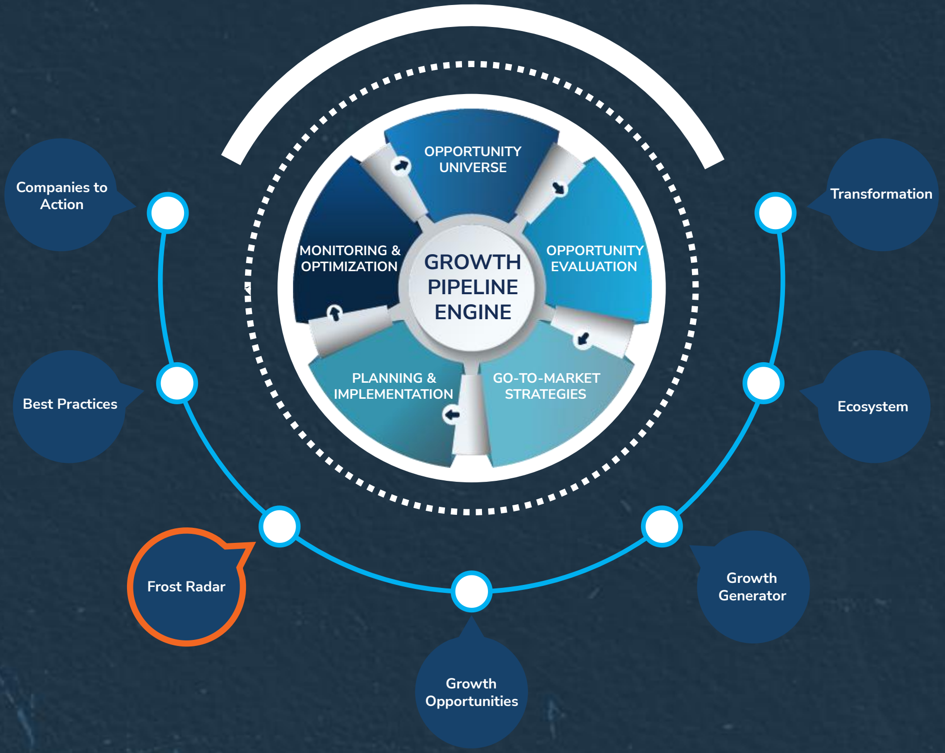
FROST & SULLIVAN

Frost Radar™: Data Security Posture Management, 2024

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

Authored by: Daphne Dwiputriane
Contributor: Jarad Carleton



PFO3-74
December 2024

FROST & SULLIVAN

Strategic Imperative and Growth Environment

Source: Frost & Sullivan

Strategic Imperative

- Frost & Sullivan’s 2023 Cloud Survey of 2,138 C-level executives in 13 countries illustrates the recent exponential increase in data volume, with 29% of respondents sharing that their data volume had grown by at least 50% in the past 12 months, while 34% said that their data volume had grown by 25% to 49% in the same period.
- The surge in the amount of data being generated, collected, and analyzed daily is driven by digital transformation initiatives, with many organizations incorporating cloud services, the Internet of Things, wearable devices, and other technologies into their operations to realize higher productivity and agility, improve business models, and enhance customer experiences.
- With organizations also storing more data than ever, many have adopted a distributed storage strategy across multiple locations, including on premises and in public and private clouds, to benefit from the scalability and performance that centralized storage could not offer. With hybrid and multicloud strategies, organizations are not confined to a single provider, and business-critical workloads can remain on premises and under the direct control of their security teams.
- A major issue with distributed storage, however, is data sprawl, which refers to the accumulation of vast amounts of data to the point that it becomes impossible for a security team to manually manage and monitor it all. The proliferation of cloud and enterprise data platforms means that data stored for future use continues to spread out.
- Data sprawl exposes organizations to security breaches, insider threats, unauthorized access, data leaks, and compliance violations. It has created attractive targets for attackers simply because distributed storage locations offer more potential entry points. Stolen data is lucrative: it often includes sensitive personal data, financial records, and intellectual property.

Source: Frost & Sullivan

Strategic Imperative (continued)

- Because each repository has its own configurations, policies, and frameworks, data sprawl has made it difficult for organizations to implement and enforce consistent security policies and controls. Limited visibility also has made it extremely challenging for organizations to uncover, classify, and secure sensitive data, and to detect security risks and misconfigurations associated with their data.
- At its core, a data security posture management (DSPM) solution continuously discovers, classifies, and secures sensitive data, but a key capability is a uniform overview of all data repositories with a centralized control to identify, prioritize, and mitigate risks and misconfigurations. Organizations also benefit from consistent policy enforcement, automated remediation and response workflows, and streamlined compliance monitoring and reporting.
- The most basic DSPM solution includes several features:
  - **Data inventory and visibility** for automatic discovery; identification of specific categories; classification into broader groups based on sensitivity, types, and requirements; and tagging based on insights from the discovery and classification process
  - **Security posture assessment** for comprehensive evaluation of existing policies and controls to identify potential security risks and misconfigurations
  - **Risk prioritization** based on data sensitivity, access patterns, and potential impact
  - **Streamlined compliance** so that all sensitive data complies with security policies, standards, and regulations
  - **Reporting and analytics**, including a dashboard that offers a centralized overview of an organization’s data repositories for insights into the security posture
  - **Integration with third-party security tools** for workflows and incident response

Source: Frost & Sullivan

Strategic Imperative (continued)

- Comprehensive visibility regardless of where data resides enables contextual analysis that boosts the understanding of the relationships between data and its broader environment, resulting in more accurate remediation actions to effectively secure data.
- The DSPM industry is still emerging. The inherent nature of data security, especially in the context of sensitive data and regulatory compliance, does not completely prevent innovation but limits the scope for experimentation, resulting in incremental improvements rather than radical revolutions. Thus, potential customers today may see only small variations in functionalities from one vendor to another.
- As gradual innovation continues in the space, organizations can consider the following features to extend foundational DSPM functionalities into a more comprehensive solution:
    - **Risk prioritization with contextual and behavioral analytics** that moves beyond static risk assessments based on predefined or baseline rules to a more dynamic risk evaluation that incorporates artificial intelligence and machine learning (AI/ML) to continuously analyze data access patterns, user behaviors, and environmental factors. With contextual and behavioral analytics, DSPM solutions can identify anomalies and assess risks in real time based on the context of the data, user, and environment and produce a more accurate risk scoring methodology, enabling a more effective remediation process.
    - **Real-time data movement monitoring** that constantly observes data activity across environments and identifies unusual data flows, unauthorized access, and potential breaches rather than only scanning periodically. Dynamic tracking of data flows helps DSPM solutions understand the movement of data and ensures that security policies and controls are consistent regardless of where it is moving, who is accessing it, and where it resides.

Source: Frost & Sullivan

Strategic Imperative (continued)

- **Identity-centric data security** that provides more in-depth visibility into the relationship between human and non-human identities and data for more granular insights into whether an individual or system should have access to specific data, creating more dynamic behavioral profiles with access rights that can be adjusted as needed.
- **Privacy data protection** that includes data masking and anonymization to ensure secure data exchange internally among employees and externally with third-party stakeholders.
- **Real-time detection and response** that continuously scans data repositories and monitors activity related to sensitive assets to identify security risks and misconfigurations. Any identified security risks or misconfigurations will trigger an automatic remediation process in real time without the need for manual intervention.
- **Multiple remediation options** that allow for customized workflows in line with an organization's security policies, manual remediation for sensitive situations, collaboration with employees through communication channels, and multi-tier remediation based on severity.
- **Automated compliance management** in response to a new or amended data privacy regulation.
- **Comprehensive coverage across multiple environments** for consistent enforcement of security policies and controls on premises, in the cloud, and in hybrid configurations.
- **Consolidation into a broader data security platform or cloud-native application protection platform (CNAPP)**, using DSPM as a foundational component of a more holistic security approach.

Source: Frost & Sullivan

Growth Environment

- Frost & Sullivan's 2023 Voice of the Enterprise Security Customer survey asked 2,448 C-level executives across the United States, France, Germany, the United Kingdom, Japan, Australia, and Brazil which security solutions they planned to prioritize in their annual cybersecurity budget. Data security topped the list in Germany, Australia, and Brazil and shared the top spot with cloud security in other locations.
- Organizations in North America generally have a higher cybersecurity maturity level and are more open to embracing new technologies, including DSPM solutions. High-profile data breaches and new or amended data privacy regulations in many other countries, however, have forced organizations in other regions to take data security more seriously.
- The European Union General Data Protection Regulation (GDPR), the Privacy Protection Law in Israel, the Personal Data Protection Law in Saudi Arabia, and the African Union Convention on Cybersecurity and Personal Data Protection have been major catalysts for the adoption of DSPM in Europe, the Middle East, and Africa (EMEA), which Frost & Sullivan considers as a single region in its cybersecurity assessments. Those regulations compel organizations to prioritize data security or risk severe legal and financial consequences.
- Organizations in more digitally mature Asia-Pacific countries, such as Singapore and Australia, and in countries with strict data privacy regulations, such as Indonesia and China, will likely lead the charge toward DSPM implementation, although budgetary constraints and unfavorable exchange rates may restrain adoption throughout the region.
- In Latin America, investments in DSPM remain limited because of a greater focus on foundational security capabilities rather than advanced solutions, as well as an overall lack of security expertise. DSPM vendors will likely gain the most traction in Brazil and Mexico because of the countries' personal data protection laws.

Source: Frost & Sullivan

Growth Environment (continued)

- The DSPM market is still in its early stages of growth. Frost & Sullivan estimates that DSPM revenue will total $415.1 million in 2024—a 64.9% increase from the previous year—and projects a 37.4% compound annual growth rate (CAGR) from 2024 to 2029, reaching $2.03 billion.
- Economic uncertainties worldwide continue to restrain cybersecurity investments to a certain degree as inflation and higher interest rates persist. Decision makers may also be reluctant to invest in an emerging technology, such as DSPM, that has yet to demonstrate consistent outcomes, particularly if they think that legacy systems are still sufficient for their security requirements.
- The banking, financial services, and insurance (BFSI), technology, and retail/eCommerce industries are leaders in DSPM implementation because they handle user data at scale and are bound by stringent data privacy regulations.
- Very large (10,000 or more employees) and large (2,5000–9,999 employees) organizations contributed the majority of DSPM industry revenue in 2024. They commonly use hybrid or multicloud environments that span multiple locations and result in data sprawl, making it difficult for their security teams to manually monitor data flows and enforce consistent data governance. Medium-sized (1,000–2,499 employees), small (100–999 employees), and micro-sized (fewer than 100 employees) organizations with simpler data environments also are adopting DSPM solutions, but at a slower pace because of budgetary constraints.
- More established cybersecurity players entered the market in 2024 either through in-house development or acquisitions of early-stage data security start-ups. Eight acquisitions in the DSPM space since 2023 reflect the consolidation trend in the larger cybersecurity industry and indicate a demand for DSPM solutions to be part of a broader security portfolio rather than a stand-alone solution.

Source: Frost & Sullivan

Growth Environment (continued)

- Frost & Sullivan studies related to this independent analysis:
  - Growth Opportunities in Global Data Security Posture Management, 2024-2029 (PFO2-72; soon to be published)
  - SaaS Security Posture Management (SSPM) and Data Security Posture Management (DSPM)
  - Global Cloud-native Application Protection Platform Growth Opportunities
  - Growth Opportunities in Global Cloud Security Posture Management, 2024–2028

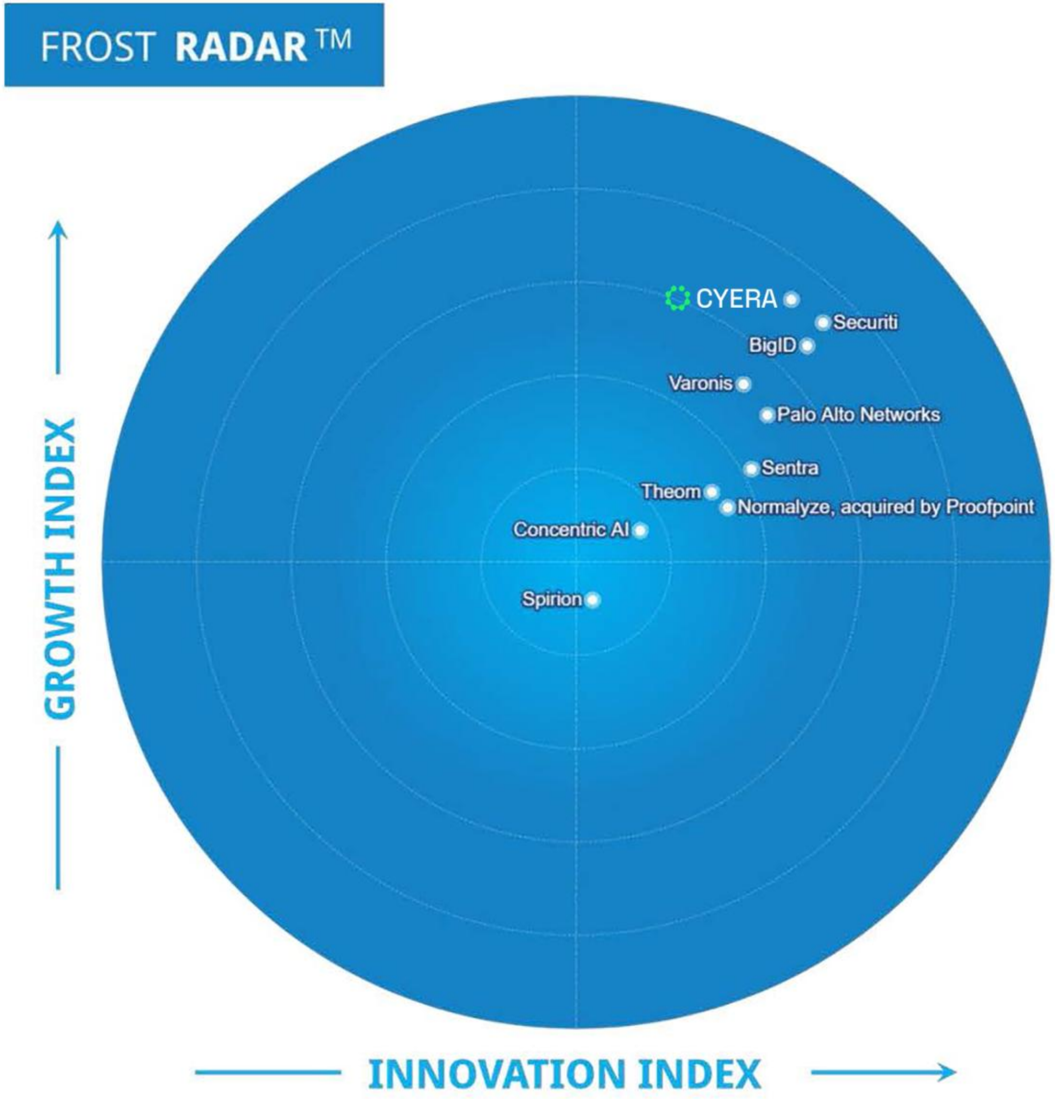
Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Data Security Posture Management, 2024

Source: Frost & Sullivan

Frost Radar™: Data Security Posture Management, 2024



Source: Frost & Sullivan

Frost Radar™ Competitive Environment

- From more than 20 vendors in the DSPM space, Frost & Sullivan selected 10 power players for further analysis in this Frost Radar™ publication. Considerations for selection included end-user focus, geographic presence, solution portfolio, and an estimated annual revenue of at least $3.5 million or a market share of at least 1% globally in 2024. Vendors that met the inclusion criteria but were unable to share detailed insights about their business performance and DSPM solutions were excluded to ensure fair scoring and comparison.

Growth Index

- Cyera is the leader on the Growth Index due to its remarkable performance since its establishment in 2020 as it registered a tremendous YoY growth of 136.4%. The company quickly gained prominence in the market through its AI-powered classification engine that can auto-learn and deliver 95% accuracy. It was the first cloud-native DSPM company that provides data security across IaaS, SaaS, and PaaS environments. Its DSPM highly resonates with the market, propelling the company to achieve a billion-dollar valuation in April 2024 and has further increased its valuation to $3 billion, highlighting the confidence investors have in its approach.
- Securiti is the second growth leader in the analysis due to its consistent growth momentum in the DSPM market, recording a remarkable YoY growth of 104.6%. The company's growth performance can be attributed to its success in winning several large-sized deals that ranges from 6 figures to high 7 figures. Its DSPM solution is incorporated into its flagship Data+AI Command Center platform, allowing the company to cross-sell or upsell to its customer base.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- BigID maintains a stable growth trajectory in 2024, recording a YoY growth of 35.5%. The company's YoY growth is considerably lower than other players in the analysis, but its early entry into the market has solidified its status as a leading player. The company took advantage of the wide customer base it has built for its work in privacy, compliance, and governance to push for its DSPM offering, which now serve as the foundational capability across the company's pricing models.

- Varonis also had an early start in the DSPM market, registering a stable YoY growth of 31.0% in 2024 as it continues to capitalize on its reputation in the data security and analytics field to push for its DSPM solution. The company provides its DSPM solution through its SaaS-based Data Security Platform, which has garnered a wide customer base due to its exceptional access management capabilities, and bundles the solution into different data protection packages, which allows it to address a wide range of use cases in the market.

- Palo Alto Networks entered the DSPM market through the acquisition of Dig Security, an early-stage DSPM company that provides an agentless and multi-cloud data security platform that discovers, classifies, protects, and governs sensitive data. Its DSPM solution is available as both an a la carte and combined module, integrated into its Prisma Cloud platform, and this flexibility has enabled the company to record a strong growth trajectory in 2024, recording YoY growth of 129.0%.

- Sentra continues to grow at a solid pace and register a strong YoY growth of 54.6%, establishing itself as one of the leading players in the DSPM market. The company predominantly targets "born-in-the-cloud" medium-sized to large organizations, offering an inclusive pricing model tailored to accommodate organizations of all sizes with four tiered options that meets the specific needs and budgets of the organization.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Theom continues to grow at a robust pace, as it combines data governance capabilities and DSPM under its flagship Cloud Data Protection Platform, which also encompasses other suites, such as insider risk detection and data loss prevention. Its ability to address a wide range of use cases offers a unique value proposition to the market but its reputation is still closely tied to its data governance capability, which is set to have a huge influence in its growth momentum if it is not addressed.
- Normalyze has a positive perception in the market thanks to the comprehensiveness of its DSPM platform. The company recently announced that it has been acquired by Proofpoint, which will allow the company to leverage Proofpoint's channel partner ecosystem and its GTM strategies to push its offerings, but the company first needs to communicate its strategy to existing customers that might be worried about the potential changes to its DSPM solution.
- Concentric AI provides a data security governance platform and uses machine learning in its DSPM to help organizations identify, classify, and protect sensitive data. The emphasis on its utilization of AI in its DSPM solution has helped the company to create a distinction, but its name is still less known in the broader DSPM market. The company recently raised $45 million, which might provide the boost that it needs to raise its profile in the market.
- Spirion is widely recognized for its strength in identification and classification of sensitive data, which helps the company to push its DSPM solution in the market. Its DSPM solution serves as the foundation of its Data Governance suite, but majority of its use cases are still around its strengths and not the broader DSPM capabilities, which greatly affects the perception of its DSPM solution.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

Innovation Index

- Securiti, BigID, Cyera, Palo Alto Networks, and Sentra are the leaders on the Innovation Index, with each providing comprehensive visibility into data, its usage and its access patterns. They utilize AI in multiple domains, such as classification, risk assessment, and threat mitigation that allow the DSPM to be more dynamic rather than baseline-driven posture management.
- Securiti delivers a built-in DSPM solution through a comprehensive platform that offers a comprehensive data mapping capability that provides an overview between data assets that have been discovered and classified and automatically discovers AI models and identities that have access to the data and how those identities are using the data. This data mapping capability is further extended to enable the tracking of cross-border data movement, data flows between different environments, data ownership, compliance requirements, and redundant, obsolete, and trivial (ROT) data, providing organizations with in-depth insights into their data posture.
- BigID's strength lies on its exceptionally advanced scanning capabilities, where it employs up to 10 different methods. This includes its Hyperscan technology that reduces scanning time of large-scale data volume by 95%, the industry's first dual hybrid scanning solution that utilizes its side-scanning method to rapidly onboard thousands of data sources, and its direct scanning method that analyzes metadata and file attributes across the entire cloud ecosystem, allowing its DSPM to provide in-depth context and visibility of entire data repositories.
- Cyera leverages novel ML and NLP technologies to perform continuous, multidimensional data risk assessments, combining pre-defined data classes with environment-specific analyses that enable the company to learn an organization's unique data and business purpose. This allows Cyera to improve its classification accuracy after each scan, now reaching up to 95% accuracy, and automatically trigger remediation workflows across its comprehensive third-party integrations, such as SIEM and ITSM tools.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Palo Alto Networks delivers robust DSPM capabilities designed to discover, classify, and automatically remediate security risks associated with sensitive data. A standout feature of its DSPM is its posture score that uses risk scoring and prioritization to help security teams to assess their progress over time. Because the solution is part of its Prisma Cloud, this allows the company to provide more comprehensive protection across cloud environments.
- Sentra is also well-placed on the Innovation Index in this analysis thanks to its novel data authorization graph. This enables Sentra to provide an interactive contextual view that maps the relationship between identities in the cloud, roles, permissions, data stores, and sensitive data classes, which then enables security teams to have a deeper insights on data movement and identity overprivileged permissions across data repositories.
- Varonis is a well-established name in the data security field and is highly regarded for its permission management capabilities. It leverages its expertise in permissions management to deliver a DSPM solution that can map all data interactions and perform permissions analysis to produce insights into the risk associated with the sensitive data. However, it is lacking expertise on cloud-native capabilities and its data protection packages are priced at a per-user basis and only comes at a premium price, which makes its DSPM less accessible for organizations that have an imbalance ratio of user and data or a smaller budget.
- Theom has a DAG-centric background but has built relatively comprehensive DSPM capabilities. A unique use case that Theom offers is its data exchange contracts capability, where the company would extract relevant details from an organization’s data sharing contracts with third parties and utilize the extracted information to ensure that the shared data comply with the agreement that both parties signed and perform actions, such as anonymization, if a violation is detected.

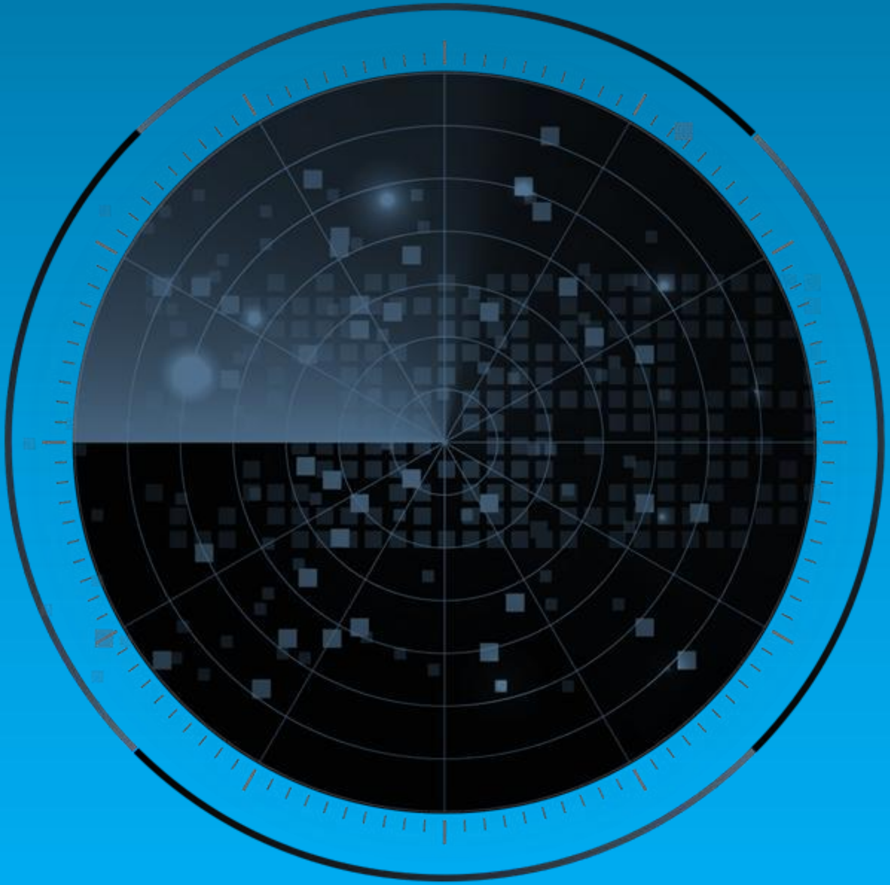
Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- While this is a unique use case, Theom's reputation is heavily linked with its work on DAG. It helps the company to cross-sell or upsell its DSPM, as it is offered through the same platform, but this affects the market perception, particularly because the company has a narrower integration scope in terms of both data repositories or third-party security tools. Because it comes from a DAG background, its DSPM features are not as proven as the more established DSPM players.
- Normalyze utilizes a patented technology to enable its DSPM to automatically discover data repositories at 1TB per hour without the need for extensive setup, allowing the solution to identify and classify sensitive data across large-scale data repositories. Its DSPM also uses a unique approach in highlighting risk as it assigns monetary value to the costs associated to possible exposure, allowing this information to be presented in a more understandable manner to non-technical stakeholders. The recent acquisition by Proofpoint is set to strengthen Normalyze's offering, particularly as it is set to be integrated into Proofpoint's flagship data loss prevention (DLP), offering contextual insights that can enhance detection and response.
- Concentric AI's DSPM utilizes deep learning to categorize data, assess risk, and remediate risks more efficiently without the need for complex configurations, minimizing the possibility of inaccurate labeling that usually occurs from manual intervention. While this indicates strong R&D efforts, it faces a major challenge in terms of brand recognition and resources to expand its DSPM capabilities and integrations coverage in an environment that is increasingly requesting a holistic data security platform.
- Spirion demonstrated strong R&D capabilities with the incorporation of several patented technologies, such as the AnyFinds technology that powers the discovery portion of its DSPM solution. However, its strength in discovery and privacy is not well-complemented on the remediation end, in which the company does offer flowchart-like remediation workflows to accelerate process but does not offer enough emphasis on real-time threat detection.

Source: Frost & Sullivan

Frost Radar™: Companies to Action



Source: Frost & Sullivan

Cyera

INNOVATION

- Cyera delivers an agentless, cloud-native, and AI-powered DSPM through an integrated data security platform that also encompasses data access governance and data privacy solutions. Data detection and response is an extension of its DSPM, allowing security teams to identify and remediate risks and prevent data exfiltration in real time.
- The combination of agentless and cloud-native technology and its non-invasive nature enables Cyera to deploy the solution in less than 5 minutes, allowing organizations to realize value almost immediately. The solution automatically discovers and classifies data with precision of up to 98% across cloud data sources, databases in virtual machines, folders and files in SaaS applications and recently began providing on-premises support and contextualizing data discovered in on-premises data sources for better insights on the content of the data, providing customers with comprehensive coverage across data repositories.
- Cyera's DSPM solution can detect data security events in near-real time and utilizes its dynamic data detection and classification engine to provide contexts regarding data owner, relevant business unit, and sensitivity level of data to contextualize risks, which reduces false positive alerts, and provides prioritized remediation guidance that aligns with a customer's security requirements, ensuring that the remediation does not violate any security policies or controls.
- Cyera also provides a unified view of both human and non-human identities, understanding the increasing utilization of non-human identities to access sensitive data. It extends this view to include third-party identities, offering a comprehensive overview of the relationship between data assets and identities so that permissions can be revoked more quickly if warranted.

Source: Frost & Sullivan

Cyera (continued)

GROWTH

- Frost & Sullivan's estimates that Cyera registered an impressive YoY growth of 136.4% in 2024, becoming the fourth-biggest player in the DSPM market. Its marketing campaigns targets large and very large organizations that handle massive volumes of data every day and would benefit from DSPM.
- Founded in 2021, the company emerged from stealth in December 2022 with $60 million in financing from venture capital firms including Sequoia, Accel, and Cyberstarts, and established partnerships with several Fortune 500 companies, which allowed it to grow its revenue by 800% in its first year.
- It raised another $300 million in a Series C funding round and reached unicorn status with a $1.4 billion valuation in April 2024. Seven months later, it announced that it had secured $300 million in a Series D funding round, raising its valuation to $3 billion. This indicates the trust that investors and the industry have in Cyera's strategy of securing data across multiple environments.
- In October 2024, the company acquired Trail Security, a next-generation DLP company, for $162 million. The integration of Trail Security's capabilities into Cyera's DSPM platform will boost its goal of becoming the industry's first unified data security platform.

Source: Frost & Sullivan

Cyera (continued)

FROST PERSPECTIVE

- Cyera is in an advantageous position in this Frost Radar™ analysis. Its ability to contextualize data across different repositories is a standout feature that boosts the accuracy and precision of data discovery and classification and generates prioritized remediation guidance as it adds context about the data owner, relevant business unit, and sensitivity.

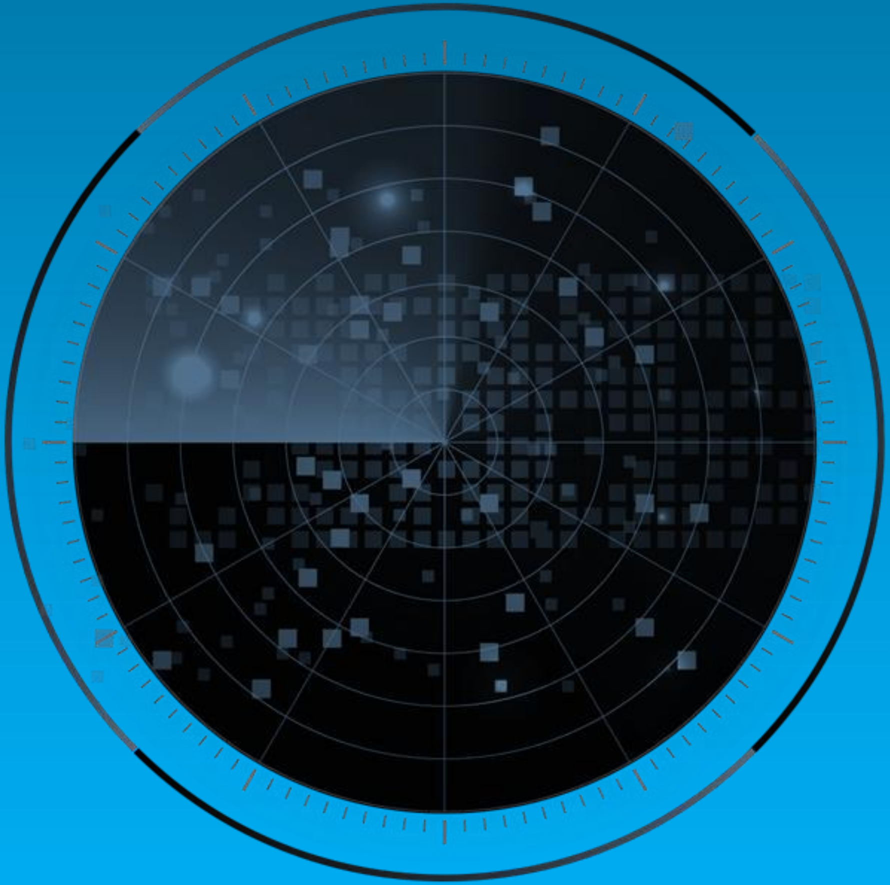
- The company is still behind its peers in terms of privacy and governance frameworks. The inclusion of the support for on-premises data repositories indicates its commitment to address data security holistically, but because it was only launched in April 2024, there might be questions about whether it can provide support as extensive as what it offers for data in the cloud.

- The Trail Security acquisition will help Cyera enhance its remediation capability. However, because the integration is ongoing and no customer feedback has yet to emerge, the actual impact and effectiveness of Cyera's newly enhanced platform remain uncertain.

- The latest funding round that raised its valuation to $3 billion will enable the company launch more aggressive marketing campaigns, increase headcount, and expand to other locations reduce its reliance on North America for revenue.

Source: Frost & Sullivan

Best Practices & Growth Opportunities



Source: Frost & Sullivan

Best Practices

1 DSPM vendors should consider providing solution that ensures seamless integration with various data repositories, such as cloud storage, on-premises databases, or lower development environments, to ensure that sensitive data can be discovered, classified, and protected regardless of where it resides. An effective DSPM solution should also be able to scale to new data repositories without the need for extensive setup.

2 As the threat landscape becomes more sophisticated, DSPM vendors must build solutions that can provide equally robust posture management and remediation capabilities. Remediation extends a solution's effectiveness by addressing security risks and vulnerabilities, helping organizations to be more proactive in protecting their data from being stolen or accessed illegally.

3 DSPM vendors and prospective customers must make sure that they share the same views on the solution's ability to address challenges. The right solution must be able to meet an organization's business requirements and help it specifically improve the security posture of its data landscape. A misaligned DSPM solution will interrupt business operations and cause issues ranging from false alerts to higher costs.

Source: Frost & Sullivan

Growth Opportunities

1 Customers are considering solutions that offers equally robust posture management and remediation capabilities to address security challenges holistically. Posture management helps them to discovery and classify sensitive data across various repositories, but they are increasingly looking for solutions that allow them to understand the context around data access and usage, a crucial component that enables proactive remediation.

2 DSPM is cloud-native in nature, but many organizations still store their data in on-premises environments to save money, have greater security control, or comply with rules and regulations. Data also can be stored in development or SaaS environments. A DSPM solution should be able to offer the same capabilities and effectiveness in any environment.

3 DSPM solutions offer visibility into the identities that have access to data, but as organizations rely more on non-human identities and data sprawl becomes even more of a problem, solutions must evolve from baseline access control and authentication to a deeper identity discovery and mapping capability and more dynamic, real-time, and context-driven identity-based risk management.

Source: 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.

II1

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

II2

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

II3

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

II4

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

II5

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

Source: Frost & Sullivan

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 CEOs 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.

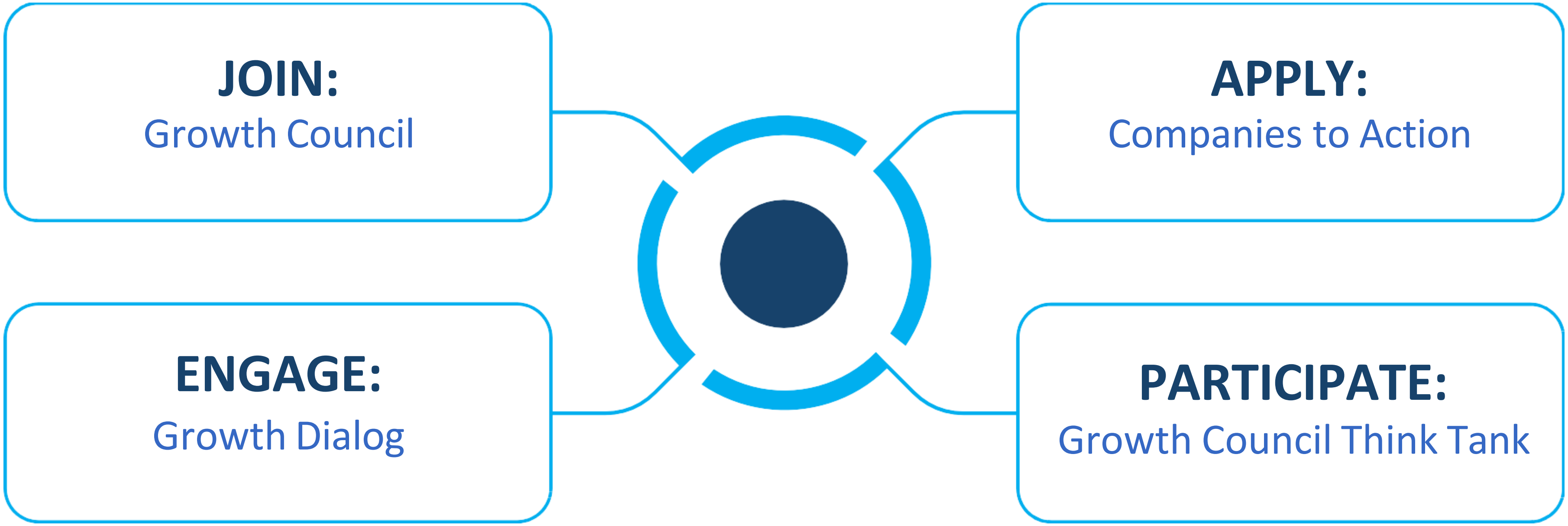
NEXT STEPS

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

Source: Frost & Sullivan

Next Steps

Transformation ○ Ecosystem ○ Growth Generator ○ **Growth Opportunities** ○ Frost Radar™ ● Best Practices ○ Companies to Action ○



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

Source: Frost & Sullivan