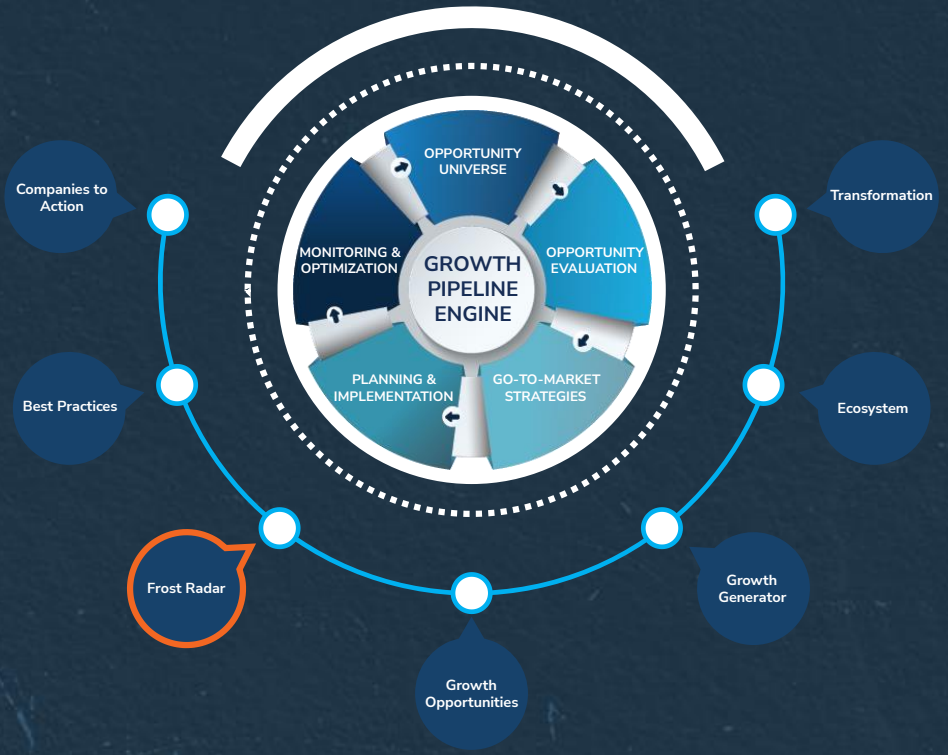
FROST & SULLIVAN

Frost Radar: Cloud-Native Application Protection Platforms, 2024

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



PFNV-74
November 2024

FROST & SULLIVAN

Strategic Imperative and Growth Environment

Strategic Imperative

- The modern cloud-native security requires a paradigm shift to a shift-left security model to protect applications by moving security closer to identified dynamic workloads and applications based on attributes and metadata, such as labels and tags. It requires early security integration and throughout the ADLC (instead of injecting security into later life cycle phases), and security management for the cloud where application deployment and execution occur, driving the need for CNAPPs.
- CNAPPs converge multiple security capabilities in cloud security stacks, spanning cloud infrastructure security, workload protection, and AppSec into a single, unified platform strongly integrating with DevOps workflows to secure and protect cloud-native applications throughout the ADLC from code to cloud and enable companies to meet industry standards and compliances.
- CNAPPs are primarily delivered via SaaS offering. However, several vendors can provide options to deploy the solution in an air-gapped / on-premises environment under the self-hosted option to cater to the requirements for data sovereignty and privacy in highly regulated industries, such as government, healthcare and banking/ finance sectors.
- CNAPPs provide protection from code to cloud across 3 layers – application, workload, and cloud infrastructure – with relevant functions and technologies protecting each layer, depending on needs.
    - **Application layer security**: This layer focuses on shift-left security capabilities in the ADLC to identify and remediate security risks in code development, OSS components, SDKs, APIs, artifacts, manifest, and serverless function templates before deploying applications in runtime/production.
    - **Workload layer security**: The workload layer security focuses on workload visibility, risk management, runtime protection to protect critical workloads, including containers/K8s, serverless functions, and host/VMs.
    - **Cloud infrastructure layer security**: This layer focuses on cloud visibility and risk management associated with cloud configurations, IaC templates, infrastructure entitlements, identity and data.

Source: Frost & Sullivan

Strategic Imperative

- Organizations can implement a CNAPP through various avenues, such as development, security, and operations (DevSecOps), cloud SecOps (CloudSecOps), or a comprehensive approach based on security needs and maturity level. In practice, many organizations begin with CloudSecOps, emphasizing cloud infrastructure security, entitlement management, and detection and response to cloud-related risks.
- Alternatively, organizations could use DevSecOps, prioritizing shift-left security approach to protect cloud-native infrastructure, workloads (such as containers/ K8s, serverless functions), software supply chain and applications (CI/CD pipeline, code security, registries, artifacts, etc.).
- Eventually, organizations can progress toward complete CNAPP adoption, which integrates DevSecOps and CloudSecOps. This comprehensive approach ensures end-to-end protection throughout the ADLC, covering everything from code development to cloud deployment.
- In many cases, most of organizations use CNAPP for the following use cases:
    - **Code to cloud visibility and control**: Secure multicloud infrastructure and maintain compliance, which includes the use of CSPM, CIEM, agentless CWPP, workload (container/ K8s and host) vulnerability management, DSPM for cloud data security and SSPM for SaaS application security.
    - **Security posture & Risk management**: This is to secure applications by design by empowering developers to fix code misconfigurations and vulnerabilities directly in their IDEs. Specific capabilities include Infrastructure as Code (IaC), SDLC scanning (CI/CD pipeline scanning, secret scanning, code repos scanning), SCA/ SBOM/ SCM, SAST/ DAST, and ASPM.
    - **Runtime protection & threat management**: Protect the application runtime environment, securing all cloud workloads and APIs from active attacks. This includes capabilities such as security host, container, Kubernetes, serverless protection, CDR/ ADR, CSPM and CWPP.

Source: Frost & Sullivan

Strategic Imperative

As a result, when making decisions on CNAPP, many organizations prioritize CNAPP solutions based on several factors, including:

- **Unified and integrated platform** that offers comprehensive coverage and build-to-run/ code-to-cloud context to help organizations identify, correlate, triage, prioritize, and remediate vulnerabilities and security risks across the full application and cloud lifecycle. The fragmented products and capabilities may lead to inconsistent security coverage and increased complexity in managing multiple tools. As a result, the integration of security capabilities such as CWPP, CSPM, CIEM, and IaC security, and AppSec is a key focus for customers. This approach simplifies operations, improves contextual risk assessment, enhances overall security posture, and reduces purchase and management costs.
- **Supporting both agentless and agent-based scanning** to provide immediate visibility and rapid assessment of their cloud environment while providing dynamic runtime protection capabilities for workloads and applications.
- **Support risk prioritization to reduce alert fatigue**. As alert fatigue will remain a top concern for CISOs as they add to the inherent complexity of the cloud and cloud-native environments, making it difficult for teams to effectively handle the risks from the vulnerabilities. CNAPP should enable organizations to allocate appropriate resources to address the most critical vulnerabilities. If developers receive too many false positives or if tools interrupt their workflow, they may become overwhelmed and desensitized to security alerts. In order to achieve this, CNAPP needs to integrate with runtime security tools, such as CDR and ADR for runtime visibility. CDR and ADR become critical integral parts of CNAPPs as they offer advanced detection and response with real-time insights across layers, including cloud, workload (containers, Kubernetes, serverless computing, and cloud logs) and application, which provides granular visibility into active threats rather than static risks.

Source: Frost & Sullivan

Strategic Imperative

- **Developer friendly**: Developers are at the forefront of building and deploying applications. Security "gates" can create bottlenecks in the development workflow and process, leading to frustration and potential security gaps. Organizations want to focus on capabilities that can help them accurately pinpoint risks with business impact, reduce noise, and enhance operational efficiency are highly valued. In addition, as developers are now being tasked with security responsibilities, they need to be equipped with capabilities, context, prioritization, and intuitive graphs for effective risk remediation. This requires a developer-centric CNAPP that integrates seamlessly into existing workflows, including IDEs, CI/CD pipelines, IaC template, software artifact scanning and ASPM, among others.

- **Ease of use and lower Total Cost of Ownership (TCO)**: In the face of expertise shortages, customers seek CNAPP solutions that are user-friendly and intuitive, enabling easy adoption. In many price-sensitive regions, TCO remains a significant driver influencing investment decisions in CNAPP.

- **Value-driven and business-aligned**: It is crucial that when making a decision on CNAPP, organizations need to choose a solution that aligns with the organization's specific business requirements. This can be achieved through a collaboration between teams and to identify the necessary functionalities to address the needs of different teams. Selecting a CNAPP solution can impact multiple areas of an organization as it involves multiple stakeholders in the organization. Effective CNAPP solutions should support business operations by enhancing collaboration between security and development teams, enabling the balance between development and security requirements and ensuring faster time-to-market for products and services.

- Moving forward, with the constant development of the threat landscape and dynamic client requirements, CNAPPs are evolving to integrate with advanced AI and ML-based risk reduction capabilities. It enables CNAPP solutions to not just highlight issues but to prioritize risks based on aggregated alerts and their aggregated risk value. This evolution aligns with the industry's move toward a more developer-focused security model, where there is an increasing shift in developers' responsibilities in security and risk assessment and mitigation.

Source: Frost & Sullivan

Strategic Imperative

- As organizations focus more on the entire cloud lifecycle, from code to cloud, it emphasizes the importance of CNAPP to offer capabilities to secure cloud environments at every stage, facilitating smoother collaboration between developers, DevOps, and SecOps. CNAPP will also provide more comprehensive risk analysis across multiple platforms, automated response mechanisms, and enhanced correlation capabilities for improved security decision-making.
- In addition, there's an increased focus on securing not just AI workloads but the entire AI lifecycle, from building and training models to deploying them in production environments. Organizations need to understand AI workflows and platforms like Kubeflow to implement effective security measures. CNAPP solutions will need to incorporate advanced AI-driven capabilities to manage and protect these workloads effectively.

Source: Frost & Sullivan

Growth Environment

- Frost & Sullivan's 2023 Voice of the Customer for Cybersecurity study indicated that investment in cloud security technologies will increase among global organizations, with cloud security to prevent breaches (31%) or detect and respond to cloud threats (30%). Many organizations are investing in cloud security solutions to prepare for unknown threats (24%) and regulatory compliance (12%), illustrating increasing cloud security awareness among global businesses.
- By 2025, an estimated 89% of organizations will use CWPPs, 91% will use CSPM, 88% will use CIEM, and an estimated 88% of organizations will explore the total cloud security platform/ CNAPP.
- CNCF's 2023 annual report shows that in 2023:
  - 90% of organizations using or evaluating cloud-native technologies
  - 91% of organizations using or evaluating containers in production; 84% for Kubernetes; 80% for Helm and 77% are using or evaluating Prometheus
- The CNAPP market landscape and development remains consistent with the findings featured in Frost & Sullivan's CNAPP 2023, CSPM and CWPP 2024 reports that were published earlier. By 2024, the CNAPP market generates a revenue of $5337.7 million, representing a strong YoY growth of 29.9%. The market is expected to grow steadily over the next five years, expected to generate a total revenue of $14.54 billion by 2029, with a robust CAGR of 22.2% from 2024-2029.
- The platform's ability to integrate various security functions, such as CWPP, CSPM, CIEM, IaC, ASPM, and more, into a single, unified solution will become increasingly attractive to organizations looking to simplify their security infrastructure while maintaining comprehensive cloud protection. As cloud adoption continues to expand and cloud-native technologies evolve, businesses will face more complex security challenges.

Source: Frost & Sullivan

Growth Environment (continued)

- The widespread adoption of multi-cloud and hybrid-cloud environments, along with the increasing use of containerized and serverless architectures, is creating a more complex and distributed cloud infrastructure. This shift introduces security challenges around visibility, control, and risk management across diverse cloud workloads, including containers, Kubernetes clusters, and serverless functions.
- Organizations need visibility into their development and production environments to make informed decisions throughout the software life cycle. Many standalone cloud and AppSec tools fail to provide correlated insights as they cannot identify what is running in environments. Visibility is essential, and security and DevOps teams must understand and address crucial risks proactively, making the shift-left and shield-right security practices more effective.
- Additionally, board-level discussions around shift-left security and software supply chain risks have elevated the importance of CNAPP solutions. As organizations face increasing scrutiny regarding how they manage their cloud environments and protect their software supply chains, the need for a comprehensive security platform that can address both development and runtime security is becoming more apparent.
- The rise of DevSecOps has transformed the way organizations approach security with the stronger requirements for embracing shift-left approach. Demand for security tools that align with this culture will grow. CNAPP solutions that offer visibility into software vulnerabilities, malware, and secrets during development are crucial in enabling developers to manage security risks more effectively. This growing trend of developer-driven security further fuels the demand for CNAPP platforms that can seamlessly integrate with existing development workflows.

Source: Frost & Sullivan

Growth Environment (continued)

- In addition, organizations also require real-time threat visibility, which traditional static scanning in a dynamic and rapidly evolving cloud-native landscape cannot offer. These threats require advanced detection and mitigation strategies, including AI/ML-driven CDR and runtime protection. CNAPP solutions are equipped with these advanced capabilities, making them more effective at identifying and responding to complex threats across cloud workloads.
- The inherent difficulty of managing security across multiple cloud providers, each with its own security protocols and tools, creates gaps that CNAPP is designed to address. By offering an integrated platform for risk prevention, vulnerability management, and automated threat detection and remediation across the entire cloud stack, CNAPP is positioned as a critical solution for unifying cloud security efforts.
- The necessity to “do more with less” means that CISOs must prioritize investments in security measures that offer the most significant risk reduction. This approach helps manage financial resources and improve the organization's resilience against cyber threats. To navigate these challenges, CISOs seek solutions bridging skills gaps between security and development teams, facilitating continuous compliance adherence, and offering comprehensive cloud security coverage.
- Alert fatigue will continue to be a primary concern for CISOs. While many security products offer modern threat visualizations, they do not inherently enhance an organization's security posture but generate a flood of alerts and add to the complexity, making it difficult for CISOs to effectively distinguish critical threats from benign anomalies. This environment creates a significant "security debt" as CISOs struggle to prioritize and address the most pressing vulnerabilities amid the noise.
- With growing regulatory pressures around data privacy and cloud security, many organizations are prioritizing security and compliance at the board level. CNAPP solutions, which provide unified risk management across cloud environments, are well-positioned to help organizations meet these regulatory requirements. The ability to provide real-time insights into vulnerabilities and compliance risks across the entire cloud infrastructure makes CNAPP an attractive option for CISOs and security teams tasked with reporting and maintaining compliance standards.

Source: Frost & Sullivan

Growth Environment (continued)

- Last but not least, organizations are seeing the benefits of consolidating security tools to address disjointed tool proliferation challenges, reduce costs, enhance visibility, and improve operational effectiveness because of the growing requirements of effective data correlation, code-to-cloud/cloud-to-code visibility, and context. This is particularly important as businesses scale their cloud operations.
- Misunderstanding the shared responsibility model in cloud security and resistance to adopting new technologies can dampen investment in CNAPP. Many organizations assume that CSPs are entirely responsible for securing their data, applications, and service configurations in the cloud without understanding that this responsibility is also on them. In addition, some stakeholders may see CNAPP as redundant or too intrusive, believing existing tools are sufficient, which delays or prevents adoption.
- The friction and distrust arising between security teams and developers can cause reluctance to invest in cloud security technologies, with security being perceived to slow down innovation and development speed. There is a prevalent lack of familiarity among DevOps teams with security responsibilities and limited knowledge of cloud services, K8s, containers, CI/CD, and their associated security risks and countermeasures. This leads to a reliance on traditional application architectures and outdated security solutions, which often cause alert fatigue and false positives, hence frustration and distrust among DevOps teams, which discourages effective collaboration between these teams, and hinder the prioritization of real risks.
- Concerns over the TCO, low performance, loss of control and visibility, and legal and compliance issues among C-level executives also may force organizations to repatriate from the cloud or hesitate to migrate to the cloud, dampening future growth of the platform. There is always resistance to change to new technologies that might be costly and often disrupt their practices, procedures, and culture.

Source: Frost & Sullivan

Growth Environment (continued)

- North America is poised to remain the largest adopter of CNAPP over the next five years, greatly driven by the strong awareness of cloud-native security requirements, stringent compliance mandates, and the need for comprehensive security solutions for risk and threat management in the multi-cloud and cloud-native environments. Organizations in the region are increasingly seeking integrated cloud security platforms that offer comprehensive coverage across complex, multi-stack environments and continue to invest in these platforms to enhance their security postures, protect against evolving threats, and meet regulatory requirements.
- The adoption of CNAPP in EMEA is on a significant upward trajectory and is expected to continue growing robustly over the next five years. The combination of strict regulatory compliance requirements, the complexity of hybrid and multi-cloud environments, and the increasing awareness of cloud-native security practices are key factors fueling this growth. Organizations are investing in adaptable, comprehensive security platforms that offer interoperability across different cloud services while meeting regional compliance standards.
- The accelerated adoption of cloud services in APAC has led to increased use of containers/ K8s, which has stimulated demand for cloud-native security among regional businesses, particularly those in China, Japan, South Korea, India, Australia, and Singapore that are experiencing significant growth in the use of containers and K8s. This has led to the solid growth of CNAPP in the region in 2024 and is expected to maintain the trajectory in the next 5 years. The growth is also driven by a growing awareness of software supply chain vulnerabilities and cloud security risks, prompting organizations to adopt CNAPP and zero-trust architectures to enhance their security postures.
- LATAM remains the least mature region in terms of CNAPP adoption, with most organizations maintaining on-premises and hybrid environments that heavily rely on VMs. The adoption of public and multi-cloud environments lags behind other regions due to limited cloud, internet infrastructure and shortage of skilled workforce. Economic conditions and disparities in technological maturity across countries also contribute to the low adoption rates of cloud services and new cloud-native technologies.

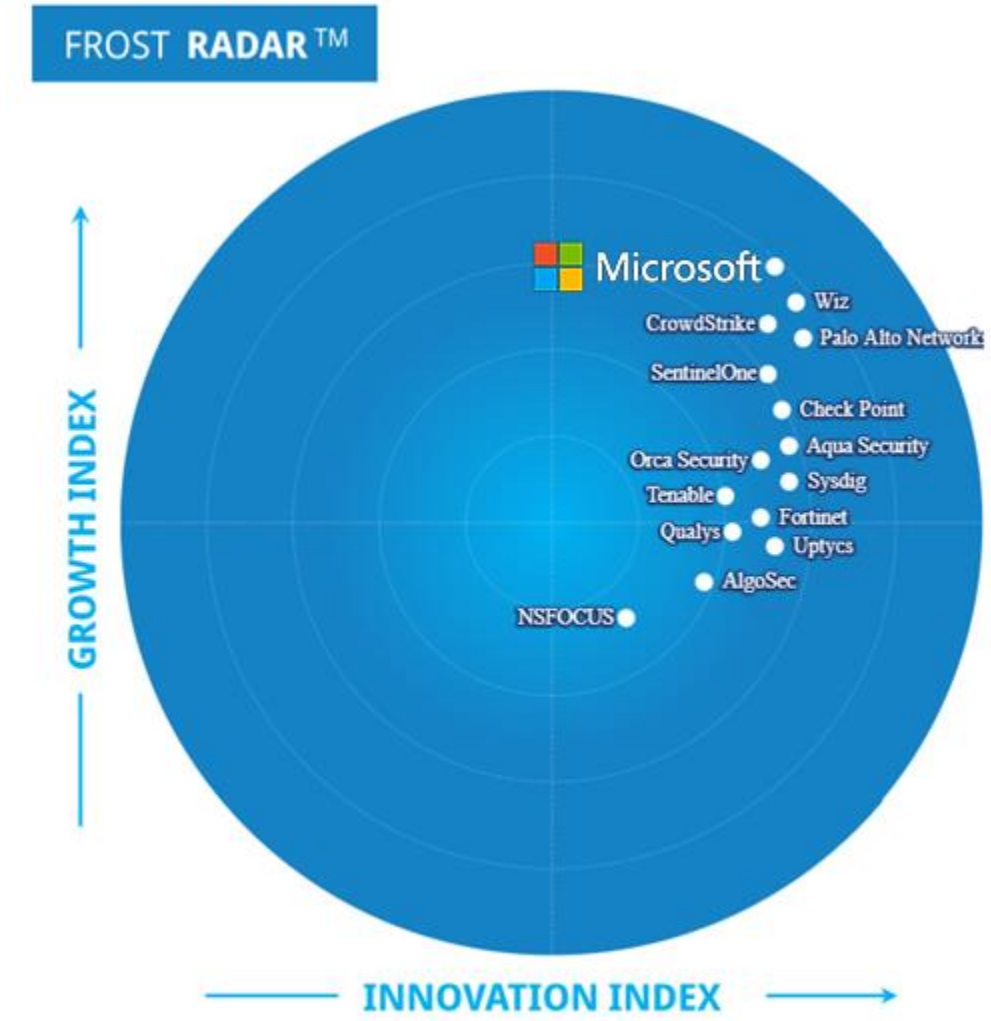
Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar

Cloud Workload Protection Platforms, 2024

Frost Radar: Cloud Native Application Protection Platforms



Source: Frost & Sullivan

Frost Radar Competitive Environment

- Vendors registering an estimated annual revenue of at least $20.0 million in 2024 have been included in this Radar analysis.
- This Frost Radar features the following vendors: AlgoSec, Aqua Security, Check Point Software Technologies (Check Point), CrowdStrike, Fortinet (Lacework), Microsoft (Security), NSFOCUS, Orca Security, Palo Alto Networks, Qualys, SentinelOne, Sysdig, Tenable, Uptycs, and Wiz. Frost & Sullivan identified these companies as the key powerhouses in the global CNAPP industry.
- Frost & Sullivan observed noteworthy innovation endeavors undertaken by several other global companies, including Bitdefender, Caveonix, Sophos, Rapid7, Sonrai Security, Trend Micros, Upwind, among others; and Chinese vendors, such as Alibaba Cloud, Asiainfo Sec, Tencent Cloud, Qingteng and QI-ANXIN. While these vendors demonstrated substantial technological advancements and market expansions, they were not included on this Frost Radar for the following reasons:
  - Their global market presence is relatively limited.
  - They declined to participate.
  - They were unable to provide direct inputs.
  - Our secondary research alone was insufficient to deliver a robust analysis.
- While revenue estimates are based on CY 2024, all qualitative insights are based on information available and market conditions as of September 2024.
- The study derives information and insights from Frost & Sullivan's secondary research and contributions from vendors, channel partners, and other industry stakeholders.
- All revenue estimates and forecasts are attributable to Frost & Sullivan's analysis and modeling.
- Though revenue calculated is mainly for cloud-native environment, not all revenue featured in the study is generated from cloud-native environment.

Source: Frost & Sullivan

Frost Radar Competitive Environment (continued)

- The CNAPP market is still in an emerging phrase, with the technologies evolving constantly to meet customers' diverse requirements. Many large businesses often invest heavily in cloud security technologies and their workforce to secure workloads, applications, and data to avoid service disruptions and data breaches and adhere to regulatory compliances. As a result, CNAPPs have been used to address many cloud and application security cases, including:
  - Cloud misconfiguration and vulnerability management
  - Cloud workload protection
  - Shift-left security with secret scanning, CI/CD pipeline security, container image scanning, K8s protection, application code security, third party software component analysis (SCA/ SBOM), API protection and ASPM
  - Threat detection & response with automated remediation capabilities.
- The increasing demand for unified and comprehensive cloud security solutions is driving vendors to expand their platform, with the focus on runtime risk visibility for risk prioritization and application security.
- Vendors are also putting their efforts in improving integration seamlessly with DevOps flows, CI/CD pipelines, and AI/ML technologies has made the industry competition stiffer, with established security companies expanding their capabilities, particularly through the integration of AI/generative AI (GenAI) technologies.
- Cloud security start-ups are also expected to emerge to tap into these opportunities. That stated, there is a trend toward industry consolidation, with many smaller vendors that are unable to sustain their growth momentum and innovation scalability being acquired by larger competitors that are seeking to expand their portfolios to maintain competitive advantages and growth.

Source: Frost & Sullivan

Frost Radar Competitive Environment (continued)

Growth Index:

- The growth landscape remains consistent with our analysis last year with Microsoft, Wiz, Palo Alto Networks and CrowdStrike remaining top leaders on the Growth Index in this analysis due to their dominant market share and robust revenue growth over the past 4 years.
    - Microsoft has maintained its market leadership as the largest CNAPP player over the past few years. In 2024, its revenue is estimated to grow at a robust year-on-year (YoY) growth of 29.4% and capture a dominant market share of 24.7% due to the massive customer base that use its Azure cloud services, which includes large organizations across various industries. Its Defender for Cloud business has grown in popularity among global businesses, particularly those using Azure cloud services.

Source: Frost & Sullivan

Frost Radar Competitive Environment (continued)

Innovation Index:

- With CNAPP continuing to evolve to provide organizations with visibility from code to the cloud and comprehensive vulnerability, and risk management and threat protection in the runtime environment, CNAPP players are in the arm race to develop new technological features and capabilities to maintain competitiveness, focusing on automated compliance and vulnerability management, real-time visibility, risk prioritization, CDR/TDR, CDR, application security and integration with DevOps and GitOps workflows for better CI/CD pipeline and software supply chain security.
- Although technological features and capabilities remain key factors in evaluating cloud security/ CNAPP solutions, customers are increasingly considering other factors when choosing a solution. These include the vendor's product ecosystem, sustainability, and support, the solution's stability, user/ developer-friendly, ease of use, problem solving, integration capability with existing and future technologies, and ROI.
- Vendors rated as innovation leaders on this Frost Radar include Aqua Security, Check Point, CrowdStrike, Microsoft, Orca Security, Fortinet (Lacework), Palo Alto Networks, SentinelOne, Sysdig, Uptycs, and Wiz. This is attributable to their comprehensive CNAPP approach with extensive features, outstanding vulnerability & risk management in cloud-native environment, strong runtime protection and real-time TDR capabilities, excellent expertise and support capabilities, and highly scalable platforms that help organizations deal with cloud security challenges from code to cloud.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar

Companies to Action

Microsoft

INNOVATION

- Microsoft's Defender for Cloud (MDC) is a unified CNAPP that goes beyond traditional cloud security solutions by integrating a broad range of security functionalities to protect cloud and hybrid environments. MDC includes workload security, CSPM, IaC security, DSPM, DevOps security with CI/CD pipeline hardening, AI-driven SPM, and CIEM (through Microsoft EPM). It offers agent-based and agentless workload protection across various infrastructure layers, including networks, servers, databases, containers, storage, APIs, and services.
- MDC leverages Microsoft's extensive ecosystem to provide end-to-end visibility and protection for cloud-native applications. During development, it integrates seamlessly with tools like Visual Studio, GitHub, and Azure DevOps to embed security early in the life cycle. In production, MDC works with Microsoft Defender XDR, Microsoft Security Exposure Management, and Security Copilot to deliver advanced threat protection, reduce attack surface, and continuously monitor security posture across multi-cloud and hybrid environments.
- The platform stands out in data-aware security, offering granular visibility into sensitive assets with advanced data classification and monitoring through Microsoft Purview integration. It excels across various workloads (e.g., Azure, AWS, and GCP) using agent-based and agentless scanning.
- Powered by Microsoft’s leading threat intelligence, its agentless scanning can cover all cloud resources (including registries and container images with runtime visibility of vulnerable running images) and provide a rich threat detection suite for Kubernetes clusters (including managed K8s services, nodes, and workloads). Particularly, MDC's management capabilities provide a centralized approach to identifying and managing vulnerabilities across multicloud environments, offering prioritized recommendations for patching and remediation to improve overall security posture.

Source: Frost & Sullivan

Microsoft (continued)

GROWTH

- Microsoft is the only CSP-based CNAPP player featured in this Frost Radar™ analysis because of its multicloud support capabilities. It has been the largest player in the market over the last four years and continues to record robust growth.
- In 2024, the vendor is set to grow by 32.5%, enabling it to solidify its leadership position with a 24.7% market share—larger than the two closest competitors combined. Microsoft has strategically positioned itself as a security player and expanded its cloud security business over the years through its comprehensive range of programs, innovative offerings, and strong partner ecosystem.
- It dominates in cloud security and has an enormous customer base from its Azure business, making its CNAPP solution popular among companies heavily using Azure cloud services and expanding to other cloud service providers, including AWS and Google Cloud.
- By positioning itself as a comprehensive security vendor, Microsoft targets large enterprises across BFSI, manufacturing, healthcare, education, and government, emphasizing its multicloud security capabilities. Its extensive network of more than 15,000 security partners, GSIs, MSSPs, and a thriving independent software vendor community promote and support its solutions.
- With significant investments in cloud security, a strong partner network, and strategic positioning as a multicloud security provider, Microsoft has a solid foundation for sustained growth in the next few years to maintain its lead in the cloud security industry as competition increases.

Source: Frost & Sullivan

Microsoft (continued)

FROST PERSPECTIVE

- Microsoft's MDC offers a unified, integrated suite for cloud security and compliance with excellent security risk management, runtime protection, and advanced TDR capabilities. The platform covers the entire cloud application life cycle, including infrastructure, entitlements, workloads, identities, networks, and application layers. It serves as an ideal starting point for larger enterprises looking for a comprehensive, all-in-one solution without the complexity of more specialized offerings.
- It stands out for the seamless integration with a wide range of tools, spanning development, application, data, and identity security, connecting smoothly with Microsoft's Defender XDR and Microsoft Security Exposure Management solutions, which makes it a strong choice for DevOps and SecOps teams to enhance shift-left security, risk management, and real-time TDR capabilities within cloud and cloud-native environments. These capabilities have positioned Microsoft as a leader in the Frost Radar™ on growth and innovation indices.
- While MDC offers extensive insights and security coverage, its complex setup and maintenance can be challenging for many organizations, particularly SMBs. To extend its leadership and strengthen its multicloud presence, Microsoft should continue to expand support to cloud platforms like VMware, Oracle Cloud Infrastructure (OCI), Alibaba Cloud, and Tencent Cloud.
- In addition, it should also keep enhancing the depth of security features to further strengthen the platform capabilities and meet diverse customers' requirements. From a business perspective, it should continue to strengthen its partner ecosystem, focusing on MSSPs, resellers, and ISVs to expand its customer base beyond the Azure environment. This would allow Microsoft to drive substantial growth across the multicloud environment and maintain leadership.

Source: Frost & Sullivan

FROST & SULLIVAN

Best Practices & Growth Opportunities

Best Practices

1. CISOs should prioritize unified and comprehensive CNAPP platforms that offer a broad range of capabilities with deep functionality, ensuring seamless integration across entire development ecosystem and cloud environments. An effective platform should leverage a single data lake, consistent data model, and an integrated graph database to unify event logging, reporting, alerting, and relationship mapping, enhancing the effectiveness of risk analysis, facilitates triage, prioritizes issues, and supports efficient remediation.

2. Alert fatigue remains a top concern for CISOs as they add to the inherent complexity of the cloud and cloud-native environments, making it difficult for teams to effectively handle the risks from the vulnerabilities. Attempting to eliminate all risks can be counterproductive. Resources should be spent on addressing the most critical vulnerabilities. If developers receive too many false positives or if tools interrupt their workflow, they may become overwhelmed and desensitized to security alerts.

3. Whatever tools are chosen, it is crucial that they need to align with the organization's specific business requirements. Selecting a CNAPP solution can impact multiple areas of an organization as it involves multiple stakeholders in the organization. Effective CNAPP solutions support business operations by enhancing collaboration between security and development teams, enabling the balance between development and security requirements and ensuring faster time-to-market for products and services.

Source: Frost & Sullivan

Growth Opportunities

1. Customers are considering solutions that secure the entire cloud life cycle, from-code-to-cloud, and shift-left security models to provide granular visibility into and context for risks across different cloud-native application life cycle stages. Securing applications requires understanding their journey from code creation to cloud deployment as code-to-cloud intelligence contextualizes alerts and offers proactive remediations based on insights from the developer to the cloud environments that deploy the apps.

2. Though offering excellent capabilities in managing code-to-cloud security posture, current CNAPPs often heavily emphasize "shifting left". While this helps reduce risks and technical debts before deployment, security teams often find it less effective in active threat management in real-time. This is driving the need for cloud-native application detection and response solutions that focus on real-time threat mitigation, which can be delivered as separate solutions or part of current CNAPP platform.

3. CNAPP has helped organizations enhance their cloud-native security posture, but implementing and managing CNAPP independently presents challenges, including complex integrations with various cloud services, misconfigurations, alert fatigue, risks of missing critical threats and slow remediation due to manual processes. Managed CNAPP service providers can help address these challenges by offering specialized capabilities around deployment, management, and monitoring and threat detection & response.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar Analytics

Frost Radar: Benchmarking Future Growth Potential 2 Major Indices, 10 Analytical Ingredients, 1 Platform

Growth Index

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.

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.

Source: Frost & Sullivan

Frost Radar: Benchmarking Future Growth Potential 2 Major Indices, 10 Analytical Ingredients, 1 Platform

Innovation Index

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.

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

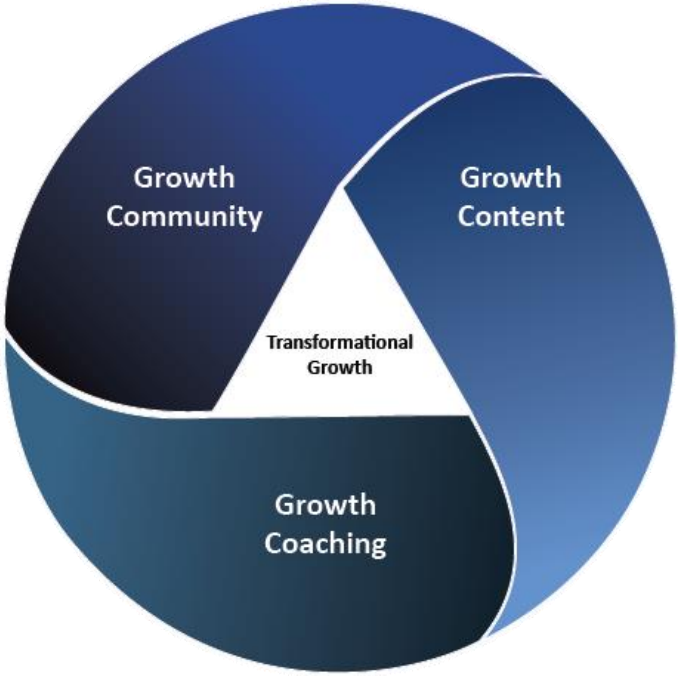
CUSTOMER ALIGNMENT
This evaluates the applicability of a company's products/services/solutions to current and potential customers, as well as how its innovation strategy is influenced by evolving customer needs.

Source: Frost & Sullivan

Take the Next Step

SCHEDULE A COMPLIMENTARY DISCUSSION WITH OUR INDUSTRY EXPERTS

https://hub.frost.com/gpdialog/



How is your organization maximizing your future growth potential?

How is the complexity of Ecosystem Impacting your Future Growth Potential?

How does your team plan to execute faster than your competitors?

Recommended Reading:

- Global Cloud Workload Protection (CWP) Growth Opportunities
- Global Cloud-native Application Protection Platform Growth Opportunities
- Global Cloud Workload Protection Platform Growth Opportunities
- Global Cloud-native Application Protection Platform Growth Opportunities
- Growth Opportunities in Global Cloud Security Posture Management, 2024–2028
- SaaS Security Posture Management (SSPM) and Data Security Posture Management (DSPM)
- Global Software Supply Chain Security Growth Opportunities
- Cloud Workload Protection Platform (CWPP) Market, Global, 2024–2028

FOLLOW US!

FROSTNSULLIVAN

myfrost@frost.com 877.GoFrost (877.463.7678) www.frost.com

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