FROST & SULLIVAN

Frost Radar™: Cloud-Native Application Protection Platforms, 2026

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

Authored by: Anh Tien Vu
Contributor: Jarad Carleton

PLYX-74
April 2026

© 2026 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.

FROST & SULLIVAN

Strategic Imperative and Growth Environment

List of Abbreviations

- **ADLC:** Application Development Lifecycle
- **ADR:** Application Detection and Response
- **AI SPM:** AI Security Posture Management
- **APA:** Attack Path Analysis
- **APAC:** Asia-Pacific
- **API:** Application Programming Interface
- **AppSec:** Application Security
- **ARR:** Annual Recurring Revenue
- **ASM:** Attack Surface Management
- **ASPM:** Application Security Posture Management
- **AWS:** Amazon Web Services
- **BFSI:** Banking, Financial Services, and Insurance
- **CARS:** Cloud/Application Runtime Security
- **CDR:** Cloud Detection and Response
- **CI/CD:** Continuous Integration and Continuous Delivery
- **CIEM:** Cloud Infrastructure Entitlement Management
- **CIO:** Chief Information Officer
- **CISO:** Chief Information Security Officer
- **CloudSecOps:** Cloud Security Operations
- **CNADR:** Cloud-Native Application Detection and Response
- **CNAPP:** Cloud-Native Application Protection Platform
- **CNDR:** Cloud-Native Detection & Response
- **CSP:** Cloud Service Provider
- **CSPM:** Cloud Security Posture Management
- **CTO:** Chief Technology Officer
- **CWPP:** Cloud Workload Protection Platform
- **DAST:** Dynamic Application Security Testing
- **DevOps:** Development and Operations
- **DevSecOps:** Development and Security Operations
- **DSPM:** Data Security Posture Management
- **eBPF:** Extended Berkeley Packet Filter
- **EDR:** Endpoint Detection and Response
- **EMEA:** Europe, the Middle East, and Africa
- **EPSS:** Exploit Prediction Scoring System
- **FIM:** File Integrity Management
- **GCP:** Google Cloud Platform
- **GRC:** Governance, Risk, Compliance
- **GTM:** Go-to-Market
- **IaaS:** Infrastructure as a Service
- **IaC:** Infrastructure as Code
- **IAST:** Interactive Application Security Testing
- **ICAP:** Internet Content Adaptation Protocol
- **IDE:** Integrated Development Environment
- **ISPM:** Identity Security Posture Management
- **IR:** Incident Response
- **ISV:** Independent Software Vendor
- **ITSM:** IT Service Management
- **JIT:** Just-in-Time
- **K8s:** Kubernetes
- **KSPM:** Kubernetes Security Posture Management
- **LLM:** Large Language Model

Source: Frost & Sullivan

List of Abbreviations (continued)

- **MCP:** Model Context Protocol
- **MDR:** Managed Detection and Response
- **ML:** Machine Learning
- **MSP:** Managed Service Provider
- **MSSP:** Managed Security Service Provider
- **MTTD:** Mean Time to Detect
- **MTTR:** Mean Time to Remediate/Mean Time to Respond
- **NAS:** Network-Attached Storage
- **NG-SIEM:** Next-Generation Security Information Event Management
- **NHI:** Non-human Identity
- **OCI:** Oracle Cloud Infrastructure
- **OSS:** Open-Source Software
- **PaaS:** Platform as a Service
- **PaC:** Policy as Code
- **RASP:** Runtime Application Self-Protection
- **ROI:** Return on Investment
- **SaaS:** Software as a Service
- **SAST:** Static Application Security Testing
- **SBOM:** Software Bill of Materials
- **SCA:** Software Composition Analysis
- **SCM:** Source Code Management
- **SDK:** Software Development Kit
- **SecOps:** Security Operations
- **SI:** System Integrator
- **SIEM:** Security Information and Event Management
- **SMB:** Small and Medium-Sized Business
- **SOAR:** Security Orchestration, Automation, and Response
- **SOC:** Security Operation Center
- **SSCS:** Software Supply Chain Security
- **SSPM:** SaaS Security Posture Management
- **TDR:** Threat Detection and Response
- **USPM:** Unified Security Posture Management
- **UVM:** Universal Vulnerability Management
- **VAR:** Value-Added Reseller
- **VM:** Vulnerability Management
- **WAAP:** Web Application Firewall and API Protection
- **WAF:** Web Application Firewall
- **XDR:** Extended Detection and Response
- **YoY:** Year Over Year

Source: Frost & Sullivan

Strategic Imperative

- Global cloud adoption continues to expand the enterprise attack surface across multicloud environments, K8s, containers, serverless functions, APIs, SaaS-connected services, hybrid estates, and increasingly AI-enabled workloads, making cloud risk more dynamic, distributed, and operationally complex than earlier posture-centric models assumed.
- Modern cloud-native security needs more than a traditional shift-left approach that requires early security integration throughout the ADLC and security management for the cloud where application deployment and execution occur, driving the need for CNAPPs.
- As requirements for modern cloud security operations evolve, CNAPPs are evolving from broad platform consolidation narratives into unified cloud risk operations layers that correlate posture, workload, vulnerability, identity, application, API, data, and emerging AI signals into a unified operating framework for risk prioritization, threat investigation, and remediation.
- CNAPPs are no longer solutions that provide basic visibility, posture data, and compliance reporting. Demand has been increasing for a unified code-to-cloud-to-runtime and to SOC operating model. In this model, security findings in development stage are continuously validated against runtime behavior, exploitability, ownership, and incident context in production, and integrate tightly with SOC workflows to help security analysts detect, investigate, and respond to active cloud threats effectively. Security now spans development code and IaC, through cloud deployment, and all the way to SOC operations and incident response in one connected ecosystem.
- AI security is moving rapidly into CNAPP buying cycles, though remaining as adjacent capabilities. Nonetheless, it is expected to become more tightly integrated into broader cloud security platforms and workflows in the next couple of years.

Source: Frost & Sullivan

Growth Environment

- In 2025, the market generated $7.37 billion in revenue—a robust YoY growth of 30.8%—and is forecast to register a compound annual growth rate of 25.0% from 2025 to 2030. Growth is being shaped by continued expansion of multicloud and hybrid cloud estates, rapid cloud-native development, and broader use of containers, Kubernetes, serverless, APIs, and AI workloads, all of which increase operational complexity and widen the attack surface that security teams must manage consistently across environments.
- Organizations' demand for CNAPP has shifted from broad visibility and posture coverage toward actionable context as they now want platforms that can correlate posture, identity, runtime, data, and application signals to show what is actually exposed, reachable, or exploitable in production.
- CNAPP adoption is moving beyond static posture and compliance management use cases toward runtime-validated risk reduction, CDR, guided remediation, and code-to-cloud or cloud-to-code correlation that can support prevention and operational response.
- Board-level discussions around shift-left security and software supply chain risks have elevated the importance of CNAPP solutions. As organizations face more scrutiny regarding how they manage their cloud environments and protect their software supply chains, the need for a comprehensive security platform that can address development and runtime security is becoming more apparent.
- Alert fatigue will remain 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, creating a significant "technical debt" to address in later days.

Source: Frost & Sullivan

Growth Environment (continued)

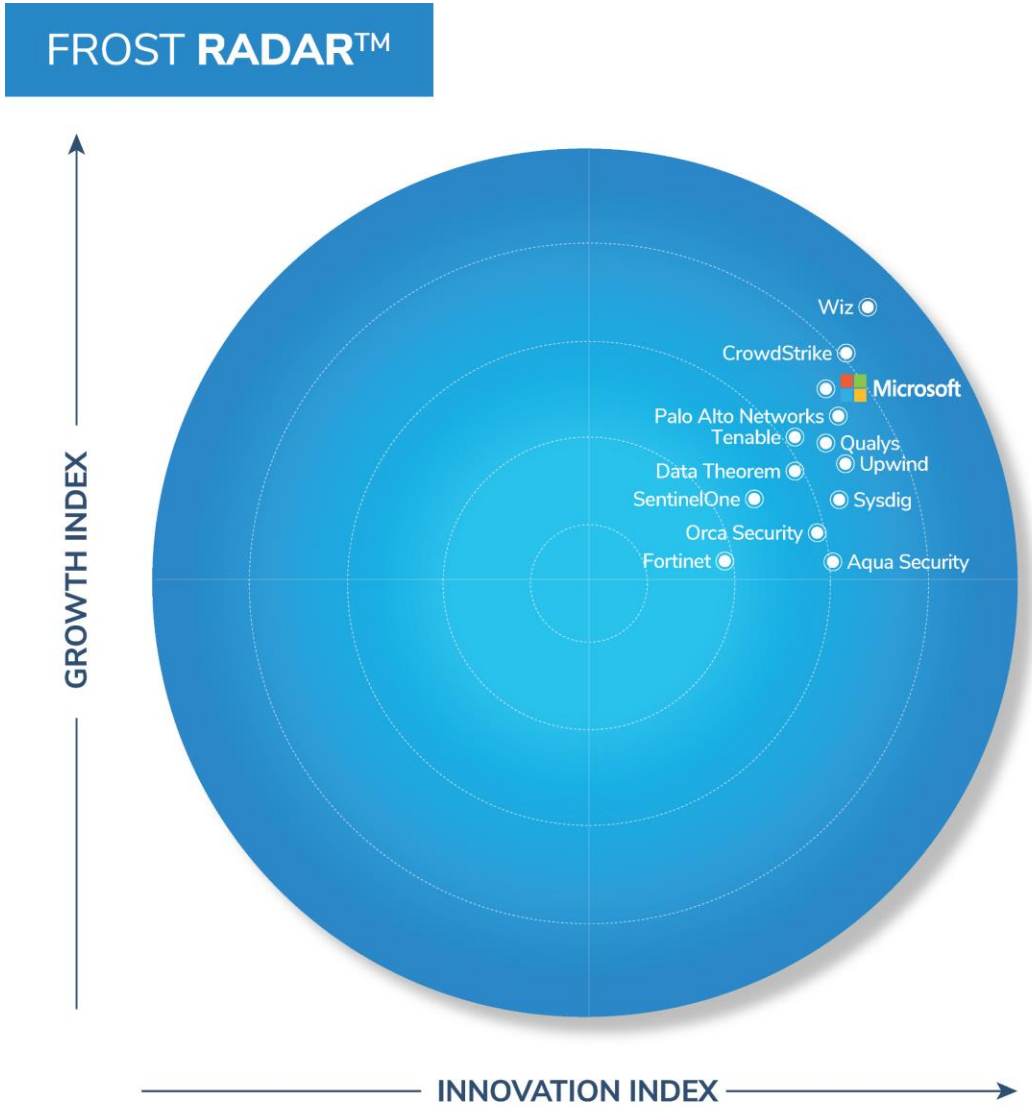
- Budget justification is becoming more pragmatic as CISOs increasingly approve CNAPP investments based on risk reduction, audit readiness, operational efficiency, headcount leverage, and consolidation benefits rather than on feature breadth alone.
- Regulatory pressure remains one of the strongest structural growth drivers, but its effect varies by region. In EMEA, privacy, sovereignty, and AI-related regulations strongly influence vendor selection, deployment models, and data processing requirements, while in North America buying is driven more by operationalization, sophisticated threat activity, and the need for real-time response.
- Regional adoption patterns are diverging in ways that matter for CNAPP vendors. North America is the most mature and platform-oriented market, EMEA is shaped by compliance and in-region data handling requirements, APAC is growing quickly but unevenly because of cloud maturity differences and skills gaps, and Latin America is earlier stage but gaining momentum through cloud expansion and digital transformation.
- Procurement preferences also affect vendor growth, with North America tending to favor direct sales and cloud marketplace transactions, while EMEA is more partner-driven and compliance-heavy. APAC more often leans on MSSPs and partners that support deployment, which means vendor ecosystem strength and channel execution increasingly influence growth outcomes.
- Several barriers continue to slow adoption even as the market grows, including integration complexity; unclear ownership across security, DevOps, AppSec, and platform teams; skills shortages; trust issues around runtime controls; and difficulty operationalizing findings across multiple tools and workflows. Cost and commercial friction also influence growth because CISOs care more about pricing transparency, licensing flexibility, and long-term platform economics, especially when renewal pressure, migration risk, or vendor lock-in concerns can disrupt adoption or expansion decisions.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Cloud-Native Application Protection Platforms, 2026

Frost Radar™: Cloud-Native Application Protection Platforms



Source: Frost & Sullivan

Frost Radar™ Competitive Environment

- Vendors featured in this Frost Radar™ analysis met the following criteria:
  - Generated at least $30 million in revenue in calendar year 2025
  - Have a CNAPP platform or related capabilities, including CSPM, CWPP, container security, IaC security, CDR, or AI SPM
  - Have business presence globally or in at least in two regions (North America, EMEA, APAC, or Latin America)
- Featured vendors include Aqua Security, CrowdStrike, Data Theorem, Fortinet, Microsoft, Orca Security, Palo Alto Networks, Qualys, SentinelOne, Sysdig, Tenable, Upwind, and Wiz. Frost & Sullivan identified these companies as leading technology players in the global CNAPP market.
- Other vendors are not included in this analysis because of one or more reasons:
  - Limited revenue and relatively small market presence globally
  - Declined participation
  - Unable to provide direct input
  - Insufficient data from secondary research to conduct a thorough analysis
- While revenue projections are based on calendar year 2025, the evaluation relies on information, vendor performance, and market conditions as of March 31, 2026.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued) (1 of 5)

- The key competition focus in 2025 and 2026 is about platform consolidation, runtime security, ecosystem integration, and SOC centricity, where companies are racing to deliver high-fidelity runtime and low-noise telemetry to help security teams gain visibility and detect active threats in the production environment, translating it into rapid and accurate detection and remediation actions.
- Vendors are differentiating themselves by embedding all capabilities, including posture management (e.g., CSPM, CIEM, and AI security), application code security, compliance, runtime security (e.g. CWPP, CDR, and ADR), and SOC in broader exposure management and CNAPP platforms to deliver end-to-end governance from code to cloud, extending beyond static posture checks to correlate runtime validation, risk correlation, and continuous compliance while also embedding capabilities into DevSecOps pipelines and SOC workflows for unified risk visibility and response.
- Autonomous security operations is a primary roadmap theme, with agentic investigation and remediation capabilities, including AI-driven SOC, that correlate telemetry, map attack paths, and generate complete incident narratives to reduce MTTR and simplify security operations to manage cloud security alert volumes better without an increase in headcount.
- Vendors are racing to deliver exploitability-based risk prioritization to reduce alert fatigue, with differentiated approaches including deep application inspection and library-level runtime filtering, behavioral baselining and execution context analysis, dynamic attack path mapping, contextual risk correlation, AI-powered prioritization, and automated and AI-guided remediation pipelines. The capabilities are tightly integrated with DevOps and CI/CD workflows for better misconfiguration and posture management in the lifecycle as well as strengthened software supply chain security.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued) (5 of 5)

- Microsoft is the only hyperscale player featured in this analysis. It continues to be the largest CNAPP vendor in terms of revenue because of its huge Azure customer base, while extending its foothold in other cloud environments, including GCP and AWS. It is also a leading CNAPP player in term of platform offerings, with its Defender for Cloud that integrates CSPM, workload protection, vulnerability, data security, CDR, and AI security in the Azure ecosystem. Its strength lies in deep integration with Azure, identity (Entra ID) and data security, and broader Microsoft security stack. The company is strengthening its platform with an emphasis on unification to increase the user experience and expanding AI workload protection as part of its broader AI strategy.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Companies to Action

Microsoft

INNOVATION

- Microsoft Defender for Cloud (MDC) has evolved to become one of the most comprehensive and deeply integrated CNAPP platforms, spanning the full cloud security lifecycle from code to cloud to SOC. The platform covers unified posture management across infrastructure, applications, data, AI workloads, and APIs; workload protection across servers, containers, databases, storage, and serverless compute; identity security through CIEM; DevSecOps integration with CI/CD pipeline hardening; and advanced TDR—all delivered through a single, converged experience across Azure, AWS, GCP, and hybrid environments.
- What distinguishes MDC is its ability to correlate telemetry across those capabilities into a unified security workflow. Findings of posture (CSPM), vulnerability data (CWPP), identity risk (CIEM), data sensitivity (DSPM), and runtime telemetry (CDR) are correlated with attack path analysis into a unified security workflow. Through integration with Microsoft Security Exposure Management and the unified Defender portal, these signals are surfaced alongside risk-based secure scoring, prioritized recommendations, and vulnerability context across devices, identities, cloud apps, data, and cloud workloads. This gives security teams the ability to manage their entire enterprise exposure surface without platform context switching, while enabling AI-assisted investigation, remediation guidance, and SOC workflow automation, significantly reducing the operational burden on security teams managing complex, multicloud environments.
- Microsoft's strengths also lie in the deep integration with its own extensive ecosystem, including Visual Studio, GitHub, Azure DevOps, and CI/CD pipelines, runtime context, and SOC workflows, allowing it to deliver code-to-cloud security capabilities that span prevention in development to runtime protection and SOC response.

Source: Frost & Sullivan

Microsoft (continued) (1 of 5)

INNOVATION

- Microsoft has expanded its CNAPP beyond IaaS into the application, AI, and data layers with AI and API security to protect AI workloads, AI agents, and associated data pipelines, applications, and unauthenticated and internet-exposed APIs.
- MDC's TDR capabilities have been enhanced with its CDR engine that processes runtime telemetry across cloud control planes, workloads, and K8s environments. Signals from CDR are fed into the unified Defender XDR platform for cross-domain incident investigation and response. Microsoft has also sharpened its APA, incorporating external entry points, realistic lateral movement scenarios, Entra OAuth application compromise vectors, and trusted IP-based internet exposure, to enhance risk prioritization and make threat prioritization more accurate and defensible for SOC teams.
- By combining its broad posture coverage, AI and API security expansion, CDR depth, unified SOC integration, and developer-first security capabilities, Microsoft positions MDC as a comprehensive CNAPP platform driven by a deep integration across its security ecosystem. Its ability to correlate cloud risk signals with identity, endpoint, data security, threat intelligence, and SecOps workflows across the Microsoft security stack gives MDC a depth of cross-domain integration that few stand-alone CNAPP vendors can match, making it a particularly compelling choice for organizations already operating in the Microsoft security ecosystem.

Source: Frost & Sullivan

Microsoft (continued) (2 of 5)

GROWTH

- Microsoft's cloud security revenue growth was estimated at more than 30% in 2025, with robust growth being maintained into 2026.
- MDC is structured around a modular, workload-based commercial model that allows organizations to expand coverage as their needs grow. The platform includes foundational CSPM capabilities and access to Microsoft Defender XDR for free (automatically enabled upon Azure subscription onboarding). Organizations that need deeper posture capabilities can activate the paid Defender CSPM plan, unlocking advanced features including agentless scanning, attack path analysis, data-aware security posture, AI SPM, API SPM, and cloud security graph capabilities.
- Organizations can activate workload-specific protection plans, including Defender for Servers, Defender for Containers, Defender for Databases, Defender for Storage, Defender for App Service, and Defender for AI Services, allowing them to adjust their cloud security investment to their specific risk profile and infrastructure footprint.
- The modular and flexible model has been a growth driver for Microsoft's cloud security business because it gives organizations affordable access to its cloud security services, creating a natural expansion path as security postures mature. This has contributed to platform-level traction, with Microsoft's CNAPP adopted widely by organizations with significant Azure footprints.

Source: Frost & Sullivan

Microsoft (continued) (3 of 5)

GROWTH

- It is also gaining traction among large enterprises running hybrid and multicloud environments spanning AWS and Google Cloud, particularly technology, BFSI, manufacturing, healthcare, education, and government organizations that leverage MDC to gain unified visibility across their multicloud environment for regulatory compliance management, cloud-native and AI workload misconfiguration detection and remediation, and SOC workflow integration.
- Microsoft's GTM strength is driven by its extensive partner ecosystems in the enterprise security industry. A broad network of channel partners, global system integrators, and MSSPs expands its market outreach and delivers MDC as part of broader digital transformation and security modernization engagements.
- A large ISV ecosystem extends the platform's reach through seamless integrations, joint commercial agreements, and co-selling arrangements across the Microsoft marketplace. Ecosystem depth increases enterprise buyers' confidence, accelerates deployment at scale, and creates long-term platform loyalty that supports Microsoft's growth across its installed base and net-new cloud security buyers.

Source: Frost & Sullivan

Microsoft (continued) (4 of 5)

FROST PERSPECTIVE

- Microsoft is an innovation leader in cloud security, with one of the most comprehensive CNAPP offerings. The platform stands out not just for its breadth of coverage across infrastructure, workloads, identities, data, and applications, but also for its deep integration with Microsoft's broader security ecosystem, allowing organizations to secure modern and AI-native application lifecycles while reducing operational complexity.
- Microsoft's ability to unify posture management and protection across cloud infrastructure, workloads, applications, and AI environments is a strategic advantage. The addition of AI SPM, API SPM, and serverless coverage reflects a clear intent to evolve MDC from a cloud infrastructure protection tool into a multidomain, risk-driven platform that secures modern application lifecycles end to end, from code to runtime and into SOC operations.
- The platform's integration with Microsoft Defender External Attack Surface Management strengthens its cloud security posture narrative, enabling organizations to correlate internal posture and exposure data with externally observed attack surface signals to identify genuinely exploitable attack paths and prioritize remediation with greater accuracy.
- By correlating posture findings, vulnerability data, identity risk, and runtime telemetry through Microsoft Security Exposure Management and attack path analysis, Microsoft is transforming cloud security from isolated signal collection to a unified, context-rich risk prioritization fabric. With Security Copilot integration for AI-assisted investigation and remediation, together with runtime context validation for developer tooling, such as GitHub Advanced Security, Microsoft is building a code-to-cloud-to-SOC platform experience that spans the full security lifecycle in a single converged workflow.

Source: Frost & Sullivan

Microsoft (continued) (5 of 5)

FROST PERSPECTIVE

- Microsoft's cloud security narrative is most naturally compelling for organizations operating in its own ecosystem. While MDC supports AWS and GCP through agentless scanning and multicloud posture management, the platform's deepest integrations, most seamless workflows, and strongest user experience are anchored in the Azure environment.
- To sustain and strengthen its leadership position, Microsoft should continue deepening its multicloud runtime protection capabilities, sharpening the visual richness and analytical depth of its exposure graph, and expanding its CDR capabilities to deliver detection and response across AWS and GCP environments to match the Azure-native experience.
- Microsoft should also broaden its cloud-centric GTM motion beyond its traditional enterprise and Azure-centric buyer base by growing its CNAPP-focused MSSP, ISV, and global reseller ecosystem, and design its GTM messaging to explicitly address multicloud security scenarios beyond Azure concentration. This would help expand MDC's addressable market and help the company compete more directly for cloud-first and multicloud-native buyers that are more likely to evaluate pure-play CNAPP vendors.
- With its continued investment in platform unification, AI-driven risk prioritization, cross-domain data correlation, and ecosystem convergence, Microsoft is well positioned to solidify MDC as a code-to-cloud-to-SOC platform. The vendor needs to translate its innovation depth and ecosystem scale into a stronger and more universally compelling CNAPP narrative to resonate with organizations that need multicloud/cloud-agnostic security platform, not just with those already operating in the Microsoft security fabric.

Source: Frost & Sullivan

Best Practices & Growth Opportunities

Best Practices

1. Organizations should treat CNAPP as a unified cloud risk operations platform rather than a collection of disconnected posture, workload, identity, and AppSec tools. It should function as a common control plane across code, cloud, runtime, data, AI workloads, and SOC workflows, correlating posture findings, vulnerabilities, identities, network and API exposures, and runtime behavior to improve risk prioritization, reduce tool sprawl and alert fatigue, and accelerate remediation and operational efficiency.

2. To strengthen prevention and operational response execution, organizations should operationalize CNAPP across the full code-to-cloud-to-SOC lifecycle, focusing on runtime validation, real-time threat detection, and incident response. The integrated model allows organizations to trace risk end to end, from code, configuration, and identity exposure to runtime behavior and downstream data impact, with SOC and developer workflows for faster investigation, clearer ownership, and more consistent remediation.

3. Organizations should treat AI and data security and ecosystem interoperability as core CNAPP requirements rather than adjacent capabilities for better governance, control, protection, and security of their AI services, models, agents, APIs, identities, and sensitive data flows in the same platform context. This will help them prioritize risk more accurately across AI infrastructure, application, access, and data exposures as AI and cloud-native applications become more central to enterprise operations.

Source: Frost & Sullivan

Growth Opportunities

1. Vendors can unlock growth by positioning CNAPP as a unified execution platform, |extending from posture, vulnerability, and compliance into runtime detection, investigation, and response across code-to-cloud-to-SOC workflows. Platforms that correlate shift-left findings with live runtime data to provide actionable insights, risk prioritization, TDR, and high-quality remediation recommendations can create stronger differentiation.

2. Vendors can expand CNAPP beyond traditional security capabilities into AI, data, API and application, and identity, as they are expected to operate in one contextual platform sharing the same data lake, engine, and architecture. CNAPP should enhance the correlation capabilities of AI assets, sensitive data, exposed APIs, identities, and runtime behavior into a unified risk view to address enterprise demands around AI governance, data exposure, and runtime AppSec.

3. Vendors and partners can drive broader CNAPP adoption by combining platform consolidation with low-friction onboarding, flexible deployment models, and open integration into existing SOC, cloud, and developer ecosystems—particularly for large enterprises, regulated sectors, and cost-sensitive markets where legacy systems are often in place. Support of phased expansion and delivery of interoperable processes across cloud environments are crucial for vendors to grow in this highly competitive market.

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 megatrends) 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

MEGATRENDS 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 megatrends 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

Next Steps

JOIN:
Growth Council

APPLY:
Companies to Action

ENGAGE:
Growth Dialog

PARTICIPATE:
Growth Council Think Tank

Does your current system support rapid adaptation to emerging opportunities?

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

© 2026 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.