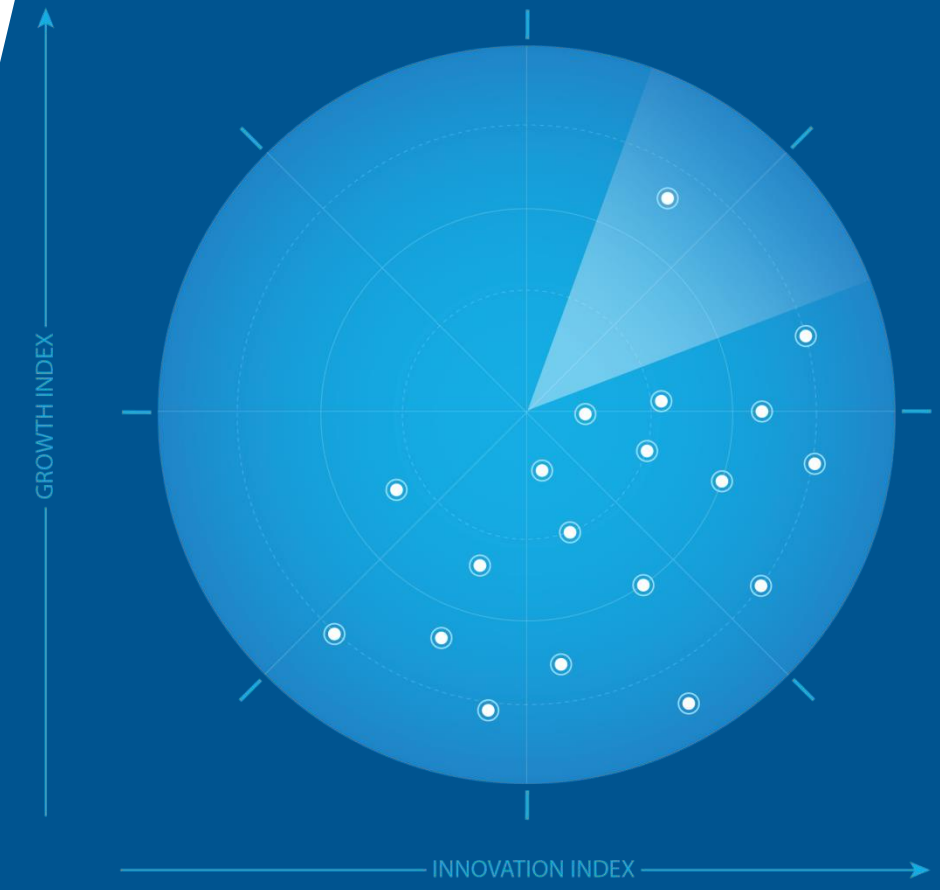
FROST & SULLIVAN

Frost Radar™: Cloud Security Posture Management, 2024

Authored by: Anh Tien Vu

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



FROST & SULLIVAN

Strategic Imperative and Growth Environment



Strategic Imperative

Factors Creating Pressure on Growth

- The increasing complexity of cloud environments creates a need for centralized cloud security posture management (CSPM) solutions for comprehensive control and oversight as organizations expand their footprint. The upsurge in cloud misconfiguration drives the urgent need for CSPM tools capable of robust risk and threat detection and remediation. Stricter regulatory requirements, exemplified by the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), also emphasize CSPM solutions to ensure compliance, mitigating potential penalties and reputational risks.
- Additionally, the growing adoption of cloud services and demand for enhanced visibility and continuous monitoring prompt investment in CSPM for real-time insights and actionable recommendations. Increased awareness of cloud security challenges drives the adoption of CSPM solutions to streamline vulnerability identification and resolution.

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- CSPM is a cloud security tool that provides automated and continuous security monitoring so organizations have a unified view of their security posture across various cloud services. It provides visibility into cloud security posture by collecting and analyzing telemetry data logs from cloud assets/resources via APIs, allowing organizations to detect, prevent, and remediate cloud misconfigurations, baseline drift, and policy/regulation violations, which lead to security risks, such as data breaches, host/virtual machine (VM) escape, or container escape.
- Typical cloud security risks that CSPM addresses relate to data/breaches, networks, compute (including host/VMs), workloads (containers, container registry, container orchestrations, API, serverless functions), users, identity, and their entitlements (often caused by improper and poor setup or management), misconfigurations, accidental exposure of sensitive data, system vulnerabilities, baseline drift due to changes, lack of security measures, and policy/regulation violations.

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- CSPM addresses these risks by automating the discovery of cloud assets, including networks, services, storage systems, workloads, applications, identities, and data (often through CSPs' APIs or scanning snapshots) and monitoring and managing them through a single dashboard.
- CSPM tools seek to:
  - Detect misconfiguration of VMs, operating systems, networks, and storage
  - Identify unpatched or vulnerable VMs, container images, and unsecured container registries
  - Flag risky container deployments
  - Assess the security of serverless computing components to prevent attacks
  - Identify exposed or vulnerable applications
  - Discover improper access control/traffic controls and identify unsecured APIs
  - Audit and ensure configurations are compliant with security control frameworks and regulatory standards (including CI/CD pipelines and IaC)
  - Enforce consistent policies across multi-cloud environments

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- These actions are essential for minimizing the attack surface, preventing the introduction of malicious images, and ensuring robust security measures to manage risks and threats in cloud environments effectively. This streamlines security management and significantly reduces the risk of human error, a common cause of security incidents in the cloud.
- CSPM tools integrate with other cloud security technologies, including cloud workload protection platform (CWPP), infrastructure as code (IaC) security, data security posture management (DSPM), SaaS security posture management (SSPM), Kubernetes security posture management (KSPM), cloud detection and response (CDR), AI security posture management (AI SPM), and the continuous integration/continuous delivery (CI/CD) pipeline security in the context of the cloud-native application protection platform (CNAPP) to maintain security posture throughout the application development lifecycle.

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- CSPM is particularly essential in hybrid and multi-cloud infrastructures, where visibility and security control over distributed cloud components can be challenging with traditional security technologies. It is also helpful to ensure that cloud infrastructures, services, and applications adhere to security best practices and compliance requirements.
- Requirements for CSPM tools continue to evolve. This reflects common changes in the approach to cloud security, which now focuses more on real-time risk and threat management, going beyond static vulnerability and misconfiguration management.
- Key features required for a CSPM tool include:
  - Performs inventory for cloud resources continuously
  - Scans and monitors cloud compute instances and other resources to identify new changes, alert, and provide recommendations or automatically remediate cloud misconfigurations, mismanagement, IoC detection, errors, anomalies, and suspicious activities; it must be able to detect and remediate cloud security misconfigurations and anomalies to ensure proper cloud infrastructure

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- Provides vulnerability assessment and runtime visibility/insights of modern cloud workloads, including container, container orchestration, serverless functions, and DevOps workflow to analyze and secure IaC artifacts early in the development cycle
- Offers real-time visibility with comprehensive asset visualization to identify and visualize all elements within cloud environments, including systems, services, applications, container, and container orchestrations, along with their security and compliance statuses
- Provides dynamic asset mapping to map cloud assets to their corresponding IaC manifest to gain knowledge and secure the cloud architecture comprehensively
- Facilitates sensitive data tracking to provide visibility into where sensitive data resides (across different cloud environments, including hybrid, public, and multi-cloud) and ensures it complies with regulatory standards
- Performs security risk analysis, risk visualization, intelligent prioritization of risks/vulnerabilities, and incident response of cloud systems using technologies, such as CDR, to help teams prioritize risks based on actual cloud usage and runtime insights, combining this with traditional static checks for a comprehensive risk overview

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- Conducts attack path analysis that visualizes attack trajectories in real-time, which helps identify potential attack paths and lateral movements within the cloud environment and mitigate complex security threats
- Offers proactive/real-time drift detection to detect configuration drifts, preventing potential security breaches; CSPM can alert for discrepancies between expected and actual configurations
- Automates or guides remediation to automatically generate incident response actions, remediation, and investigation of security incidents
- Enforces consistent policies across multi-cloud environments and provides customizable policy and enforcement that allows for the creation and enforcement of security policies both at runtime and during the IaC phase, which helps prevent misconfigurations from being deployed
- Implements Zero Trust network management principles to identify risky network misconfigurations, unsecured network protocols, and poor TLS certificate management practices
- Audits/automates compliance checks to ensure configurations are compliant with security control frameworks and regulatory standards (including CI/CD pipelines and IaC)

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- Features an intuitive and interactive dashboard that offers granular yet correlated visibility and actionable insights into risks, their impacts, and guided remediation for risks discovered

- Apart from these features, organizations evaluate CSPM tools by considering other factors influencing decision-making, including solution capabilities, stability, scalability, management, and ROIs. Choosing the right CSPM must align with the organization's security needs, operational efficiency, compliance requirements, and budget. Nonetheless, a preferred CSPM solution should be able to offer:
  - Integrability: Companies seek to reduce complexity by consolidating multiple security tools into a single platform to simplify security management and enhance the ability to respond to threats across disparate environments more effectively. CSPM tools need to support this shift to help organizations streamline workflows, reduce redundancies, and provide a holistic view of security postures across all cloud resources

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- Real-time threat detection and risk prioritization: Modern CSPM solutions should offer more than periodic assessments and provide continuous monitoring and real-time threat detection to enable organizations to respond immediately to threats and misconfigurations, thereby reducing potential security risks. This can be done by integrating AI/ML technologies. CSPM tools must prioritize security issues and risks effectively, providing actionable risk reduction and remediation insights.
- Robust innovation support: CSPM tools must accommodate rapid changes in cloud architectures and deploy new technologies without compromising security. They should support container/K8s security and integrate with DevOps workflows and CI/CD pipeline tools to empower organizations toward shift-left security. By incorporating security for modern technologies alongside traditional IT infrastructure, CSPM enables consistent security policies and practices across all workloads, enhancing the organization's ability to respond to vulnerabilities and configuration.
- Return on investment (ROI): Organizations desire CSPM tools that can deliver quick and measurable returns. This includes reducing the costs associated with security breaches and speeding up the secure deployment of cloud services. Tools that can automate security tasks, provide accurate threat responses, and decrease manual labor are particularly valued for their impact on operational efficiency.

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- Cloud agnostic for strong integration capabilities with third-party tools: Prioritizing a cloud-agnostic CSPM tool that offers seamless visibility and protection across different cloud infrastructures will maintain consistent security postures. CSPM 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.
- Scalability and ease of use: CSPM tools must be easy to use to ensure quick adoption across the organization. They must offer an intuitive UI and integrate easily with existing systems, allowing security teams to focus on strategic tasks. The CSPM solution must also be able to scale to meet organizations' growing requirements. The tool should be able to handle the growing volume of data, cover new cloud services across regions without performance degradation, and maintain cost-effectiveness at scale.

Source: Frost & Sullivan

Growth Environment

- Organizations globally 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 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.
- CSPM adoption has increased in the past three years, and the growth momentum is expected to be sustained in five years. The industry grew by 45.1% in 2023 on a year-over-year (YOY) basis, with an estimated revenue of $1639.8 million. The industry is forecast to record robust growth in the next five years, representing a compound annual growth rate (CAGR) of 27.8% from 2023 to 2028.
- Accelerated adoption of cloud services and cloud-native application development technologies amid stringent compliance requirements from regulated industries will drive spending on cloud security technologies, particularly CSPM. The tool is the foundation of an organization's cloud security strategy and journey toward CNAPP, regardless of their cloud maturity level, which will increase spending from LBs to SMBs.

Source: Frost & Sullivan

Growth Environment (continued)

- As organizations adopt and integrate new cloud services, the need for CSPM solutions to ensure consistent security policies, compliances, and practices across diverse cloud infrastructures becomes critical, particularly in regulated industries where adherence to compliance frameworks is mandatory.
- Furthermore, the need to identify, prioritize, and remediate risks associated with cloud misconfigurations, identity, data security, and compliance will drive more spending on CSPM tools or capabilities as many organizations, particularly mature ones, recognize the importance of centralized visibility, control, and risk management of their cloud infrastructure.
- CISOs face complex challenges in securing cloud-native applications, primarily balancing enabling innovation and ensuring robust security. Rapid technology adoption by application teams often outpaces the security team's ability to keep up, creating unprecedented complexities. The complexity of multi-cloud environments further challenges organizations to maintain consistent security policies and configurations across diverse landscapes susceptible to errors. Managing security across multiple cloud providers increases complexity due to varying security models and controls, leading to inconsistencies in security posture and increased potential for misconfigurations among the leading causes of security breaches in cloud environments.

Source: Frost & Sullivan

Growth Environment (continued)

- Compliance with evolving regulations and frameworks, such as GDPR in Europe and CCPA in the United States, will drive the adoption of CSPM solutions to ensure continuous monitoring and enforcement of compliance standards across cloud environments. CSPM tools automate checking, tracking, and reporting, enabling organizations to mitigate potential penalties, manage reputational risks associated with non-compliance, and reinforce their strategies in data protection and privacy regulations.
- Due to the rapid evolution of cloud technologies, CISOs face mounting challenges in managing security risks in cloud environments. Current security strategies and tools can quickly become outdated, and keeping up with the latest cloud security technologies and practices is challenging. In addition, the evolution of the threat landscape in the cloud raises an urgent call for CISOs to have cloud threat detection and response capabilities, focusing on runtime security for workloads, containers, and serverless components.
- Another pressing issue in the industry is the skills shortage. The demand for cybersecurity professionals with cloud-specific knowledge is outpacing the available talent pool, making it difficult to staff security teams and respond effectively to cloud-specific threats adequately.

Source: Frost & Sullivan

Growth Environment (continued)

- Adhering to stringent data protection laws such as the GDPR in Europe and CCPA in the United States has become paramount for organizations to ensure regulatory compliance. This, in turn, is helping to encourage the adoption of CSPM solutions to ensure continuous monitoring and enforcement of compliance standards across cloud environments. CSPM, with the ability to automate the checking, tracking, and reporting, enables organizations to mitigate potential penalties, manage reputational risks associated with non-compliance, and reinforce data protection strategies and privacy regulations.
- Alert fatigue will continue to be a primary concern for CISOs moving forward. While many security products offer modern threat visualizations, they do not inherently enhance an organization's security posture. Instead, they generate a flood of alerts and add complexity, making it difficult for CISOs to distinguish critical threats from benign anomalies effectively. This environment creates a significant "security debt" as CISOs struggle to prioritize and address the most pressing vulnerabilities amid the noise.

Source: Frost & Sullivan

Growth Environment (continued)

- It is necessary for organizations that embrace cloud technologies to have CSPM tools to manage these risks. By automating the detection and correction of misconfigurations, CSPM tools significantly reduce the attack surface, maintaining security posture and enhancing the overall security of cloud environments to minimize risks of cloud breaches. CSPM tools are especially important for organizations with complex and dynamic cloud infrastructures to prevent misconfigurations of cloud services that can expose sensitive data to potential cyber breaches and threats, reducing downtime and the resources required for maintenance—further enhancing the overall ROI.
- CISOs often find it difficult to balance budget constraints and tool proliferation. Economic constraints and budgetary pressures are forcing CISOs to optimize their resource allocation, pushing them toward a risk-based approach to security. 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.

Source: Frost & Sullivan

Growth Environment (continued)

- As organizations adopt and integrate new cloud services, the need for CSPM solutions to ensure consistent security policies, compliance, and practices across diverse cloud infrastructures becomes critical, particularly in regulated industries where adherence to compliance frameworks is mandatory. Furthermore, the need to identify, prioritize, and remediate risks associated with cloud misconfigurations, identity, data security, and compliance will boost spending on CSPM tools or capabilities as many organizations, particularly mature ones, understand the importance of centralized visibility, control, and risk management of their cloud infrastructure.
- Organizations face increasing challenges associated with DevSecOps, balancing security and innovation in the fast-paced DevOps environment more challenging. This requires collaboration between development, security, and operations teams. The growing trend toward DevSecOps is set to deepen the integration of CSPM into the CI/CD pipeline, automating security and compliance checks. Organizations need visibility into their development and production environments to make informed decisions throughout the software lifecycle.

Source: Frost & Sullivan

Growth Environment (continued)

- CSPM tools enhance visibility into cloud resources across multiple platforms and services, enabling organizations to manage their cloud environments comprehensively and quickly assess the security posture of their entire cloud infrastructure. This is particularly important in complex environments where misconfigurations can easily go unnoticed among numerous services and settings.
- Additionally, the increasing sophistication of cloud threats requires organizations to adopt modern CSPM solutions with advanced technologies such as artificial intelligence (AI), machine learning (ML), CDR, workload runtime protection, identity, and data security for effective threat detection and automated remediation across cloud layers. However, the shortage of skilled resources and expertise, particularly among developers lacking the right security skills, is seen as a primary restraint to adopting CSPM.
- Furthermore, misunderstanding the shared responsibility model in cloud security is considered a primary challenge, dampening investment in cloud security. Many organizations assume that CSPs are solely responsible for securing their data, applications, and service configurations in the cloud without knowing that this responsibility is on them. This misconception may lead to the misallocation of resources and investment in required technologies and services as they mistakenly believe that the CSPs' security measures are sufficient to protect their assets.

Source: Frost & Sullivan

Growth Environment (continued)

- The friction and distrust between security teams and developers can cause reluctance to invest in cloud security technologies, including CSPM, 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 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. Some stakeholders may view CSPM as redundant and believe that existing tools already cover their security needs, delaying or preventing the adoption of CSPM.

Source: Frost & Sullivan

Growth Environment (continued)

- In addition, economic fluctuations, such as market corrections and inflation, are prompting companies to cut back on IT and cloud security spending. Many are more likely to postpone or scale down on new investments, including CSPM solutions, which can be perceived as costly. This leads them to either consolidate their security tools or opt for less expensive alternatives.
- Geopolitical conflicts like the Russo-Ukrainian war can also decrease business confidence and reduce investment in new technologies, including CSPM. This is particularly impactful in regions and sectors experiencing direct effects from crises where operational costs have risen over the last few years. This can be a significant restraint on the growth of the cloud security industry as companies may be hesitant to invest in new security solutions during a period of financial uncertainty.

Source: Frost & Sullivan

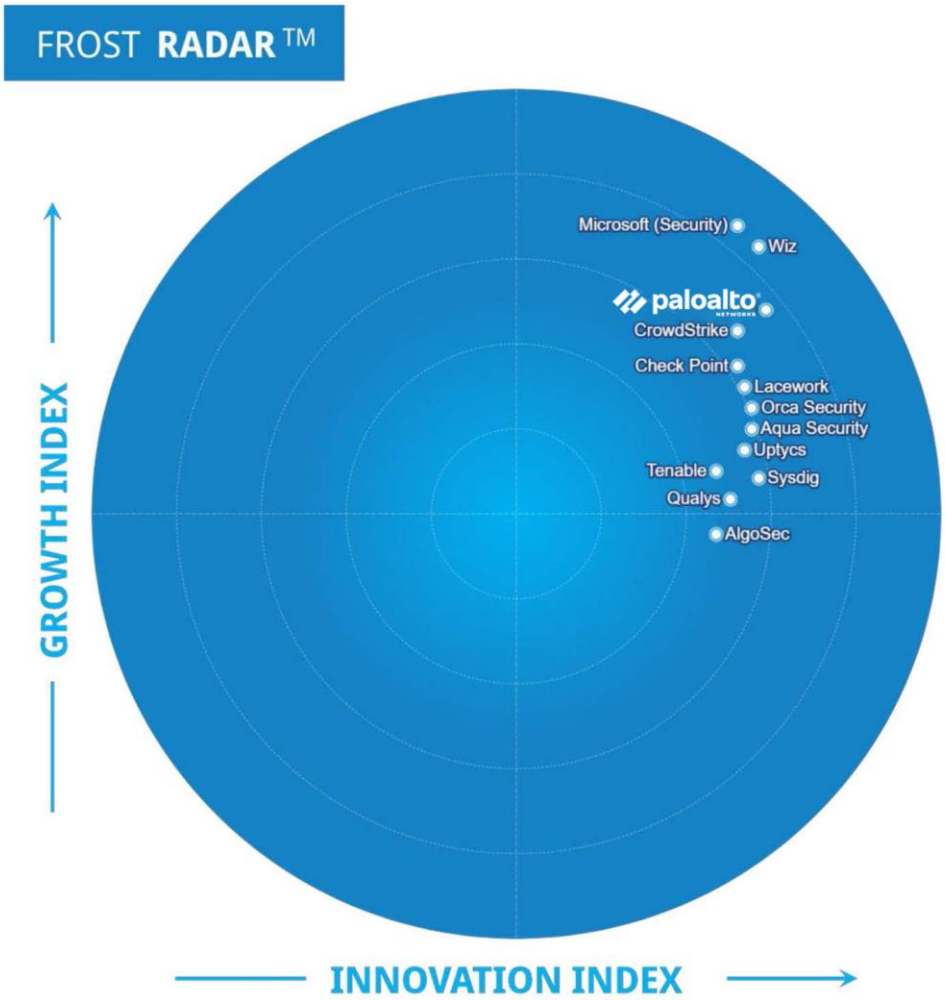
FROST & SULLIVAN



Frost Radar™

CLOUD SECURITY POSTURE MANAGEMENT, 2024

Frost Radar™: Cloud Security Posture Management , 2024



Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- Among more than 35 qualified CSPM vendors globally, Frost & Sullivan independently plotted the top 13 companies in this Frost RadarTM analysis. Factors assessed to determine vendor selection and their performance in the Growth and/or Innovation index include end-user focus, geographic presence, product features and capabilities, solution ecosystem, innovation scalability, and business strategy. As CSPM integrates with a larger cloud security platform, this radar analysis does not solely assess CSPM 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 $5.0 million in 2023 were included in this Radar analysis. This Frost RadarTM features the following vendors: AlgoSec, Aqua Security, Check Point Software Technologies (Check Point), CrowdStrike, Lacework, Microsoft (Security), Orca Security, Palo Alto Networks, Qualys, Sysdig, Tenable, Uptycs, and Wiz. Frost & Sullivan identified these companies as the key powerhouses in the global CSPM industry.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- Frost & Sullivan observed noteworthy innovation endeavors undertaken by several other companies, including AccuKnox, Cisco, Cyscale, Dynatrace (to acquire Runecast), Fortinet, JupiterOne, Rapid7, Skyhawk Security, Sophos, Trend Micro, Upwind, Zscaler, and Chinese vendors, such as Alibaba Cloud, Tencent, and NSFOCUS. While these vendors demonstrated substantial technological advancements and market expansions, they were not included in this Frost RadarTM as their global market presence was relatively limited, they declined to participate or could not provide direct input, and secondary research alone was insufficient to deliver a robust analysis. A few vendors offer CPSM functionality over other products (e.g., attack surface management, cloud management) but do not promote the solution as CSPM. These vendors were also not included in the analysis.

- The CSPM industry is in the growth phase fueled by the need for a centralized platform that provides granular visibility, comprehensive risk control, and threat detection and response capabilities against cyber threats to ensure compliance in cloud environments. CSPM has become a fundamental yet inevitable component in cloud security strategies



Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- CSPM tools have evolved to provide basic visibility and compliance capabilities for cloud infrastructure and offer organizations the capabilities of vulnerability management, threat detection, and response across cloud computers, networks, workloads, and applications. CSPM tools integrate with DevOps flows, CI/CD pipelines, and AI/ML technologies to help organizations achieve comprehensive visibility, compliance, and threat detection and response.

- Because of this, industry competition has become extremely stiff, with established security companies expanding their capabilities, particularly through integrating 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 unable to sustain their growth momentum and innovation scalability being acquired by larger competitors seeking to expand their portfolios to maintain competitive advantages and growth. This trend will likely continue in the long term.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- The Radar placement in this report is consistent with our observation and assessment of other cloud technologies, including the CWPP and CNAPP 2023 industries. Microsoft, Palo Alto Networks, CrowdStrike, and Wiz emerged as the leaders in the Growth index due to their dominant market share and robust revenue growth over the past 4 years. Microsoft has maintained its leadership as the largest CSPM player over the past few years, with an impressive YoY growth of 56.9% and a substantial market share of 16.1% in 2023. Microsoft leverages its diversified Azure customer base, which includes large organizations across various industries. Azure Cloud's large customer base allows it to offer freemium CSPM services for a basic security package and premium services for those requiring advanced services such as workload, DevOps, and CDR.

- Palo Alto Networks maintained a strong growth trajectory in 2023 to solidify its position as a prominent player in the industry, with 13.1% of the market share, remaining the leader among non-CSPM security players. Palo Alto Networks has established itself as a trailblazer in the CSPM industry with its Prisma Cloud platform.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

It is the preferred choice for many global companies with large-scale cloud deployments, particularly LBs in banking, financial services, and insurance (BFSI), technology, healthcare and medical (H&M), media and entertainment (M&E), and government. However, the company faces intense competition from Wiz and CrowdStrike, which have recorded tremendous growth in the past few years. Palo Alto Networks has implemented aggressive go-to-market (GTM) and smart acquisition strategies to drive its cloud security business, leveraging its robust customer base from the network security segment to navigate growth challenges from the network security segment.

- Wiz, the fastest-growing player in the industry, has registered impressive growth and customer recognition in the global cloud security industry since its establishment. It has become one of the most preferred CSPM/cloud infrastructure security platforms with its disruptive approach and decacorns in the market with a surge in revenue since its establishment. The vendor's market share soared from less than 1% in 2020 to 15.1% in 2023. This exceptional growth has been largely attributed to Wiz's concerted efforts to strengthen its platform capabilities through in-house research and development (R&D) initiatives and strategic partnerships. Wiz has also expanded its global footprint by opening new data centers in UAE, Australia, and India to meet the increased demand for cloud security solutions in these regions and beyond.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- CrowdStrike was also one of the fastest-growing players in 2023, expanding by 83.6% compared to 2022, making it the fifth-largest with 5.5%. As it shifts its business to a platform model, the company aligns its CSPM growth with its total cloud security business, which has considerably increased in the last 3 years. CrowdStrike's strong customer base, superior brand perception, extensive customer base for its XDR platform and MDR services, and a focused strategy on cloud security position the company for robust market share growth in its cloud security business.
- Check Point is rated relatively high in the Growth index due to its solid performance in the last 4 years, significant market share, and global expansion efforts. However, it experienced slower growth in 2023 as it slowly expanded to a new customer base. This trend will likely persist in upcoming years as the company maintains its industry focus on its existing customer base. Although this could help it maintain business profitability, the company may lose further market share.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- Lacework, once highly rated in the cloud security industry, faces operational challenges with changes at the senior management level, market direction, and overall sales performance. Its recent acquisition by Fortinet may enable the company to stabilize and improve its business performance but still leaves its future growth in question. Nonetheless, the company is still rated strongly positive in innovation due to its unified platform approach with a clear roadmap for technological advancement and business transformation in the long term.
- Orca Security, Aqua Security, Sysdig, Uptycs, Tenable, and Qualys are ranked favorably in the analysis because of their total cloud/CNAPP strategy, which sees their CSPM solutions growth align with their overall CNAPP business. However, these vendors must reinforce efforts to expand their industry influence and presence globally as their market shares remain relatively small compared to other leading players.



Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- AlgoSec is a new entrant in cloud security following its acquisition of Prevasio in December 2022. The company has seen significant adoption of its CSPM solution globally across North America, Europe, the Middle East, Africa (EMEA), and Asia-Pacific. However, the perception of the company remains low, which requires it to put more effort into increasing its visibility among customers and strengthening its channel partners and ecosystem.

- In terms of an innovation strategy, most companies are in the race to develop new technology features and capabilities to maintain competitiveness. While vendors focused more on compliance and vulnerability management capabilities over the past 18 months, the focus has shifted to new capabilities that help organizations gain real-time visibility, threat detection and response, automated compliance checks, CDR, risk prioritization, and integration with DevOps workflows, data security and AI security (AI SPM) with increased AI adoption at the backend for enhanced detection and response. As such, top vendors are bridging the gaps in technology features and capabilities as most stand neck-to-neck with each other.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- Although technological features and capabilities remain key factors in evaluating CSPM solutions, customers increasingly consider other factors when choosing the right solution. These include the vendor’s product ecosystem, sustainability and support, the solution's stability and ease of use, integration capability with existing and future technologies, and ROI.
- As a result, most vendors featured are rated as Innovation leaders in this Radar analysis, with Palo Alto Networks, Wiz, Microsoft (Security), CrowdStrike, Check Point, Sysdig, Lacework, Aqua Security, Uptycs, and Orca Security placed highest on this index. This is attributable to their comprehensive CNAPP approach, extensive features, excellent expertise and support capabilities, and highly scalable platforms that help organizations deal with cloud security challenges, particularly the CSPM use cases.
- Frost & Sullivan also acknowledges the efforts of other companies, including Tenable, Qualys, and AlgoSec, in this analysis. These companies are favorably ranked in the Innovation Index, although their presence in the cloud security industry remains moderate compared to other competitors.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- Qualys and Tenable are known for their vulnerability management platforms and are expanding to the cloud security industry. Tenable has acquired Emertic (and Accunics before) to strengthen its platform with strong CIEM capabilities from Emertic. Adding Emertic's CIEM and CSPM capabilities enables Tenable to expand its cloud security portfolios with more identity-centric security and risk management for cloud infrastructure. Qualys is rated positively for its total cloud platform, given its focus on risk management across cloud layers leveraging AI/ML capabilities from its Blue Hexagon acquisition in 2022.
- Uptycs is also seen as an Innovation leader due to the integration of CNAPP and XDR platforms that deliver holistic security capabilities. Its CNAPP offers the most critical capabilities, including CWPP, KSPM, CSPM, CIEM, and CDR, across data centers, laptops, build pipelines, containers, and cloud environments. However, it needs to put more effort into making its platform more marketable and recognized as, for now, its solutions are mainly known in North America.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- AlgoSec, recognized for its cloud network security management, has acquired Prevasio, an agentless CSPM company, to offer CNAPP solutions. Its platform is capable of network security management, application, CI/CD risk management, and K8s security, helping organizations effectively manage network security rules and identify and fix risks in applications, CI/CD pipelines, GitHub repos, and K8s.



Source: Frost & Sullivan

FROST & SULLIVAN



Companies to Action:

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

Company to Action: Palo Alto Networks

Innovation

- Palo Alto Networks, a CNAPP trailblazer and Innovation leader in a previous CNAPP Radar analysis, provides robust security measures covering the entire application development lifecycle, from the earliest stages of code development to the deployment and ongoing management of cloud-native applications. Prisma Cloud has been highly rated again in this year's analysis for its recent platform, developments, and enhancement with the integration of AI security, DSPM/DDR, XDR, and application security (SAST and ASPM). Prisma Cloud also stands out in cross-platform integration, as it integrates seamlessly with major cloud environments, including AWS, Azure, Google Cloud, Oracle, Alibaba Cloud, and IBM, delivering a consistent security approach across diverse cloud platforms.

- Prisma Cloud enables teams to have code to cloud intelligence by ensuring excellent security capabilities across IaC, software composition analysis (SCA), software bill of materials (SBOM), CI/CD pipeline, cloud apps, hosts, VMs, serverless, containers, and K8s. The platform provides powerful cloud infrastructure security capabilities, including CSPM, CIEM, DSPM, CDR, and cloud discovery and exposure management (CDEM). It also offers detailed compliance monitoring and alerts that support a wide range of security standards, such as SoX, LGPD, GDPR, and CIS.

Source: Frost & Sullivan

Company to Action: Palo Alto Networks

Innovation

- Palo Alto Networks is one of the few vendors that have achieved the FedRAMP High in Ready and GovCloud certifications, which are critical requirements for providing cloud security services to the public sector in the United States.

- Palo Alto Networks is also a trailblazer in the CSPM industry. The company's CSPM solution identifies dynamic cloud asset inventory in multi-cloud and hybrid environments and ensures that no new service or resource goes unnoticed. This proactive approach provides security teams with real-time insights into all deployed resources, enabling them to maintain stringent security controls as new technologies and services are adopted. This proactive approach helps prevent potential security gaps and ensures continuous compliance and visibility across all cloud environments.

- Prisma Cloud helps bridge security gaps left by traditional CSPM tools that offer only static snapshots by providing continuous monitoring of asset and configuration states, allowing security teams to track changes in real-time and maintain a historical record of configuration states, which is crucial for forensic analysis and understanding the sequence of events leading up to a security incident.

Source: Frost & Sullivan

Company to Action: Palo Alto Networks

Innovation

- Particularly, by leveraging its extensive library of over 1,500 built-in misconfiguration checks, combined with customizable policy models, Prisma Cloud allows organizations to tailor and customize security policies and create additional configuration checks to meet their specific needs, enabling teams to identify and address all potential misconfigurations promptly to reduce the risk of security breaches due to human error or misconfigured resources.

- The platform supports over 90 compliance frameworks and allows the creation of custom frameworks, which make Prisma Cloud an invaluable tool for regulatory compliance. Its continuous monitoring and one-click reporting capabilities streamline compliance audits and reporting processes to help organizations easily comply with industry standards and regulatory requirements. Additionally, Prisma Cloud's attack path analysis and risk context that helps correlate security signals across various domains—such as configurations, identities, vulnerabilities, and network flows—enables it to identify and analyze complex attack paths, providing deeper insight into potential attack vectors and enabling more effective risk mitigation strategies.

Source: Frost & Sullivan

Company to Action: Palo Alto Networks

Innovation

- Prisma Cloud offers granular visibility into network communications by processing over a trillion cloud events daily, including detailed network flow data, allowing security teams to quickly identify and address true network vulnerabilities, reducing the risk of data breaches and other security incidents. The platform's flexible query model allows security teams to explore complex cloud environments effectively, and its automated remediation capabilities further enhance operational efficiency by resolving issues with minimal human intervention. Prisma Cloud's user and entity behavior analytics (UEBA) detects anomalous activities indicative of potential security threats. At the same time, its Code to Cloud™ Intelligence traces misconfigurations back to their source in IaC files, preventing future misconfigurations. By providing real-time visibility, detailed risk analysis, and actionable remediation, Prisma Cloud ensures that organizations can confidently manage Prisma Cloud ensures that organizations can confidently manage and secure their multi-cloud environments by providing real-time visibility, detailed risk analysis, and actionable remediation and secure their multi-cloud environments.

Source: Frost & Sullivan

Company to Action: Palo Alto Networks

Innovation

- Particularly, the announcement of Prisma Cloud with numerous new features such as AppDNA for risk classification with application context, attack path Graph to illuminate interconnected cloud risks, Code to Cloud Vulnerability Management for tracing issues back to their source for end-to-end visibility, Code to Cloud Remediation for fixing issues across code and cloud, Code to Cloud Dashboard for measuring and reporting success, Cloud Discovery and Exposure Management (CDEM) to manage cloud's unmanaged assets, and the ability to take the Prisma Cloud console everywhere using its new mobile app, sets Prisma Cloud apart from other competitors. In addition, its latest launch of DSPM and AI SPM, along with the integration with AI Copilot with the CNAPP platform, makes Prisma Cloud the most comprehensive cloud security platform on the market.

Source: Frost & Sullivan

Company to Action: Palo Alto Networks

Growth

- Palo Alto Networks has established itself as a leading player in the cloud-native security industry based on the success of its Prisma Cloud platform, making it the preferred choice for cloud-native security. As one of the first cloud security tools in the industry, Palo Alto Networks CSPM, as part of its Prisma Cloud platform, is widely adopted by global companies with large-scale cloud deployments.

- Palo Alto Networks accounted for 12.5% of the total market share in 2023, experiencing solid growth of 27.2% on a YoY basis, maintaining its market leadership. Leveraging the existing customer base of its flagship product—network security— Palo Alto Networks can effectively cross-sell and upsell Prisma Cloud solutions to many customers across different verticals, particularly BFSI, technology, retail/eCommerce, telco, and healthcare. Prisma Cloud also appeals to businesses with small to very large cloud deployments, especially those looking for a solution to bridge the challenging gap between security and development teams.

- Prisma Cloud benefits from a robust partner ecosystem with over 8,000 global partners with strong security expertise and experience, including channel partners, global systems integrators, and CSPs. The company's extensive partner ecosystem enables it to increase industry penetration and ensure the delivery of service coverage, capacity, and capabilities to end users.

Source: Frost & Sullivan

Company to Action: Palo Alto Networks

Growth

- Palo Alto Networks' popularity is also backed by a massive user community of 320,000 global users, which helps drive knowledge sharing and support to end users. Prisma Cloud's Global Customer Services (GCS) team, comprising over 2,200 members and 170+ Authorized Support Center partners, provides 24x7 support, enhancing customer satisfaction and retention. With proven ROI, time savings, and risk reduction validated by third-party research, Prisma Cloud stands out as a reliable and effective investment for organizations seeking comprehensive cloud security solutions.

Source: Frost & Sullivan

Company to Action: Palo Alto Networks

Frost Perspective

- Palo Alto Networks is a pioneer in the cloud security industry. An innovation trailblazer in Frost & Sullivan's previous CNAPP Radar assessments, the company is rated a distinct innovator in this CSPM Radar for its complete CNAPP platform and comprehensive CSPM capabilities.
- Prisma Cloud is one of the industry's most innovative cloud security platforms. It provides organizations with a full set of technological capabilities for protecting cloud infrastructure, workloads, and applications throughout the application development, deployment, and runtime lifecycle.
- Its comprehensive cloud security approach provides the ideal balance of best-of-breed functionality and platform integration, giving it a competitive edge and enabling it to stand out in the competitive cloud security space. Prisma Cloud's substantial R&D investments, with over 700 R&D staff and more than 21 major product releases in 2023, position the company at the forefront of cloud security technology innovation.
- To maintain its leading position, Palo Alto Networks will benefit from further enhancements to its platform integration across in-house developed and acquired solutions to improve end-user experience. The company should continue expanding its industry presence across regions such as APAC and EMEA and consider more accessible pricing models to diversify its customer base.

Source: Frost & Sullivan

FROST & SULLIVAN



Key Takeaways

Key Takeaways

1

Companies increasingly seek to reduce complexity by consolidating multiple security tools into a single platform to simplify security management and enhance the ability to respond to threats across disparate environments more effectively. CSPM tools must support this shift to help organizations streamline workflows, reduce redundancies, and provide a holistic view of security postures across all cloud resources. This requires CSPM to tightly integrate with the broader cloud security platform (CNAPP) to streamline security operations and increase collaboration between DevOps and SecOps teams. In this light, CSPM tools must accommodate rapid changes in cloud architectures and deploy new technologies without compromising security.

2

Modern CSPM solutions must offer more than periodic assessments and provide continuous monitoring and real-time threat detection to enable organizations to respond immediately to threats and misconfigurations, thereby reducing potential security risks. This can be done by integrating with AI/ML, which can help prioritize security issues and risks effectively, providing actionable insights for risk reduction and remediation. CSPM solutions must also be able to scale to meet growing requirements as organizations expand. The tool needs to handle the growing volume of data, provide coverage of new cloud services across regions without performance degradation, and maintain cost-effectiveness at scale.

Source: Frost & Sullivan

Key Takeaways

3

Selecting a CSPM can be difficult for organizations because vital factors influence decision-making, including solution capabilities, stability, scalability, management, and ROIs. Choosing the right CSPM must align with the organization's security needs, operational efficiency, compliance requirements, and budget. Organizations need to balance and consider the true values 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

© 2024 Frost & Sullivan. All rights reserved. This document contains highly confidential information and is the sole property of Frost & Sullivan.
No part of it may be circulated, quoted, copied, or otherwise reproduced without the written approval of Frost & Sullivan.