry-specific regulations on container security have increased. Organizations must also comply with industry frameworks on cloud security, such as the International Organization for Standardization 27001.

Founded in 2013 and based in San Francisco, Sysdig provides security software to secure and operate containers, Kubernetes, and the cloud. It is known for its software-as-a-service (SaaS) platform built on an open-source stack comprising Falco, Sysdig OSS, Sysdig Monitor, and Sysdig Secure. The Sysdig cloud security platform helps businesses address key challenges in container, DevOps, and Kubernetes security and makes every cloud deployment secure and reliable. It also helps customers mitigate challenges to the security, compliance, health, and performance of cloud applications. The company specializes in digital supply chain security, securing serverless computing implementation, zero-trust networking for containers and Kubernetes, CSPM, and simplifying the operations of Kubernetes admission control and IaC security.

> *"By providing customers with a comprehensive and fully integrated cloud-native platform for cloud and container security, Sysdig has emerged as the leader in the container security space. Its robust platform covers IaC security, CIEM, CSPM, vulnerability management for containers and hosts, compliance, container and cloud detection and response, and cloud and Kubernetes monitoring. Frost & Sullivan is impressed with how the Sysdig platform supports customers in effectively managing threats while keeping management overheads minimal, which often arise when customers use multiple security tools."*
>
> ***– Anh Tien Vu,***
> ***Industry Principal***

Security software providers often focus on specific container security areas, such as container image scanning, or use disjointed solutions to address challenges. Unlike its competitors, Sysdig's key selling point is its integrated, holistic platform for cloud, container and Kubernetes security, which has enabled it to gain customer preference rapidly and globally. To address digital supply chain risks, Sysdig provides customers with the capabilities to scan and identify inherent vulnerabilities and dependencies of third-party open-source codes through image profiling, Risk Spotlight for vulnerability prioritization, and Falco threat detection. Sysdig complements these features with first-class integrations with partners such as Snyk for early phase security testing to identify vulnerabilities and detect threats at the beginning and throughout the workload life cycle as new dependencies are introduced to the build, delivery, and runtime.

With the increasing adoption of technologies such as AWS Fargate, Google Cloud Run, and Azure Container Instances to streamline systems delivery, security teams must implement appropriate security controls to secure workloads. The Sysdig platform supports serverless computing within major cloud providers, such as AWS and Azure, enabling threat and anomaly detection and incident response for serverless computing environments. Frost & Sullivan finds Sysdig's ability to help customers facilitate zero-trust networking for containers and Kubernetes contributes to Sysdig's preferred vendor status due to the growing popularity of the zero-trust security model.

The Sysdig platform also simplifies the operations of Kubernetes admission control to enable allow-listing and block unsafe workloads from being deployed. Kubernetes admission controllers are powerful but difficult to implement and operate. Sysdig makes it easy for teams to unify admission controllers'

security and non-security policies, detect vulnerabilities or availability issues, and take appropriate actions such as instituting resource constraints or blocking workloads.

In addition, Sysdig offers IaC security for Kubernetes, with plans to extend the IaC security coverage for the cloud. Customers can use the Sysdig platform for automated risk remediation and policy violations with a simple Git pull request, reducing the manual efforts of cloud security teams. This feature is a unique capability of Sysdig Secure.

Visionary Scenarios through Mega Trends

Frost & Sullivan identifies cloud computing adoption as a Mega Trend that will grow in the next five years, transforming how businesses invest in information technology (IT) infrastructure, the application development life cycle, and security operations. Organizations are adopting cloud-native tools for application development, greatly facilitated by container technologies and serverless computing. These technologies are changing application development strategies as organizations flexibly design, develop, test, and launch applications in the market to enhance the customer experience. With containers and a DevOps workflow, companies today can deploy application updates, fix bugs, and add new features weekly or daily, which was impossible 10 years ago.

Sysdig was launched originally with open-source projects. It continues to use the open-source approach for its products, with both Sysdig Secure and Sysdig Monitor built on open-source projects, including Prometheus, Sysdig OSS, Falco, and OPA that capitalize on community contribution for enhanced features, security, integration, and problem-solving. The open-source approach enables customers to avoid vendor lock-ins when using proprietary solutions from other competitors.

Ever the visionary, Sysdig drives its cloud security business based on cloud Mega Trends. It leads the market with its solutions that address cloud security challenges through three areas: container and Kubernetes to facilitate new application development using the microservice architecture, public cloud infrastructure-as-a-service and product-as-a-service offerings as building blocks, and the DevOps process to align development and operations teams closely to develop and release software continuously. By focusing on container and Kubernetes security, Sysdig has gained significant traction among large enterprises that have embraced cloud-native application development tools in their environment. Sysdig has built a platform unifying security solutions and monitoring capabilities, making it a market pioneer in adopting the approach for container and Kubernetes security.

With many organizations focused on the shift-left security model, Sysdig has built capabilities to “shift left” and “shield right”. It merges build and runtime protection for containers to help customers manage high-profile zero-day attacks in development and production environments. The company also pays significant attention to other Mega Trends, such as IaC and serverless computing security. Seeing how IaC has become vital to IT provisioning and administration strategies among global businesses, Sysdig acquired Apolicy in 2021 to strengthen its container security solution and help customers manage risks and vulnerability at the first stage of the application development life cycle. For serverless computing security, Sysdig developed robust capabilities such as image scanning, runtime security, posture management, compliance and audit, incident response, and forensics. The runtime security and detailed record for incident response and forensics are based on Falco, which was created by Sysdig.

Leadership Focus

Sysdig is a recognized pioneer in the container and Kubernetes monitoring, visibility, and security market. Its open-source tools (Sysdig OSS and Falco[1]) were the first to have the technical capabilities of seeing into containerized workloads, collecting rich telemetry from them, and contextualizing it for analysis and response or remediation actions. Sysdig is a long-time supporter of Prometheus and offers commercial support that is fully compatible with the project. These open-source capabilities form the foundation for its commercial platform offerings, Sysdig Secure and Sysdig Monitor.

Sysdig spearheads and invests in uncontested market segments, including cloud infrastructure entitlements management (CIEM) and IaC security. The Apolicy acquisition added infrastructure and posture security into Sysdig's portfolio, strengthening its security capabilities. The Kubernetes security posture management segment is not well-covered by most cloud security posture management (CSPM) tools in the market. Sysdig is committed to investing in this segment per its strategic investments and technology acquisitions roadmap to cement its leadership in the cloud and container security market.

To maintain its market leadership in container, Kubernetes, and cloud workload security, Sysdig also forms strategic partnerships with public cloud service providers (CSP), such as AWS, GCP, Azure, and IBM Cloud, to integrate its solutions with their ecosystems. The strong integration allows customers to deploy solutions across different cloud environments easily and avoid vendor lock-ins. This approach also helps Sysdig keep pace with key CSPs' new developments to increase the interoperability and efficiency of its solutions.

In addition, Sysdig stays ahead of the rapidly evolving threat landscape by focusing on and investing in threat research, specifically threats to cloud and container environments. Its threat research team dedicates time to identifying new threats and threat actors, discovering unknown vulnerabilities, and creating detection rules and machine learning models to protect customers from advanced attacks and malicious actors.

By providing customers with a comprehensive and fully integrated cloud-native platform for cloud and container security, Sysdig has emerged as the leader in the container security space. Its robust platform covers IaC security, CIEM, CSPM, vulnerability management for containers and hosts, compliance, container and cloud detection and response, and cloud and Kubernetes monitoring. Frost & Sullivan is impressed with how the Sysdig platform supports customers in effectively managing threats while keeping management overheads minimal, which often arise when customers use multiple security tools.

[1] Sysdig created Falco and contributed it to the Cloud Native Computing Foundation (CNCF) in 2018

Financial Performance

More than 700 enterprise customers worldwide use the Sysdig security platform. Most of Sysdig's customers are highly digitalized and from various sectors, such as financial technology, high technology, media, telecommunications, government, and healthcare.

In 2021, Sysdig experienced solid growth across regions, with accelerated growth in Europe, Japan, and Asia-Pacific partially attributed to the COVID-19 pandemic that drove businesses' adoption of cloud security solutions to adapt and expand online offerings. Sysdig recorded atremendous annual net revenue retention of 149%. Its customer base also increased 140% YoY, resulting in solid annual recurring revenue (ARR) growth YoY. On average, Sysdig achieved almost $900,000 ARR across its top 50 purchasing customers. In 2021, it also experienced a 300% rise in Sysdig Secure sales and a 120% YoY increase in sales in the large enterprise segment.

> *"Sysdig recorded an annual revenue run rate of more than 300% YoY for cloud security platform sales in 2021 because of its tremendous annual net revenue retention of 149%. Its customer base also increased 140% YoY, resulting in solid ARR growth of almost 100% YoY. On average, Sysdig achieved almost $900,000 ARR across its top 50 purchasing customers. In 2021, it also experienced a 300% rise in Sysdig Secure sales and a 120% YoY increase in sales in the large enterprise segment"*
>
> ***– Anh Tien Vu, Industry Principal***

In addition to customer and revenue growth, Sysdig's headcount doubled to cater to its business expansion requirements. The company ended 2021 with nearly 600 employees, of which more than 45% resided outside the United States. The company also expanded its SaaS hosting locations from 9 to 16, including the addition of Australia.

Customer Purchase and Service Experience

Sysdig adopts simple and transparent pricing for its products. For container and Kubernetes workloads, Sysdig prices its solutions based on the number of agents deployed. For serverless functions like Fargate, their pricing is based on tasks. While for the cloud environment, it is based on compute resources. This simple and transparent pricing model clarifies potential costs and helps customers prioritize and monetize their investments. Sysdig's pricing model differentiates the company from competitors that often use complex pricing models.

In addition, Sysdig simplifies the purchasing process by placing its solutions on cloud marketplaces, such as AWS, GCP, Azure, and Oracle. Customers can also purchase its solutions from its channel partners through licensing models (annual or monthly billing). The simplified purchasing process enhances customer value, particularly in a multi-tiered sales ecosystem.

Sysdig offers a systematic and integrated proof-of-value process for customers to evaluate its products against their requirements and purchase criteria, helping them save time and maximize their investment value. The company also provides customers with post-purchase proactive training and enablement through its Customer Success and Technical Account Manager teams to help them effectively operate and manage their solutions, boosting their confidence and satisfaction. Sysdig's fast, reliable, and high-

touch support is another factor driving its high customer and revenue retention rates. The company consistently checks in with customers for feedback and timely support. It also offers technical support and knowledge training to customers and channel partners without additional costs. Frost & Sullivan lauds Sysdig's robust initiatives that instill customer confidence throughout the customer life cycle.

Conclusion

As organizations migrate to the cloud, many have adopted cloud-native application development tools such as IaC, serverless computing, function-as-a-service, containers, and CI/CD platforms. Containers and Kubernetes are vital tools facilitating this paradigm shift, but their accelerated usage has raised security concerns and made business environments more complex. The growing shift to the containerized approach and reliance on open-source dependencies and libraries drive the shift-left security model among global businesses, in which container and Kubernetes security is a core part.

Sysdig is a pioneer and leader in the global container and Kubernetes security market. Its integrated cloud security platform is designed to help businesses address key challenges in container, DevOps, and Kubernetes security. Its comprehensive solution and customer-centric growth strategies position the company as the top-of-mind choice for container and Kubernetes security among large organizations worldwide. The company experienced tremendous growth in 2021, outperforming its competitors in customer base growth, customer retention rate, and revenue growth.

For its strong overall performance, Sysdig is recognized with Frost & Sullivan's 2022 Global Company of the Year Award in the container security industry.

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

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™

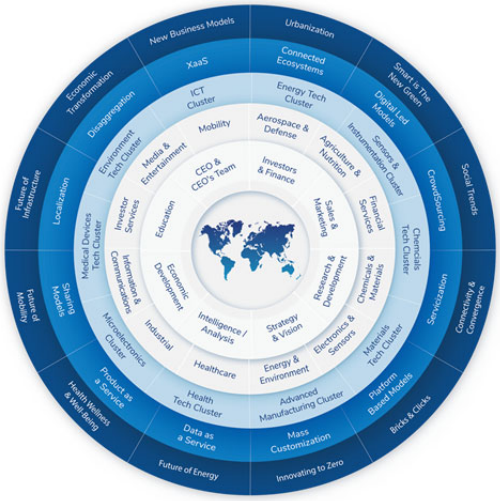
Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.
Learn more.

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)