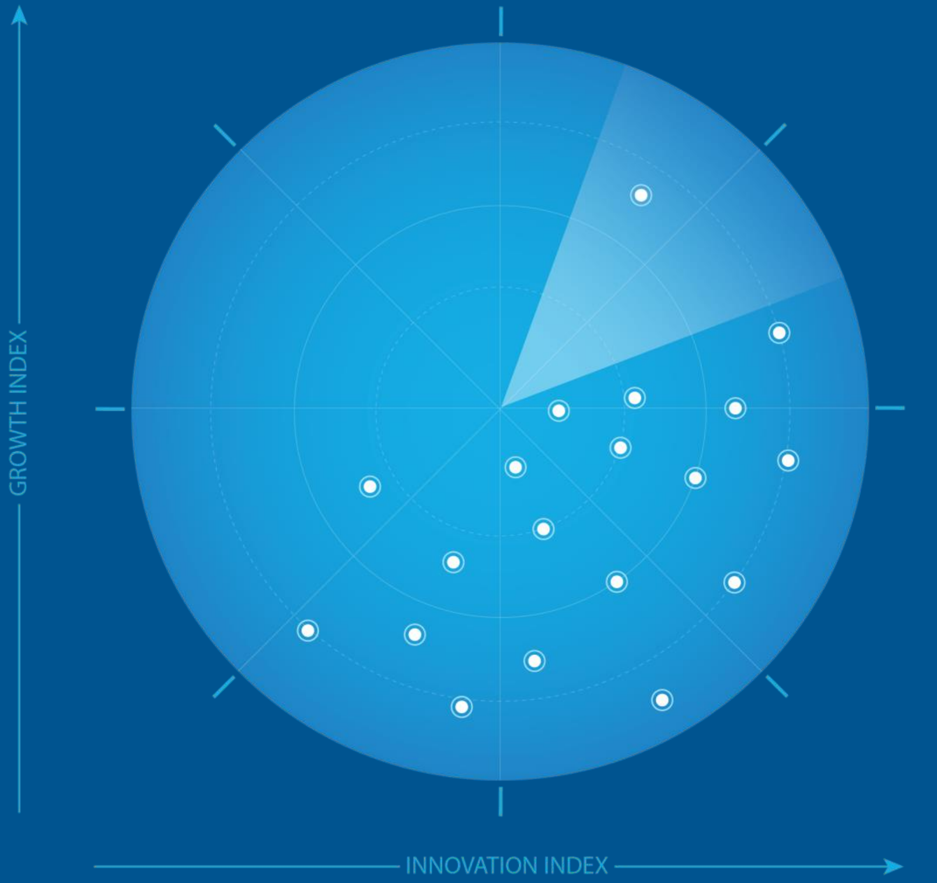
FROST & SULLIVAN

Frost Radar™: Cloud-native Application Protection Platforms, 2022

A Benchmarking System to Spark Companies to Action - Innovation That Fuels New Deal Flow and Growth Pipelines



Author: Anh Tien Vu
Industry Principal, Global Cybersecurity

PD8C-74
November 2022

Strategic Imperative and Growth Environment

Strategic Imperative

Cloud computing is becoming the norm in the business environment with a variety of cloud models and services available. The accelerated migration to the cloud has enabled businesses to embrace their digital transformation journey and simplify their IT infrastructure and operations.

The use of cloud computing is transforming the application development life cycle, security operations, and the way organizations build, operate, and manage back-end infrastructure and front-end, customer-facing applications with cloud-native technologies such as containers/Kubernetes, serverless, infrastructure as code (IaC), and other continuous integration/continuous delivery (CI/CD) platforms for cloud management, application, development, and deployment.

With a more intense focus on cloud-native application development technologies, organizations are shifting from a traditional monolithic application development model to a microservice architecture and containerized approach using more open-source dependencies and libraries.

Container/Kubernetes technologies and serverless computing are changing application development strategies as they enable organizations to flexibly design, develop, test, and launch their applications to the market, enhancing customer experience. The Cloud Native Computing Foundation (CNCF) 2021 Annual Survey showed that 96% of organizations are either using or evaluating Kubernetes and 93% are currently using, or planning to use, containers in production. However, the use of open-source software, libraries/dependencies, and registries has introduced more security threats and concerns because these application artifacts remain at risk to container image vulnerability, host security, code injection (for serverless applications), and compliance issues.

Source: Frost & Sullivan

Strategic Imperative (continued)

The increasing complexity of the hybrid and multi-cloud environment as well as the expanding attack surface and security operation challenges require an integrated and cloud-native platform to provide organizations with visibility, control and protection to secure modern cloud compute architectures (e.g., virtual machines [VMs], containers, Kubernetes, serverless) as well integrate security into the software development life cycle and help organizations effectively deal with compliances. This makes the legacy security approach outdated because it is not designed to support micro-segmentation or be robust enough to keep pace with the application changes, particularly in container and serverless environments.

As a result, the CNCF has called for a paradigm shift to a “shift-left and shield-right” security model to protect cloud-native applications by moving security closer to dynamic workloads that are identified based on attributes and metadata such as labels and tags. The model requires security to be integrated early and throughout the application development life cycle instead of only to the later phases, as well as security management for the cloud environment in which the applications are deployed and running, which is driving the need for a cloud-native application protection platform (CNAPP).

With CNAPP, organizations are able to deal with these security threats and challenges with an integrated security platform as opposed to point security solutions such as cloud security posture management (CSPM), cloud workload protection platform (CWPP), or vulnerability management. CNAPP also enables better collaboration among security, IT/platform, and development teams to improve productivity and manage risks more efficiently for their cloud environments.

Source: Frost & Sullivan

Growth Environment

The global CNAPP market recorded revenue of $1,720.6 million in 2021, representing year-over-year growth of 48.8%. Frost & Sullivan projects that momentum to continue at a compound annual growth rate of 25.7% from 2021 to 2026, with revenue reaching $5,406.8 million in 2026 because of the increasing demand for a unified cloud security platform that strengthens cloud infrastructure security and protects applications and data throughout their life cycle.

Organizations generally have been adopting CNAPP components individually for quite some time, led by CSPM for cloud security visibility and control and CWPP for runtime protection and compliance. Investment in DevOps security has increased recently due to the need for shift-left security to inject security in the early stage of the software development life cycle. Likewise, cloud infrastructure entitlement management (CIEM) and cloud network security are in wide use among early cloud adopters that used cloud-native solutions from their cloud service providers.

That said, organizations around the world have been spending significantly on different forms of CNAPP. Most are for individual products to address specific use cases and challenges. The CNAPP concept of consolidating all these tools remains new (as does the acronym), resulting in some confusion among potential users and a cautious approach to investment. Nonetheless, the accelerated adoption of cloud services and cloud-native application development technologies along with the increase in attack surface in the cloud environment will encourage more spending on cloud security technologies as a whole and CNAPP platforms in particular.

Source: Frost & Sullivan

Growth Environment (continued)

Many organizations, particularly mature ones, understand that siloed application risk, open-source risk, and the inability to quickly respond to threats facing infrastructure and workloads can create security gaps and complexity for their teams. The need to identify, prioritize, and remediate risk in a centralized view will intensify demand for CNAPP.

A single platform that delivers better security protection, granular visibility, and risk management efficiency is required to manage security and compliance risks together. This comes with the increasing acceptance of the multi-cloud strategy, the continuous need to secure workloads against attacks, and the pressure to centralize consistent policy enforcement across different environments, be it cloud infrastructure, containers/Kubernetes, IaC, or CI/CD pipelines.

There is a growing need for better integration of CNAPP with the DevOps software development life cycle framework and CI/CD pipeline platforms to enable the security-by-design approach (shift-left security) in every stage of software building (development, testing, and release). The integration of CNAPP with DevOps is to address key concerns revolving around application artifact scanning (static and dynamic application security testing [SAST/DAST], application programming interface [API] scanning, software composition analysis [SCA], and vulnerability management), cloud risks associated with configuration, runtime behavior analysis, and compliance requirements. The shift is driving the need for cloud-native security solutions to protect cloud-native platforms, particularly containers/Kubernetes, hosts, application dependencies, serverless applications/codes, CI/CD tools, and other orchestration platforms.

Source: Frost & Sullivan

Growth Environment (continued)

In terms of consumption, CSPM, CWPP, and DevOps security will continue to be key CNAPP features, but CIEM and cloud network security services also will see an uptake in the next 5 years. Many organizations seems to use at least two components from one vendor at the same time for better management and protection efficiency.

Consolidation of cloud security use cases will continue in the next few years. More vendors will enter the CNAPP space either with their own proprietary technologies or through acquisitions. Companies that have strong CWPP offerings, including Kaspersky, Fortinet, and VMware, will most likely enter the market through technology expansion or acquisition. Nonetheless, the market is likely to see more innovative development and competition from start-ups with their own cloud-native security solutions focusing on CSPM, CWPP, and DevOps security.

Frost & Sullivan studies related to this independent analysis:

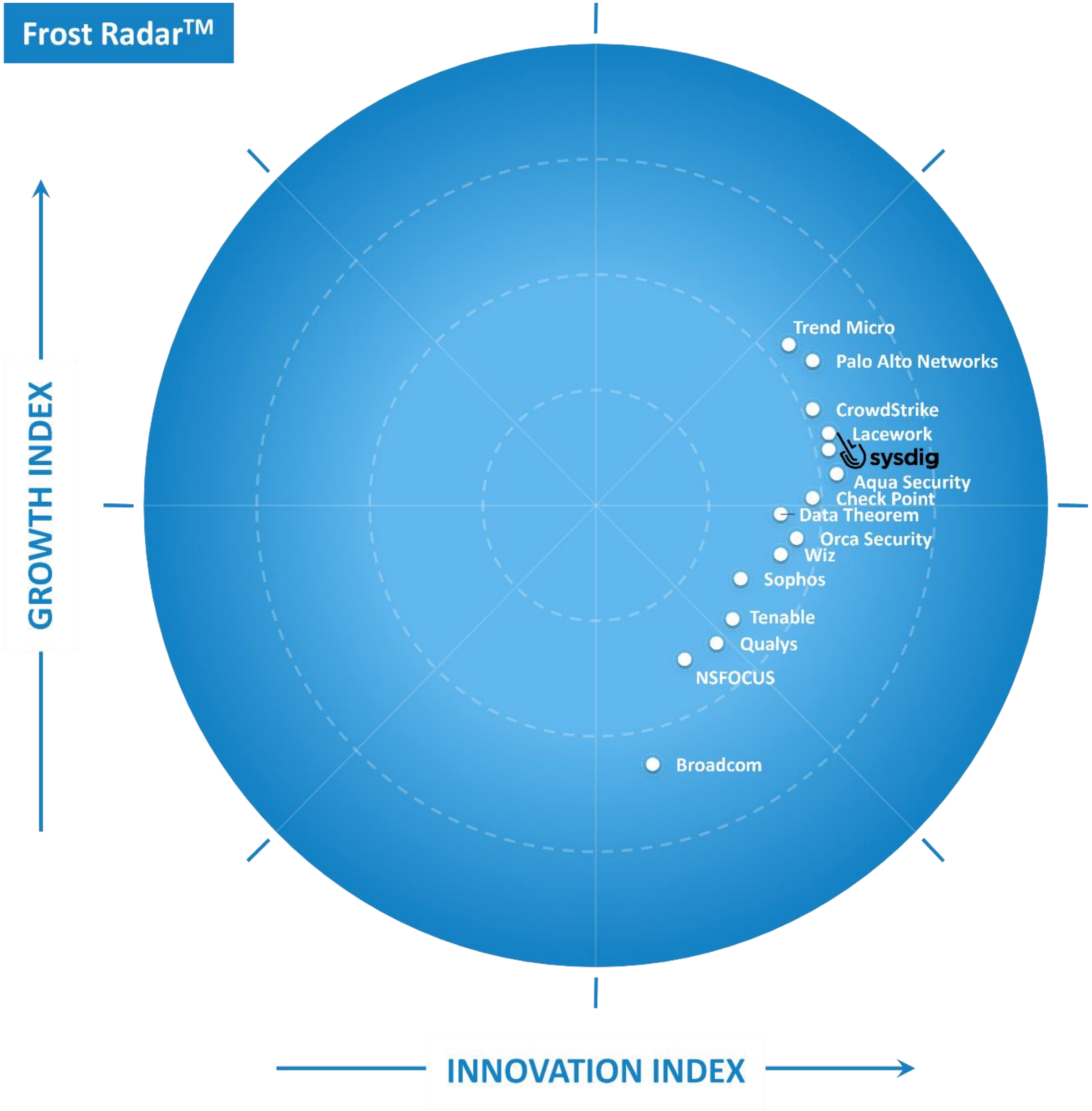
- Global Cloud Workload Protection (CWP) Growth Opportunities
- Global Cloud-native Application Protection Platform Growth Opportunities, 2022

Source: Frost & Sullivan

Frost Radar™

Cloud-native Application Protection Platforms

Frost Radar™: Cloud-native Application Protection Platforms



Source: Frost & Sullivan

Frost Radar™

Competitive Environment

The CNAPP market remained relatively nascent and fragmented with the participation of traditional network and endpoint security vendors, vulnerability assessment vendors, and start-ups that specialize in cloud security. From a field of more than 20 industry participants globally, Frost & Sullivan independently plotted the top 15 companies in this Frost Radar™ analysis. Vendors included in the report meet the following criteria:

- presence in at least two regions (North America; Europe, the Middle East, and Africa [EMEA], Asia-Pacific [APAC], or Latin America) in 2021 and in the first half of 2022;
- annual revenue of at least $20 million in 2021 and at least a 1% market share; and
- a qualified CNAPP platform by September 2022 (i.e., a platform that includes at least CSPM and CWPP capabilities).

As the market continues to evolve, more large cybersecurity companies and cloud security start-ups will enter it. Frost & Sullivan believes that the market will become even more competitive and that the landscape will change significantly in the next couple of years in terms of both go-to-market strategies and technological innovation.

Source: Frost & Sullivan

Frost Radar™

Competitive Environment (continued)

A vendor’s ability to provide an integrated platform that consolidates and unifies security capabilities to help business manage security posture and detect and respond to security risks and threats throughout the application development life cycle in the cloud-native environment is the key factor in customers’ decision-making process, along with the strong support capabilities, affordability, and a flexible and transparent pricing model.

Customers are looking for a broader set of capabilities that can provide them with visibility and security from build to production and across DevOps, DevSecOps, and cloud infrastructure. This means that they want CNAPP solutions that cover the entire stack (code, application, workload, and infrastructure). In fact, these solutions can help them achieve a holistic security strategy and reach a zero-trust security state across different cloud environments.

Organizations are increasingly leveraging artificial intelligence/machine learning (AI/ML) capabilities to better manage risks in the cloud environment. As a result, CNAPP solutions will have to shift left into the earliest stages of code inception and development and integrate with AI and ML to create better insights into the workload/application behavior and how it interacts within the cloud infrastructure in order to increase the automated threat detection and response capabilities.

Demand for stronger integration with web application protection is increasing because of the need to converge such protection with those of the underlying cloud workloads powering them.

Source: Frost & Sullivan

Frost Radar™

Competitive Environment (continued)

Sysdig is a the leader on the Innovation Index, particularly because of their focus on and integrated platform approach for CNAPP. Sysdig is recognized for its features and capabilities for container security using open-source technologies.

Source: Frost & Sullivan

FROST & SULLIVAN

Companies to Action:

Companies to Be Considered First for Investment, Partnerships, or Benchmarking

Sysdig

INNOVATION

- The Sysdig platform provides security capabilities for container, DevOps, and Kubernetes and to secure cloud deployment. It also helps customers mitigate challenges to the security, compliance, health, and performance of cloud applications. Sysdig provides both agent-based and agentless deployment models, with its Sysdig Secure CWP and Sysdig Secure CSPM.
- The CWP module enables organizations to detect runtime threats, anomalous threats across containers, hosts, and serverless environments. It helps manage vulnerabilities in CI/CD and registries and prioritize those that are exposed at runtime. This helps reduce vulnerabilities needing immediate attention by up to 95%, as reported by the company). The CSPM module provides visibility into cloud infrastructure, validates container compliance, supports FIM requirements, as well as manages misconfiguration.

GROWTH

- Frost & Sullivan's estimate shows that Sysdig was one of the fastest-growing CNAPP vendors in 2021 with year-over-year growth of 144.4%, enabling it to increase its share in the global CNAPP market to 4.4%, up from 2.7% in 2020.
- Sysdig's growth has been consistent for the past 2 to 3 years as it gains traction for its container/Kubernetes security using open-source technologies.
- The company has a strong presence in North America, where its revenue grew 242.1% in 2021, contributing about 70% of its CNAPP revenue for the year. EMEA revenue for the period grew 92.9%.
- The vendor focuses on large and very large organizations, which contribute more than 80% of its revenue. They are the early adopters of cloud-native technologies, which will help the company to maintain strong growth.
- In 2021, Sysdig added IaC security after acquiring Apolicy to strengthen CWP and CSPM capabilities.

FROST PERSPECTIVE

- Sysdig is one of the Innovation leaders in this Frost Radar^{TM} analysis. It is among the few vendors that provide a CNAPP platform with full security protection across the application development life cycle, software supply chain security, CSPM, CWPP, CIEM, and CNWS.
- It has a commitment to technological innovation as it continues to put efforts in R&D and product enhancements, such as malware scanning for hosts/ VMs, CIEM with the risk prioritization capabilities, and improved remediation for runtime.
- Sysdig should provide better support in terms application code review capability as it is delivered via the partnership with Snyk now, which may make the service unavailable or cause concerns over performance and privacy.
- It is also advised that Sysdig put more effort in expanding business footprint, go-to-market strategies, channel ecosystem, and marketing activities globally to maintain its rapid growth momentum.

Source: Frost & Sullivan

FROST & SULLIVAN

Strategic Insights

Strategic Insights

1

Though the CNAPP market remains nascent, it is becoming increasingly competitive with more vendors entering in the next two to three years. This will put huge onus and pressure on existing vendors to maintain their competitive edges with both technology innovations and pricing models. The stiff competition will require participants to put more efforts in R&D and M&A activities to strengthen their platform capabilities to gain traction and find ways to lower the total cost of ownership, while still being able to provide better support and experiences to their customers.

2

Market education is important for the success of the nascent CNAPP market. It is imperative that vendors work closely with their industry stakeholders to enhance awareness of cloud security among global businesses and the importance of the CNAPP concept in their cloud journey.

Vendors' growth is greatly driven by their channel partner programs. As such, it is vital for vendors to have right channel partners that can help educate the market, promote their solutions, engage with clients, and provide local support to gain customers' confidence and preference.

3

Choosing and purchasing a CNAPP is not a decision that a CISO can make alone. CNAPP requires tighter collaboration across the board because it involves various development, security, and operations teams, each with their own strategies, preferences, and key performance indicators. The decision must include input from chief information officers, lead developers, and business leaders because they want to achieve a common goal.

Source: Frost & Sullivan

Next Steps: Leveraging the Frost Radar™ to Empower Key Stakeholders

Significance of Being on the Frost Radar™

Companies plotted on the Frost Radar™ are the leaders in the industry for growth, innovation, or both. They are instrumental in advancing the industry into the future.

GROWTH POTENTIAL

Your organization has significant future growth potential, which makes it a Company to Action.

BEST PRACTICES

Your organization is well positioned to shape Growth Pipeline™ best practices in your industry.

COMPETITIVE INTENSITY

Your organization is one of the key drivers of competitive intensity in the growth environment.

CUSTOMER VALUE

Your organization has demonstrated the ability to significantly enhance its customer value proposition.

PARTNER POTENTIAL

Your organization is top of mind for customers, investors, value chain partners, and future talent as a significant value provider.

Source: Frost & Sullivan

Frost Radar™ Analytics

Frost Radar™: Benchmarking Future Growth Potential

2 Major Indices, 10 Analytical Ingredients, 1 Platform

VERTICAL AXIS

Growth Index (GI) is a measure of a company's growth performance and track record, along with its ability to develop and execute a fully aligned growth strategy and vision; a robust growth pipeline system; and effective market, competitor, and end-user focused sales and marketing strategies.

GROWTH INDEX ELEMENTS

- **GI1: MARKET SHARE (PREVIOUS 3 YEARS)**
  This is a comparison of a company's market share relative to its competitors in a given market space for the previous 3 years.
- **GI2: REVENUE GROWTH (PREVIOUS 3 YEARS)**
  This is a look at a company's revenue growth rate for the previous 3 years in the market/industry/category that forms the context for the given Frost Radar™.
- **GI3: GROWTH PIPELINE**
  This is an evaluation of the strength and leverage of a company's growth pipeline system to continuously capture, analyze, and prioritize its universe of growth opportunities.
- **GI4: VISION AND STRATEGY**
  This is an assessment of how well a company's growth strategy is aligned with its vision. Are the investments that a company is making in new products and markets consistent with the stated vision?
- **GI5: SALES AND MARKETING**
- This is a measure of the effectiveness of a company's sales and marketing efforts in helping it drive demand and achieve its growth objectives.

Frost Radar™: Benchmarking Future Growth Potential

2 Major Indices, 10 Analytical Ingredients, 1 Platform

HORIZONTAL AXIS

Innovation Index (II) is a measure of a company's ability to develop products/services/solutions (with a clear understanding of disruptive Mega Trends) that are globally applicable, are able to evolve and expand to serve multiple markets, and are aligned to customers' changing needs.

INNOVATION INDEX ELEMENTS

- **II1: INNOVATION SCALABILITY**
  This determines whether an organization's innovations are globally scalable and applicable in both developing and mature markets, and also in adjacent and non-adjacent industry verticals.
- **II2: RESEARCH AND DEVELOPMENT**
  This is a measure of the efficacy of a company's R&D strategy, as determined by the size of its R&D investment and how it feeds the innovation pipeline.
- **II3: PRODUCT PORTFOLIO**
  This is a measure of a company's product portfolio, focusing on the relative contribution of new products to its annual revenue.
- **II4: MEGA TRENDS LEVERAGE**
  This is an assessment of a company's proactive leverage of evolving, long-term opportunities and new business models, as the foundation of its innovation pipeline. An explanation of Mega Trends can be found here.
- **II5: CUSTOMER ALIGNMENT**
  This evaluates the applicability of a company's products/services/solutions to current and potential customers, as well as how its innovation strategy is influenced by evolving customer needs.

Appendix

List of Abbreviations

CNAPP: Cloud-native Application Protection Platform

DAST: Dynamic Application Security Testing

IAST: Interactive Application Security Testing

SAST: Static Application Security Testing

CSPM: Cloud Security Posture Management

CWPP: Cloud Workload Protection Platform

IaC: Infrastructure as Code

CIEM: Cloud Infrastructure Entitlement Management

CI/CD: Continuous Integration / Continuous Delivery

API: Application Program Interface

SCA: Software Composition Analysis

SBOM: Software Bill of Materials

CNWS: Cloud Networks Security

WAAP: Web Application and API Protection

Source: Frost & Sullivan

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, write to: permission@frost.com