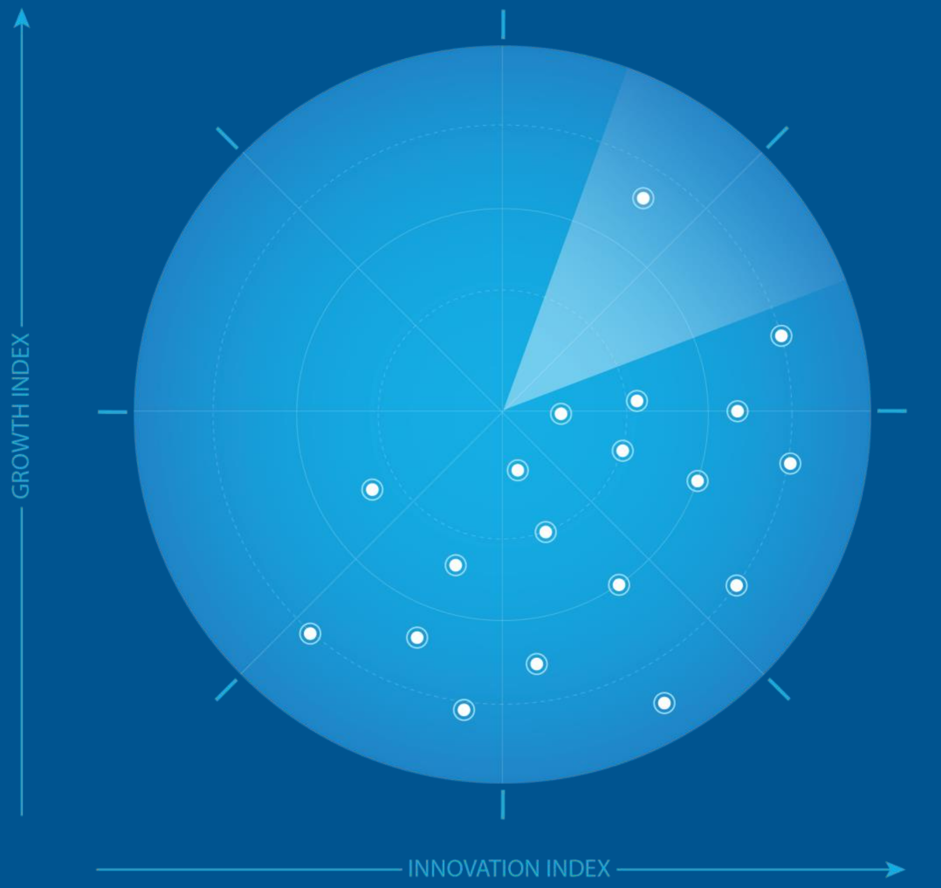
FROST & SULLIVAN

Frost Radar™: Cloud Workload Protection Platforms,2023

Authored By: Anhtien Vu

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



August 2023

Strategic Imperative

- The adoption of cloud workload protection platforms (CWPPs) is rapidly increasing as more organizations migrate their workloads to the cloud, embrace cloud-native technologies, and accelerate cloud IaaS spending growth. The need for real-time threat detection and response and better vulnerability management requires organizations to implement CWPP to address these challenges when other cloud security solutions, such as cloud security posture management (CSPM) and other legacy security solutions, fail.
- A CWPP, normally agent-based, is a server workload-centric security solution to protect computing workloads in cloud environments (private, public, hybrid, and multi-cloud) from cybersecurity risks and attacks regardless of the workload's location. CWPP secures typical workloads, including cloud hosts, virtual machines, containers, K8s, databases (SQL and NoSQL), and APIs. CWPP is typically integrated with other solutions to create a holistic approach to protect the cloud-native environment, such as CSPM, cloud infrastructure entitlement management (CIEM), cloud network security, and DevSecOps tools.
- The need for consolidation and cost savings has led organizations to evaluate their security stack and pursue best-in-breed platforms that deliver ROI. Overall, the need for effective and efficient security solutions will continue to drive demand for CWPP.

Source: Frost & Sullivan

Strategic Imperative (continued)

- Key capabilities of a typical CWPP solution should include the following:
    - Detection and prevention of threats to the host, virtual machines, and containers at runtime, with features such as malware scanning, workload behavior monitoring, and endpoint/network detection and response (EDR/NDR)
    - Container image vulnerability management in the continuous integration/continuous delivery (CI/CD) process
    - Micro-segmentation of workloads across the network, micro-services, and API levels
    - Management of serverless permission and performing serverless template scanning for template drift
    - Checks to ensure container compliance
    - Workload assurance maintenance with system/file integrity monitoring (SIM/FIM)
    - Runtime forensics analysis and incident response for workloads (specifically K8s and containers)
- In many cases, organizations leverage CWPP solutions to secure workloads from code to cloud, whether they are running on public, private, hybrid, or multi-cloud environments and address core use cases of pre-deployment security/shift-left security for container images, machine images, and IaC templates for better vulnerability management across workloads, repositories, CI/CD, and code. This shift-left approach to security enables organizations to automate remediation and reduce their exposure to supply chain attacks.

Source: Frost & Sullivan

Strategic Imperative (continued)

- Nonetheless, the complexity of hybrid and multi-cloud environments, along with expanding attack surfaces and security operation challenges, necessitate an integrated, cloud-native security platform (CNAPP). This drives more integration between CWPP and other cloud security technologies, including CSPM/KSPM, CIEM, and Web Application Firewall and API Security (WAAF).
- Additionally, customers seek risk-based approaches that provide context to prioritize their efforts and increase visibility into application vulnerabilities, threats, malware, and secrets associated with their software bill of materials (SBOM), which provides organizations with visibility, control, and protection, securing modern cloud computing architectures such as virtual machines, containers, Kubernetes, and serverless environments. It also facilitates the integration of security into the software development life cycle and helps organizations effectively handle compliance requirements.

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, most 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 also align with adopting other cloud security solutions, including CSPM, SaaS security posture management (SSPM), (CIEM), and CNAPP.
- In 2022, the global CWPP market recorded revenue of $3049.0 million, representing a year-over-year growth of 47.9%. Frost & Sullivan projects that momentum to continue at a compound annual growth rate of 26.3% from 2022 to 2027, with revenue reaching $9,800.9 million in 2027 because of the increasing demand for runtime protection and automated threat response.

Source: Frost & Sullivan

Growth Environment (continued)

- Despite potential economic slowdowns and uncertainty impacting organizations' IT and infrastructure spending, cloud security and CWPP investments are expected to persist in the long term. CWPP will be integrated into CNAPP, reducing the complexity and costs associated with macroeconomic challenges for organizations.
- Macroeconomic issues may encourage many organizations and industries to continue migrating workloads to multi-cloud and hybrid environments. The increased migration will subsequently lead to a heightened focus on security investment as cybersecurity risks associated with these environments increase.
- More robust adoption of CWPP is also attributed to a growing trend of more board-level conversations regarding shift-left and software supply chains, indicating an increased awareness of the importance of these areas for cloud security. Discussions on cloud identity management and understanding least privilege as a method of mitigating risk and a vital element of a Zero Trust strategy are also becoming more frequent.

Source: Frost & Sullivan

Growth Environment (continued)

- Additionally, there is a greater realization of a time gap between vulnerability disclosure and remediation (patching), making runtime detections a critical element for overall cloud security. More importantly, the increase in cloud-native workloads, replacing older lift-and-shift workloads, requires organizations to embrace better serverless computing, containers, and K8s across cloud providers and platforms (OpenShift, Tanzu), which will drive investment in cloud-native security.
- However, the lack of understanding of cloud-native security technologies and their benefits may hamper growth in the short term. Concerns over the total cost of ownership (TCO), low performance, loss of control and visibility, and legal and compliance issues may force organizations to repatriate from the cloud or make them hesitant to migrate to the cloud, dampening future growth of the platform. Like other cloud security projects, the lack of in-house expertise and awareness of application modernization will cause hesitancy in adopting CWPP.
- The Russo–Ukrainian war can negatively impact global cybersecurity budgeting and short-term cloud security spending. Frost & Sullivan's Voice of Customer for Security showed that 62% of organizations saw an impact from the war on their security budget.

Source: Frost & Sullivan

Growth Environment (continued)

- While CWPP solutions can be costly, the lack of technical security controls can also result in substantial expenditure in the long term. Integration with other security tools and processes is necessary for effective use, although it can increase the overall complexity of the security architecture. Managing multiple cloud providers with varying protection levels, inconsistent policies, and fragmented logging/reporting systems pose a challenge to in-house security teams, hindering their ability to prioritize issues and resulting in wasted time and missed critical alerts.
- The acute talent shortage in security and cloud becomes even more challenging with a reduced workforce, causing security teams to be overworked. This results in a struggle to protect workloads in the software lifecycle and continued difficulty for businesses to find qualified personnel to manage and maintain CWPP solutions.
- Moreover, organizations may face complications when implementing CWPP solutions due to compliance regulations, such as GDPR or HIPAA. Some CWPP solutions may also adversely impact system performance, increasing compute costs and decreasing user experience.

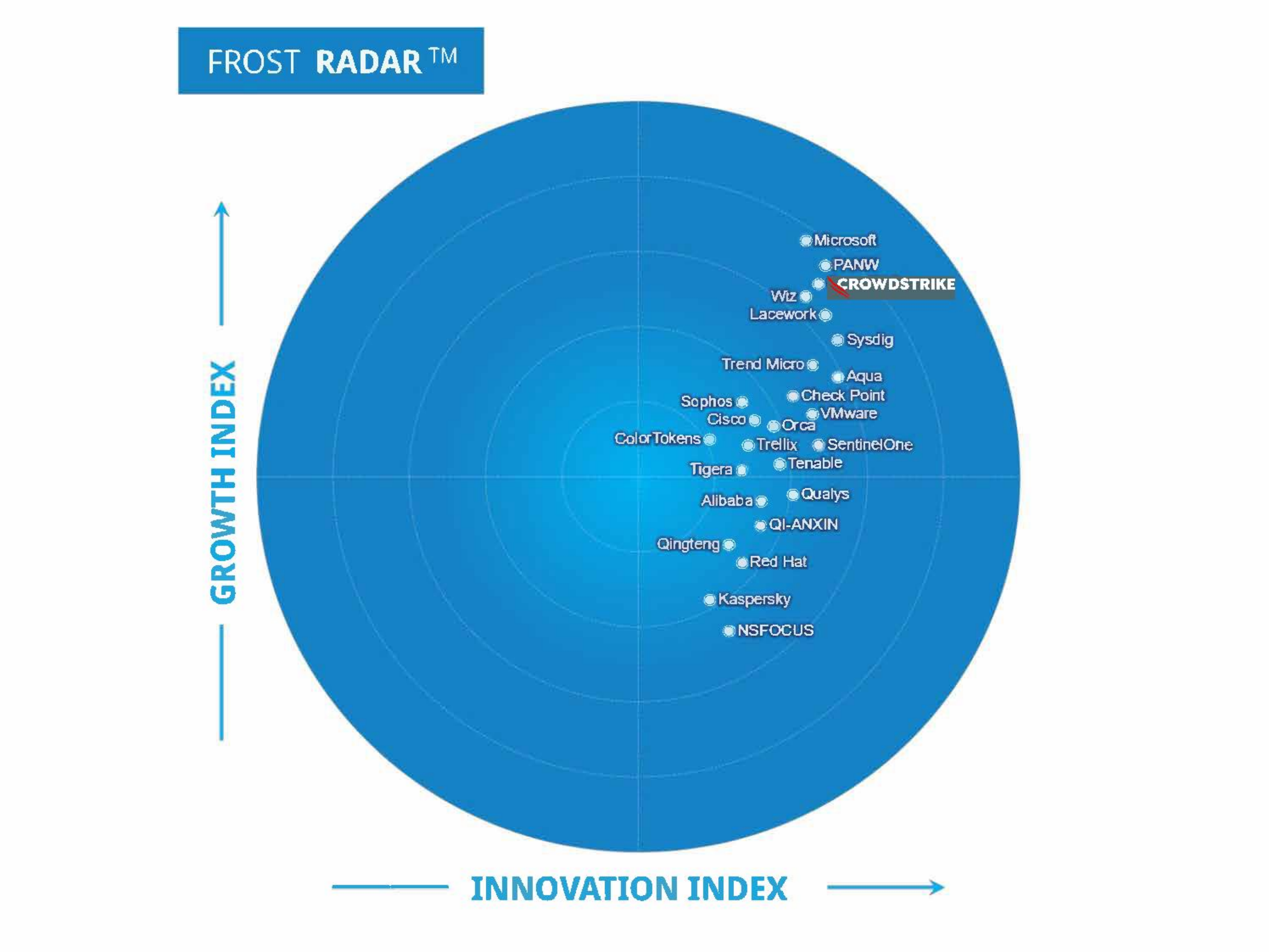
Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™

Cloud Workload Protection Platforms, 2023

Frost Radar™: Cloud Workload Protection Platforms, 2023



Source: Frost & Sullivan

Frost Radar™

Competitive Environment

- The CWPP market is highly fragmented, comprising cloud service providers (CSPs), traditional network and endpoint security vendors, vulnerability assessment vendors, and start-ups specializing in cloud security. More than 50 vendors compete in the CWPP space globally. Frost & Sullivan independently plotted the top 25 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 must meet the following requirements:
    - Recorded an annual revenue of at least $20 million in 2022
    - Have a CWPP business history for at least three years (2020, 2021, and 2022)
- Vendors that met the criteria for inclusion in the Frost Radar but could not share detailed insights into their solution were excluded to ensure fair scoring and comparison.
- This Frost Radar features 25 vendors: Alibaba Cloud, Aqua Security, Check Point, Cisco, ColorTokens, CrowdStrike, Kaspersky, Lacework, Microsoft, NSFOCUS, Orca Security, Palo Alto Networks, Qi-AnXin, Qingteng, Qualys, Red Hat, SentinelOne, Sophos, Sysdig, Tenable, Tigera, Trellix, Trend Micro, VMware, and Wiz.

Source: Frost & Sullivan

Frost Radar™

Competitive Environment (continued)

- Other companies are entering the market with different capabilities and approaches, mostly start-ups; Frost & Sullivan identified these companies as the powerhouses dominating and shaping the CWPP market for now.
- As the market evolves, more large cybersecurity companies and cloud security start-ups are expected to emerge. Moreover, growing multi-cloud support requirements will likely prompt more cloud service providers to offer capabilities supporting multiple cloud environments in the future instead of only supporting their cloud platform.
- Frost & Sullivan predicts a growing trend toward consolidation, with further acquisitions and mergers expected. This will likely lead to fewer yet more robust options for organizations, as larger vendors with more resources can better provide comprehensive solutions that meet the needs of their customers.
- The anticipated increase in the adoption of CWPP solutions over the next five years is attributable to several factors. First, increased cloud IaaS spending drives the need for robust security measures to protect cloud environments. Second, a heightened awareness of cloud attack vulnerabilities and the growing accountability of CISOs and their teams contribute to the demand for comprehensive cloud security solutions. Third, the prevalence of multi-cloud, hybrid cloud, and containerized environments in modern application development exacerbates security challenges by creating visibility and control gaps within the supply chain. This, alongside the tendency to shift security responsibilities to developers, necessitates effective CWPP solutions.

Source: Frost & Sullivan

Frost Radar™

Competitive Environment (continued)

- From an economic standpoint, short-term economic uncertainties across different regions impact the adoption of cloud security, including CWPP solutions. Due to high-interest rates and inflation, businesses are hesitant to spend, resulting in reduced cash flow and capital. Consequently, many customers are deferring purchases to mitigate economic uncertainty. However, in the long term, cost-saving motivations drive organizations to migrate to the cloud, presenting opportunities for cloud security solutions to flourish.
- 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. Conversely, global CISOs increasingly recognize the need to secure cloud environments, prevent breaches, and protect corporate data. They prioritize return on investment (ROI) and seek best-in-breed solutions offering value to ensure wise spending practices.
- Consolidation and convergence will become mainstream in the next few years as organizations focus more on streamlining security operations to reduce TCO and increase efficiency. Organizations seek broader capabilities to provide them visibility and security from build to production and across DevOps, DevSecOps, and cloud infrastructure.

Source: Frost & Sullivan

Frost Radar™

Competitive Environment (continued)

- This creates more requirements for CNAPP solutions covering the entire stack (code, application, workload, and infrastructure) to help them achieve a holistic security strategy and reach a zero-trust security state across different cloud environments. As a result, advanced capabilities such as API Security, shift-left security, CIEM, and DSPM, are important value-adds for CISOs.

- CrowdStrike stands out in the Growth Index for its impressive and consistent growth over the past 3 years, surpassing larger competitors like Trellix, Cisco, Check Point, Sophos, and VMware. Frost & Sullivan acknowledges CrowdStrike's strong customer base, excellent brand perception, and a focused strategy on cloud security, positioning the company for robust growth in its cloud security business, including CWPP, CSPM, CIEM, and CNAPP, and enabling it to capture additional market share. From an innovation standpoint, CrowdStrike demonstrates comparable capabilities to other Innovation leaders, such as PANW and Lacework, with its strong runtime protection, integration with its XDR platform, and MDR services.

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

Companies to Action: CrowdStrike

INNOVATION

- CrowdStrike's CWPP, an integral part of its CNAPP platform, offers robust capabilities for managing and securing virtual machines, applications, and containers/Kubernetes (K8s) environments. The solution effectively safeguards workloads from potential risks by providing early vulnerability identification, TDR, runtime protection, and compliance enforcement.
- One of its key strengths lies in its ability to deliver comprehensive visibility into workloads, containers, serverless workloads, and hosts, empowering businesses to uncover hidden threats, address misconfigurations, and mitigate exploitable vulnerabilities proactively. By leveraging behavior analytics, CWPP effectively detects non-malware threats and fileless attacks, bolstering the security posture of cloud workloads and applications, including vulnerabilities in running containers.

GROWTH

- CrowdStrike has emerged as one of the fastest-growing cloud security vendors, fueled by its XDR/EDR and MDR solutions. The company's focus on the cloud security market has contributed to its global traction.
- In 2022, CrowdStrike's CWPP business registered impressive YoY growth of 108.9%, solidifying its position as a leading cloud-native endpoint and workload security vendor. North America continued to lead its global CWPP business, accounting for a significant portion of its total revenue, while EMEA and APAC made notable contributions.
- Supported by a robust channel partner ecosystem, CrowdStrike is well-positioned to sustain its growth trajectory by effectively cross-selling and upselling cloud security modules to large businesses across various verticals.

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.
- Including IR, assessment, MDR, and Cloud Threat Hunting services sets CrowdStrike apart from competitors, enhancing customer confidence and improving the overall solution experience.
- To strengthen its cloud security offerings, including the CWPP/CNAPP solutions, CrowdStrike should explore diversifying use cases beyond CWPP by incorporating capabilities such as vulnerability scanning.

Source: Frost & Sullivan

Companies to Action: CrowdStrike (continued)

INNOVATION

- In addition, the solution integrates seamlessly with all major CSPs, which enables extended protection and facilitates cross-platform XDR capability. Its recent enhancements, including automated remediations, cloud threat hunting, custom policies, and asset inventory for CSPM, demonstrate CrowdStrike's commitment to continuously improving its solution and addressing evolving security challenges.

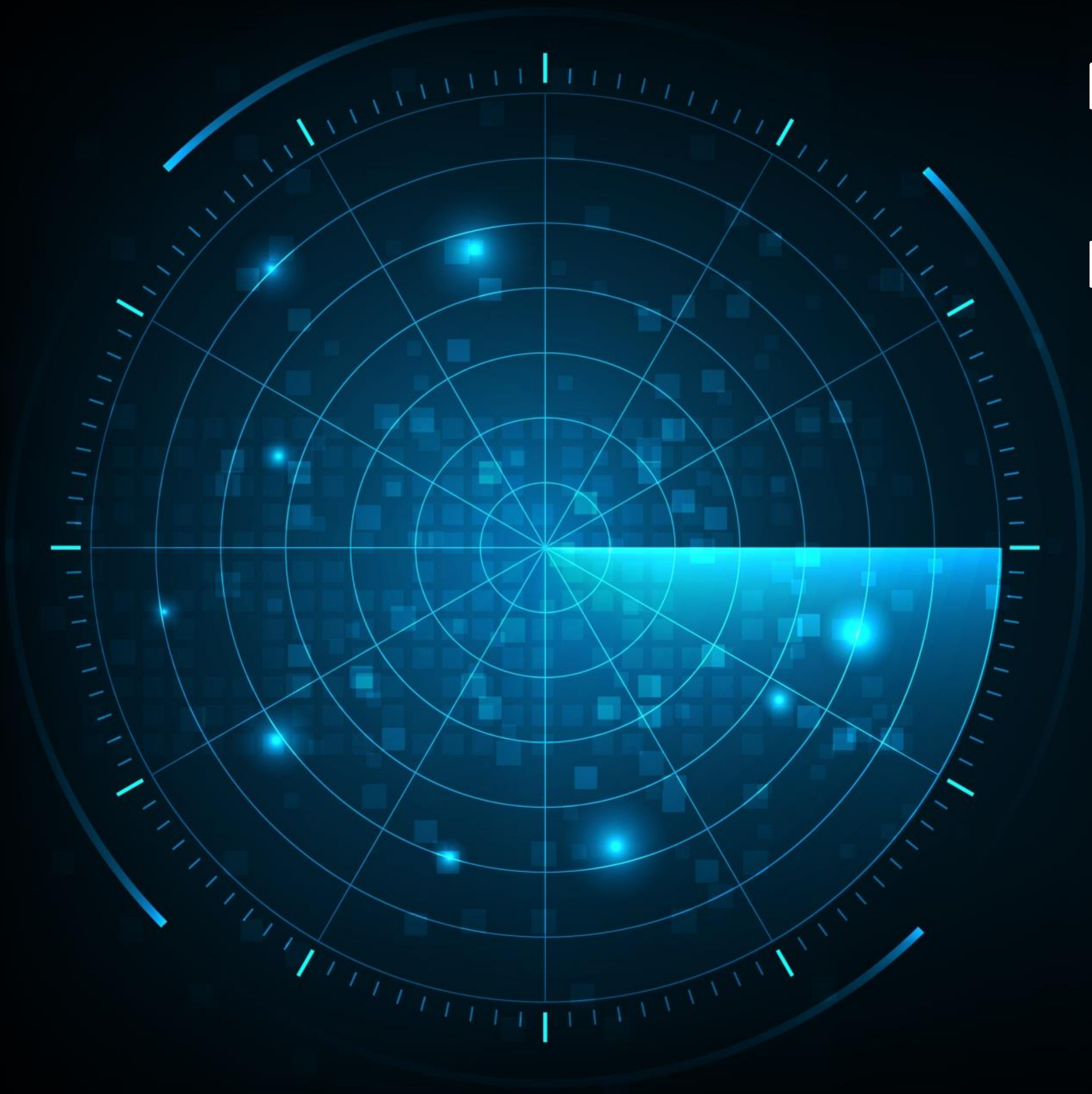
GROWTH

- The ability to cross-sell and upsell its cloud security modules has driven this success. CrowdStrike has secured deals with prominent customers across multiple industries, including BFSI, tech, H&M, media and entertainment (M&E), and retail/eCommerce. Compliance requirements, particularly for customer-facing workloads, have catalyzed adoption in these verticals, emphasizing the need for robust runtime protection.

FROST PERSPECTIVE

- CrowdStrike's roadmap prioritizes user experiences, 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



Frost Radar™

Key Takeaways

Key Takeaways

1 The CWPP market is highly competitive and fragmented, featuring established security vendors, cloud service providers, and start-ups. This dynamic landscape offers organizations access to affordable and innovative solutions for their cloud security needs. However, it also pressures existing vendors to maintain their competitive edge through technological advancements and pricing strategies.

2 Participants in this market must focus on R&D and M&As to strengthen their platform capabilities, gain market traction, and find ways to reduce the TCO while improving customer support and experiences.

3 In many cases, the current channel partner ecosystem often prioritizes traditional network and endpoint security, leading to a lack of focus and expertise in cloud security. This affects vendors' success and hampers market growth. To address this, vendors must enhance their channel ecosystem capabilities with a more proactive and targeted approach to help end users tackle cloud security concerns and stay competitive.

Source: Frost & Sullivan

Key Takeaways (continued)

4

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.

5

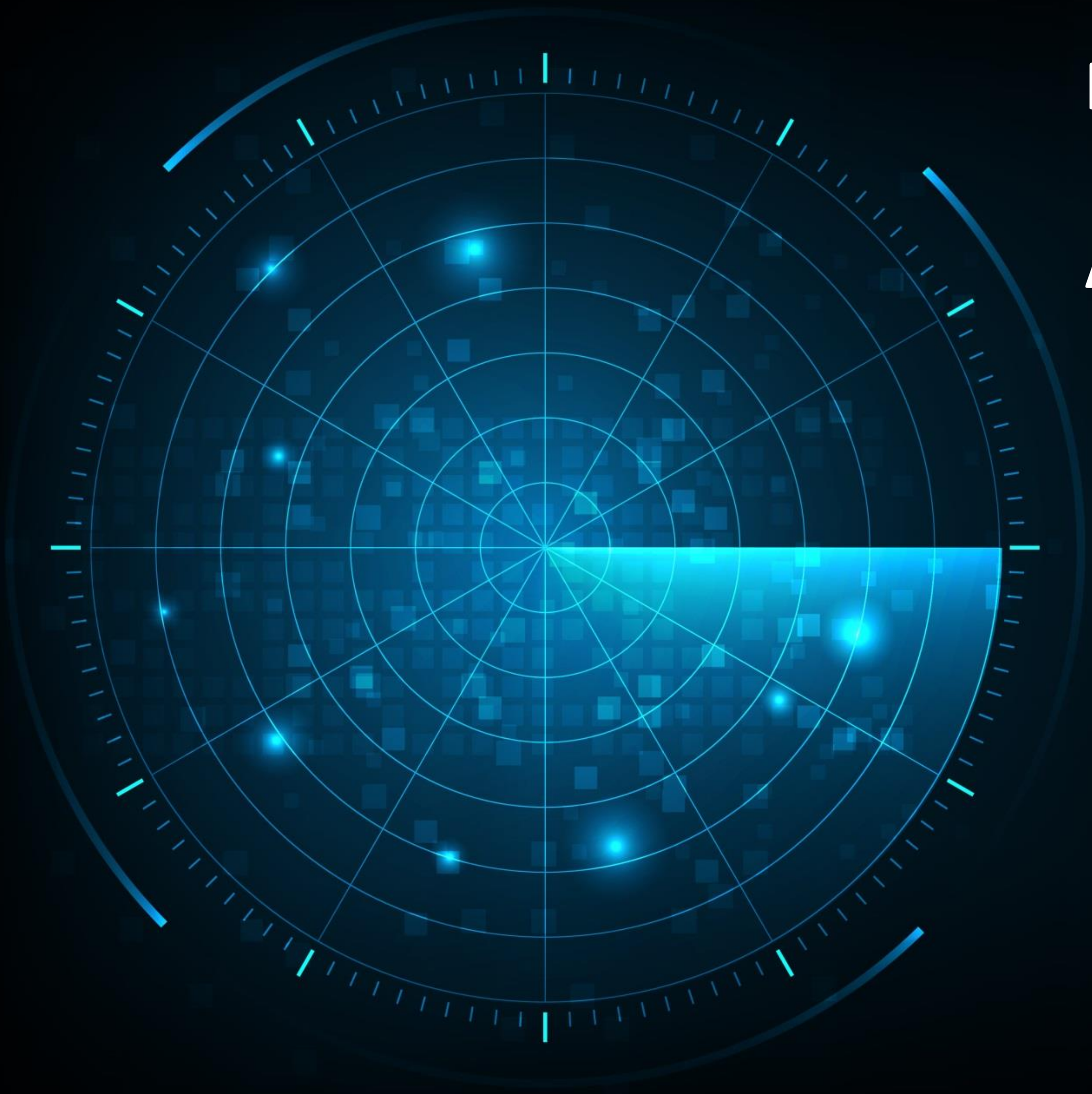
CISOs increasingly face greater challenges integrating CWPP within a comprehensive cloud-native security framework. As a result, they must consider technical and business aspects, prioritizing real-time detection, forensic visibility, innovation, competitive advantage, operational stability, security performance, compliance, and value realization.

6

CISOS must optimize the utilization of existing products, services, and resources to maximize benefits and make the most of their licensing arrangements. This will help them effectively align CWPP with their overall security strategy and achieve enhanced security posture and operational efficiency.

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