FROST & SULLIVAN

Frost Radar™: Cloud Workload Protection Platforms, 2024

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

Authored by: Anh Tien Vu

August 2024

Strategic Imperative

- The accelerated adoption of cloud services and cloud-native application development technologies, coupled with stringent compliance requirements from regulated industries, is driving increased spending on cloud security technologies, including CWPP and CSPM.
- Simultaneously, the growing trend towards DevSecOps is deepening the integration of CWPP and CSPM with the CI/CD pipeline to enable automated security and compliance checks, as this integration provides granular visibility into the entire application development lifecycle. As a result, shift-left and shield-right security practices have become more effective in addressing security risks proactively. The increasing sophistication of cloud threats is driving the need for modern CWPP solutions with advanced capabilities, such as AI/ML, cloud detection & response (CDR), workload runtime protection, and identity and data security for effective threat detection and automated remediation across cloud layers.
- This, along with the growth of cloud spending, better awareness of the cloud threat landscape, and heightened accountability of CISOs and their teams, will drive CWPP adoption over the next 5 years. The trend is also fueled by the increasing use of multi-cloud, hybrid-cloud, and containerized environments in modern application development, which exacerbates inherent cloud security challenges that create gaps in visibility and control in the supply chain.
- Demand for CWPPs to protect workloads in the Infrastructure-as-a-Service (IaaS) environment, especially host-based or agent-based solutions, remains high as they provide greater visibility and improved vulnerability and runtime protection. As virtual machine (VM)-based workloads are gradually displaced by containers, the need for container security integrated with CWPP solutions, such as visibility into K8s environments and protection for container images and application components in CI/CD pipelines, will increase.

Source: Frost & Sullivan

Strategic Imperative (continued)

- A CWPP, which is 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. Typical workloads that CWPPs secure include cloud hosts, VMs, containers, K8s, databases (structured query language [SQL] and NoSQL), and application programming interfaces (APIs).
- The requirements of CWPP tools have evolved over the last few years and continue to develop, reflecting the changes in the approach to cloud security with a greater focus on real-time risk/threat management and runtime protection solutions.
- Key features required of a CWPP tool include:
  - **Workload discovery and continuous monitoring** for newly added environments and workloads.
  - **Comprehensive and real-time visibility.** CWPP solutions must support hybrid and multi-cloud deployments, spanning on-premises and public cloud platforms, such as Amazon Web Services, Microsoft Azure, Google Cloud, Alibaba Cloud, and Tencent Cloud, protecting modern workloads across various environments, including VMs, containers, and K8s. It must also provide contextual visibility and risk prioritization to help customers prioritize risks, focus on the most critical security issues, and reduce management and monitoring overheads.
  - **Vulnerability management.** CWPP must provide vulnerability management of workloads and applications across various environments, registries, and CI/CD processes to ensure secure code deployment. Drift prevention for workloads is also required to ensure they comply with security policies. It also needs to offer automated mapping to pre-built compliance frameworks, policies with minimal performance impact, and context-based risk prioritization capabilities to help teams prioritize the most critical security issues.

Source: Frost & Sullivan

Strategic Imperative (continued)

- **Runtime protection and advanced TDR.** This includes runtime protection with real-time application control, file integrity management (FIM), and malware detection to prevent unauthorized access or changes; integration with CDR for real-time TDR to minimize the impact of security incidents, particularly threats associated with sensitive data, vulnerability, and compliance; anti-malware and behavior-based monitoring to protect customers' workloads from malware and monitor their workloads' behavior to detect anomalies and threats; investigation and forensics to provide information to help customers understand the nature and impact of security incidents and remain in compliance with security policies; microsegmentation for workloads to enhance network security as well as capabilities to visualize cloud-native network traffic; automatic security processes and continuous monitoring to detect unusual behavior and provide deep insight into potential detection; and automated correlation of multiple detections from multi-source signals to create highly contextual alerts.
- **Automated reporting and compliance.** This includes automated response and robust reporting capabilities with visibility and control through a graph-based visualization for a better understanding of security posture and threats, and continuous compliance assessment and management, including CIS benchmarks and compliance assessment of K8 control planes.

- In many use cases, a CWPP is integrated with other cloud and application security solutions, such as CSPM, cloud infrastructure entitlement management (CIEM), web application firewall and API protection (WAAP), CDR, AppSec, software supply chain security, and other developer security tools, to create a holistic approach to protect the cloud-native environment. Organizations also evaluate CWPP tools by considering solution capabilities, stability, scalability, management needs, and ROIs.
- Choosing the right CWPP must align with the organization's security needs, operational efficiency, compliance requirements, and budget. A CWPP solution should be able to offer the following:

Source: Frost & Sullivan

Strategic Imperative (continued)

- **Integrability.** As silos in cloud security are broken down, customers expect CWPP solutions to integrate seamlessly into a broader cloud-native application protection platform (CNAPP). This integration ensures comprehensive risk management across different tools and other security areas, supporting the entire cloud security strategy within a unified platform. Companies increasingly look to reduce management complexity by consolidating multiple security tools into a single platform to simplify security management and enhance their ability to respond to threats across disparate environments more effectively.
- **Cloud-agnostic features for integration with third-party tools.** Prioritizing a cloud-agnostic CWPP tool that offers seamless visibility and protection across different cloud infrastructures will maintain consistent security postures. CWPP tools must operate and provide consistent functionality, features, and capabilities across various cloud platforms (e.g., AWS, Azure, Google Cloud), enabling seamless security management regardless of the cloud service provider (CSP).
- **Real-time visibility, risk prioritization and mitigation.** CWPP needs to be compatible with organizations' cloud environments and cover multiple cloud providers. CWPP solutions must support hybrid environments and offer real-time visibility into active cloud risks, including configuration vulnerabilities, identities, and workloads. Effective CWPP must provide risk prioritization and mitigation capabilities so that security teams can clearly quantify and report risks, helping them remediate the highest priority threats based on the criticality of cloud resources.
- **Comprehensive protection coverage.** As CWPP solutions are converging with other solutions to include more than just traditional cloud workload protection, customers and prospects need to consider vendors' strategic vision and roadmaps. When making purchasing decisions, it is important to consider current offerings and short- and long-term plans to ensure that the platform can continue to meet the growing demands of all teams involved in cloud-native security.

Source: Frost & Sullivan

Strategic Imperative (continued)

- **Support for rapid innovation and business requirements.** CWPP must accommodate rapid changes in cloud environments and the adoption of new technologies without compromising security. They should support modern DevOps workflow and container/K8s and CI/CD pipeline tools to empower organizations to adopt a shift-left security approach. Effective CWPP solutions support business operations by fostering collaboration between security and development teams, enabling the balance between development and security requirements, and ensuring faster time-to-market for products and services.
- **Scalability and ease of use.** Scalability is critical for handling large-scale cloud deployments, ensuring performance, resource utilization, and cost efficiency. Ease of adoption and user-friendliness are essential to encourage the use of CWPP solutions. Customers require intuitive and integrated solutions to bridge the skills gap in handling security challenges in the cloud and cloud-native environments. Solutions that offer managed services, such as 24/7 managed detection and response (MDR) and cloud threat hunting, are particularly attractive to organizations lacking in-house expertise.
- **ROI.** Organizations desire CWPP tools that can deliver quick and measurable returns. Key elements contributing to ROI include ease of use, speed of deployment, and the ability to integrate seamlessly across multi-cloud and hybrid environments. Organizations evaluate tools that provide accurate responses based on real-world threat intelligence and close the skills gap through intuitive platforms or managed services. Effective CWPP solutions help reduce the time and cost of remediating threats, accelerate time-to-market for products and services, and minimize the business, financial, and legal impact of breaches.

Source: Frost & Sullivan

Strategic Imperative (continued)

- The future of CWPP is being shaped by the evolution of the threat landscape and business requirements, organization readiness, and cloud and security maturity models, among other factors. Frost & Sullivan believes the future of CWPP will be characterized by the following:

  - **Consolidation towards CNAPP.** Customers are seeking a broader set of capabilities that cover them from build to production and tightly integrate security capabilities, information, and access across DevOps, DevSecOps, cloud infrastructure, and platform and security teams. CWPPs will increasingly see integration into CNAPPs, which, in turn, will be integrable with other platforms, including extended detection and response (XDR), secure service edge (SSE)/secure access service edge (SASE), and security analytics platforms, to provide comprehensive security coverage across the entire stack at the infrastructure, workload, and application and the network levels to achieve a zero-trust state. This process will drive greater demand for customization options that allow organizations to tailor their solutions to their specific needs. This is especially true for XDR integrations, which can help enrich CWPP-centric telemetry with other solution data. This integration can help organizations gain a more complete view of their security posture and respond more effectively to threats.

Source: Frost & Sullivan

Strategic Imperative (continued)

- **Deeper integration with CDR.** CDR capabilities as a subset of CNAPPs can work alongside CWPPs to provide comprehensive cloud security. With the rise of cloud threats, organizations must have breach detection and incident response capabilities that can help them identify and respond to cloud-based attacks. Agentless CDR solutions can offer pre- and post-breach telemetry analysis, which can enhance visibility and accelerate incident response. As SecOps teams grapple with an ever-increasing volume of security incidents and alerts, they need a unified approach to detect and respond to threats that can impact cloud-native architectures. CWPPs and CNAPPs can provide the necessary guidance to security analysts, helping them integrate with other organizational systems to enable digital forensics and incident response. Continuous monitoring and behavior-based threat detection, which are important CNAPP and CDR features, can help organizations scale their security efforts. This approach is important in the cloud, where traditional solutions are often inadequate and cannot keep up with the evolving threats. CWPP solutions can work with CDR solutions to provide a comprehensive and effective security strategy for cloud workloads.
- **Greater focus on risk management and risk prioritization.** As organizations adopt CWPP solutions for securing their cloud workloads, risk management becomes an important point of focus for SecOps teams to avoid wasting time on low-risk events. CWPPs will evolve as part of CNAPPs to calculate composite risk values from multiple alerts on the same or neighboring cloud systems, considering the business priorities of specific systems. The ability to aggregate and correlate risk across various sources, including declarative files, pre-deployment artifacts, and live production workloads, will become a differentiator for cloud security tools, including CWPPs. These tools should go beyond vulnerability prioritization and incorporate compliance, threat detection, and other areas of concern to provide a holistic view of the risk posture. CWPPs' alert and risk prioritization features will become more important in helping SecOps teams quickly identify and respond to high-risk incidents.

Source: Frost & Sullivan

Strategic Imperative (continued)

- **Increasing adoption of AI/ML to increase TDR and streamline security operations.** As the threat landscape continues to evolve, organizations are seeking advanced solutions to detect and respond to threats in real time. This includes automating security workflows, such as incident response, and using orchestration to better manage security policies and configurations. Many CWPP solutions are leveraging AI/ML-powered security solutions to enhance their TDR capabilities. Adopting AI/ML will also improve the ability to prioritize and address risks, which, in turn, will enable SecOps teams to focus on the most critical issues by evaluating multiple alerts simultaneously and aggregating risk assessments. This is especially crucial for managing the increasing volume of security data and alerts in cloud environments, as it helps analyze risks and provide contextual recommendations. AI/ML enables organizations to quickly and efficiently identify and mitigate security incidents, which is essential in today's fast-paced digital environment. The adoption of automation for remediation and runtime prevention is increasing, especially for workloads containing sensitive data or critical applications. This approach streamlines SecOps and reduces the risk of cyberattacks. The trend of integrating AI/ML-powered security solutions and increasing automation for remediation and runtime prevention will continue in the CWPP sector as organizations seek to secure their cloud workloads and protect against evolving cyber threats. In addition, natural language processing (NLP) and natural language models will play a crucial role in making cloud security management tools more user-friendly and accessible as they help teams interact with cloud security tools using natural language, making it easier to navigate, configure, and manage security settings, enhancing the user experience.

Source: Frost & Sullivan

Strategic Imperative (continued)

- **Integration with shift-left and supply chain security.** As containerization and serverless computing gain traction, the demand for container-specific security solutions is increasing, and CWPPs' integration with CI/CD pipelines is becoming more common, allowing for continuous security testing and vulnerability scanning throughout the development process. Organizations are focusing on software supply chain security, requiring seamless integration with the DevOps SDLC framework and CI/CD pipeline platforms. Integrating supply chain security with CWPP will involve advanced scanning and monitoring tools that detect vulnerabilities at every stage of the software development process—from initial code writing to production deployment. This protects against vulnerabilities introduced through third-party libraries and open-source software components, enabling organizations to reduce risks and enhance security for containers and the underlying cloud infrastructure. CWPPs have evolved to include application artifact scanning—for example, static AppSec testing/dynamic AppSec testing, API scanning, and software composition analysis (SCA)—during development and testing, runtime behavior analysis, cloud configuration, risk identification, and compliance requirements to ensure a robust security posture throughout the container life cycle.
- **Greater focus on runtime protection despite the prevalence of agentless deployment.** Agentless solutions continue to have the strongest growth because of their high value and low total cost of ownership (TCO). Agentless visibility across cloud infrastructure and workloads will continue as organizations seek to understand what is happening in their cloud environments with the minimal overhead necessary. However, the focus on runtime protection, including behavioral-based detection and response, ML, and AI-powered TDR capabilities, will only increase. The need for these capabilities to protect workloads, particularly those containing sensitive data or critical applications, will continue to drive organizations, especially those mature in their cloud journey, to adopt and deploy agent-based solutions for better real-time TDR.

Source: Frost & Sullivan

Strategic Imperative (continued)

- **Increased focus on compliance automation.** With the increasing importance of data privacy regulations such as General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) of 2018, the focus on compliance management is growing. Organizations must ensure they comply with these regulations, which can be complex and time-consuming, leading to an increase in demand for compliance management tools that can help organizations manage and monitor their compliance activities. With the increasing complexity of compliance regulations and standards, organizations are seeking ways to automate their compliance management processes by integrating CWPP solutions into compliance automation platforms.

Source: Frost & Sullivan

Growth Environment

- Organizations across regions focus on cloud security technologies to help them manage cyber risks better. Based on the recent Voice of Customer for Security survey by Frost & Sullivan of more than 2,360 chief information security officers (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.
- The CWPP sector is set to maintain a robust growth momentum in the next 5 years and generate a total revenue of $11,461.2 million in 2028, representing a CAGR of 23.4% from 2023 to 2028.
- As of 2023, the adoption of CWPP solutions is driven by a combination of regional growth, technological advancements, and the need to address complex cloud security challenges. Despite economic and geopolitical constraints, the increasing sophistication of cloud threats and the need for comprehensive security solutions will continue to propel CWPP adoption.
- Regionally, North America is set to remain the largest adopter of cloud security solutions, including CWPP, primarily due to the strong awareness of container vulnerabilities and other cloud-native technology risks. The mature cloud infrastructure and stringent compliance requirements further drive the adoption rate. APAC has emerged as the second-largest CWPP adopter, driven by strong spending in China and the region's growing cloud presence, which has driven the need for robust security controls. In addition, data localization and sovereignty are also prompting CWPP adoption to meet these demands.

Source: Frost & Sullivan

Growth Environment (continued)

- In Europe, the Middle East, and Africa (EMEA), despite short-term impacts from political and economic factors like the Russo-Ukrainian War, long-term cloud security spending is expected to remain strong. Compliance and data privacy concerns will drive the adoption of cloud security and sustained investment in CWPP solutions. Conversely, adoption in Latin America (LATAM) remains low due to underdeveloped levels of cloud adoption, low awareness, and limited budgets for cloud security projects. Still, as cloud use matures, there may be a gradual increase in CWPP adoption.
- Technologically, the accelerated adoption of cloud services and cloud-native application development technologies, coupled with stringent compliance requirements from regulated industries, drives increased spending on cloud security technologies, including CWPP and CSPM. The increasing use of multi-cloud, hybrid-cloud, and containerized environments is exacerbating inherent cloud security challenges and creating gaps in visibility and control, which prompts organizations to adopt robust cloud security technologies, such as CWPP, to manage these complex environments and provide comprehensive visibility and security protection for their cloud workloads, applications, and data. Particularly, as VM-based workloads are gradually displaced by containers, the need for integrated container security within CWPP solutions is set to grow with the increased focus on visibility into K8s environments, protection for container images, and application components in CI/CD pipelines.
- Organizations face increasing challenges associated with DevSecOps, making it more difficult to achieve a balance between security and innovation in the fast-paced DevOps environment. This requires collaboration between development, security, and operations teams. The increasing focus on shift-left security practices, which focus on addressing security risks proactively during the development phase, drives CWPP adoption to help DevOps and SecOps teams gain visibility and identify vulnerabilities for their container images, machine images, and IaC templates in the pre-deployment stage. This improves vulnerability and risk management, reducing exposure to supply chain attacks.

Source: Frost & Sullivan

Growth Environment (continued)

- Many businesses realize that they must adopt cloud-native security tools and strategies to address these challenges by enabling automation, deep visibility, and the detection of anomalous behaviors and threats across cloud workloads, such as containers, K8s clusters, and serverless functions. In this context, CWPP solutions can provide critical 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 and automated remediation to reduce exposure to supply chain attacks. In a way, the increased CWPP adoption is also driven by more board-level discussions regarding shift-left security and software supply chains, reflecting awareness of the importance of cloud security.
- The need for runtime protection beyond traditional network-based detections and anti-malware measures is driving the implementation of CWPP with automated remediation and runtime protection as they enable organizations to automatically discover running workloads, identify workload-level misconfigurations, manage vulnerabilities, and detect threats with CDR capabilities. These capabilities are particularly important for workloads containing sensitive data or critical applications.
- Security responsibility in global organizations is being pushed further to developers, driving demand for CWPP solutions that provide a risk-based approach and enhance the visibility of vulnerabilities, threats, malware, and secrets associated with their software bill of materials (SBOM) during their application development process.
- CISOs are facing complex challenges in securing cloud-native applications and often find it difficult to balance budget constraints and tool proliferation, forcing them to optimize their resource allocation, and pushing them toward a risk-based approach to security. The rapid technology adoption by application teams and the complexity of managing multi-cloud environments further complicate this task. The shortage of skilled cybersecurity professionals with cloud-specific knowledge exacerbates these challenges, driving demand for comprehensive CWPP solutions that can bridge these gaps.

Source: Frost & Sullivan

Growth Environment (continued)

- 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.
- Compliance with evolving regulations and frameworks, like GDPR and CCPA, drives the adoption of CSPM solutions. These tools automate compliance monitoring, helping organizations mitigate potential penalties and manage reputational risks associated with non-compliance. Misunderstanding the shared responsibility model in cloud security and resistance to adopting new technologies can dampen investment in CWPP. Some stakeholders may view CWPP as redundant, believing existing tools are sufficient, delaying or preventing adoption.
- 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. This misconception may lead to the misallocation of resources and investment in required technologies and services, as they may mistakenly believe that the CSPs' security measures are sufficient to protect their assets.

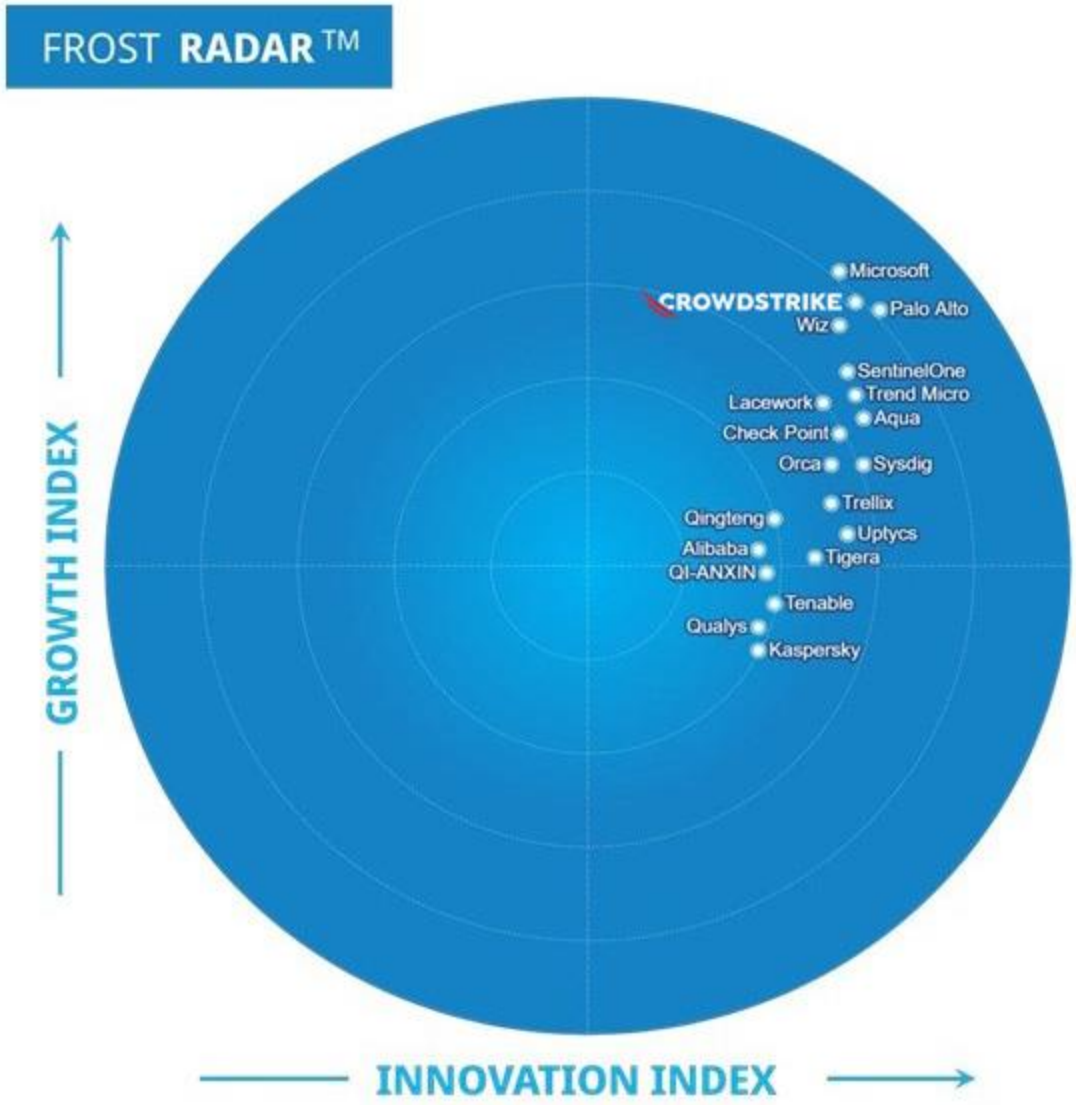
Source: Frost & Sullivan

Growth Environment (continued)

- The friction and distrust that can arise between security teams and developers can cause reluctance to invest in cloud security technologies, with security being perceived to slow down modern DevOps-style development. 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, 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 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.
- Despite these challenges, the increasing sophistication of cloud threats and the need for comprehensive security solutions will continue to propel CWPP adoption. The need for effective threat detection and automated remediation across cloud layers remains critical, driving the adoption of advanced CWPP solutions in the face of complex cloud security challenges.
- As organizations recognize the importance of these measures, there is a significant shift in spending from large businesses (LBs) to small and medium-sized businesses (SMBs), largely due to the growing realization that point solutions create silos, hindering business agility and slowing down innovation. This is driving the need for comprehensive security solutions that support faster innovation and better collaboration across development, operations, and security teams.
- Because of this, along with cloud spending, awareness of the cloud threat landscape, and the accountability of CISOs and their teams, CWPP adoption is expected to rise over the next five years.

Source: Frost & Sullivan

Frost Radar™: Cloud Workload Protection Platforms



FROST & SULLIVAN

Source: Frost & Sullivan

Frost Radar™ Competitive Environment

- As CWPP is increasingly integrated with cloud security platforms that encompass other security solutions, this Radar does not solely assess CWPP solutions and their technological features and capabilities; it also evaluates the segment in the context of the broader cloud security industry.
- Vendors registering an estimated annual revenue of at least $20.0 million in 2023 have been included in this Radar analysis. This Frost Radar™ features the following vendors: Alibaba Cloud, Aqua Security, Check Point Software Technologies (Check Point), CrowdStrike, Kaspersky, Lacework, Microsoft (Security), Orca Security, Palo Alto Networks, Qi-ANXIN, Qingteng, Qualys, SentinelOne, Sysdig, Tenable, Tigera, Trellix, Trend Micro, Uptycs, and Wiz. Frost & Sullivan identified these companies as the key powerhouses in the global CWPP industry.
- Frost & Sullivan observed noteworthy innovation endeavors undertaken by several other companies, including Bitdefender, Caveonix, Carbon Black, ColorTokens, F5, Sophos, Rapid7, Skyhawk Security, Red Hat, Sonrai Security, Sophos, Upwind, Zscaler, and Chinese vendors, such as Asiainfo Sec, Tencent Cloud, TopSec, Hillstone Networks, and NSFOCUS. 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 input.
  - Our secondary research alone was insufficient to deliver a robust analysis.
- While revenue estimate are based on CY2023, this analysis and vendor assessment are based on information available, vendor performance and market conditions as of June 2024.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- The CWPP industry is in a growth phase. 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. In this context, CWPP is often used as a part of CNAPPs with other security tools, such as vulnerability management, SCA, CI/CD pipeline security, K8s protection, CSPM, and API protection with automated remediation capabilities.
- Customers in the banking, finance, and tech industries are the largest adopters of CWPP, as they need robust cloud security solutions to manage compliance, shift-left security, vulnerability/risk management, and runtime protection/threat management. Organizations in these sectors have been seen to take a proactive approach to cloud security and cyber-risk management as they accelerate their cloud migration for their critical workloads.
- As a result, CWPP has become an important cloud security tool for organizations to manage risks, ensure compliance, secure their cloud workloads, and help security teams handle threats in runtime environments effectively. CWPP tools have evolved to not only provide basic vulnerability and compliance management but also offer organizations the capabilities of real-time threat detection and response across cloud computes, networks, workloads, and applications.
- The increasing demand for comprehensive cyber security solutions and the integration of CWPP with DevOps flows, CI/CD pipelines, and AI/ML technologies has made industry competition fierce, 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. This trend will likely continue in the long term.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Companies to Action

CrowdStrike

INNOVATION

- CrowdStrike is an innovation leader on this Frost Radar™ for its unified cloud security approach and powerful workload security capabilities. Its Falcon Cloud Security (FCS) platform offers a comprehensive suite of tools designed to secure cloud environments. It integrates multiple security functions, including pre-runtime/shift-left CSPM, CWPP, CIEM, and ASPM, providing robust visibility, vulnerability management, runtime protection, and compliance management across multi-cloud environments such as AWS, Azure, and Google Cloud, enabling organizations to streamline their cloud security operations and detect, prevent, and remediate security threats effectively. These capabilities are unified into a single platform with holistic attack-path visualization from host to cloud. It combines runtime and cloud metadata to provide near-real-time insights into potential attack paths for proactive TDR.
- The CWPP module is an integral part of its FCS platform, offering robust capabilities for managing and securing VMs, applications, hosts, and containers/K8s environments. It provides comprehensive visibility into and protection of these cloud resources and workloads, empowering organizations to uncover hidden threats, address vulnerabilities and misconfigurations, and mitigate exploitable vulnerabilities proactively with its reputed TDR capabilities.
- The CWPP module also leverages the company's behavior analytics, AI/ML capabilities, globally well-trained security data with an extensive library of Indicators of Attack (IoAs) and adversary-based threat intelligence to detect non-malware threats and fileless attacks, improving the security posture of cloud workloads and applications. It also offers comprehensive runtime protection with exploit prevention and behavior monitoring capabilities, firewall, and system integrity monitoring for various operating systems and kernels, including Linux, Windows, and MacOS, VMs, containers, serverless services, and advanced application control to prevent malicious applications from running.

Source: Frost & Sullivan

CrowdStrike (continued)

INNOVATION

- The solution leverages an eBPF agent that delivers granular visibility into traffic behaviors at a kernel level without impacting overall system performance. CrowdStrike's CWPP also provides robust container security with a single agent to protect the host that supports DaemonSet and per-node deployments, as well as an admission controller for K8s security. Its protection capability also extends to serverless container services like AWS Fargate and integrates with 16 different image registries to scan for vulnerabilities, malware, secrets, and misconfigurations.
- CrowdStrike's CWPP stands out for its seamless integration with its XDR and MDR services, providing end-to-end visibility and protection to prevent breaches across all layers, including cloud, endpoint, and identity. CrowdStrike's MDR service is a big selling point, particularly for businesses that need 24/7 managed threat-hunting capabilities to ensure continuous protection and expert threat analysis. The deep combination of technology and its world-class MDR and threat-hunting expertise allows for comprehensive threat visibility and protection across endpoints, workloads, and cloud environments.
- CrowdStrike has demonstrated its commitment to technology innovation through recent feature enhancements. These include the one-click deployment of sensors and attack path visualization for on-premises and cloud VMs, further streamlining security operations. The fully integrated FCS SKU package, combining CWPP, CSPM, and CIEM, simplifies the security management process, making it more efficient and effective than turning to the highly bespoke cloud security sector. It also expanded its AI/ML integration to enhance TDR capabilities, allowing the platform to process and analyze vast amounts of data from various sources, identifying patterns and IoCs across cloud workloads and applications that security teams might miss.

Source: Frost & Sullivan

CrowdStrike (continued)

INNOVATION

- The integration also improves threat intelligence quality to provide proactive, automated, guided remediation with actionable insights and recommendations, threat hunting, and real-time response to sophisticated cloud-based attacks. It addresses other security risks effectively while minimizing the impact on cloud operations. Moving forward, CrowdStrike is expected to continue to work on advanced features like attack-path graphing of all cloud assets, ASPM, integration of DSPM (including data context and exposure and cloud data protection for runtime data access), runtime protection for serverless functions, and expanded support for VMware environments.

Source: Frost & Sullivan

CrowdStrike (continued)

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 CNAPP industry. In 2023, its cloud workload security business accounted for a large chunk of its overall cloud security business and recorded a tremendous 83.6% growth after a phenomenal 117.8% growth in 2022. These impressive financial results have enabled the company to grow its market share over the years and made it the second-largest CWPP player in the industry, with 8.5% of the total market share. With its rapid growth momentum, CrowdStrike is expected to increase the gap with its closest competitors in the market while bridging the gap with the largest player in the next 1 to 3 years.
- 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 cloud security solutions to large businesses in multiple verticals to maintain its momentum. The company is gaining traction among prominent customers from various industries, including BFSI, tech, H&M, M&E, and retail/eCommerce. Its recent shift from a modular approach to combining all CNAPP capabilities into a single license makes it easier for customers to scale to suit their needs per the changes in their cloud environments. This will allow CrowdStrike to maintain robust growth in its cloud security business in the next few years.

Source: Frost & Sullivan

CrowdStrike (continued)

FROST PERSPECTIVE

- CrowdStrike is rated as an innovation and growth leader in this Radar analysis for its unified cloud security platform, tremendous growth trajectory over the last 4 years, and its future growth vision. CrowdStrike's FCS provides visibility and protection across different cloud stacks, including hosts, VMs, container/K8s, serverless services, and application layers. Its CWPP provides robust, comprehensive, and powerful security capabilities to address the critical needs of modern cloud security. Its advanced runtime protection, extensive platform support, and integration with XDR and MDR services position it as a leading choice for organizations seeking to enhance their cloud security posture and detection and response capabilities against evolving threats.
- The company's recent acquisitions of Bionic and Flow Security to expand its capabilities in managing data protection and application risks are a testament to its strong commitment to technology innovation and business transformation. These acquisitions are expected to help CrowdStrike further increase its visibility and cloud security perception.
- CrowdStrike should consider more support for private cloud environments (e.g., Oracle Cloud, VMware, and Red Hat) and other regional CSPs (e.g., Alibaba Cloud and Tencent) to maintain its edge. The vendor should also quickly introduce other capabilities, such as AI SPM, and improve integration with DevOps and CI/CD pipelines (e.g., Jenkins, GitLab, CircleCI, and Azure DevOps).
- CrowdStrike's steady growth momentum, extensive customer base from XDR/EDR offerings, and robust channel partner ecosystem are the main reasons for its position on the Growth Index. The company will benefit from strengthening its targeted GTM strategy, while educational campaigns with local and regional partners will boost its cloud security perception.

Source: Frost & Sullivan

FROST & SULLIVAN

Best Practices & Growth Opportunities

Source: Frost & Sullivan

Best Practices

1. Companies want to reduce management complexities and increase operational efficiency. Many are taking the platform approach by consolidating multiple security tools into a single platform. This integration ensures comprehensive risk and threat management across different tools and other security areas, supporting the entire cloud security strategy within a unified platform to simplify security management and enhance the ability to respond to threats across disparate environments more effectively.

2. Multi-cloud environments' complexities challenge organizations to maintain consistent security policies and configurations across diverse landscapes that are susceptible to errors. Owing to differences in security models and policies, managing security across several cloud providers further challenges enterprises, potentially increasing the risk of misconfigurations. They are also in urgent need of cloud TDR capabilities as cloud environments demand real-time TDR capabilities, with a focus on runtime security.

3. Selecting the right CWPP or cloud security tool can be difficult, and it depends on factors including solution capabilities, stability, scalability, management, and ROIs. The right CWPP must align with the organization's security needs, operational efficiency, compliance requirements, and budget. Organizations need to strike the balance and consider the true solution's values, such as business impacts, technical aspects, real-time detection and response capabilities, competitive advantage, and operational stability.

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. 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. The rapid development and deployment of AI applications have outpaced the implementation of security measures, elevating the risk of exploitation by malicious actors. Organizations, thus, are rethinking their cybersecurity strategies to deal with new challenges in the AI era by looking to security solutions that can protect their AI-based applications from code to cloud to improve their defense against these sophisticated threats.

3. The demand for safe adoption of AI/ ML workloads is driving the need for AI application modernization and protection with deeper integration of dynamic threat detection, risk management, and security hygiene practices. This has led to the increasing requirements for a shift-left security approach to strengthen their cloud security to enable a proactive policy security enforcement for insecure resources before they are deployed in production.

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 (continued)

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

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