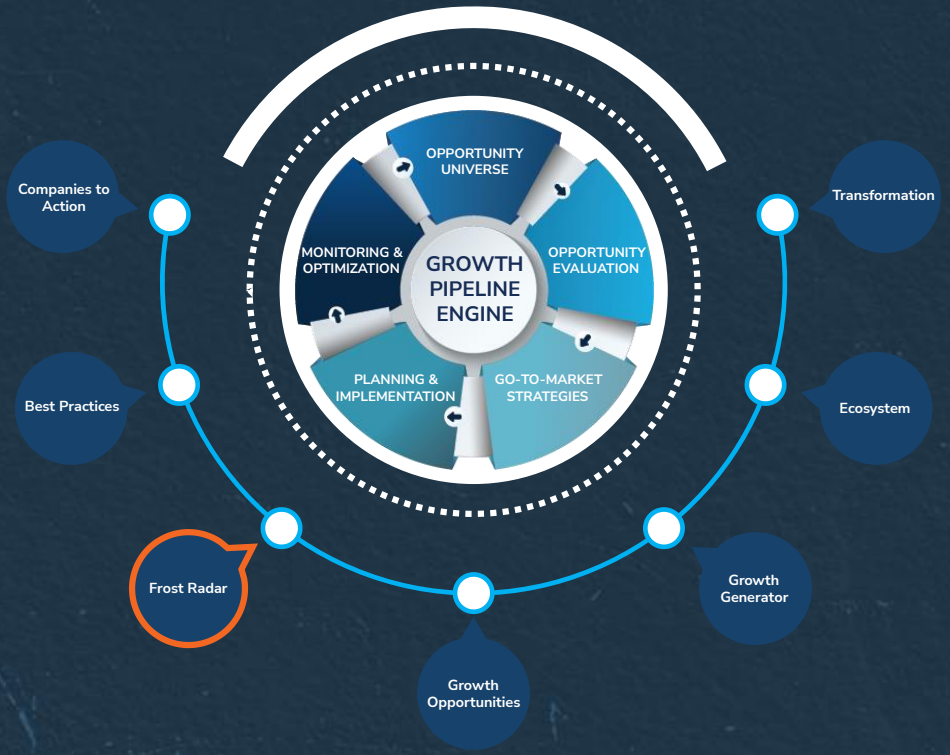
FROST & SULLIVAN

Frost Radar™ : Application Security Posture Management, 2024

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



Authored by: Vivien Pua

Contributor: Jarad Carleton

PFL3-74
September 2024

FROST & SULLIVAN

Strategic Imperative and Growth Environment

Source: Frost & Sullivan

Strategic Imperative

- Organizations face challenges managing security risks in the ever-more complex software development environment. The increasing use of cloud services and cloud-native technologies, AI-generated code, and other large language models (LLMs), coupled with the siloed deployment of various software testing, scanning, and other application security tools, has resulted in an overwhelming volume of alerts and vulnerabilities with increasing risk of new and emerging security threats. The expanding application risks pose more significant challenges for organizations to maintain end-to-end visibility and control over their application security posture.
- The increasing complexity of modern software development and the overload of noise due to application security tool sprawl necessitate the role of application security posture management (ASPM) in application security programs. An ASPM solution provides a holistic view of the application security landscape with centralized control to identify, prioritize, and remediate vulnerabilities that pose the most critical risks to business operations.
- An emphasis on development, security, and operations (DevSecOps) and a shift-left security approach are also driving ASPM adoption to meet organizations' increasing security requirements. By integrating with the DevOps pipeline and developer workflows, ASPM solutions help organizations accelerate the process of secure application development with a developer-first security approach, fostering better collaboration between security and development teams.
- With applications still the primary targets of attack, organizations' heightened concern about cyberthreats also drives ASPM adoption, as it allows chief information security officers (CISOs) to align their application security strategy with business objectives. This shift in security strategy to focus on better managing business risk will require ASPM solutions to identify, correlate, prioritize, and remediate security vulnerabilities in applications across the software development life cycle (SDLC).

Strategic Imperative (continued)

- It is imperative to provide an organization's CISOs and security team a consolidated code-to-cloud view of security and risk status that positions them to take a proactive approach to better managing the security posture of their applications.
- ASPM platforms empower organizations to better manage the security posture of their applications by continuously managing application risks through data aggregation, correlation, and contextualization; risk-based prioritization considering vulnerability exploitability, reachability, and business context; unified policy enforcement; automated scanning, triaging, remediation, and response workflows; and streamlined compliance monitoring and reporting. Comprehensive visibility into the entire SDLC generates rich security findings and contextual analysis that help with risk-based prioritization and resolution of vulnerabilities.
- The following are 6 key features required of an ASPM tool.
  - Application inventory and visibility: This includes automatic identification of applications across on-premises and cloud-hosted platforms to provide visibility into application architecture, code components, dependencies, application programming interfaces (APIs), frameworks, and other relevant data for contextual analysis.
  - Triage and prioritization: ASPM solutions need to automatically triage and prioritize security risks associated with application vulnerabilities based on vulnerability exploitability, reachability, and business impact factors to help organizations prioritize the critical vulnerabilities.
  - Remediation and mitigation: It is important for ASPM solutions to provide actionable remediation guidance on how to fix security vulnerabilities.

Source: Frost & Sullivan

Strategic Imperative (continued)

- Streamlined compliance: ASPM solutions need to ensure that organizations' applications comply with security policies, standards, and regulations.
- Reporting and analytics: This feature includes generating reports and dashboards that help organizations understand the security posture of their applications.
- Integration with third-party tools: By aggregating and analyzing data from different sources, including software development, deployment, and operation stages, an ASPM solution can correlate and provide a unified view of security findings.

- Organizations can find selecting an ASPM solution difficult because the market is still developing, and vendors are taking different approaches to achieving ASPM outcomes. As such, organizations should consider an ASPM solution that aligns with their security needs, risk management strategy, DevSecOps approach, operational efficiency, and compliance requirements during the evaluation process. A solid ASPM solution should offer the following 8 features.
  - Risk-based prioritization through data aggregation, correlation, deduplication, and contextualization that considers severity, exploitability, asset context, and exposure factors so that customers can prioritize the most critical issues to their business operations
  - Orchestration capabilities and streamlined application security workflows that improve efficiency, reduce manual efforts and mean time to resolution, and standardize and centralize application security policies and service level agreement (SLA) enforcement
  - Automated asset discovery, dependency scanning, and mapping to provide accurate application inventory and generate up-to-date software bills of materials (SBOMs) and software-as-a-service BOM (SaaS BOM) as required

Source: Frost & Sullivan

Strategic Imperative (continued)

- Comprehensive code-to-cloud data sources coverage by ingesting and unifying data from the integration of native, open-source, or third-party application security scanning tools such as software composition analysis (SCA), source code management (SCM), static application security testing (SAST), dynamic application security testing (DAST), and container and infrastructure-as-code security; security tools such as application programming interface (API) security, software supply chain security (SSCS), and cloud security posture management (CSPM); and developer tools such as artifact registry, continuous integration and continuous delivery/deployment (CI/CD) tools and platforms, and cloud development platforms spanning where the applications are built (pre-production), deployed, and operated (production).
- Flexible and efficient remediation process that integrates with popular notification and ticketing systems to provide auto-remediation or semi-automated remediation directly within the CI/CD pipelines depending on customer preference; actionable guidance with complete and relevant context when sending fixes to the right code owner required to enable quick resolution to identified issues
- Flexible deployment options that support SaaS, private cloud, on-premises, multi-cloud, or hybrid-cloud environments to secure a mix of cloud-native and legacy applications
- User-friendly interface with customizable dashboard to display relevant security metrics and insights for different stakeholders, including security, developer, and business executives
- Compliance posture management that facilitates compliance audits and generates reports that demonstrate continuous adherence to a wide and expanding range of regulations, frameworks, and industry standards

Source: Frost & Sullivan

Strategic Imperative (continued)

- While many ASPM solutions primarily focus on code-level context, a rising trend is to leverage runtime context for a more holistic view from both development and runtime environments. ASPM solutions will increasingly integrate with CSPM and cloud-native application protection platform (CNAPP) for code-to-cloud runtime risk visibility and holistic risk management. Correlation and contextual analysis between code-level context and cloud runtime data will improve the accuracy of risk-based prioritization and enable a more effective remediation process.
- ASPM vendors increasingly prefer to integrate native application security scanning capabilities into ASPM tools to reduce dependency on third-party tools while improving the accuracy and quality of scanning results, maintaining consistency, and enhancing the correlation between security findings and relevant context.
- Nonetheless, ASPM vendors need to support open integration with third-party scanners and help customers who take a best-of-breed approach by consolidating scan results from multiple application security testing (AST) tools, development tools, and other security solutions for comprehensive security findings. The additional data from third-party tools will complement the native scanning capabilities. However, ASPM vendors must ensure seamless interoperability when exchanging data from diverse security tools to obtain high accuracy and consistent, standardized scan results.
- ASPM solutions are on track for expanded integration with CI/CD tools, DevOps platforms, cloud platforms, and others for improved developer-friendly workflows and better remediation orchestration. As developers play a critical role in resolving issues with the codebase, ASPM will continue to help them fix issues quickly, with actionable remediation guidance and clear remediation steps.

Source: Frost & Sullivan

Strategic Imperative (continued)

- The evolution of ASPM solutions is marked by the increasing use of AI and ML. Customers are using these technologies in predictive analytics, automated remediation processes, and correlation and prioritization. This adoption will significantly improve efficiency and enhance the security posture of AI-based applications.
- The rapid growth of cyberattacks related to software supply chains caused by the surge in adoption of open-source and third-party tools, libraries, code, frameworks, and services has emphasized the need for ASPM to incorporate software supply chain security (SSCS) as part of the platform.
- In 2023, the introduction of a software bill of materials (SBOM) requirement for those who provide software to US government agencies has necessitated the vetting of third-party components for security vulnerabilities. The stringent regulation will continue driving more robust requirements among organizations to incorporate SSCS findings into the ASPM platform for comprehensive application security posture management.

Source: Frost & Sullivan

Growth Environment

- The transition to modern application development and the increasing adoption of DevSecOps practices are set to drive the deployment of ASPM as part of an organization's cybersecurity strategy. ASPM adoption has increased significantly in the last two years, and the market is set to maintain strong growth momentum during the next five years, with a compound annual growth rate (CAGR) of 30.1% from 2024 to 2029.
- North America (NA) will remain the largest revenue contributor in the global ASPM market in the next five years, dominating with more significant advancements in modernizing application security strategies and embracing the approach. The acceleration of DevOps and stringent regulations in the Europe, Middle East, a and Africa (EMEA) is set to drive more robust adoption of ASPM for organizations to manage application risks and enhance their application security posture. The rapid digital transformation and acceleration of application development activities in Asia-Pacific (APAC) have increased awareness about the need to adopt application security to secure the DevOps process. Countries with high maturity levels in cybersecurity, such as Australia, Japan, and Singapore, will drive the adoption of ASPM in the next five years. Investment in ASPM in Latin America (LATAM) remains limited because of low awareness about adopting shift-left security and application security during the DevOps process.
- The growing complexity of modern DevOps practices due to the widespread adoption of cloud-native technologies while developing applications; the overload of alerts and false positives from siloed application testing and security tools; the stronger emphasis on embedding security in the DevOps pipeline; the stringent regulations with heightened attention to software supply chain and data privacy; and the rising application and software supply chain attacks will remain the top factors driving ASPM adoption. Organizations will increasingly leverage ASPM for comprehensive visibility and control over managing application risks across the SDLC, supported by effective governance and guardrails that align with their risk tolerance without slowing the application development process.

Source: Frost & Sullivan

Growth Environment (continued)

- However, several factors will lead to slower adoption of ASPM solutions and thereby hinder market growth in the next five years: confusion about ASPM solutions as numerous new vendors enter with varying approaches; a lack of security professionals to implement and manage ASPM tools; ASPM solutions largely tailored to serve large enterprises and often overlooking the small and midsize business (SMB) market segment; budgetary constraints due to economic and geopolitical factors; and resistance to change and acceptance of new technologies and processes.
- Despite these challenges, the acceleration of development due to increasing adoption of AI-generated code and LLMs in the last one to two years has put greater pressure on CISOs to manage the increased risk exposure and obtain unified visibility into their application security risk and SDLC.
- The urgency to provide protective guardrails, risk-based prioritization, and remediation against the rising volume of vulnerabilities without disrupting development workflows will drive the adoption of ASPM, particularly among large enterprises with complex, distributed development environments and software-driven technology companies.
- It is essential for ASPM vendors to educate the market and promote higher awareness and understanding of the benefits that ASPM can bring to security and development teams in helping organizations strengthen their application security posture. The growing recognition of integrating ASPM as part of the application security strategy to proactively identify and address security vulnerabilities that pose critical risks to business operations began only in 2023, and mature regions, such as North America, mainly drive solution adoption. The growth opportunities in other regions, such as EMEA and APAC, will drive the future of ASPM as these solutions continue to evolve to address more comprehensive use cases.

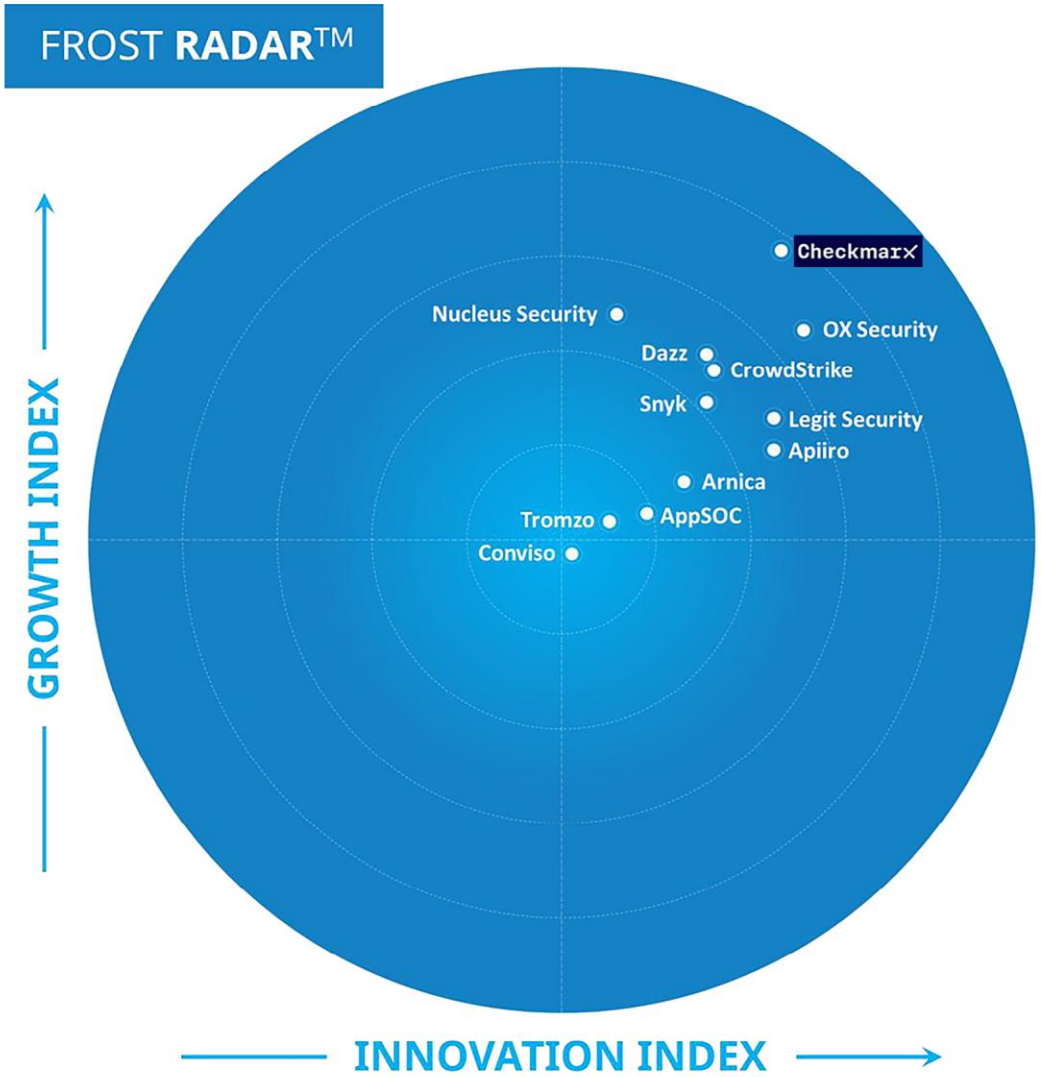
Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Application Security Posture Management, 2024

Source: Frost & Sullivan

Frost Radar™: Application Security Posture Management, 2024



FROST & SULLIVAN

Source: Frost & Sullivan

Frost Radar™ Competitive Environment

- The ASPM market is still in its nascent stage. As it continues developing, the vendor list is expanding, with numerous new competitors entering and introducing various approaches. These ASPM vendors typically fall into the following three categories:
  - Vendors that take signals from third-party AST tools and add value to the consolidated results, with limited native scanners or without native scanning capability
  - Application security solution vendors that add ASPM modules to their proprietary application scanning tools while enabling integration with third-party AST tools for comprehensive data sources
  - Cloud security solution vendors that acquire application security companies as part of their shift-left security strategy
- While all ASPM vendors continue to provide flexibility and practice open integrations to ingest data and signals from a variety of security tools for code-to-cloud visibility, it is important for them to ensure the quality and depth of integration between these third-party tools and the ASPM platform for data standardization and higher accuracy and quality of scan results. Therefore, ASPM vendors that offer solutions with native scanning capabilities have the advantage of providing greater value to their customers with more effective prioritization and remediation of issues.
- Another growing trend is the incorporation of cloud runtime context into ASPM analysis to provide continuous visibility into the cloud runtime environment, allowing better contextual understanding of vulnerabilities and the higher accuracy of risk-based prioritization. As a result, ASPM vendors are expanding their technology partnerships with leading cloud security vendors including Wiz, Orca Security, Sysdig, Lacework, and Palo Alto Networks to provide end-to-end visibility into application risks.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- In the next three years, Frost & Sullivan expects ASPM companies to continue expanding their ASPM capabilities through acquisitions, enhancements of open-source tools, or in-house developments to provide comprehensive security coverage across the SDLC.
- With organizations giving more attention to managing application risks and strengthening their application security posture, the global ASPM market continues expanding, with more than 30 vendors offering ASPM solutions, including established cybersecurity vendors with experience in application security, cloud security, and vulnerability management; and SaaS-based start-ups focusing on different areas to address challenges in managing application security posture.
- Of those vendors, Frost & Sullivan evaluated the top 12 ASPM companies in this Frost Radar™ analysis, each of which meet the following criteria:
  - Integrate self-developed, open-source, or third-party application security testing tools to correlate data and offer a comprehensive code-to-cloud visibility
  - Achieve annual revenue of at least $1.0 million in the total ASPM market in 2024
- The 12 companies featured are Apiiro, AppSOC, Arnica, Checkmarx, Conviso, CrowdStrike, Dazz, Legit Security, Nucleus Security, OX Security, Snyk, and Tromzo.
- Frost & Sullivan based company revenue on CY 2024, and all qualitative insights on information available and market conditions as of August 2024.
- Vendors that met the inclusion criteria mentioned above but could not share detailed insight into their solution were excluded to ensure fair scoring and comparison.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Checkmarx and OX Security are the leaders on both the Growth and Innovation Indexes for their excellent business performance and commitment to expanding their ASPM solution capabilities in the past three years.
- Checkmarx leverages its long-standing leadership position in application security to dominate the global ASPM market with a market share of 21.3% in 2024. The company experienced tremendous growth in 2023 as it strategically moved its existing application security customers to the Checkmarx One platform, of which ASPM is an integral component. All Checkmarx One customers can access the ASPM solution automatically at no additional cost when they subscribe to Checkmarx One. By leveraging the existing customer base in application security, the company has strengthened its footprint in every region and leads the global ASPM market as the largest player.
- In terms of innovation, Checkmarx has introduced application risk management that allows customers to focus remediation by application criticality and risk associated; an analytics module that enables customers to manage their application security posture under a single view; a tailored dashboard to present relevant metrics to business executives; and the ability to integrate findings from third-party AST tools to provide customers with greater flexibility in consolidating their existing tools into Checkmarx One.
- OX Security, one of the fastest-growing players, achieved solid triple-digit growth in 2024. It stands out on the Growth Index for its growth momentum in the past three years, which strengthened its leadership position in the global ASPM market. The company's exceptional growth results from effort in expanding its local and international channel partners and relentless focus on customer experience and success.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- On the Innovation Index, OX Security demonstrated leadership by offering a comprehensive ASPM platform with breadth and depth of coverage through its AppSec Data Fabric. The capabilities of its ASPM solution, including in-depth visibility into application environments across code, APIs, and cloud; rich contextual analysis; comprehensive BOM overview; and no-code response and remediation workflow automation position the company distinctly ahead of other ASPM solution providers that lack this level of comprehensiveness and visibility across all applications and components.
- Nucleus Security is another leader on the Growth Index. The company has demonstrated strong growth momentum in 2023 and 2024, with YoY market growth rates of 92.9% and 99.6%. Solid business performance has positioned the company to maintain its leadership position in the global ASPM market in 2024. Leveraging its extensive experience in risk-based vulnerability management solutions, the company has incorporated ASPM in its broader platform. The company takes a neutral position to work with all industry players, including ASPM vendors, to address various use cases.
- Dazz, CrowdStrike, and Snyk are positioned favorably on the Growth Index.
- Dazz experienced tremendous growth in 2023 and 2024. Ongoing efforts to streamline remediation processes and improve mean-time-to-response (MTTR) through patented AI, automation, and root-cause analysis technologies fueled its excellent business performance. The recent fundraising of $50 million to enhance risk prioritization and remediation using AI technologies is likely to drive more robust adoption of its ASPM solutions in the next three years.
- As a leading endpoint and cloud security player, CrowdStrike's expansion into the ASPM market after acquiring Bionic positioned it to maintain leadership as the third-largest ASPM player, with year-over-year (YoY) growth of 32.2% in 2024. The robust channel partner ecosystem and excellent customer support will continue to drive adoption of its ASPM solutions across global regions.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Following the launch of its ASPM solution, Snyk AppRisk, in late 2023, Snyk achieved tremendous growth in 2024 to increase its market share at a YoY growth rate of 359.9%. The significant adoption of its application security tools among developers provides the company an advantage over other ASPM vendors in upselling its ASPM solution. Snyk's well-established channel partner ecosystem and its holistic approach to customer experience help organizations build and scale their application security programs, allowing them to successfully implement and maximize value from their investment in Snyk.
- Apiiro is another leader on the Innovation Index. The company's unique approach to mapping all software components, connections, and material changes with its patented deep code analysis (DCA) and runtime context help organizations unify risk visibility, assessment, prioritization, and governance across applications and software supply chains. Apiiro continually enhances its ASPM capabilities by providing deeper insights into applications, expanding open platform integrations, and introducing more enterprise-grade features to address customer needs.
- Legit Security is another leader on the Innovation Index that has demonstrated commitment to advancing its ASPM platform with native secret scanning, AI discovery, and government; expanded integrations with developer tools, application security scanners, and cloud security solutions; extended compliance capabilities to support more regulatory frameworks; and expanded AI-SPM capabilities in 2023 and 2024. Its strategic R&D investment to enhance its ASPM platform capabilities exemplifies commitment to innovation. The enhancements align with the ASPM market megatrends that Frost & Sullivan identifies, particularly around AI application security and software supply chain security.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Dazz, CrowdStrike, and Snyk are positioned favorably on the Innovation Index. Dazz's ASPM solution demonstrates strong remediation capabilities to help organizations effectively streamline the remediation process, in addition to the depth of the dependency graph, comprehensive mapping of attack path analysis under its pipeline visibility function, and patented root cause analysis capability that provides visibility in code, cloud, infrastructure, on-premises environments.
- CrowdStrike stands out on the Innovation Index with its agentless approach and native scanning capabilities for mapping application pipelines and providing visibility into applications, including microservices and their database connections, APIs, dataflows, libraries, configuration files, and dependencies. The company's up-to-date application inventory allows it to address the increasing requirements of organizations around SBOM.
- Snyk leverages its extensive experience in application security to provide comprehensive visibility into applications across the SDLC with its AppRisk solution. The structured inventory of the assets involved in building, deploying, and running applications helps go address security coverage gap, drive risk-based prioritization, and provide an overview of the organization's application security program with program performance and risk key performance indicators (KPIs).
- Arnica has adopted a pipelineless approach and developed its security tools, including SAST, SCA, secrets detection and mitigation, IaC security, behavior-based security, and zero trust security model, to provide comprehensive security coverage across the SDLC. The native integration between its in-house-developed security tools and ASPM platform helps reduce developer friction and accelerates identifying and remediating vulnerabilities without extensive CI/CD pipeline configurations.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- AppSOC demonstrates laser focus on developing AI application security to complement its ASPM platform. The company's ASPM solution integrates with more than 200 third-party tools to consolidate, deduplicate, and correlate vulnerabilities with risk-based scoring through its contextual risk engine. The flexibility to customize dashboards that provide relevant insights to business and technical users enhances the overall user experience.
- Tromzo's ASPM solution is designed and funded by CISOs, with sharp focus on addressing security leaders and professionals' requirements. Since the release of its core platform in 2023, the company has continued to expand its integrations with different third-party tools, including code repositories, cloud platforms, scanners, and other security solutions.
- Conviso is a leading ASPM player in the LATAM market. Leveraging its extensive experience with helping customers build their application security program through its professional services, the company developed its ASPM platform based on customer pain points to improve their application security posture.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Companies to Action

Source: Frost & Sullivan

Checkmarx

INNOVATION

- Checkmarx's ASPM solution is an integral part of the Checkmarx One platform. Leveraging its long-standing application security capabilities, the company built its ASPM solution to deliver comprehensive application security coverage, supported by a wide range of native AST tools, all in a single platform.
- While the native scanning tools help to provide high-quality and rich security findings, the ASPM solution allows integration with third-party security tools, including AST, mobile application security testing, cloud security solutions, penetration testing, open-source scanners, and other complementary solutions for more comprehensive application security coverage.
- The combination of Checkmarx's AST tools and third-party security tools in the company's ASPM solution offers complete code-to-cloud visibility that helps customers correlate and understand exploitable paths. The correlation capabilities allow customers to prioritize critical vulnerabilities based on business risk and potential impact through the Application Risk Management functionality, enabling effective remediation efforts.
- To offer a frictionless developer experience, Checkmarx embeds security throughout the SDLC by seamlessly integrating with DevSecOps pipelines and tools, including CI/CD platforms, integrated development environments (IDEs), SCMs, and other developer tools.
- While organizations increasingly use AI for code generation, Checkmarx has introduced several AI application security features into its AST tools as part of the broader Checkmarx One platform. These features include AI Security Champion, which provides AI-guided remediation and auto-remediation; real-time in-IDE scanning that performs security checks for AI-generated code as developers write it; and AI Query Builder, which integrates generative AI support into the query editor tools.

Source: Frost & Sullivan

Checkmarx (continued)

GROWTH

- Frost & Sullivan finds Checkmarx achieved tremendous growth in its ASPM business in 2023 and is experiencing solid growth in 2024 with focus on moving existing application security customers to Checkmarx One, in which ASPM is integral. With strong growth momentum, the company solidified its market leader position, capturing market share of 21.3% in 2024.
- North America drives the company's global ASPM business, recording 59.1% of its total ASPM market share. In addition to its established brand name in the NA and EMEA markets, Checkmarx continues to expand its ASPM business in APAC and LATAM. It is one of the few vendors with an active business presence across all regions.
- Checkmarx has the advantage of a large application security solutions customer base that it can move to the Checkmarx One platform, which will drive the growth opportunity for its ASPM business in the next three years. The company has a well-developed and standardized global channel partner program, and its introduction of Checkmarx One has made it easier for channel partners to sell and implement as the full range of AST solutions is consolidated into one platform.
- In addition to technical services and support, Checkmarx offers a range of tailored service options with rapid response times, regular business reviews, and the ability to work with customers before problems arise. It also demonstrates an excellent customer-first approach by helping customers evaluate and improve the maturity of their application security programs through a self-developed industry-standard framework (APMA).

Source: Frost & Sullivan

Checkmarx (continued)

FROST PERSPECTIVE

- Checkmarx is a leader on the Frost Radar™ Growth and Innovation Indexes. Its well-established brand name, solid position in a market, extensive application security coverage, strategic go-to-market strategy (moving its existing customers to Checkmarx One), and well-established channel partner ecosystem position it to achieve an outstanding performance in the global ASPM market.
- The bring your own results (BYOR) initiative, which integrates findings from third-party tools to complement security findings from the various native wide AST tools, showcases its strong commitment to offering more comprehensive code-to-cloud visibility and supporting broader use cases as customer requirements evolve.
- Though most ASPM capabilities are available in the broader Checkmarx One offering, the Application Risk Management functions more like a displaying dashboard, and some functions are not offered directly from this single ASPM dashboard.
- The company should consider extending its ASPM capability to AI-SPM to provide complete visibility into the AI pipeline through continuous monitoring, to maintain protection against AI-related risks, and to ensure compliance with AI applications.
- Given the complex and fast-evolving regulatory requirements, Checkmarx should consider including features that will help customers map their existing application security strategy or policies with regulations or compliance frameworks to better evaluate their compliance posture.

Source: Frost & Sullivan

FROST & SULLIVAN

Best Practices & Growth Opportunities

Source: Frost & Sullivan

Best Practices

1. ASPM vendors should continue expanding their security coverage and offering CISOs a comprehensive understanding of their organizations' risk posture. The ability to connect the development and runtime environments and provide context into the application's deployed state is vital, as a comprehensive view of application risks will help with effective risk-based prioritization.

2. Considering exploitability, reachability, severity, business risk, and other critical factors is imperative to improve the accuracy of risk-based vulnerability prioritization. Incorporating these factors provides contextual insights that help organizations focus on the most crucial issues and security risks to their business operation.

3. ASPM vendors must take a developer-first approach and prioritize developer experience during the remediation process by providing actionable remediation guidance, streamlined workflows, and automatic fixes that align with customer preference. This approach helps to achieve a more effective remediation process without slowing down the application development process.

Source: Frost & Sullivan

Growth Opportunities

1. ASPM vendors need to incorporate security findings from application security tools that focus on identifying security issues in the pipeline and from cloud security tools that provide insights into security posture in production. The ability to offer visibility into every software asset from code to cloud and the deployed state of applications will contribute to a better contextual analysis of vulnerability through a holistic application-based risk view.

2. Organizations need continuous visibility into how developers use AI-generated code tools to safeguard AI use across the SDLC and prevent the use of risky AI models when developing applications. ASPM vendors should consider extending their coverage to identify and address vulnerabilities, misconfigurations, and potential risks associated with AI-based applications to prevent cyberattacks from exploiting AI-based applications.

3. ASPM tools must integrate seamlessly into the development workflow to facilitate smooth and effective remediation without disrupting the fast-paced application development process. ASPM vendors need to continuously improve their solutions' automation and orchestration capabilities to optimize remediation workflow and effectively accelerate secure application release.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™ Analytics

Source: Frost & Sullivan

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.

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.

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.

PRODUCT PORTFOLIO
This is a measure of a company's product portfolio, focusing on the relative contribution of new products to its annual revenue.

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.

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

FROST & SULLIVAN

Next Steps: Leveraging the Frost Radar™ to Empower Key Stakeholders

Source: Frost & Sullivan

Significance of Being on the Frost Radar™

Companies plotted on the Frost Radar™ are the leaders in the industry for growth, innovation, or both. They are instrumental in advancing the industry into the future.

GROWTH POTENTIAL

Your organization has significant future growth potential, which makes it a Company to Action.

BEST PRACTICES

Your organization is well positioned to shape Growth Pipeline ™ best practices in your industry.

COMPETITIVE INTENSITY

Your organization is one of the key drivers of competitive intensity in the growth environment.

CUSTOMER VALUE

Your organization has demonstrated the ability to significantly enhance its customer value proposition.

PARTNER POTENTIAL

Your organization is top of mind for customers, investors, value chain partners, and future talent as a significant value provider.

Source: Frost & Sullivan

Frost Radar™ Empowers the CEO's Growth Team

STRATEGIC IMPERATIVE

- Growth is increasingly difficult to achieve.
- Competitive intensity is high.
- More collaboration, teamwork, and focus are needed.
- The growth environment is complex.

LEVERAGING THE FROST RADAR™

- The Growth Team has the tools needed to foster a collaborative environment among the entire management team to drive best practices.
- The Growth Team has a measurement platform to assess future growth potential.
- The Growth Team has the ability to support the CEO with a powerful Growth Pipeline™.

NEXT STEPS

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**
- **Growth Pipeline™ Dialogue with Team Frost**

Source: Frost & Sullivan

Frost Radar™ Empowers Investors

STRATEGIC IMPERATIVE

- Deal flow is low and competition is high.
- Due diligence is hampered by industry complexity.
- Portfolio management is not effective.

LEVERAGING THE FROST RADAR™

- Investors can focus on future growth potential by creating a powerful pipeline of Companies to Action for high-potential investments.
- Investors can perform due diligence that improves accuracy and accelerates the deal process.
- Investors can realize the maximum internal rate of return and ensure long-term success for shareholders.
- Investors can continually benchmark performance with best practices for optimal portfolio management.

NEXT STEPS

- **Growth Pipeline™ Dialogue**
- **Opportunity Universe Workshop**
- **Growth Pipeline Audit™ as Mandated Due Diligence**

Source: Frost & Sullivan

Frost Radar™ Empowers Customers

STRATEGIC IMPERATIVE

- Solutions are increasingly complex and have long-term implications.
- Vendor solutions can be confusing.
- Vendor volatility adds to the uncertainty.

LEVERAGING THE FROST RADAR™

- Customers have an analytical framework to benchmark potential vendors and identify partners that will provide powerful, long-term solutions.
- Customers can evaluate the most innovative solutions and understand how different solutions would meet their needs.
- Customers gain a long-term perspective on vendor partnerships.

NEXT STEPS

- **Growth Pipeline™ Dialogue**
- **Growth Pipeline™ Diagnostic**
- **Frost Radar Benchmarking System**

Source: Frost & Sullivan

Frost Radar™ Empowers the Board of Directors

STRATEGIC IMPERATIVE

- Growth is increasingly difficult; CEOs require guidance.
- The Growth Environment requires complex navigational skills.
- The customer value chain is changing.

LEVERAGING THE FROST RADAR™

- The Board of Directors has a unique measurement system to ensure oversight of the company's long-term success.
- The Board of Directors has a discussion platform that centers on the driving issues, benchmarks, and best practices that will protect shareholder investment.
- The Board of Directors can ensure skillful mentoring, support, and governance of the CEO to maximize future growth potential.

NEXT STEPS

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**

Source: Frost & Sullivan

Next Steps

Engage:

Growth Dialog

Join:

Growth Council

Participate:

Growth Council Think Tanks

Apply:

Companies to Action

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

Source: Frost & Sullivan