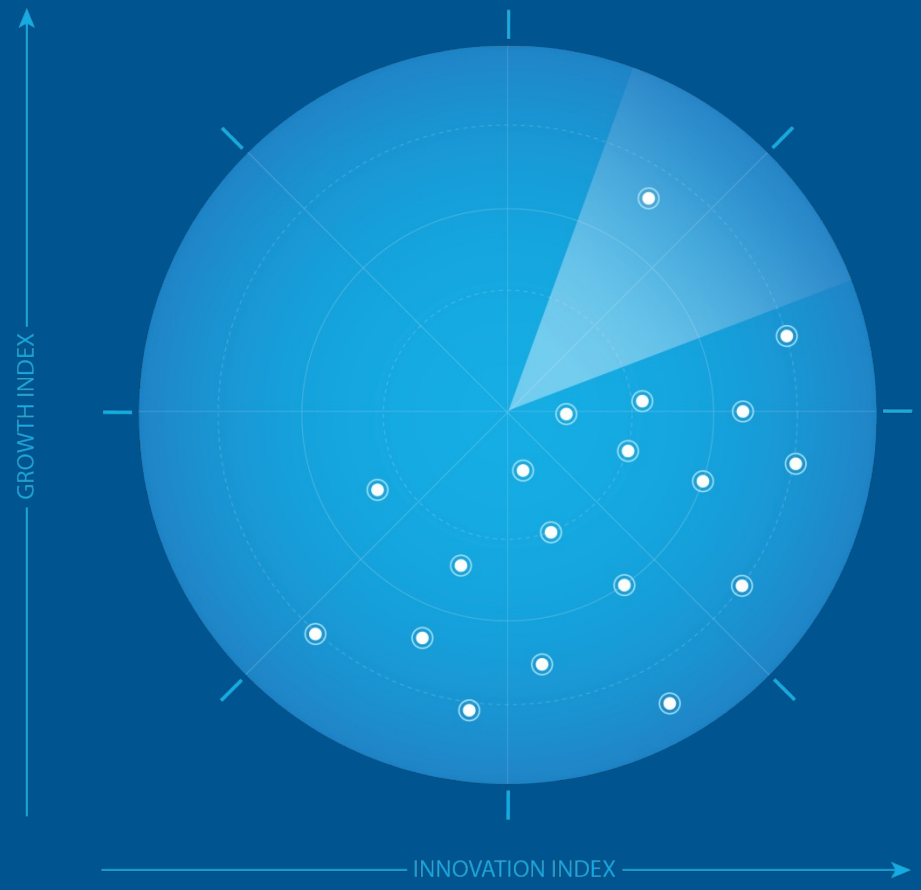
FROST & SULLIVAN

Frost Radar™: Cloud-Native Application Protection Platforms, 2023

Authored by: Anh Tien Vu

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



October 2023

FROST & SULLIVAN

Strategic Imperative and Growth Environment

Strategic Imperative

Customers' acceptance of cloud-native application protection platforms (CNAPPs) has grown rapidly. Industries such as finance, internet, manufacturing, and retail have demonstrated a strong interest in unified management and protection through CNAPPs.

- While the global deployment of CNAPPs is on a steady rise, it is essential to note that adoption is primarily among a small percentage of users, particularly large-scale enterprises with ample resources to explore advanced development models and security defenses, as CNAPPs adoption extends beyond just security teams.

- More teams within organizations are adopting and directly utilizing the platform to take charge of the security of the resources they manage. This democratization of security enables organizations to scale their security programs in tandem with cloud growth. As a result, CNAPPs have evolved from solely a security team's tool to becoming a holistic organization-wide security solution that empowers teams across security, cloud builders, developers, and operation teams.

Source: Frost & Sullivan

Strategic Imperative (continued)

- A CNAPP is a platform that converges multiple security capabilities in the cloud security stacks spanning cloud infrastructure security, workload protection, and application security into one single, unified platform featuring strong integration of cloud infrastructure security and workload protection with the DevOps process to secure and protect cloud-native applications throughout the application development life cycle, from code to cloud. It also enables companies to meet industry standards and compliances. Frost & Sullivan defines that a CNAPP provides security protection from code to cloud across 3 layers, including Application, Workload, and Cloud infrastructure, with each layer protected by relevant CNAPP functions and technologies.

- **Application layer security:** This layer focuses on shift-left security capabilities in the entire application development lifecycle to identify and remediate security risks in the code development, OSS components, SDKs, APIs, artifacts, manifest, and serverless function template before the applications are deployed in the runtime/production environment. Security at this layer includes artifact scanning and application runtime security capabilities using tools such as Software Composition Analysis/ Software Bill of Materials (SCA/SBOM), code repository, CI/CD pipeline security, IaC scanning, container security, SAST, DAST, IAST/RASP, and serverless function scanning.

Source: Frost & Sullivan

Strategic Imperative (continued)

- **Workload runtime layer security:** This layer emphasizes runtime security at the workload layer, including Container/Kubernetes, Serverless functions, and Host/VMs. Typical functions include CWPP and Kubernetes Security Posture Management (KSPM).

- **Cloud infrastructure layer security:** This layer focuses on cloud configurations, infrastructure as code (IaC) templates, infrastructure entitlements and identity management (CIEM), and data security posture management. Typical functions include CSPM, IaC scanning, KSPM, CIEM, and DSPM.

- Many organizations prioritize CNAPP solutions based on several factors, including:
    - Supporting 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.

Source: Frost & Sullivan

Strategic Imperative (continued)

- A unified and integrated platform that offers comprehensive coverage and context awareness, enabling seamless risk correlation and consolidation of tools. Integrating security capabilities such as CWPP, CSPM, CIEM, and IaC security is a key focus for customers. This approach simplifies operations, improves contextual risk assessment, enhances overall security posture, and reduces purchase and management costs.
- Support shift-left security: Customers prioritize CNAPPs that support the shift-left approach, enabling risk identification in the development phase. Integrating CNAPP checks into CI/CD pipelines for IaC templates and software artifacts helps identify vulnerabilities and misconfigurations before production.
- A unified platform that provides build-to-run or code-to-cloud context/intelligence to help organizations identify, prioritize, and remediate threats across the full application and cloud lifecycle.

Source: Frost & Sullivan

Strategic Imperative (continued)

- **Providing risk prioritization and empowering developers**: Organizations that 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 tasked with security responsibilities, they need to be equipped with capabilities, context, prioritization, and intuitive graphs for effective risk remediation.

- **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.

- Moving forward, with the constant development of the threat landscape and dynamic client requirements, CNAPP will further evolve to integrate with advanced AI and ML-based risk reduction capabilities, which will enable CNAPP solutions not just to 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, with an increasing shift in developers' responsibilities in security and risk assessment and mitigation.

Source: Frost & Sullivan

Strategic Imperative (continued)

- 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.

Source: Frost & Sullivan

Growth Environment

- Organizations globally increasingly focus on cloud security technologies to help them manage cyber risks better. Based on the recent Voice of Customer for Security study by Frost & Sullivan across more than 2,360 CISOs and C-level leaders, the majority of organizations want to use cloud security to prevent breaches (31%) and detect and respond to cloud threats (30%). Many also invest in cloud security solutions to prepare for unknown threats (24%) and regulatory compliance (12%). This shows a significant improvement in awareness of cloud security among global businesses.
- 48% of organizations currently use CWPP, while 41% plan to use it in the next 24 months. Only 10% indicated that they do not plan to add the solution in the years to come. The findings align with adopting other cloud security solutions, including CSPM, SaaS security posture management (SSPM), CIEM, and CNAPP.
- In 2023, the global CNAPP market recorded revenue of $3878.4 million, representing a year-over-year growth of 31.3%. Frost & Sullivan projects that momentum to continue at a compound annual growth rate of 22.8% from 2023 to 2028, with revenue reaching $10818.8 million in 2028 because of the increasing demand for holistic cloud-native security solutions.

Source: Frost & Sullivan

Growth Environment (continued)

- CISOs currently face a complex landscape of challenges in ensuring robust cloud security. The dynamic nature of cloud environments, marked by rapid scalability and continuous innovation, presents a profound disparity between the speed of cloud expansion and the ability of security programs to scale. This mismatch creates concerns for CISOs, as their security teams often find themselves overwhelmed by routine tasks, leaving limited capacity to tackle critical risks. The resulting strain on security teams and the risk of overlooking vulnerabilities hampers innovation and strains relationships between security and development teams.
- CISOs often find it difficult to balance between the constraints of budget limitations and tool proliferation. The need for efficient security operations has prompted CISOs to seek consolidation of security tools and streamlined operations. Balancing these challenges within multi-cloud architectures, which organizations increasingly adopt, further compounds the complexity CISOs must address. To navigate these challenges, CISOs seek solutions bridging skill gaps between security and development teams, facilitating continuous compliance adherence, and offering comprehensive cloud security coverage.

Source: Frost & Sullivan

Growth Environment (continued)

- More importantly, the rise of cloud-native applications, including those developed using containers/Kubernetes and other low-code/no-code platforms, has heightened security awareness. Organizations are aware of the risks in using these technologies and platforms, driving an increasing requirement for cloud-native and integrated security approaches to securing digital assets in their transformation journey. This leads to the growing requirements for security, such as code-to-cloud infrastructure, cloud threat detection and response, threat intelligence, and machine learning as part of the cloud-native integrated platforms.
- As a result, CNAPP is adopted by more organizations, particularly large and very large, and digital companies. These organizations are moving away from standalone solutions that only cover specific security aspects such as CSPM, CWPP, vulnerability management, and container security. This shift is prompted by the realization that these standalone tools lack comprehensive coverage and context awareness, leading to manual risk correlation, operational overhead, and blind spots. They recognize the need to consolidate tools for simplified operations, contextual risk assessment, and overall security posture improvement. This demand for a unified platform that addresses multifaceted cloud security requirements spans various regions and industries.

Source: Frost & Sullivan

Growth Environment (continued)

- More importantly, the friction and distrust between security teams and developers can cause hesitance in investing in CNAPP, as security is perceived as slowing down modern DevOps-style development. The 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 remains prevalent among organizations. This leads to a reliance on traditional application architectures and outdated security solutions, which often cause alert fatigue and false positives, discourage 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 are other factors that may force organizations to repatriate from the cloud or be hesitant to migrate to the cloud, dampening future growth of the platform.
- The Russo–Ukrainian and Israeli wars can negatively impact global cybersecurity budgeting and short-term cloud security spending. Frost & Sullivan's Voice of Customer for Security 2023 report showed that 62% of organizations saw an impact from the war on their security budget.

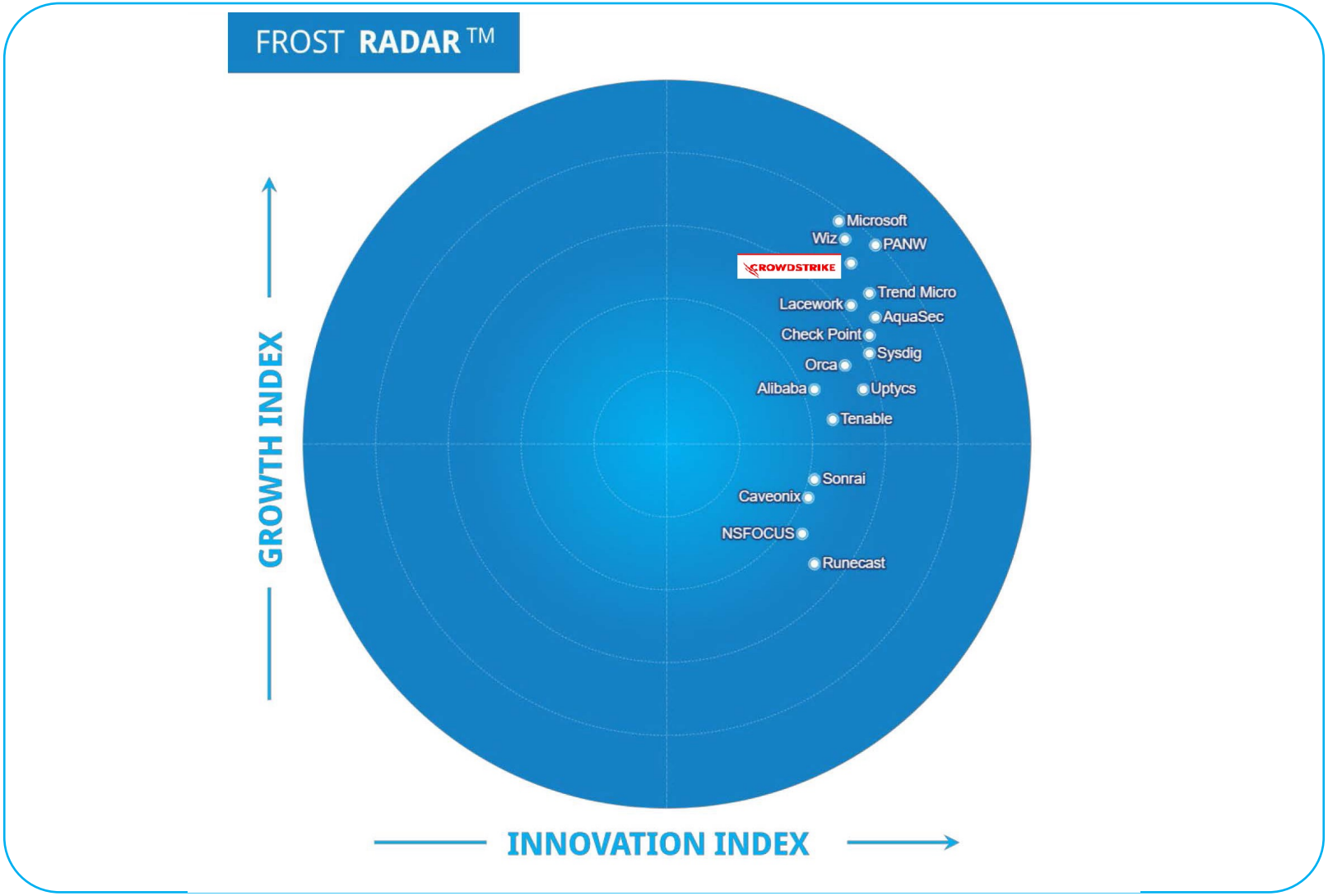
Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™

Cloud-Native Application Protection Platforms, 2023

Frost Radar™: Cloud-Native Application Protection Platforms, 2023



Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- The CNAPP market is in its early stages, experiencing fragmentation and intensifying competition as numerous vendors seek to innovate, restructure, and incorporate their existing cloud security solutions into CNAPP offerings. While various companies claim the title of CNAPP vendors, many lack crucial functionalities, such as runtime protection, CSPM, CIEM, and/or appsec. Only a handful of vendors in the market provide a comprehensive set of CNAPP capabilities, covering everything from cloud infrastructure to application security. However, even among these vendors offering full CNAPP capabilities, more efforts are needed to enhance the depth and convergence within their platform's security functionalities.
- Among more than 30 qualified CNAPP vendors globally, Frost & Sullivan independently plotted the top 17 companies in this Frost Radar analysis.
- Factors assessed to determine vendor selection and their performance in the Growth and/or Innovation index include end-user focus, geographic presence, and solution portfolio.
- Vendors registering an annual revenue of at least $5 million (estimated) in 2023 were included in this Radar analysis. Vendors that met the criteria for inclusion but could not share detailed insights into their solution were excluded to ensure fair scoring and comparison.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment (continued)

- This Frost Radar features the following vendors: Alibaba Cloud, Aqua Security, Check Point, Caveonix, CrowdStrike, Lacework, Microsoft (Security), NSFOCUS, Orca Security, Palo Alto Networks, Runecast, Sonrai Security, Sysdig, Tenable, Trend Micro, Uptycs and Wiz. Frost & Sullivan identified these companies as the critical powerhouses in the global CNAPP market.
- Frost & Sullivan also observed the noteworthy innovation endeavors undertaken by several CNAPP companies, including AccuKnox, Cyscale, Datadog, PingSafe, Qualys, Rapid7, and Sophos. These vendors demonstrate substantial efforts toward technological advancements and expanding their market reach. However, their global market presence is relatively limited, or they could not provide insights into their solutions by the study's deadline and hence did not qualify for this year's evaluation.
- The CNAPP market continues to evolve with the evolution of the CNAPP concept, technological advancement, the threat landscape, and regulatory developments. Established security companies will expand their offerings to offer CNAPP capabilities, while more cloud security start-ups are expected to emerge. Nonetheless, there will be a growing trend toward consolidation, with further acquisitions and mergers anticipated in the future.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment (continued)

- CrowdStrike has made considerable strides in this CNAPP Radar analysis compared to last year’s edition. It stands out in the Growth index for its impressive and consistent growth over the past 3 years. CrowdStrike's strong customer base, excellent brand perception and extensive customer base for its XDR platform and MDR service, and a focused strategy on cloud security position the company for robust growth in its cloud security business, including CWPP, CSPM, and CIEM, enabling it to capture additional market share.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment (continued)

- Frost & Sullivan acknowledges CrowdStrike, Wiz, Check Point Software Technologies, Lacework, Sysdig, and Microsoft (Security) as Innovation leaders in this Radar analysis. Of these vendors, CrowdStrike, Wiz, and Check Point Software have significantly improved their Innovation index scores. In contrast, Microsoft first appears in this year's Radar assessment.
- CrowdStrike demonstrates comparable capabilities to other Innovation leaders with its unified cloud security platform and single lightweight agent, delivering strong runtime protection and the ability to integrate with its XDR platform and MDR services. Its recent acquisition of Bionic, an application security posture management company, is evidence of its commitment to continuous innovation advancements.

Source: Frost & Sullivan

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 & SULLIVAN

Companies to Action:

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

Company to Action: CrowdStrike

Innovation

- CrowdStrike offers a unified CNAPP platform with its Falcon Cloud Security portfolio that provides CIEM, CWPP, container security, IaC security, and CSPM with KSPM feature, offering robust capabilities for managing and securing cloud infrastructure, VMs, apps, containers/Kubernetes (K8s) environments as well as on-premises workloads.
- The platform uses behavior analytics technologies for non-malware threat and fileless attack detection to help businesses detect and prevent cloud misconfigurations, ensure compliance, manage, and protect hosts, VMs, applications, containers/Kubernetes through early vulnerability identification, threat detection and response, runtime protection, and compliance enforcement.
- The solution integrates seamlessly with all major CSPs, which enables extended protection and facilitates cross-platform XDR capability by using a single agent across different environments and many partner applications, reducing agent proliferation, which makes the platform completely unified and easy to manage.

Source: Frost & Sullivan

Company to Action: CrowdStrike (continued)

Innovation

- CrowdStrike rolled out key updates for its platform recently, including IaC support for major CSPs and K8s, 1-click deployment of sensor, agentless snapshot scanning, attack path visualization for legacy environments (on-premises and cloud VMs), drift prevention for container, automated remediations, cloud threat hunting, custom policies, and an enhanced CSPM compliance dashboard for entire cloud.
- The company aims to strengthen its platform using a clear roadmap, such as expanding attack path visualization for containers, serverless function vulnerability analysis, extension of CSPM cloud compliance, and agentless snapshot for malware detection. In addition, the acquisition of Bionic, an application security posture management (ASPM) vendor, will help the company further strengthen the platform and provide protection across the entire CNAPP stack.

Source: Frost & Sullivan

Company to Action: CrowdStrike

Growth

- CrowdStrike has maintained an impressive growth momentum over the last few years, becoming one of the fastest-growing and largest players in terms of revenue in the market. In 2023, CrowdStrike's CNAPP business registered a robust YoY growth of 41.2%, significantly faster than the total market growth average, enabling it to increase its market share and solidify its position as the fourth largest CNAPP player in the market, with a significant market share of 8.2% of the pack.
- As one of the fastest-growing cloud-native endpoint security vendors with an extensive channel partner ecosystem (including GSIs, MSSPs, and CSPs), CrowdStrike cross-sells and upsells its cloud security solutions to large businesses in multiple verticals to maintain a strong growth momentum.
- CrowdStrike has secured deals with prominent customers across multiple industries, including BFSI, tech, H&M, media and entertainment (M&E), and retail/eCommerce. The recent change from a modular approach to combining all CNAPP capabilities into one single license makes it easier for customers to scale to suit their needs per the changes in their cloud environments. This is expected to enable CrowdStrike to maintain the robust growth of its cloud security business in the next few years.

Source: Frost & Sullivan

Company to Action: CrowdStrike

Frost Perspective

- CrowdStrike's cloud security sales have grown rapidly in recent years. Frost & Sullivan acknowledges its sustained growth momentum, extensive customer base from XDR/EDR offerings, and robust channel partner ecosystem as the main contributors to its success.
- The inclusion of endpoint security, incident response, security assessment, and MDR and Cloud Threat Hunting services enable customers to extend protection from endpoint to the cloud with excellent support, enhance customer confidence, and improve the overall solution experience, setting CrowdStrike apart from competitors.
- CrowdStrike's roadmap prioritizes user experience, cloud service coverage expansion, and pre-deployment risk assessments to help organizations streamline operations, increase visibility into adversary attack paths, and foster collaboration between security teams and application developers. These enhancements should enable CrowdStrike to maintain its competitive edge in the cloud security market.

Source: Frost & Sullivan

Company to Action: CrowdStrike (continued)

Frost Perspective

- Though the recent acquisition of Bionic helps CrowdStrike expand its capabilities to manage risks at the application stack, we look forward to seeing how the acquisition will further accelerate its ability to deliver capabilities such as application code vulnerability scanning and SCA to make its platform more comprehensive and compelling. At the same time, CrowdStrike should enhance its targeted GTM strategy and educational campaign with local and regional partners to boost its cloud security perception and business, as many of these still focus on its endpoint security solutions.

Source: Frost & Sullivan

FROST & SULLIVAN

Key Takeaways

Key Takeaways

1

As CNAPP is a new concept, vendors mainly focus on innovation to strengthen their platform capabilities to gain traction and competitive advantages. However, as CNAPP is still seen as an intrusive concept as it cuts across many existing technologies, such as application security testing, EDR, CSPM, and workload runtime protection, organizations may find it difficult or unnecessary to adopt the entire concept overnight. As a result, organizations should develop a practical strategy to build CNAPP in phases according to their actual situation. This requires CISOs to consider their current and future IT architecture and strategy changes extensively and assess if CNAPP satisfies them. From a vendor perspective, they should also focus on capabilities to help organizations address their challenges in a practical and affordable manner.

2

The CNAPP market is nascent, but increasingly competitive, putting more pressure on vendors to maintain their competitive edge with technology innovations and GTM strategies. Vendors need to strengthen their channel partner programs with a more proactive and targeted approach to help end users tackle cloud security concerns and stay competitive. As confusion and concerns regarding the capabilities of local channel partners persist, strengthening these capabilities is crucial for vendors to remain relevant in the market.

Source: Frost & Sullivan

Key Takeaways

3

As CNAPP is a holistic yet intrusive concept, choosing a CNAPP solution needs to involve many stakeholders, including application developers, cloud builders, operations, and security teams. Organizations need to balance and consider the true values that the platform can deliver with extensive consideration of technical and business aspects, prioritizing real-time detection, forensic visibility, innovation, competitive advantage, operational stability, security performance, compliance, and costs.

Source: Frost & Sullivan

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.

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