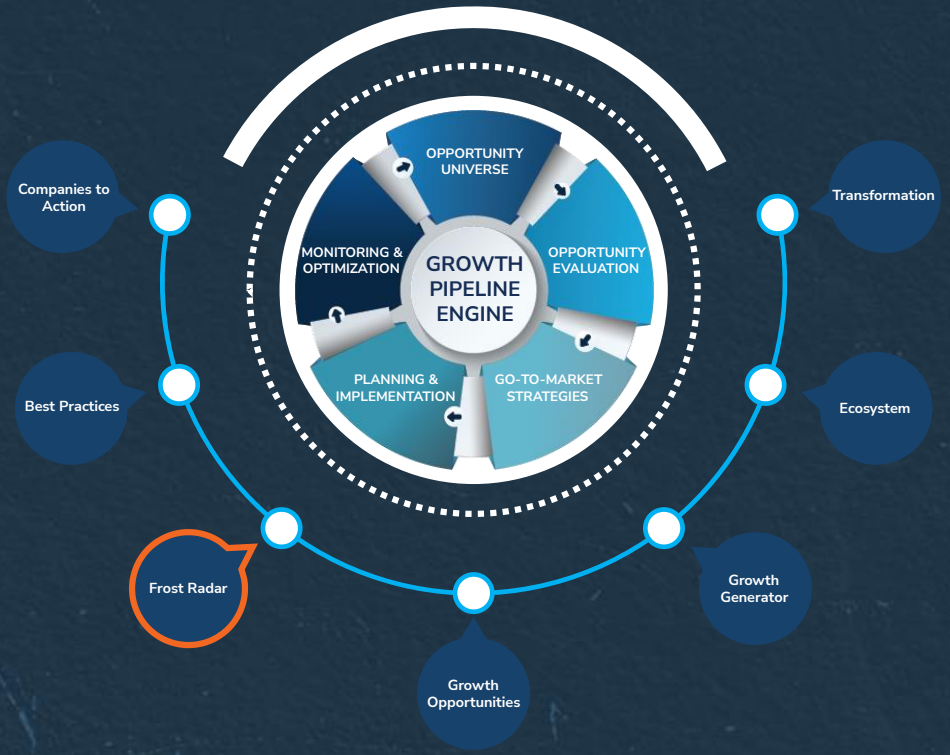
FROST & SULLIVAN

Frost Radar: SaaS Security Posture Management, 2024

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



PFQO-74
December 2024

FROST & SULLIVAN

Strategic Imperative and Growth Environment

Strategic Imperative

- The Frost & Sullivan's 2023 Cloud User Survey surveyed 2,138 C-level executives in 13 countries across the globe and found that 32% of respondents believed that the cloud is the most crucial part of their digital transformation journey. Many decision-makers believe that cloud adoption can help improve operational efficiency and customer experience, enabling organizations to realize sustainable growth in the modern business landscape.
- As the cloud adoption rate increases exponentially, as-a-service technologies emerge, including Software-as-a-Service (SaaS) applications—Microsoft 365, Google Workspace, Salesforce, and Slack, for instance. These have become widely popular and are quickly becoming an integral component of many organizations' business operations.
- SaaS applications have received an enthusiastic reception among organizations globally. They reduce the need for large upfront investments or lengthy implementation cycles because SaaS applications typically operate on a subscription model and can connect easily with other cloud-based services through application programming interfaces (APIs), minimizing the need for an extensive setup.
- Their ease of integration, scalability, and flexibility drive the adoption rate of SaaS applications among organizations globally. However, as users benefit from SaaS applications, mass adoption of SaaS applications has unintentionally caused SaaS sprawl.
- SaaS sprawl refers to the process of accumulating numerous SaaS applications across departments to the point where security teams cannot have full visibility into their entire SaaS ecosystem because business owners and department leaders procure new SaaS applications without informing the security teams beforehand.

Strategic Imperative

- On a micro level, each SaaS application comes with its own set of configurations, policies, and access controls. Many business owners and department leaders often overlook this factor and do not inform the security teams when they adopt new SaaS applications because they see security as an inhibitor to growth. As a result, they are willing to sacrifice security for higher productivity and business goal achievement.
- For security teams, manually managing these aspects for a small pool of SaaS applications is a viable task, but performing across tens or even hundreds of SaaS applications becomes increasingly impractical, and it is challenging for them to ensure the continuous protection of SaaS applications that they are not aware of.
- As the SaaS ecosystem expands without check, it becomes difficult for organizations to have full visibility into the applications used, their configurations, the identities using those SaaS applications, and how those SaaS applications interact with each other. This lack of visibility limits the security teams' ability to enforce consistent security policies and controls, creating blind spots and massive security gaps that attackers can easily exploit.
- The rapidly increasing number of SaaS applications in the SaaS ecosystem effectively expands the attack surface that security teams need to monitor. Each application represents a potential entry point for attackers, especially if the application is poorly configured or lacks proper security controls. SaaS applications onboarded without the knowledge of security teams are also a potential entry point because those applications often do not have security policies and controls.
- This unchecked SaaS ecosystem growth has created an environment ripe for attacks, and SaaS applications are becoming an increasingly attractive target. SaaS-related breach incidents in the past 12 months include high-profile victims, such as Microsoft Outlook, Activision Blizzard, and Snowflake.

Strategic Imperative

- Organizations are becoming increasingly aware of the importance of full visibility and control over their entire SaaS ecosystem, driving the need for a security solution that addresses these issues. At its core, a SaaS security posture management (SSPM) solution provides a single-pane-of-glass view of an organization's SaaS ecosystem with centralized controls to identify and mitigate the risks and misconfigurations of SaaS applications.
- SSPM solutions empower organizations to secure their rapidly expanding SaaS ecosystem by continuously monitoring and identifying security risks and misconfigurations, identifying sanctioned and unsanctioned SaaS applications, generating alerts based on prioritized risks, revoking excessive permissions, and remediating identified risks and misconfigurations. Alert generation in an SSPM solution often incorporates contextual analysis, analyzing vulnerabilities, misconfigurations, access anomalies, and potential threats by factoring the broader context, such as the sensitivity of data inside the SaaS applications, integrations with other SaaS applications, and the role of the SaaS applications within the organization's environment.
- The features below are the foundational capabilities of an SSPM solution.
- SaaS Applications Inventory and Visibility: This includes automatic discovery of SaaS applications and regular maintenance of an up-to-date inventory that contains all SaaS applications in the organization's SaaS ecosystem.
- Configuration Monitoring and Management: SSPM solutions must continuously monitor and evaluate SaaS application configurations to identify misconfigurations and risks, ensure compliance with regulatory standards, and assess alignment with the organization's broader security policies and controls.

Strategic Imperative

- Risk Management: SSPM solutions must assess risks associated with SaaS applications, configurations, and access patterns and prioritize those risks based on severity, internal security controls, and potential impact.
- Remediation Support: SSPM solutions must ensure an efficient remediation process that is not strictly automated and, as a result, has the flexibility to adjust responses based on organizational preferences. This includes providing remediation advice, manual remediation, or outsourcing remediation to third-party security tools.
- SaaS-to-SaaS Applications Management: This includes tracking of app-to-app integrations and third-party connections to ensure inactive SaaS-to-SaaS or third-party connections no longer have access to the SaaS applications and the data in them.
- Identity Access Management: An SSPM solution must monitor and evaluate both human and non-human identities to ensure secure and appropriate access.
- Streamlined Governance and Compliance: SSPM solutions ensure that SaaS applications comply with regulatory standards and internal security policies.
- Reporting and Analytics: This includes providing a dashboard that offers a centralized overview of the entire SaaS applications, with insights into the security posture of the SaaS ecosystem.
- Organizations may find it difficult to select an SSPM solution because the market is still developing, and vendors are taking different approaches to achieve SSPM outcomes.
- The multi-faceted nature of SaaS security requires adaptive solutions. Vendors have taken the chance to provide solid foundational SSPM capabilities and offer deeper expertise in specialized areas, such as identity risk management, data-centric approach, and SaaS-to-SaaS governance.

Strategic Imperative

- As a result, it is critical that organizations select an SSPM vendor that can address their security challenges and does not disrupt their business operations during evaluation.
- Organizations consider the following features that extend the functionalities of a foundational SSPM solution into a more comprehensive SSPM solution.
- Identity-driven SaaS security that provides comprehensive monitoring and control over all types of identities, such as human users, API tokens, service accounts, OAuth keys, and connected devices within the SaaS ecosystem. This includes continuously tracking identity life cycles, access patterns, and risk levels while providing contextual risk scoring based on many factors, including device health, location, data sensitivity, and behavior patterns. This ensures that all identities are continuously authenticated, authorized, and monitored.
- Enhanced visibility into SaaS-to-SaaS connections that provides an in-depth look into the connections between SaaS applications because these integrations let them share data. Enhancing visibility enables the monitoring and identification of security risks, possible data exposure from data flows, and compliance violations, which then allows relevant remediation actions, such as revoking permissions or disabling inactive or redundant SaaS-to-SaaS applications.
- Real-time detection and response capabilities that continuously monitor application behaviors, user activities, and data movements to identify security risks and misconfiguration in real time. Any identified security risks and misconfigurations will immediately trigger response actions before escalating further, without human intervention.

Strategic Imperative

- Consolidation into broader SaaS security or Secure Access Secure Edge (SASE) platforms to capitalize on the consolidation trend, because demand increases for a centralized platform that integrates security capabilities. Using SSPM as a foundational component to build a SaaS Security Platform that addresses use cases beyond security posture management enables a more holistic SaaS security approach. Integrating into SASE enables more robust protection for modern organizations, ensuring secure connectivity to enhanced SaaS security.
- Risk-based prioritization based on contextual and behavioral analysis that moves beyond static risk assessments based on pre-defined or baseline rules and toward a more dynamic risk evaluation (incorporating AI/ML to bring contextual awareness to SaaS activity monitoring) enables organizations to understand how certain user behaviors, environmental factors, and SaaS activities results in risks and misconfigurations. The additional context that this capability provides enhances the accuracy of its prioritization capability, producing highly accurate risk scoring that reduces false positives and accelerates remediation.
- Expansive breadth and depth of coverage for SaaS applications due to the increasingly expansive SaaS ecosystem, resulting from the rapid utilization rate of SaaS applications, increases the need for SSPM solutions to feature comprehensive SaaS application coverage to ensure consistent security policies and controls across all SaaS applications in an organization, including industry-specific applications.

Growth Environment

- Based on Frost & Sullivan's 2023 Voice of the Enterprise Security Customer survey, which surveyed more than 2,448 C-level executives across the United States, France, Germany, the United Kingdom, Japan, Australia, and Brazil, 49% of respondents claimed that SSPM has been used in their daily security operations, while 40% of them shared that they have plans to add the solution by the end of 2024. This is in line with the projected compound annual growth rate (CAGR) of 51% from 2024 to 2029.
- The rapid emergence of SSPM as a critical security solution to address risks and misconfigurations in the SaaS ecosystem is the result of the growing awareness of its functionalities and benefits, particularly among forward-looking regions such as North America, which will remain the largest revenue contributor in the global SSPM market in the next five years. The region has a mature SaaS ecosystem and a higher cybersecurity maturity level than others.
- Europe, the Middle East, and Africa (EMEA), meanwhile, are increasingly recognizing the importance of SaaS security and will explore SSPM in the coming years, but the region's methodological and risk-avoidant approach due to the need to comply with stringent regulations, such as the General Data Protection Regulation, has resulted in a slightly slower adoption rate than North America.
- Asia-Pacific is experiencing a rapid digitalization trend that has accelerated its adoption rate of SaaS applications. However, the market cannot be treated as a singular market because the maturity level varies between countries. Countries with higher cybersecurity maturity levels, such as Singapore, Australia, and Japan, will drive the adoption of SSPM while Indonesia and Malaysia may lag due to their cost-effectiveness priority.
- Investments in SSPM in Latin America remain limited due to the region's preference for on-premises environments, resulting in lower cybersecurity maturity. Highly regulated sectors, such as banking, financial services, and insurance (BFSI) will be the main SSPM growth driver in the region.

Growth Environment

- Awareness of SSPM may benefit from the growing number of high-profile security incidents linked to SaaS applications, such as Microsoft Outlook and Equifax, which have spooked many organizations, forcing them to secure their SaaS application environments.
- This urgency has driven organizations of all sizes to invest in SSPM solutions. Large organizations currently lead the way in SSPM adoption due to their vast SaaS ecosystems, which often span multiple departments, countries, and regions, and have strict compliance requirements.
- Small organizations are also adopting SSPM but at a slower pace due to budget restraints and lack of in-house security expertise. This forces them to focus on foundational security rather than embrace more advanced tools, such as SSPM. Those two factors will continue to loom over small organizations, which might hinder market growth over the next five years. Even so, the segment will still see rapid SSPM adoption.
- The disparity in adoption between large and small organizations also extends to different sectors, such as BFSI, retail/eCommerce, technology, and healthcare medical, which lead SSPM adoption due to stringent compliance requirements, the urgent need to secure sensitive data within the SaaS applications, and the critical urgency to ensure secure access to SaaS applications regardless of geographical locations. Manufacturing and energy, meanwhile, are also adopting SSPM but at a steadier pace due to the sectors' unique operational needs.

Growth Environment

- The growing urgency and horizontal/vertical-driven SSPM adoption has come after many business owners and department leaders overlooked the security risks associated with SaaS applications. Many decided to prioritize productivity and business goals by adopting SaaS applications without first informing their security teams.
- As stated before, this has created SaaS sprawl, because the pace of SaaS adoption far outstrips the security teams' ability to keep track of all SaaS applications in their environment. They lack comprehensive visibility across their entire SaaS ecosystem, leaving organizations with a massive security gap.
- Organizations' growing need for SSPM is one of the many factors driving the global SSPM market. In 2024, the market recorded an estimated revenue of $290.7 million with a strong year-on-year growth rate of 75.3%.
- Frost & Sullivan projects that the global SSPM market will achieve a CAGR rate of 51% from 2024 until 2029—it will achieve a revenue of $2.28 billion at the end of the CAGR period in 2029 because the utilization of SaaS applications will increase exponentially over the years, particularly in Asia-Pacific and Latin America, increasing demand for SSPM.
- With organizations globally becoming more reliant on SaaS applications, the latter will become a prime target for attackers seeking access to sensitive and critical data.

Growth Environment

- While spending in the cybersecurity markets has grown steadily in the last few years, high inflation rates and unfavorable exchange rates are forcing organizations to take a more conservative approach to cybersecurity investments and focus on revenue-generating activities until the economic landscape stabilizes. This will be a large factor in the slowdown of the SSPM market in the long run.
- Besides the economic slowdown, the volatile geopolitical landscape will play a big part in limiting the growth of the SSPM market. The possible imposition of tariffs could strain organizations' financial resources, discouraging many organizations from investing in security tools, such as SSPM, which is often treated as an emerging security solution with an unproven return on investment compared to older, more established security solutions.
- A factor explaining the hesitancy that surrounds emerging technology adoption, such as SSPM, is organizations' belief that it can be costly and time-consuming. They consider that they lack the time to properly develop their skills in an era where trends are rapidly evolving. However, failure to adapt to the latest trends might cause them to lose customers to competitors that can adapt to the latest consumer needs faster.

Growth Environment

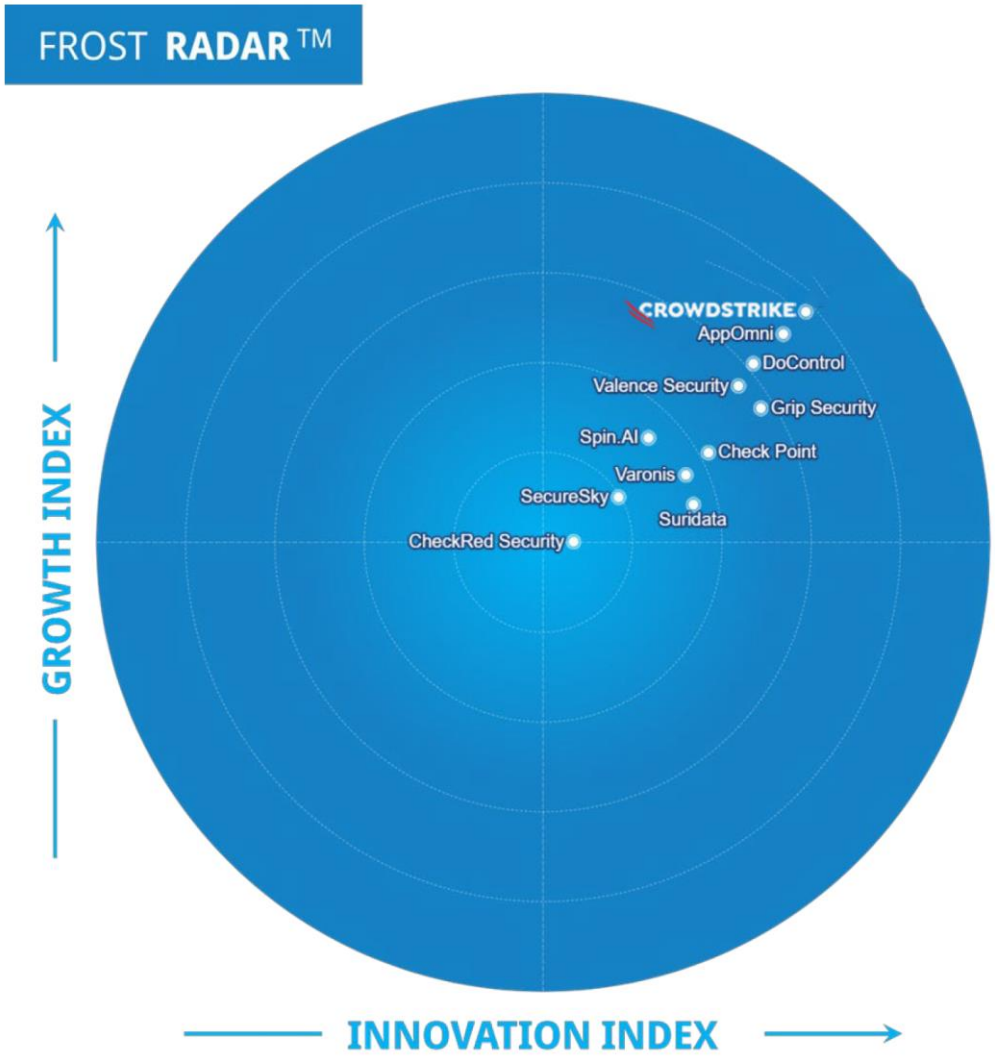
- Frost & Sullivan has covered this and related topics in the following analyses:
  - Growth Opportunities in Global SaaS Security Posture Management, 2024–2029 (soon to be published)
  - SaaS Security Posture Management (SSPM) and Data Security Posture Management (DSPM)
  - Global Cloud-native Application Protection Platform Growth Opportunities
  - Global Cloud-native Application Protection Platform Growth Opportunities
  - Growth Opportunities in Global Cloud Security Posture Management, 2024–2028

FROST & SULLIVAN

Frost Radar

SaaS Security Posture Management, 2024

Frost Radar: SaaS Security Posture Management



Frost Radar Competitive Environment

- Frost & Sullivan has included more than 17 vendors in the Growth Opportunities in Global SaaS Security Posture Management, 2024–2029 market study. Most of the players are start-ups specializing in securing SaaS, unlike more mature cybersecurity markets where older cybersecurity vendors dominate. The market very likely includes more than 17 vendors due to the rapid growth of the SSPM landscape.
- Frost & Sullivan has evaluated the top companies in this Frost Radar analysis. The factors considered to select vendors and assess their performance on the Growth and Innovation Axes include end-user focus, geographic presence, and solution portfolio. Companies must have recorded an estimated annual revenue of at least $3 million in 2024 or have possessed a market share of at least 1% in the total SSPM market in 2024.
- Frost & Sullivan has excluded certain vendors that meet the inclusion criteria for this Frost Radar but were unable to share detailed insights into their business performance and container/K8s security solutions to ensure a fair scoring and comparison. As a result, this Frost & Sullivan analysis features 11 vendors: Adaptive Shield, AppOmni, CheckRed Security, Check Point Technologies, DoControl, Grip Security, SecureSky, Spin.AI, Suridata, Valence Security, and Varonis. These are the power players in the SSPM market today.
- The SSPM market will see more participation from start-ups and established cybersecurity vendors because the demand to secure SaaS environments will grow exponentially. It will become an increasingly important component of organizations' business operations, and more organizations will need to have a better understanding of SSPM solutions' functionalities and benefits.
- More established cybersecurity vendors will introduce SSPM as a feature of other security products to expand its use cases, putting themselves in an advantageous position due to the massive consolidation demand from customers. Start-ups, in turn, might want to capitalize on the growing demand for SaaS security and offer more advanced capabilities that disrupt the current SSPM market.

Source: Frost & Sullivan

Frost Radar Competitive Environment (continued)

- **Growth Axis**
- The SSPM market is still in its early stages of growth, with many players aggressively battling each other to establish a solid presence. In that context, companies such as Adaptive Shield, AppOmni, DoControl, and Valence Security have demonstrated excellent business performance and have emerged as Growth Axis leaders.
- Adaptive Shield has experienced solid growth momentum. Its revenue is estimated to have grown at a robust YoY growth of 101.7% in 2024. The company was able to record triple-digit growth because it expanded its channel partner ecosystem, with more than 300 active business partners worldwide, which, in turn, allows it to aggressively expand its customer base. The November 2024 announcement of its acquisition by CrowdStrike will help the company maintain sustainable growth momentum because it can capitalize on the wide reach that CrowdStrike has built for its other products.
- AppOmni is the second growth leader in the analysis thanks to its consistent performance in the SSPM market, recording a steady 40.8% YoY growth in 2024. AppOmni's SSPM solution is designed to meet the needs of enterprise-level customers. This approach has proven successful in its vast customer segments, including BFSI, technology, and healthcare, and it claims that 30% of the Fortune 100 companies are its customers.
- DoControl has also maintained a strong growth trajectory in 2024, recording a YoY growth of 90.3% in 2024 and solidifying its position as one of the leading players in the industry. The company has remarkably highlighted its unique features, such as multi-contextual analysis, bulk remediation, and employee management, which have helped it stand out in the market. DoControl will expand its business into EMEA, Latin America, and Asia-Pacific, boosting the company's growth trajectory in the coming years.

Frost Radar Competitive Environment (continued)

- Valence Security is the fastest-growing SSPM player in 2024, recording a tremendous YoY growth of 409.4%. This has helped the company increase its market share by 2% in 2024. It managed to record triple-digit growth thanks to its strategic partnership with Microsoft which has given them a major competitive advantage. The partnership enables business and product teams to collaborate closely to develop joint offerings. This allows it to capitalize on Microsoft's wide customer base to push its solution to the market.
- Grip Security is a new SSPM market player that began to record revenue-generating activities in 2024. However, the company has established itself as one of the top players in the market by registering a remarkable YoY growth of 161.3%. Its reputation as a pioneer in SaaS identity risk management and its focus on helping organizations discover shadow SaaS applications has helped Grip Security successfully differentiate itself from competitors.
- Spin.AI is growing steadily, which reflects favorably on its Growth Axis score. The company offers its SSPM solution as part of its flagship SpinOne platform. This enables it to upsell or cross-sell and bundle a broader SaaS security solution featuring its SSPM offering. However, it is mainly perceived as a backup and recovery company rather than an SSPM provider, which puts its growth momentum at risk.
- Check Point entered the SSPM market after acquiring Atmosec, an early-stage SaaS security company that provided capabilities such as discovery of malicious SaaS applications, prevention of risky third-party SaaS communications, and remediation of SaaS misconfigurations. Its SSPM solution can be purchased as a standalone product but is available as part of its SASE, cloud security posture management (CSPM), or email security product. This will have an enormous influence on its growth momentum because Check Point is one of the most recognizable names in the cybersecurity market.

Frost Radar Competitive Environment (continued)

- Varonis and SecureSky record a solid growth momentum and have a relatively similar approach to how they position their SSPM solution in the market. Varonis is widely known for its flagship Data Security Platform. The company has used its platform's popularity to push for its SSPM solution by bundling it into its data protection packages. This allows the company to cross-sell and upsell existing customers who might need to enhance their SaaS security and protect their data.
- SecureSky provides services and products, with its SSPM solution being a part of its continuous threat exposure management (CTEM) platform. Its position as a service provider that also offers patented products has enabled the company to position itself uniquely in the market because it can leverage the relationship it has built with its services to push for its SSPM.
- However, SSPM is not Varonis and SecureSky's biggest priority. Varonis focuses on its data security business while SecureSky mainly pushes its CTEM platform to the market. This will cause the market to overlook their SSPM solutions, affecting their market perception, which can hugely impact their growth momentum despite the company's ability to cross-sell or upsell to wide customer bases.
- Suridata has a positive perception in the market thanks to the comprehensiveness of its SSPM solution, which is integrated into SaaS detection and response (SDR) to form Suridata's flagship SaaS Security Platform. It has strong momentum because it is onboarding several Fortune 500 companies onto its platform, but it has a small market share and revenue compared to other vendors in this analysis.
- CheckRed Security is a new player in the SSPM market. Its SSPM solution is part of its broader cloud native application protection platform (CNAPP), and it is working closely with managed service providers to push for its CNAPP. However, it is still mainly known as a CNAPP player, while its SSPM solution is not as popular as those of other players in this analysis.

Frost Radar Competitive Environment (continued)

- **Innovation Axis:**
- Adaptive Shield, AppOmni, Grip Security, and DoControl are Innovation Axis leaders, with each platform offering a unique approach to help organizations enhance their SaaS security posture.
- Adaptive Shield combines SSPM and identity threat detection and response (ITDR) to provide a comprehensive security solution that remediates SaaS applications' misconfigurations and ensures that the identities accessing those SaaS applications are continuously monitored for suspicious behavior. Its SSPM has two standout features that enhance its comprehensive protection across the entire SaaS stack—the first is its extensive number of out-of-the-box integrations and the second is its device-to-SaaS risk management. No other companies in this analysis offer integration support as expansive as Adaptive Shield. It is the only vendor that provides comprehensive device-to-SaaS protection.
- AppOmni covers security for all SaaS applications by leveraging its experts' insights to identify the latest security trends and immediately address risks to prevent further damage. It offers a streamlined compliance process that reduces compliance reporting time by 90% and helps protect top SaaS applications that store 80% of their most sensitive data. It is particularly strong at securing Salesforce applications.
- Grip Security is a pioneer in SaaS identity risk management. It offers end-to-end visibility into the identity life cycle across SaaS applications from discovery to offboarding, using identity as a focal point for managing SaaS risks. Its user-focused, identity-centric approach enables the company to discover and minimize risks on sanctioned and unsanctioned SaaS applications.

Frost Radar Competitive Environment (continued)

- DoControl is known for supporting a wide range of SaaS security use cases, such as data access governance, ITDR, identity risk management, shadow application governance, SaaS misconfiguration management, data loss prevention, and insider risk management. However, the strength of its SSPM solution lies in its multi-contextual analysis that identifies risky user behavior through SaaS events by pulling metadata from sources such as endpoint detection and response (EDR), identity provider (IdP), human resources information system (HRIS), and employee interactions.
- This allows DoControl to have a deeper insight into user activity so it can classify threats accurately and ensure effective insider threat management. The company lags slightly on the Innovation Axis due to its limited support for identity security, making it less favored in a market that increasingly looks to ensure secure access to SaaS applications.
- Valence is well-positioned on the Innovation Axis thanks to its expertise in securing SaaS-to-SaaS connections. Valence specializes in providing visibility and control: it continuously monitors the topology of an organization's SaaS ecosystem and tracks the movement of sensitive data between applications, ensuring that their relationships and data flows remain protected and comply with regulatory standards.
- However, it has a narrow coverage for integration support. This may complicate an organization's efforts to have a full topology of its SaaS ecosystem if Valence does not support its SaaS applications.
- Check Point has broad SSPM capabilities designed to continuously analyze the behavior of SaaS applications and SaaS-to-SaaS communications. It utilizes AI/ML to automate remediation actions. The company's solution can leverage insights from its other products, such as firewalls and email security, which enriches its threat intelligence capability to identify risks effectively. However, it has paid little attention to its SSPM following the acquisition, raising questions about the company's strategy for this solution.

Frost Radar Competitive Environment (continued)

- Suridata has demonstrated its ability to innovate with the integration of SSPM and SSDR into its SaaS Security Platform that addresses risks and misconfigurations. However, the company does not have a strong focus on securing identities even though the market is heading towards an identity-first approach, which may cause the company to lag behind the other players in this analysis.
- Varonis is well-known for its data security platform and its user behavior analytics capability to identify abnormal behavior. The company takes a data-centric approach to SSPM, analyzing the data inside SaaS applications to identify excessive permissions and perform automated remediation on excessive access. Given that it focuses largely on the data, it provides a more niche focus than other players that concentrate on securing the entire SaaS ecosystem.
- Spin.AI built a formidable reputation in backup and recovery and forayed into the SSPM market with SpinSPM. A standout feature of its SSPM solution is its ability to continuously monitor and evaluate browser extensions based on 15 attributes, including business operations and security aspects to generate risk scores for every extension.
- A major weakness of Spin.AI, however, is its limited coverage for integrations because it only allows four of the most popular SaaS applications. This has limited its ability to provide comprehensive protection, particularly because many organizations continue to add new SaaS applications to their ecosystems.
- SecureSky and CheckRed Security forged a similar path in the SSPM market. Both companies have SSPM as part of their flagship platform, CTEM for SecureSky and CNAPP for CheckRed. Both vendors are still primarily recognized for their flagship platform's business, affecting their perception in the SSPM market.

FROST & SULLIVAN

Frost Radar™: Companies to Action

Adaptive Shield (CrowdStrike)

INNOVATION

- Adaptive Shield's platform takes an identity-first approach to offer real-time visibility into the security of business-critical SaaS applications. The centralized platform offers SaaS misconfiguration management, identity protection, automated alerts and notifications, streamlined remediation, posture-over-time monitoring, compliance checks, custom security checks, frameworks, rules and integrations, customizations, integration with third-party ticketing systems and security tools, threat detection, and automated workflows and playbooks. With the CrowdStrike acquisition, a unified platform will deliver complete protection against identity-based attacks across hybrid cloud environments, from on-premises active directory to cloud-based identity providers and SaaS apps.
- The comprehensive coverage of the SaaS ecosystem fueled by solid threat prevention, detection, and response capabilities helps customers accurately detect and prioritize critical risks posed to their SaaS environment. By supporting a breadth and depth of integrations with more than 150 SaaS applications, and custom or home-grown applications, Adaptive Shield empowers organizations to leverage its platform and address risks in SaaS security.
- Joining forces with CrowdStrike enables the company to mitigate device-to-SaaS risks by identifying users with poor cyber hygiene on their devices, non-compliant devices, and unmanaged devices.
- In 2023 and 2024, Adaptive Shield released several technology enhancements as part of its broader SaaS security strategy. This enhancement includes the expansion to more than 150 integrations with SaaS applications, the Integration Builder to monitor additional and homegrown applications, ITDR expansion, enhanced automated workflows and playbooks, shadow IT discovery, flexible reporting engine, generative AI SaaS security, and improved SaaS entitlement management.

Adaptive Shield (CrowdStrike) (continued)

GROWTH

- Frost & Sullivan estimates that Adaptive Shield experienced a tremendous YoY growth of 101.7% in its SSPM business in 2024, which led to a market share increase of 1% in 2024.
- The company operates in North America, EMEA, and Asia-Pacific. North America and EMEA were the key revenue contributors, with a combined 83% share of its global SSPM business. The company has expanded its market reach to Asia-Pacific and has yet to establish an active presence in Latin America. To support its international operations, the company provides localized customer support, including engineering, sales, customer success, and support teams in the United States, Japan, Australia, France, the United Kingdom, Germany, and other countries. The acquisition by CrowdStrike will accelerate growth and further global expansion.
- Adaptive Shield uses a channel-first approach. Besides direct sales, the company has forged strong partnerships with more than 300 active business partners worldwide, supported by a Fast Forward Partner Program and Partner Portal to drive business growth. The company maintains strong technology alliances with security leaders.
- Adaptive Shield demonstrates dedication to its customers with around-the-clock support to ensure they receive assistance quickly based on the service-level agreements. The company's tailored SaaS security programs and best practices include assigned account managers and customer success managers who know SaaS security to provide proper onboarding, regular check-ins, and strategic support. A dedicated customer enablement lead will ensure customers are consistently well-trained on the latest product enhancements and best practices, helping them successfully implement their SaaS security strategy. With the recent acquisition, these capabilities can be further expanded to enhance customer success and drive even greater value.

Adaptive Shield (CrowdStrike) (continued)

FROST PERSPECTIVE

- Adaptive Shield is an Innovation leader on this Frost Radar because of its comprehensive SSPM capabilities that bolster its broader flagship SaaS Security Platform, enabling the company to offer a holistic security posture management and threat protection across the SaaS ecosystem.
- The company stands out in the market thanks to its large catalog of supported SaaS applications—which currently stands at more than 150—while providing organizations with the option to integrate with any custom or home-grown applications through its Integration Builder. Through its extensive support, organizations can streamline their SaaS security management by monitoring and securing their entire SaaS ecosystem using the company's single platform. This allows security measures to scale easily as organizations adopt new SaaS applications. In that context, the company should expand its coverage to cover more industry-specific SaaS applications.
- The company's device-to-SaaS risk management is a standout feature that identifies devices with poor security and correlates the device's health with the risks those devices pose to the organization's broader SaaS ecosystem. By correlating device health with user privileges, it enables organizations to implement a zero-trust security model, ensuring that only secure devices can access the organization's SaaS ecosystem. To solidify its position as an Innovation leader, Adaptive Shield should enhance its risk prioritization with more context-aware analytics that consider business context and specific API connections and provide a more granular analysis of data flow patterns between apps.
- Its recent acquisition by CrowdStrike, which closed during CrowdStrike's fourth fiscal quarter, enables the company to capitalize on CrowdStrike's channel partner ecosystem to grow its business. The company should address possible questions about its direction, following the acquisition.

FROST & SULLIVAN

Best Practices & Growth Opportunities

Best Practices

1. Chief information security officers (CISOs) should prioritize SSPM solutions that address identity security, data protection, and the broader SaaS ecosystem, enabling organizations to mitigate more risks and reduce their attack surface. Effective SSPM monitors and protects human and non-human identities, provides visibility into data access, enforces relevant controls to prevent unauthorized access, and maps the relationship between SaaS applications to detect risks from third-party integrations.

2. Alert fatigue is a top concern for many CISOs. Security teams spend much time parsing irrelevant alerts before identifying and mitigating genuine threats. Many SSPM solutions prioritize risks to counter this issue. However, this capability can benefit from including contextual analysis that correlates alerts with deeper insights about the environments, improving efficiency by producing high-risk alerts only.

3. With the abundance of SSPM solutions in the market, CISOs must select an SSPM solution that addresses their organization's needs and meets its specific business requirements. Selecting a misaligned SSPM solution can lead to poor integration into the organization's environment, generate irrelevant alerts, or be unable to support compliance requirements, which can result in higher costs than expected.

Growth Opportunities

1. Customers increasingly seek solutions that offer a holistic approach to SaaS security, shifting from traditional posture management to more comprehensive visibility and control that monitor human and non-human identities accessing SaaS applications and data flows between SaaS applications. This ensures that the right users access SaaS application data and implements a better approach for increasingly dynamic SaaS environments.

2. While SSPM solutions currently meet the current demands of the market through the identification and mitigation of risks and misconfigurations in SaaS applications, customers increasingly demand the ability to detect and remediate threats in real time. This allows security teams to mitigate those issues before they can be exploited or escalated to create further damage. This drives the need for more proactive SSPM threat mitigation.

3. SSPM solutions have helped organizations map the relationship between the SaaS applications in their environment. However, there are still challenges when identifying shadow IT and unsanctioned apps. These often pose hidden risks because security teams cannot implement relevant security policies and controls that stand outside of their organization's SaaS ecosystem. This highlights the growing need for a greater focus on discovering shadow IT and unsanctioned apps.

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

Innovation Index

Innovation Index (II) is a measure of a company's ability to develop products/ services/ solutions (with a clear understanding of disruptive Mega Trends) that are globally applicable, are able to evolve and expand to serve multiple markets and are aligned to customers' changing needs.

II1

INNOVATION SCALABILITY
This determines whether an organization's innovations are globally scalable and applicable in both developing and mature markets, and also in adjacent and non-adjacent industry verticals.

II2

RESEARCH AND DEVELOPMENT
This is a measure of the efficacy of a company's R&D strategy, as determined by the size of its R&D investment and how it feeds the innovation pipeline.

II3

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

II4

MEGA TRENDS LEVERAGE
This is an assessment of a company's proactive leverage of evolving, long-term opportunities and new business models, as the foundation of its innovation pipeline. An explanation of Mega Trends can be found here.

II5

CUSTOMER ALIGNMENT
This evaluates the applicability of a company's products/services/solutions to current and potential customers, as well as how its innovation strategy is influenced by evolving customer needs.

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