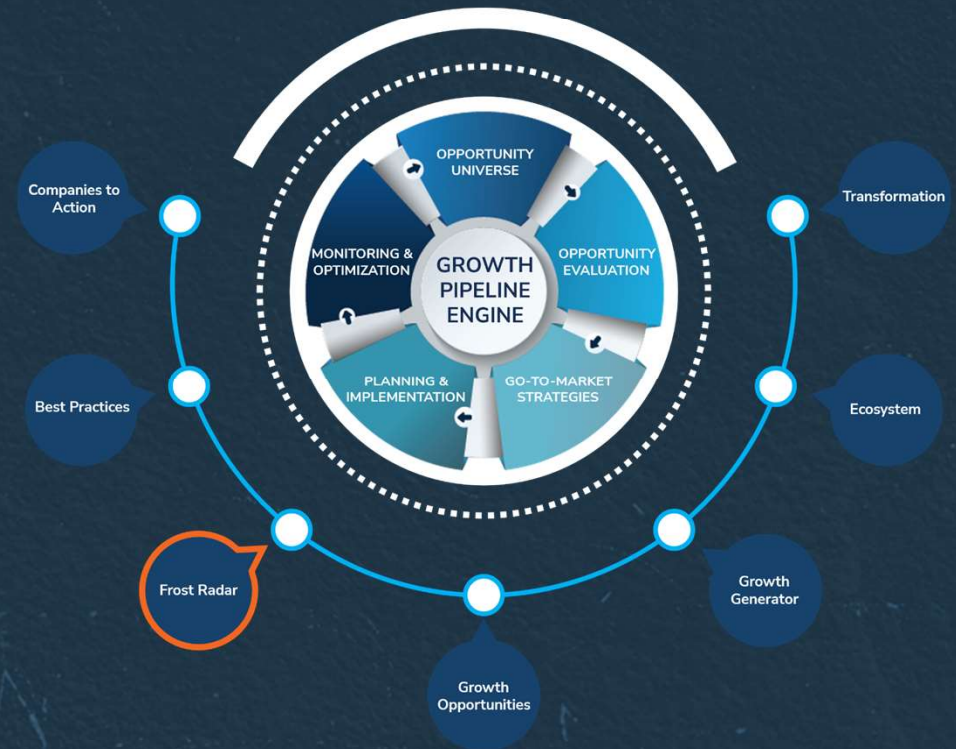


Frost Radar™: Data Security Platforms, 2025

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

Authored by: Daphne Dwiputriane

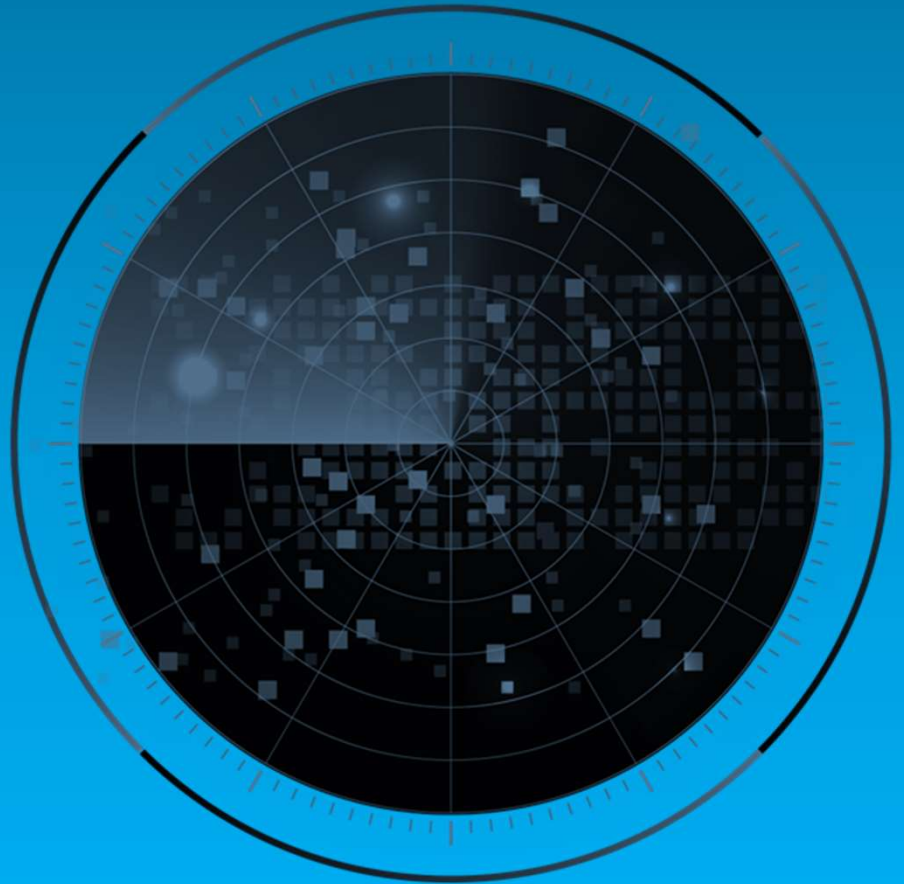
Contributors: Jarad Carleton, Anh Tien Vu



PG3B-74
November 2025

F R O S T  S U L L I V A N

Strategic Imperative and Growth Environment



List of Abbreviations

- **AI:** Artificial Intelligence
- **API:** Application Programming Interface
- **BFSI:** Banking, Financial Services, and Insurance
- **CASB:** Cloud Access Security Broker
- **CNAPP:** Cloud-Native Application Protection Platform
- **DAM:** Database Activity Monitoring
- **DB:** Database
- **DDR:** Data Detection and Response
- **DevSecOps:** Development, Security, Operations
- **DLP:** Data Loss Prevention
- **DSP:** Data Security Platform
- **DSPM:** Data Security Posture Management
- **EDR:** Endpoint Detection and Response
- **EMEA:** Europe, the Middle East, and Africa
- **ETL:** Extract, Transform, Load
- **EPS:** Event-Per-Second
- **GenAI:** Generative AI
- **GTM:** Go-to-Market
- **GSI:** Global System Integrators
- **IRM:** Insider Risk Management
- **ITM:** Insider Threat Management
- **LLM:** Large Language Models
- **MFA:** Multi-Factor Authentication
- **ML:** Machine Learning
- **MSP:** Managed Service Provider
- **MSSP:** Managed Security Service Provider
- **NLP:** Natural Language Processing
- **NGFW:** Next-Generation Firewall
- **OEM:** Original Equipment Manufacturer
- **PAM:** Privileged Access Management
- **REST:** Representational State Transfer
- **ROT:** Redundant, Obsolete, and Trivial
- **SaaS:** Software-as-a-Service
- **SASE:** Secure Access Service Edge
- **SDK:** Software Development Kit
- **SIEM:** Security Information and Event Management
- **SLM:** Small Language Models
- **SOAR:** Security, Orchestration, Automation and Response
- **SOC:** Security Operations Center
- **SSO:** Single Sign On
- **UEBA:** User Entity and Behavior Analytics
- **XDR:** Extended Detection and Response

Strategic Imperative

- Data has always been central to how an enterprise operates and makes decisions, regardless of the sector, size, or maturity. The rise of big data, cloud, and GenAI has effectively multiplied the value of data, making it an even more attractive target for attackers.
- Cybersecurity has long played an integral role in protecting data through mature, widely adopted solutions, such as encryption, tokenization, masking, and DLP, with encryption often used in regulatory compliance and controlled sharing while DLP is used to prevent leakage of sensitive information. Some data security tools focus on monitoring file activity while others emphasize privacy, regulatory compliance, and data lifecycle governance. DSPM recently emerged as a tool that specifically focuses on providing visibility and context across cloud and SaaS workloads.
- The landscape for data security solutions is fragmented because data risks exist in multiple entry points, from databases, cloud environments, and SaaS applications to endpoints, access permissions, and identities. Enterprises need a solution to address each challenge, but many of these solutions were deployed at different times. As a result, it is difficult for enterprises to maintain consistent context or enforce uniform policies across all data security controls.
- This is why data protection should be viewed through the data lifecycle lens from creation to storage and deletion, where visibility, governance, and protection are applied continuously as data changes type and state. From this, an ideal DSP should deliver core capabilities spanning data discovery and classification, access and identity governance, data protection and control mechanisms, real-time detection and response, and compliance enforcement and posture management with extended support to protect data used in AI systems.

Strategic Imperative (continued)

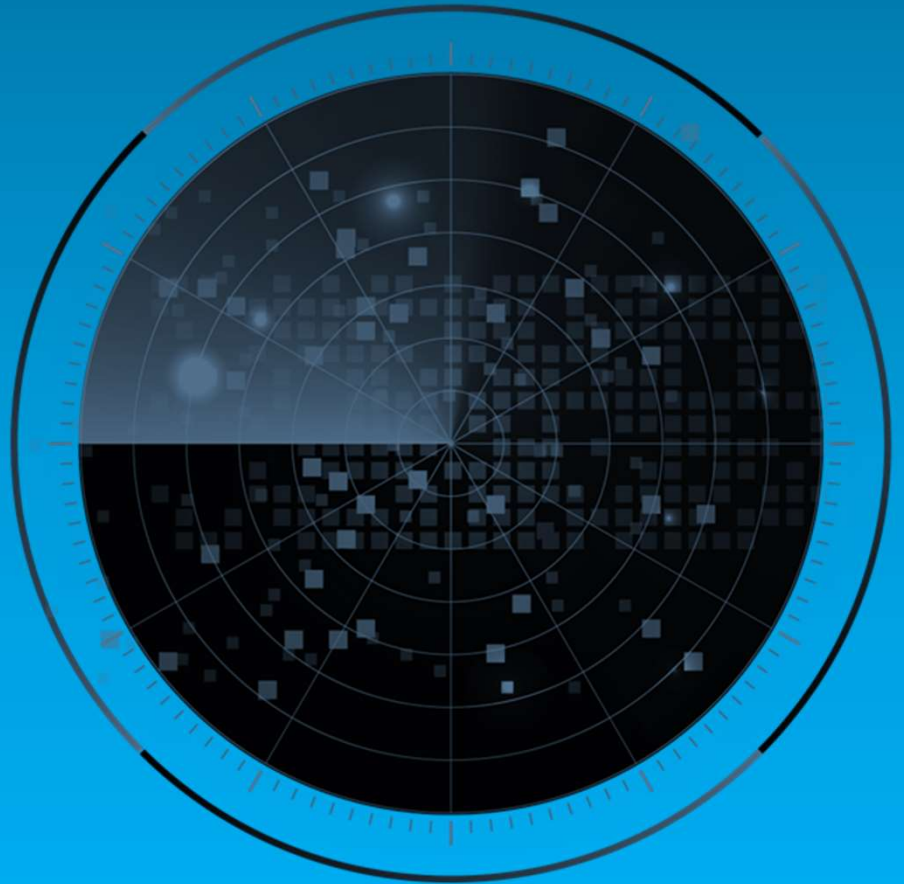
- Once data is created, an enterprise must first build governance and contextual intelligence to establish a strong foundation. This architecture-driven flow ensures that every subsequent action, such as detecting anomalous behavior or enforcing protection controls, is accurate, precise, and consistently aligned across the data lifecycle. All capabilities are anchored by a centralized policy and intelligence engine that serves as the platform's decision-making brain to ensure that all capabilities work in concert, regardless of whether subsequent remediation actions are done natively or via third-party orchestration workflows.
- The platform must also have flexible deployment options across cloud, on-premises, and hybrid environments to meet diverse regulatory and operational requirements while preserving full functionality regardless of deployment choice. The ideal DSP should also integrate seamlessly with the broader security ecosystem to ensure compatibility with existing architectures and streamline orchestration workflows to avoid costly rip-and-replace efforts as well as maintain cohesive security operations.
- Defining a DSP based on the data lifecycle allows the elimination or minimization of utilizing a traditional hierarchy of acronym-driven point solutions, which has made the market more confusing for customers because of the explosion of acronym usage. This shifts the focus to underlying capabilities tied together by a centralized engine, rather than the acronyms. With the acronyms now removed, vendors can enter the DSP space by addressing use cases that best anchor on their historical strengths and supplementing them with additional capabilities across the data lifecycle.
- As vendors naturally focus on use cases that align with core strengths, the market becomes extremely competitive, with differentiation driven by the breadth, depth, and integration of capabilities rather than acronyms. To stand out in this extremely competitive landscape, DSP vendors must continue to evolve to deliver end-to-end coverage across the data lifecycle.

Growth Environment

- The DSP market is fast-growing, with its revenue growth rate for 2025 expected to be 29.0%, indicating a high demand and accelerated adoption rate. Its compound annual growth rate (CAGR) for the 2025-2030 period is anticipated to be 23.2%, signaling steady growth opportunities.
- Cyberattacks have seen an exponential increase in volume and become more sophisticated and difficult for security teams to detect. Regulatory bodies have either introduced or updated regulations to help enterprises secure their data better in this modern threat landscape.
- North America leads the adoption of DSP. Enterprises here are more mature in terms of security and open in experimenting with the latest technologies to have stronger security controls. EMEA is a close second as strict regulations, such as GDPR, increase awareness about the need for DSP. The regions will continue to be the main DSP markets. Latin America and Asia-Pacific contribute considerably less revenue but will grow at a significantly faster rate as more enterprises become aware on the benefits of DSP, particularly in countries with strict data privacy regulations.
- Very large (at least 10,000 employees) and large (2,500–9,999 employees) enterprises will contribute the most to the DSP market globally in 2025 and are expected to remain the largest contributors until 2030. They have more complex data environments and regulatory requirements than smaller enterprises. DSP's ability to discover and classify sensitive data and apply relevant compliance frameworks is attractive to highly regulated sectors, such as BFSI, and technology sectors.

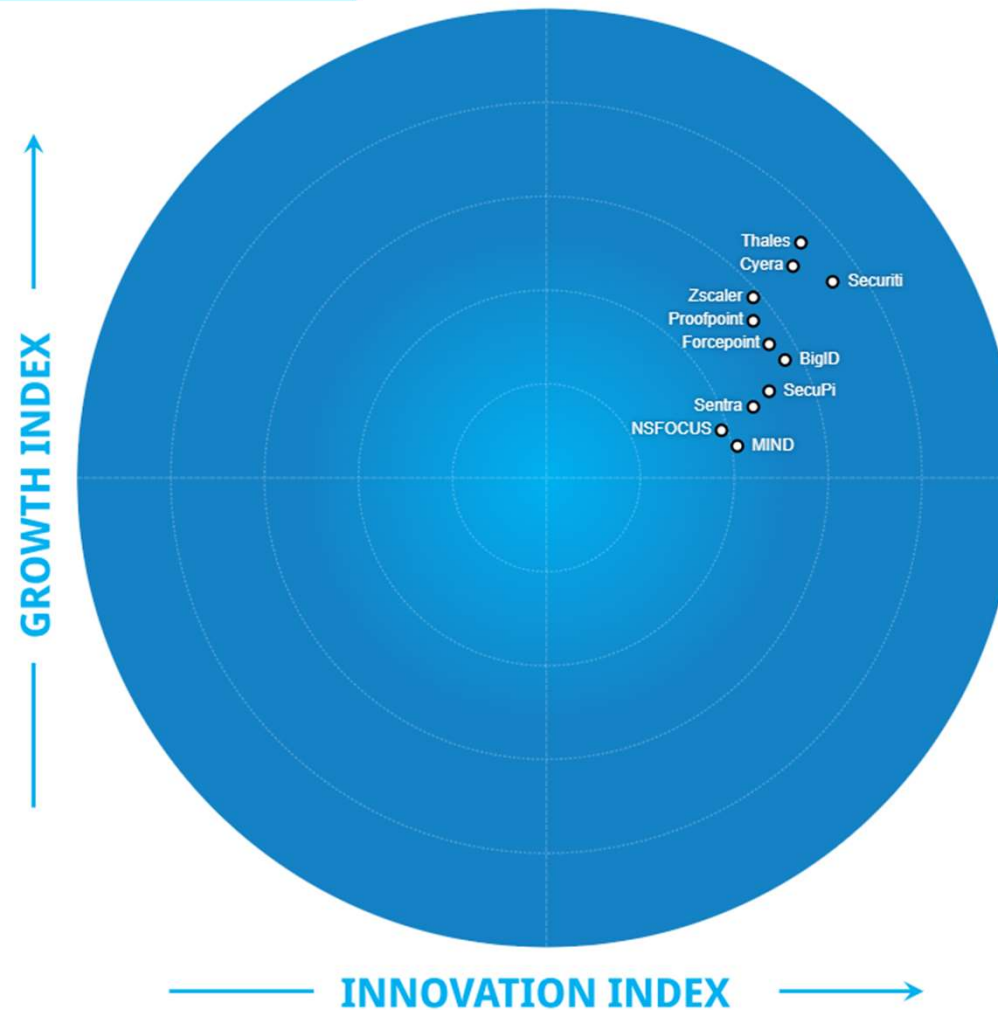
F R O S T  S U L L I V A N

Frost Radar™: Data Security Platforms



Frost Radar™: Data Security Platforms

FROST RADAR™



Frost Radar™ Competitive Environment

- From more than 20 participants in the space, Frost & Sullivan has shortlisted 11 growth and innovation leaders for this Frost Radar™ analysis based on a minimum estimated annual revenue threshold of \$4 million in 2025.
- The lifecycle-centric perspective directly shapes the strategic imperatives driving the DSP market. At its core, it emphasizes delivering the core promises of data security through a single, unified platform that is anchored by a centralized policy and intelligence engine that connects data lineage, governance, and behavior to provide shared context and consistent protection across all environments.
- The 11 vendors can be classified into two groups: governance-led, whose strength lies in visibility by providing solid discovery and classification; and protection-led, whose strength lies in enforcement capability and can be further segmented into DLP-centric and encryption-centric. The groups are gradually meeting in the middle, with governance-led vendors extending into policy enforcement and remediation and protection-led vendors strengthening discovery, classification, and visibility, marking the market's natural progression toward convergence without losing the diversity of historical strengths.
- The protection-led group is dominated by vendors that came from adjacent markets, such as encryption and DLP, which allows them to leverage an existing customer base to dominate the DSP market. The governance-led group has a stronger growth trajectory as it flips the usual enforcement-first model by addressing governance first before extending into enforcement so that its DSP can use metadata collected from the discovery and classification process to ensure that accurate actions are taken.

Frost Radar™ Competitive Environment (continued)

- As the market converges, evaluating DSPs becomes more difficult because each vendor approaches the problem from different historical strengths and supplements those strengths with adjacent capabilities to extend across the data lifecycle. This diversity means that feature-for-feature comparisons are extremely challenging. For this reason, Frost & Sullivan not only considered a vendor's ability to deliver the core promises in a single platform, but also advancements in areas such as identity-centric control for securing data, policy simulation, management of ROT data, data drift detection; flexibility in deployment models and enforcement mechanisms; and the presence of a centralized policy and intelligence engine so that all capabilities share the same context.
- Ultimately, differentiation between vendors is small because every vendor can address core DSP needs, which makes each vendor an ideal partner. The difference lies in how effectively each vendor aligns its historical strengths to specific use cases and extends them into a coherent DSP architecture that delivers measurable operational outcomes. For enterprises, this means the right fit depends more on matching immediate priorities with a vendor's core strength rather than a feature checklist.
- Frost Radar™ Growth Index leaders Thales, Cyera, Securiti, Zscaler, and Proofpoint have managed to exploit their strengths in strategic funding, established customer base, and strong capability differentiation to capture opportunities in the DSP market.
- Thales is the Growth Index leader thanks to its strategy of leveraging its own and Imperva's extensive customer base to drive adoption of CipherTrust DSP, which is already well-known for its deep data encryption capability. The platform became an even more compelling choice for many enterprises after Thales significantly strengthened its visibility and control portion with the Imperva acquisition. The combination of two historically different domains provides a strong differentiator for Thales, opening opportunities that other DSP players do not address extensively.

Frost Radar™ Competitive Environment (continued)

- Cyera leveraged its \$6 billion funding to aggressively extend its reach across different regions, sectors, and sizes, and this has produced incredibly solid growth opportunities. Securiti, meanwhile, has solid credibility from adjacent markets, such as privacy and governance, and centers its marketing campaigns on its DataCommand Graph™, which makes it particularly attractive to enterprises seeking accurate enforcement grounded in solid governance foundation. Both are investing in many of the most important industry developments and market trends, and this will continue to drive revenue growth for the foreseeable future.
- Zscaler and Proofpoint both benefit from strong growth pipelines and established presence in other cybersecurity markets (SASE and DLP for Zscaler, email security and DLP for Proofpoint), allowing them to obtain two of the highest market shares. Their extensive customer portfolios and channel partner ecosystem provide a viable path to new DSP opportunities because it enables them to leverage existing relationships to accelerate adoption.
- Frost Radar™ Innovation Index leaders Securiti, Thales, Cyera, BigID, and Forcepoint come from a different lineage and illustrate that DSP is an ecosystem of complementary philosophies converging toward the same outcome: consistent and intelligent data protection anchored on a centralized, unified policy engine.
- Securiti is the overall Innovation Index leader thanks to its DataCommand Graph™ that powers its DataAI Command Center, in which the graph serves as a unified intelligence layer that connects discovery, privacy, and protection under a centralized engine that allows functionalities and new features to operate in a shared context. Its decision to position governance and intelligence as the foundation of control signals to the market that a DSP can be built from a data governance background rather than security enforcement.

Frost Radar™ Competitive Environment (continued)

- Thales ranks second on the Innovation Index, offering a counter-narrative to the DSP status quo by proving that deep encryption capability and data intelligence can coexist in a single operational model. Its architecture is designed to ensure that even if the visibility or governance layer fails, sensitive data remains protected through specialized encryption techniques. By anchoring protections at the data layer itself, Thales delivers genuine defense-in-depth capability.
- Cyera and BigID demonstrate that DSPs can converge on a centralized architecture while pursuing complementary paths, delivering native enforcement when possible and seamless integration with broader security stacks. Cyera delivers strong visibility and deep integration for remediation across SaaS and cloud workloads while strategically expanding its coverage with an Omni DLP that consolidates intelligence from multiple DLPs to enable context-aware policy enforcement. BigID build its DSP around metadata intelligence, turning discovery and classification insights into actionable policies while allowing enforcement either directly in place or through existing security integrations.
- Forcepoint leverages its DLP expertise to demonstrate how a DSP can evolve from a mature, enforcement-driven foundation. By unifying DLP, DSPM, and DDR, as well as SaaS, web, and email security in a single platform while powering these capabilities with a distributed intelligence layer, Forcepoint can deliver context-aware, real-time policy enforcement across all data states. The changes in management indicate the company is doubling down on its “Data Security Everywhere” vision.

Frost Radar™ Competitive Environment (continued)

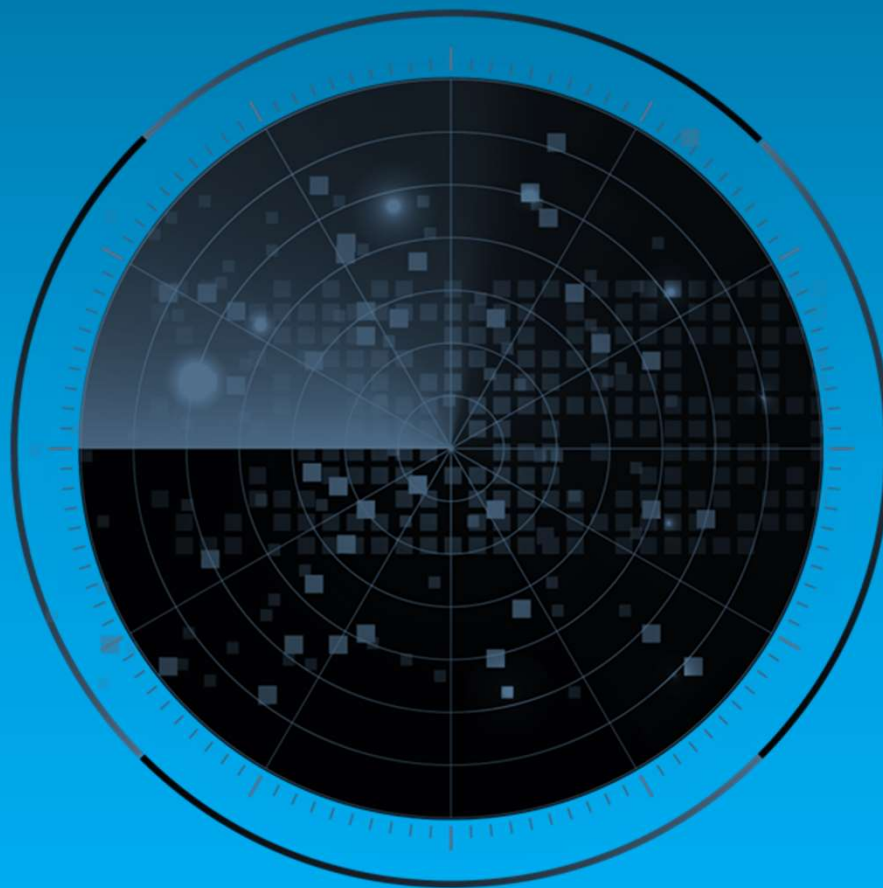
- SecuPi illustrates the trade-off between architectural depth and coverage breadth. Its central management unifies the attribute processor, sensitive data catalog, and policies to enable precise, context-aware enforcement through tokenization, format-preserving encryption, and dynamic masking while also regularly sending event logs to SIEM tools for centralized reporting. Deep specialization allows SecuPi to have a strategic niche among Fortune 500 and Global 2000 enterprises in highly regulated sectors that still rely on databases but limits its presence in other sectors. This is reflected in its smaller market share.
- Proofpoint and Zscaler share a common heritage as mature DLP providers that have evolved into DSP providers and leverage their presence across other spaces in the cybersecurity industry. Proofpoint delivers a DSP built based on a strong human-centric data protection vision and, thus, convergence of its enterprise DLP, DSPM, and ITM in a single platform. Zscaler treats its DLP as the core engine for its DSP, allowing the company to consolidate multiple control points into a unified policy framework across cloud, SaaS applications, endpoints, and personal devices.
- Sentra's origins can be traced back to DSPM, placing it as part of the governance-led group, but it has extended its capability into enforcement through an independent policy engine that can natively enforce context-aware policies or integrate with existing security stacks to align actions with broader enterprise workflows. Sentra may emerge as the vendor with the most flexible approach in future analysis once it broadens its native and integrated enforcement actions.

Frost Radar™ Competitive Environment (continued)

- MIND shares the same DLP-oriented DNA as other DLP subgroup players from the broader protection-led group but has less legacy burden because it is a newer market entrant. Its capabilities are compelling, and it does address one of the core needs in data security well through a solid multiclassification engine that enables more intelligent and accurate prevention. However, from a DSP perspective, MIND still needs to demonstrate its ability to operate at scale, integrate more deeply with the broader security stack, and clarify whether it intends to position itself as DLP-focused or evolve into a full DSP platform.
- NSFOCUS offers a solid DSP solution but lags other top players in innovation because its platform primarily is for on-premises deployment, though it increasingly supports integrations with SaaS applications and cloud data sources. Its roadmap signals a promising future as it works to balance the needs of its largest market (China) with alignment to global trends. Improving accessibility and deployment effectiveness outside China could drive revenue growth and demonstrate broader operational maturity.
- Several notable vendors, such as IBM and Varonis, were considered for this Frost Radar™ analysis but were not included because of a lack of sufficient secondary information for benchmarking.

F R O S T  S U L L I V A N

Frost Radar™: Companies to Action



BigID

INNOVATION

- BigID delivers a cloud-native DSP that can be deployed across on-premises, cloud, and hybrid environments, allowing enterprises that operate under strict data residency and sovereignty regulations to benefit from its DSP without architectural compromise.
- Originating from data discovery and governance roots, the company has one of the broadest coverages for data discovery with native integrations across diverse data sources in on-premises, AI models, SaaS applications, and cloud storage, as well as high classification accuracy with the ability to provide custom classifiers and more than 1,000 prebuilt classifiers. The combination of breadth (data sources) and depth (classification) allows BigID to form a strong foundation for lifecycle-wide protection.
- BigID's architecture implicitly reflects a centralized policy and intelligence design through its central console that unifies governance, privacy, and security insights in a single operational layer. BigID uses ML-based contextual analysis to understand data context around data owner, data location, and user access so that remediation and risk reduction actions are applied consistently across environments. With this centralized decision-making, uses cases including DSPM, DLP, privacy, AI governance, and compliance can be consolidated more seamlessly, forming a unified and scalable architecture that allows an enterprise to operate under a single policy framework.
- Building on this centralized decision-making, enterprises can use the same insights to remediate either through BigID's unique in-place remediation that allows native actions, such as quarantining, revoking, deleting, and masking data, in real time without needing those data to be relocated, or through external security stacks, such as SIEM, SOAR, DLP, and CNAPP. This dual approach allows enterprises to choose the remediation option that best aligns with their needs.

BigID (continued)

INNOVATION

- BigID has already begun incorporating GenAI-specific controls into its DSP to help teams in detecting and mitigating GenAI-related risks. BigID uses its patented ML and NLP models to identify whether sensitive or regulated content is being used for model training and quarantine improperly used data in real time. By building these GenAI-specific controls, BigID allow its customers to adopt AI tools with confidence, balancing innovation with security.
- BigID's latest updates and innovations include a patent for identity-aware AI for privacy and security; an innovative hybrid scanning method for cloud-native workloads that enables customers to discover, classify, and protect cloud data better; and GenAI-specific controls for Microsoft Copilot with the introduction of capabilities such as Access Intelligence, Data Activity Monitoring, and AI data security.

BigID (continued)

GROWTH

- BigID has significant DSP revenue that continues to grow at a consistent rate yearly, thanks in part in leveraging its strong presence across important and adjacent cybersecurity markets, such as governance and compliance, to upsell its DSP, driving revenue and providing strong growth opportunities.
- BigID targets large enterprises in the BFSI, healthcare, telecom, retail, and government sectors that operate under high regulatory pressure and manage complex data environments. This focus has helped BigID build a strong foothold in compliance-driven sectors across the world.
- The company has made slight adjustments to its pricing model to extend its reach to medium-sized and smaller enterprises that face similar risks but may not have the same resources or maturity. This includes setting its pricing model as modular-driven, where smaller teams start with one use case and expand over time, and releasing BigID Express, a lighter deployment option of its DSP.
- BigID operates a hybrid GTM model where the core upselling deals are often handled directly, while partners engage in sourcing, co-selling, and implementation in new geographies, sectors, and modular use cases, such as DSPM or privacy automation. This combination allows BigID to not only leverage its customer base but deliver DSP in its core regions of North America and EMEA, as well as Latin America and Asia-Pacific, which contribute a smaller but still significant part of the company's revenue.

BigID (continued)

FROST PERSPECTIVE

- BigID's biggest differentiator in the DSP market is its mature discovery and classification capability, which the company has since expanded to address the broader data lifecycle framework. Its successful transition from visibility to actionable controls is driven by its ability to collect metadata from data it has discovered and classified and use those metadata to unify governance, security, and privacy insights in a single operational layer. This allows remediation and risk reduction to share the same context from the moment data is discovered; thus, policies are applied consistently.
- Consistently applied policies can be enforced either through BigID's in-place remediation or by orchestrating actions across existing security stacks, ensuring that remediation and risk reduction can be performed depending on customers preferences. This flexibility signals the company's commitment to delivering actionable data protection. Looking ahead, BigID can consider deepening scalability and agility for cloud deployments as well as strengthening its enforcement actions by introducing capabilities such as attack path analysis, policy simulation, and the triggering of automatic remediation actions that can remediate dynamically depending on user, risk level, and data sensitivity.
- BigID's innovation efforts are aimed in the right direction with its efforts to further enhance its core strength of discovery and classification through the launch of hybrid scanning and data activity monitoring while extending its expertise to help customers mitigate GenAI risks. The company should continue to extend its capabilities into GenAI security to meet the growing demand for actionable governance in AI-driven environments.
- BigID's hybrid GTM model has been effective for a steady growth trajectory, but sustaining growth momentum would require deeper expansion in locations such as Asia-Pacific and additional sectors, such as technology and media.

Cyera

INNOVATION

- Cyera was founded to solve the challenge of discovering and classifying data across cloud environments and has since evolved to delivering cloud-native, API-driven DSP that extends visibility and control into on-premises environments.
- Cyera uses an agentless approach to continuously discover structured and unstructured data across diverse data sources. Its classification engine utilizes custom LLMs, heuristics, and Regex to achieve high classification accuracy, and it enriches visibility by continuously mapping each data asset with metadata, such as identity, access, and ownership context. Once deployed, its AI-based classification continuously learns enterprise-specific data types, which allows for context to always be updated based on the latest changes.
- Contextual insights feed into a centralized policy and intelligence layer that correlates data, identity, and usage signals for consistent policy enforcement across environments. This highlights Cyera's ability to stay ahead of emerging trends, such as identity-centric data security, while strengthening its governance and visibility foundation essential for a more complete data lifecycle protection.
- Cyera originated with a focus on managing data risks in the cloud, and its core strength is automated threat detection and response for data stored in the cloud. The platform can continuously detect and remediate data exposures by performing automatic dynamic masking (via integrations in Snowflake) or sending alerts to CNAPP or data management tools. The company also offers integration with SIEM and SOAR for broader remediation actions to accelerate response times.

Cyera (continued)

INNOVATION

- The recent launch of its Omni DLP showcases Cyera's innovative efforts to redefine DLP by building a centralized intelligence layer that aggregate signals from existing DLPs and combines them with insights from its AI-native data classification for a more context-aware, unified enforcement. This approach helps Cyera avoid a rip-and-replace dilemma with customers that may not be comfortable with replacing their DLPs, while positioning itself as a visionary that addresses the high false positive rates that have long limited DLP effectiveness.
- To detect emerging GenAI risks, Cyera has launched various features that monitor the use of external AI services via Omni DLP's integrated sensors, where findings can be fed to an asset model that maps AI models, agents, and assistants to datastores and identities and flags any data-egress issues.
- Cyera releases a new feature approximately every six weeks, which demonstrates product velocity and a commitment to R&D. This pace of innovation enables customers to benefit from incremental feature delivery without long upgrade cycles. The company's roadmap focuses on improving its data intelligence, providing more support for privacy operations, and continuing its work in developing capabilities to mitigate GenAI risks.

Cyera (continued)

GROWTH

- Cyera continues to grow its DSP revenue at a rapid pace, registering the highest yearly growth among the market leaders. While the company is only five years old, it has already built significant investor and customer trust. It reached a \$6 billion valuation and expanded its Fortune 500 customer base by 353%, capturing 10% of the segment in the past year alone.
- Most of Cyera's customers are in North America, followed by EMEA. Its recent funding round and growing partner ecosystem are helping the company expand its reach across Latin America and Asia-Pacific to build its regional sales capacity and initiate new enterprise engagements.
- Most of Cyera's revenue comes from the BFSI, healthcare, service provider, and technology sectors, but it adopts an industry-agnostic stance because Cyera views data security as a universal challenge across sectors, maturity, and sizes. Because of this, Cyera designed its pricing model on the foundation of universality, allowing it to serve a broad customer base with a scalable and adaptable pricing model.
- Cyera has significantly grown its channel partner ecosystem to include more than 40 resellers, GSIs, MSPs, and MSSPs, and supports these partners by providing industry-relevant training programs that enhance capabilities and alignment. This integrated approach has been instrumental in driving the company's growth momentum in the past 12 months. It has also started to roll out localized support in French and Portuguese to attract customers in countries that speak those languages.

Cyera (continued)

FROST PERSPECTIVE

- Cyera's rapid feature release has helped the company to evolve quickly from its DSPM roots into a more holistic DSP company, regularly enhancing and introducing new features, such as identity-driven data security, GenAI security, remediation, and automation, as well as deepening its integrations with the broad security ecosystem. Further investments to deepen its expertise in these areas would help Cyera cement its position as one of the most innovative vendors in the space.
- The Omni DLP launch is also a reflection of Cyera's rapid innovation cycle. Omni DLP does not force customers into a rip-and-replace situation with their existing DLP tools but rather integrates with them and provides an additional layer of intelligence to produce more accurate alerts because false positives is a long-standing issue in the cybersecurity space. This is a high-risk, high-reward strategy that, if executed well, could redefine how enterprises approach data protection. Cyera needs to sustain focused development and proof-of-value efforts to demonstrate its effectiveness in real-world deployments.
- Cyera has made notable investments to deepen its expertise around data and identity with plans to further enhance its access audit and data lineage capabilities. Incorporating attack path analysis could be a logical consideration because it can help customers visualize how data exposure or identity compromise might propagate through assets and users.
- Cyera's growth trajectory remains undeniable, and this has positioned it well for continued expansion into underrepresented regions, such as Asia-Pacific and Latin America. More regional channel partners can help the company to extend its reach.

Forcepoint

INNOVATION

- Forcepoint is a long-established player in the data security market known for its leadership in the DLP space, and it has also ventured into adjacent markets, such as NGFW, CASB, and SASE. The company recently pivoted toward a more unified vision through its “Data Security Everywhere” mission that aims to secure data through a single policy engine, and in April 2025 doubled down on this mission with the launch of the Data Security Cloud offering that unifies capabilities including DSPM, DDR, DLP, SaaS security, web security, and email security into a single platform. This allows customers to manage the full spectrum of data security lifecycle through a single console, simplifying operations as well as ensuring consistent, context-aware data protection across environments.
- At the core of Forcepoint Data Security Cloud is its AI Mesh, a distributed AI architecture that is trained on domain-specific contexts to deliver a more precise data classification. AI Mesh itself originates from Forcepoint’s acquisition of Getvisibility, helping the company to accelerate its goal of providing end-to-end data security. The Data Security Cloud can also dynamically adapt enforcement policies in real time, helping customers ensure that controls are always aligned to actual business risks while showcasing Forcepoint’s adaptability to ensure fewer false positives as threats become harder to detect and, thus, require more effective and rapid remediation actions.
- Its DLP is also supported by a risk-adaptive protection capability that looks at risky behaviors over time and changes policy enforcement based on real-time scoring of each user. This approach uses Forcepoint’s Indicator of Behavior (IOB) analytics model and enables more accurate enforcement policies. The platform also integrates with SIEM and SOAR tools to help customers in streamlining incident response and aligning data security events with their wider SOC workflows.

Forcepoint (continued)

INNOVATION

- Forcepoint enables its customers to utilize GenAI safely by helping to discover which AI applications are being used by employees and identify data that are being shared with the applications as well as generated data. To prevent inappropriate sharing of sensitive data with these applications, Forcepoint blocks risky services and users while automatically correcting data classification tags.

Forcepoint (continued)

GROWTH

- Forcepoint ranks among the top three vendors in the global DSP space in terms of market share, underscoring its established reputation in data security, particularly in the DLP space. Its growth rate trails the market's growth rate, but this reflects its scale and maturity as a leading data security incumbent in a competitive landscape, particularly as the company saw several directional shifts after being acquired by Francisco Partners in 2021.
- Forcepoint considers BFSI, service providers, and government sectors as its three biggest revenue contributors, which highlights its strength in regulated environments. However, the company's reach extends well beyond these sectors, reflecting a broad market coverage. This reach is supported by its reputation in the data security space through its recognized DLP solution, which creates strong opportunities for Forcepoint to cross-sell and upsell its DSP across sectors, sizes, and regions.
- The company's pricing model follows an enterprise-grade structure with minimum user thresholds and standardized support across modules, ensuring consistent service levels. Its global network of channel partners, which consists of MSSPs, GSIs, and CSPs, enables further market penetration and localized support amid an increasingly competitive data security landscape.
- In February 2025, Forcepoint announced a new channel leader whose focus would be enhancing and growing the company's global channel partner ecosystem. It also hired a new chief financial officer to support Forcepoint's growth momentum as it sets to aggressively push its DSP in the market.

Forcepoint (continued)

FROST PERSPECTIVE

- Francisco Partners' 2021 acquisition of Forcepoint saw the company undergo an extended period of strategic transformation, rearchitecting and repositioning nearly every part of its portfolio. The company has realigned its strategy around a coherent "Data Security Everywhere" messaging and, thus, anchors the architecture of its DSP around a vision that delivers unified visibility and control across all data states, regardless of the data's location. The Data Security Everywhere vision is a step in the right direction, but it will require significant investments on its R&D and product alignment across modules to ensure better cohesion and interoperability across different modules.
- The company has made commendable progress expanding from on-premises to hybrid and cloud deployments. Further investments to ensure that capabilities are delivered equally across different environments will be critical to maintaining consistent policy orchestration. Forcepoint's product roadmap is also aimed in the right direction, with plans to introduce attack path analysis and policy enforcement simulation. Forcepoint can also consider deeper unification of its analytics and telemetry layer to enhance correlation between user, data, and alerts to turn its vision into operational reality as well as deepening oversight of AI model usage to tackle AI-driven workflows.
- Forcepoint's recent leadership appointments indicate its alignment with its Data Security Everywhere vision. To fully capitalize, Forcepoint must further refine its marketing and GTM strategy to better communicate its platform differentiation against newer DSP entrants and legacy competitors. Continued investments in its branding, ecosystem partnerships, and channel readiness can help to translate its vision into measurable customer outcomes.

MIND

INNOVATION

- A finalist at the recent RSAC Innovation Sandbox contest, MIND is a rising vendor in the data security space that takes on the long-standing DLP challenge through a multilayered AI classification engine that combines methods such as EDM, RegEx pattern matching, and OCR with advanced statistical models and LLMs so that sensitive files are categorized more accurately, allowing it to not only understand the business context better but deliver more accurate prevention.
- Its SaaS-based solution is lightweight. can be deployed in the cloud as well as on premises via the deployment of a Docker container for on-premises file servers and storage systems. It can analyze billions of events in real time so that it can build information-rich context to assess risk severity around the sensitive data.
- MIND uses those contexts to enrich its prevention capability and automatically applies relevant remediation policies or automatically blocks suspicious data movements, which accelerates response times. The company also provides the option to collaborate with data owners to remediate issues, allowing customers to keep their team in the loop to serve as the last line of defense against possible misinterpreted actions.
- Since emerging from stealth, MIND has rapidly expanded its capabilities to automate the data security lifecycle. The company has added more data source integrations to cover data at rest, expanded its endpoint agent to discover data at rest on the endpoint, and introduce more data protection methods to secure data at rest.

MIND (continued)

INNOVATION

- MIND's capabilities are extremely compelling, particularly as the DLP market is actively looking to improve prevention accuracy. It also demonstrates meaningful innovation through its multilayered AI classification engine as well as the consolidation of DLP and IRM in a single platform. However, as a new entrant, it is still in the early stages of expanding its coverage and maturity.

MIND (continued)

GROWTH

- Since MIND exited stealth mode in October 2024, it has been growing at an incredibly rapid pace, achieving 500% customer growth, and gained major traction among Fortune 1000 companies. Its meteoric rise helped the company secure \$30 million in Series A funding just seven months after exiting stealth mode, indicating strong investor confidence and early market validation of its DSP.
- Its customer base is predominantly North America-centric from diverse sectors that include telecommunications, BFSI, and healthcare. However, the vendor aims to deliver its DSP to enterprises across different regions in the future, which increases its growth opportunities. MIND's main targets are enterprises of all sizes, with large and medium-sized enterprises contributing significantly to revenue.
- MIND regularly engages with customers to conduct market validations, and insights shared by customers are used to directly shape its roadmap prioritization. This allows it to continuously deploy new capabilities that address the latest customer needs, effectively broadening its market base.

MIND (continued)

FROST PERSPECTIVE

- MIND's approach flips the traditional model by incorporating a multilayered classification engine to build a solid discovery and classification foundation that makes prevention smarter, more intelligent, and adaptive. Expanding this strength into data sources, such as databases and data lakes, represents a natural, though technically challenging, next step for MIND because this would enable MIND to deliver unified visibility across structured and unstructured data—an evolution from its current focus on protecting data after it leaves data lakes and databases.
- MIND's roadmap shows that the company is moving in the right direction toward providing a more holistic DSP, while also deepening its expertise around prevention with the recently expanded coverage of its endpoint agent that allows it to provide full data lineage, native application protection to protect data used in locally installed applications, prevention of data leaks to external devices, and evidence collection for investigations and audits. The company has yet to offer native capabilities, such as encryption, masking, or tokenization, which falls outside of its core focus, but MIND can consider adding integrations with specialized vendors to complement its prevention-driven model. To further enhance its prevention model, it can incorporate attack path analysis to provide more value to its customers.
- As a newer entrant, MIND benefits from a modern architecture unburdened by legacy design constraints and is well positioned to expand its footprint. North America is expected to be the company's focus as it scales its operations, but it is a highly saturated market. EMEA, Latin America, and Asia-Pacific provide more space for growth. However, MIND should first establish a more consistent market messaging on whether it aims to be a modern DLP or holistic DSP because this distinction will shape customer perception.

NSFOCUS

INNOVATION

- NSFOCUS delivers a SaaS-based DSP that can be deployed across on-premises environments and clouds, such as AWS, Tencent Cloud, and Alibaba Cloud, allowing it to help customers of different deployment models address challenges across the data lifecycle within its platform.
- With discovery accuracy exceeding 80% and multiple built-in classification templates, its DSP ensures that sensitive data is correctly identified across structured and unstructured data and reduces the need for manual policy tuning. As a result, NSFOCUS customers face fewer false positives and build a strong foundation for effective remediation because there is less risk of missing high-risk data or wrongly executing policies that do not match with the data's risk profile.
- NSFOCUS also supports more than 100 UEBA detection models, allowing it to detect a wider variety of anomalous behaviors and increasing the customers' chance of detecting unusual activity, and has 8,000 EPS factual detection performance that allows its DSP to process a large volume of events in real time, enabling it to alert customers to potential incidents faster.
- With multiple UEBA detection models and high EPS performance, NSFOCUS can accurately map data transfer paths from human to machine and machine to machine and provides visualization through situational dashboards. This provides customers with visibility into how sensitive data moves and allows appropriate remediation actions to be taken if data is moving suspiciously.
- NSFOCUS's roadmap indicates the company's focus on shifting its DSP to be more proactive, with plans to apply AI/ML capabilities to further filter noise, produce more context-rich analysis, and automate more remediation response.

NSFOCUS (continued)

GROWTH

- As a Chinese company, all NSFOCUS's DSP customers are in China, but the company has a footprint in other parts of Asia-Pacific, EMEA, Latin America, and North America through regional offices because of its broad portfolio. This provides a pathway for NSFOCUS to explore growth opportunities beyond its domestic market.
- It registers enterprises in government, service provider, travel and transportation, BFSI, and education as its customers, with the government sector contributing more than half of the company's revenue in 2025. This is because stringent regulatory and data governance requirements, such as the Personal Information Data Protection Law (PIPL), the Cybersecurity Law (CSL), and the Data Security Law (DSL) across these sectors (particularly the government sector) align well with NSFOCUS's strengths in compliance and security.
- NSFOCUS's pricing model is separated by functional modules, such as classification, categorization, and security analysis, and supports gradual expansion from a single module into multiple other modules, allowing customers to expand when they are ready.

NSFOCUS (continued)

FROST PERSPECTIVE

- While global data security trends often set the pace for innovation, NSFOCUS demonstrates a pragmatic strategy that prioritizes alignment with domestic regulatory priorities while gradually bridging toward global best practices.
- The company's focus on the Chinese market may seem geographically narrow but it is strategically smart as the country's scale continues to drive steady demand for its DSP and its experience in operating under stringent regulatory conditions positions it well to help enterprises in neighboring Asia-Pacific countries, where data regulations are becoming increasingly strict. NSFOCUS can also consider expanding into Latin America, where the market is less saturated but compliance-driven. Its expertise in strict regulatory requirements as well as its competitive pricing model position it well to address cost-sensitive enterprises in the region.
- NSFOCUS prioritizes integrations with on-premises data sources due to customer needs, but its underlying architecture has been designed to cover data lakes and SaaS applications and even allows customers to leverage granular access controls from its DSP for data sources in SaaS applications. Continued investments to enhance these capabilities would further balance its DSP, allowing NSFOCUS to serve enterprises that are operating in hybrid environments or are undergoing rapid digital transformation. Investments in other areas, such as policy simulation, attack path analysis, or capabilities preventing data from being fed into AI training models, would also help its DSP to be more holistic and future-proof.

Proofpoint

INNOVATION

- Proofpoint Data Security is a SaaS-based solution that integrates DSPM, DLP, and ITM in a single platform, tying all three modules together with a unified data classification engine to ensure consistent enforcement of data security policies across different environments.
- Using agentless scanners, it discovers and classifies data across diverse data sources and correlates findings with user roles, locations, and activities such as uploads and downloads to identify where the greatest data exposure sits in a customer environment.
- These aggregated insights allow Proofpoint to provide in-depth visibility into how human and non-human identities access sensitive data across cloud, SaaS, email, and endpoints. To help customers better understand potential attack surfaces, Proofpoint extends this visibility with a built-in attack path graph to visualize how attackers might move laterally to reach sensitive data.
- Its human-centric approach to data security is highlighted with its Human Risk Explorer capability that can identify users that most likely will cause a breach by combining findings from threat telemetry, identities, and behavioral analytics. The capability and comprehensive data access mapping allow Proofpoint to assign risk scores to identities with risky access and enforce policies, such as least privilege, to minimize access to authorized identities only.

Proofpoint (continued)

INNOVATION

- The company provides integrations with notable SIEM, SOAR, EDR/XDR, and CNAPP partners to extend enforcement across the broader environment. It also provides integrations with its native DLP that enables customers to handle prevention directly. For customers that already have Microsoft Purview and Google Workspace DLP, its adaptive controls can still be applied without having to duplicate entire policies again, which streamlines policy management and avoids policies duplication.
- Proofpoint has released support for several GenAI use cases, such as data redaction for GenAI sites, and the ability to differentiate between personal and corporate use of ChatGPT. It has also leveraged GenAI to help security analysts by providing AI-assisted query that can accelerate investigations with AI-assisted prompts.
- Proofpoint has made many enhancements to its DSP in the past 12 months, introducing new features that include but are not limited to DSPM through its acquisition of Normalyze, unified policy engine for data classification, one-click remediation for Office 365 and Google Workspace, Human Risk Explorer, and cross-channel data lineage. The company's roadmap signals its focus in enhancing its capabilities around mitigating threats.

Proofpoint (continued)

GROWTH

- Proofpoint is one of the leading vendors in the DSP market, registering a high market share because the company leverages its extensive customer base and long-standing enterprise relationships from its DLP and email security business, which drives revenue and provides massive growth opportunities.
- Many of Proofpoint's customers are in the BFSI, utilities, healthcare, and technologies sectors. Proofpoint delivers its DSP in its core market of North America as well as EMEA, Latin America, and Asia-Pacific, which contribute a smaller part of the company's revenue. Proofpoint's channel-driven distribution model includes an extensive network of more than 6,000 partners globally.
- Its GTM messaging revolves around a human-centric approach to data security, shifting the conversation from data as an object to the people who handle it. This narrative puts Proofpoint in a unique position because the market mainly talks about protecting "data everywhere" rather than the "people interacting with the data."
- The company's strategy involves selling its DSP to its email security customers. To support this strategic initiative, Proofpoint has adopted a dual-strategy approach: offering attractive migration incentives for customers switching from other email security or DLP vendors, which accelerates platform adoption; and providing DSP capabilities in a single subscription to lower overall pricing friction and accelerate time to value.

Proofpoint (continued)

FROST PERSPECTIVE

- Proofpoint is following an important trend in the broader cybersecurity space, developing a single solution that combines DLP, DSPM, and ITM. Its DSP primarily serves data security and insider risk management teams with a unified UI while privacy and compliance are secondary, reflecting the company's focus on its core strength. Its DSPM is not yet fully integrated into its unified UI, highlighting the modular nature of the platform. Continued investments on converging these three modules under a single interface would enhance workflow cohesion.
- While the company integrates with various data sources that include SaaS applications and cloud storage via its CASB integration, Proofpoint can consider deepening visibility into these non-communication data sources by providing a native convergence with its DSP to help unify visibility and control and improve end-to-end data protection.
- Proofpoint's DSP architecture is cloud-native, which aligns with customer needs, and provides the flexibility to connect to on-premises data sources through integrations as well as a lightweight endpoint agent that monitors a wide range of user activities. The architecture allows extensive visibility without requiring on-premises deployment, but Proofpoint can consider introducing a lightweight on-premises or hybrid control plane that allows customers with strict regulatory requirements to benefit from its DSP.
- It strategically leverages its established email security business to accelerate DSP adoption, providing the company with a head start in a very large customer base. While this strategy accelerates adoption, expanding into non-core customer segments, especially in Asia-Pacific, will be critical to sustaining growth in a competitive market. It can consider adding discovery and classification in its lowest pricing package because this capability is often the entry point for customers.

SecuPi

INNOVATION

- SecuPi delivers its DSP through SaaS and a self-hosted K8s for cloud and on-premises and revolves around a management server that acts as the brain of the platform, enabling consistent enforcement across on-premises, hybrid, data federation, and cross-cloud data operations. SecuPi also provides native integrations with DSAR platforms, governance tools, and discovery and classification tools to enrich policy context and improve event correlation.
- The central management server acts as a coordinator that distributes enforcement instructions to the designated enforcers that are self-contained, and aligns with distributed performant architecture, such as native enforcers, DB driver, ETL agent, API/SDK, transparent gateway, and application agent. The enforcers can be deployed without requiring any changes to be performed on the IT architecture, which resonates with highly regulated sectors, such as BFSI and government, that must balance strict on-premises and data sovereignty requirements with growing perimeter expansion.
- With strong traction in highly regulated sectors, SecuPi has further refined its architecture to go deeper into the data layer, which is a rare move in the DSP space. This has led it to anchor its DSP around four core modules: next-generation DAM for real-time visibility and control; data de-identification that includes Format Preserving Encryption (FPE), dynamic and static data masking, and vault-less tokenization; dynamic authorization that adapt permissions in real time; and privileged account brokering that grants time-bound access without exposing credentials, all delivered through its various enforcers. This enables seamless deployment of multiple capabilities in a single platform regardless of a customer's infrastructure, which allows the company to address broad use cases across regulation, business, and security domains, effectively eliminating rip-and-replace complexity and high TCO.

SecuPi (continued)

INNOVATION

- SecuPi offers multiple protection methods across deterministic, non-deterministic, reversible, and non-reversible approaches that can be selectively applied based on the appropriate scenarios, providing flexibility to customers to choose the methods that suit them best.
- Through its MCP access control for GenAI feature that can be accessed with a prompt interface, SecuPi offers data anonymization and contextual access control for AI agents to help customers ensure that their access control and security are governed and enforced throughout the process. This allows customers to safely experiment with GenAI tools without exposing regulated data and breaking workflows because the original structure is retained and never exposed.
- SecuPi's roadmap signals its commitment to secure the most sensitive control plane and help reduce credential-based attacks by integrating with third-party password vaults to provide passwordless SSO/MFA for all admin tools. SecuPi has also laid out plans to support Apache Iceberg, a high-performance table format to allow customers to leverage Iceberg's scalability and SecuPi's in-depth data protection and controls at the same time. To support secure utilization of GenAI, SecuPi has also released a capability that allows simple prompt to discover sensitive data and automatically enforces appropriate policies when the sensitive data is not protected according to regulatory requirements.

SecuPi (continued)

GROWTH

- In terms of market share, SecuPi is not among the leading vendors in the DSP space. However, its growth rate has consistently been significantly above the market's growth in the past few years, thanks to its position as a niche specialist in structured data while also offering extensive support for semi-structured data. The vendor has established itself globally, with its most significant presence in North America, and has been seeing an increasing revenue income from EMEA, Latin America, and Asia-Pacific.
- The company primarily focuses on Fortune 500 and Global 2000 enterprises in highly regulated industries and counts BFSI and healthcare as its top contributors to DSP revenue. This strategy allows SecuPi to secure multiple new wins every year and align its DSP with stringent compliance and data governance requirements, creating strong differentiation and consistent demand across sectors where regulatory pressure is high.
- SecuPi's pricing model is based on annual subscription and is segmented based on the type of protection capabilities. Customers can purchase a single module, such as privileged access brokering, first and gradually expand once they are ready.
- SecuPi extensively collaborates with GSIs and local service partners for its distribution model and encourages its partners to focus on business outcomes rather than technology capabilities in conversation with potential customers. This approach allow customers to see the value of its DSP in ROI terms rather than strict technical controls.

SecuPi (continued)

FROST PERSPECTIVE

- SecuPi's specialization is a smart differentiator in the market as it makes the company uniquely positioned to serve highly regulated sectors that rely on structured data for their business operations and compliance purposes. SecuPi's technical expertise in delivering real-time data security, privacy, and compliance for structured and semi-structured data allows the company to build solid customer trust and credibility in these sectors, where privacy and compliance requirements are extremely strict.
- This specialization positions SecuPi well to attract customers in Asia-Pacific and Latin America, where DSP growth is driven by highly regulated sectors. The establishment of regional offices and partnerships with local partners in recent years has helped it win deals from notable enterprises. To further extend its reach, the company can consider more aggressive marketing efforts to raise its stature and reach more customers easily.
- SecuPi supports structured and semi-structured data and relies on Microsoft MIP/RMS (Purview) to tag, classify, and protect unstructured data at creation. It also integrates with CyberArk to enforce privileged access control. Deepening its native capabilities for unstructured data would improve its position on the Frost Radar™ Innovation Index.
- SecuPi's roadmap signals continued enhancements around its core specialization, such as support for Apache Iceberg and integration with password vaults, as well as the launch of its MCP server to provide support to automatically enforce appropriate policies once sensitive data is discovered in the AI pipelines. The company can also consider providing attack path analysis and policy enforcement simulation to strengthen its value proposition and multiply the value of its DSP.

Securiti

INNOVATION

- Securiti's flagship DSP, the DataAI Command Center, provides flexible deployment options, such as hybrid SaaS, SaaS-only, and on premises. The hybrid SaaS is customers' preferred option because they can use the platform without sending sensitive data outside of their environment while benefiting from ease of use of the SaaS delivery model.
- To ensure that customers with limited underlying data support can still achieve consistent visibility across their entire data estate, Securiti provides an agent-based deployment option that helps customers access additional data that API-based integrations cannot fully access. Keeping its promise to deliver full visibility, Securiti can discover data at rest and in motion across diverse data sources and leverages AI/ML and NLP to accurately detect sensitive data types with minimal tuning.
- Built on a modular architecture that allows it to address the data lifecycle comprehensively, Securiti's DSP is built around the DataCommand Graph™, a relationship engine that correlates thousands of metadata signals across data estate, identities, locations, entitlements, AI models, regulatory obligations, and more. This DataCommand Graph™ provides end-to-end visibility into all data and data flows, enabling more consistent, context-aware discovery, classification, risk prioritization, and policy enforcement.
- Securiti can detect regulatory violations, anomalous data placements, and unauthorized modifications on configurations such as encryption and audit logs for sensitive data as well as anomalous access activities by users, such as data accessed from unauthorized locations, external sources, or unusual volumes.

Securiti (continued)

INNOVATION

- Customers can enforce automatic response actions through its native, SOAR-like Workflow Orchestrator, effectively closing the loop from discovery to detection to remediation in a single console.
- Its DSP also addresses the high false positive problem common in legacy DLP with the launch of xDLP. With xDLP, the platform applies its AI/ML-powered data classification to intelligently correlate signals across cloud, endpoint, browsers, emails, and firewalls so that only the truly high-priority risks are surfaced.
- Securiti can also help customers discover data that are redundant or obsolete for possible deletion and quarantining, enabling them to minimize their attack surface and optimize resources, effectively turning data hygiene into a strategic advantage.
- Securiti has made mitigation of GenAI risks the logical evolution of its DSP. Customers can automatically detect sanctioned and shadow AI models across their entire enterprise; continuously monitor AI systems and connected data sources for misconfigurations, excessive privileges, and compliance violations; and prevent sensitive data from being used for AI model training and RAG as well as leaking into output responses using context-aware LLM firewalls and automated policy enforcement.
- Securiti's product roadmap indicates that it is focused on helping customers mitigate the increasingly sophisticated GenAI threat landscape, leveraging its DataCommand Graph™ to coordinate data, identity, and AI security enforcement, while its threat research team is working on adding new LLM firewall rules to defend against emerging AI threats. The company is also set to further enhance its classification accuracy by experimenting with agentic AI for classification tuning.

Securiti (continued)

GROWTH

- Thanks to its comprehensive visibility and in-depth capabilities across discovery, classification, policy enforcement, and governance, Securiti is growing rapidly. As a testament to the success of its DSP, it registered high triple-digit yearly growth while its average deal sizes have more than doubled in 2025.
- The company's largest presence remains in North America, but it has seen increasing revenue contributions from EMEA and Asia-Pacific in the past year, indicating its rising reputation as a reliable provider of a comprehensive DSP that addresses not only data security challenges but also security challenges around AI, which is increasingly intertwined with data security.
- Securiti's revenue has diverse sources, with significant contributions from the technologies, BFSI, and retail/eCommerce sectors. It has designed its pricing model to support enterprises across all sizes from Fortune 500 to midsize enterprises, ensuring an accessible entry point while allowing for scaling up without the need for structural changes. Different tiers of its pricing model address different security maturity levels, and its pricing is tied to the volume of data under management, ensuring a balance between costs, usage, and delivered value.
- In its pursuit to accelerate growth across sectors, sizes, and regions, Securiti has revamped its channel partner program, the Unify Partner Program. This includes developing new certifications and implementation playbooks to guide partners in customer engagements as well as launching a free data risk assessment to create quick time to value for potential customers.
- The company recently announced that it has been acquired by a leading backup and recovery company, Veeam. This provides Securiti with massive growth opportunities because it has gained access to a broader customer base, sales force, and customer success teams.

Securiti (continued)

FROST PERSPECTIVE

- Securiti's position as an Innovation Index leader of the DSP Frost Radar™ stems from its long-term bet on a deeper form of unification across security, privacy, and governance and its continuous investment in that vision, which materialized in the form of its DataCommand Graph™ that forms the underlying architecture of its DataAI Command Center Platform.
- The DataCommand Graph™ serves as an intelligence layer that allows Securiti to evolve naturally from its PrivacyOps origins to a unified platform covering data and AI security, governance, and compliance. This design allows subsequent functionalities, such as discovery, classification, data lineage, and remediation, to operate in a shared context, ensuring centralized visibility, controls, and orchestration across the platform for multiple stakeholder teams.
- Securiti's new features, such as xDLP, LLM firewalls, and AI security and governance, as well as its product roadmap, are designed to maximize the DataCommand Graph™, highlighting its ability to build innovative features that leverage its architectural advantage while staying aligned with market trends toward a context-aware, unified DSP.
- The same shared intelligence ensures that remediation is consistent regardless of whether the actions were taken via its native SOAR-like workflow orchestrator or an external security stack, such as SIEM and SOAR. To remain in this leading position, Securiti should focus on keeping the platform operationally manageable without becoming too complex for customers while also deepening its capabilities around real-time protection.

Securiti (continued)

FROST PERSPECTIVE

- Securiti's marketing messages span data and AI governance, privacy, security, and compliance, which may appear inconsistent, but this signals the company's ability to engage customers through multiple entry points, creates diversified revenue opportunities, and helps it close larger deal sizes. To maintain its growth trajectory, Securiti could emphasize its holistic DSP capabilities to shed the perception of being primarily privacy-focused and pursue expansion in less-saturated markets, such as Latin America and Asia-Pacific, to capture new growth opportunities.
- The acquisition announcement by Veeam provides massive growth opportunities and offers Securiti a unique narrative that revolves around unifying data security and resilience in a single solution, which can be valuable as enterprises look to accelerate AI adoption in a secure manner.

Sentra

INNOVATION

- Sentra's cloud-native DSP is lightweight and easy to deploy. While it was first purpose-built for cloud-first customers, those with an on-premises requirement can still utilize its DSP because the company can deploy a local on-premises scanner to ensure that only relevant metadata are passed to Sentra. Sentra leverages its DSPM background to provide a strong governance foundation for its DSP, providing customers with cross-domain visibility into where data is residing, how it flows across environments, and which identities interact with it.
- Once the DSP is deployed, Sentra can automatically discover data across cloud storage, SaaS apps, databases, data lakes, and data warehouses, and leverages its proprietary SLMs to achieve high classification accuracy. This also allows Sentra to continuously learn about each customer's business context, improving accuracy over time as the model becomes tailored to the customer's data environment.
- The core of Sentra's DSP is an independent policy engine that separates policy logic from enforcement and enables policies to be executed through either native integrations or external security stack. This allows consistent governance across environments without locking customers into a specific control layer and avoids a rip-and-replace trap because it allows customers to use Sentra's independent policy engine without replacing existing DLPs, CASBs, or SIEMs.
- To accelerate the detection and remediation process, Sentra assigns risk scores by combining data sensitivity, access permissions, and exposure context. High-priority risks are automatically remediated through actions such as tagging or labeling data, removing excess permissions or exposures, masking sensitive data, and suspending suspicious users.

Sentra (continued)

INNOVATION

- Sentra DSP also features an interactive contextual map view that allows customers to see exactly where data resides and continuously monitors for suspicious data movements. It leverages context around the data's behaviors, such as access and security posture, to determine whether the data was transformed, moved, or duplicated, and delivers remediation guidance so security analysts can take actions faster. Sentra also maps which identities are accessing what data and continuously monitors to spot anomalies around data access, ensuring that actions such as least privilege can be taken to protect data.
- Sentra DSP assists customers in mitigating GenAI risks by extending its classification capability across AI/ML pipelines to prevent unsafe model training; monitoring GenAI sources and outputs in real time to identify leakage; flagging unmanaged models and AI projects that lack proper governance; and helping customers apply access rules based on AI governance standards.
- Sentra's roadmap indicates concrete plans to enhance its DSP across the board, including broader coverage of on-premises data sources; providing monitoring for crucial data protection controls, such as encryption and masking; and further upgrading its remediation capability.

Sentra (continued)

GROWTH

- Despite having a small market share, Sentra continues to register growth rates that are significantly higher than the market's yearly growth rate. This indicates a growing brand recognition in an extremely competitive market.
- Not only it has amassed trust from a broader customer base that now includes multiple Fortune 500 customers, but Sentra has also earned strong investor confidence, in reference to the April 2025 announcement where it closed a \$50 million Series B funding round that brought its total investment to over \$100 million.
- The company mainly delivers its DSP in North America and EMEA but has seen traction in Asia-Pacific, presenting lucrative growth opportunities for Sentra to continue its growth momentum as many enterprises in the region undergo a digital transformation. Main revenue contributors for Sentra are large and medium-sized enterprises across the BFSI, retail/eCommerce, and technology sectors.
- Sentra structures its pricing in tiers based on data volume that needs to be scanned, allowing flexibility across different enterprise sizes, while maintaining all-inclusive fees that cover all necessary features without hidden costs.
- While Sentra is new, it has built a rapidly growing network of channel partners and is a channel-first vendor. In the last 12 months, Sentra has expanded its channel partner program to more than 25 transacting partners and consultants. The company offers self-paced training, hands-on enablement, dedicated field resources, and sales incentives to build strong partner relationships and fuel growth.

Sentra (continued)

FROST PERSPECTIVE

- Sentra has invested heavily in developing a DSP that delivers proprietary SLM-based classification, a unified map view of data assets, and intelligent threat response across multicloud and hybrid environments. Its recent investments in capabilities around mitigating GenAI risks reinforces Sentra's commitment to delivering data protection beyond the perimeter, aligning with the market's evolution toward broader protection and governance against emerging GenAI risks.
- The DSP market needs a player with an open architecture that can orchestrate policies across native and external enforcement mechanisms without imposing a closed platform model. Sentra can fill this gap because its independent policy engine can orchestrate policies directly or through existing security tools. However, realizing this vision will require expanding its native enforcement capability, especially in automatic data masking and anonymization, as well as deepening integrations with external tools, such as Google Labels. Sentra can also consider introducing policy simulation as well as extending its contextual map view to provide attack path analysis to make its DSP more proactive.
- The April 2025 funding provides Sentra with the necessary money to expand its sales and marketing teams to accelerate marketing campaigns and increase visibility of its brand, which is still a bit tied to its excellent discovery and classification capability rather than a holistic DSP.
- Sentra's presence outside of North America is still largely project-driven. To sustain its growth momentum, the company should consider strengthening its channel partner ecosystem in EMEA, Asia-Pacific, and Latin America to build customer engagement and accelerate regional adoption.

Thales

INNOVATION

- Thales delivers a multilayered DSP architecture anchored by CipherTrust DSP (CDSP) for centralized management of data discovery, classification, encryption, key management, and tokenization, and its Data Security Fabric (DSF) for real-time data visibility and risk analytics. While this might appear bolted-on, it creates a full-spectrum approach to data protection across on-premises, hybrid, and cloud environments because CDSP centralizes policy decisions and DSP ensures consistent contextualized enforcement across all data states.
- To secure data at rest, Thales relies on its CDSP layer, which centralizes encryption, masking, and tokenization using a unified key management system. It enforces specialized encryption techniques on any data that enters an enterprise's environment through the network, application, database or file level: Transparent Encryption, which allows data to be encrypted without requiring changes to applications or workflows; Application Protection with an SDK, removing the burden of managing keys from developers; and Database Protection with column-level encryption. This context-appropriate protection allows enterprises to enforce consistent policies depending on data type and locations.
- It offers a centralized management for cloud-native, BYOK and HYOK keys through the CipherTrust Cloud Key Management as well as Secrets Management that automates the process of creating, storing, rotating, and removing secrets. It can also apply several tokenization techniques, such as vaulted tokenization to protect data directly within an application or vaultless tokenization that can create and decrypt tokens without needing a central vault. This is extremely valuable when a data format needs to be maintained while applications are tested.

Thales (continued)

INNOVATION

- Its DSF delivers unified visibility and focuses on securing data in motion. DSF detects and prevents suspicious behavior by combining predetermined rules with rich context that includes access patterns and risk profiles generated from application and database traffic. This contextual approach enables more accurate anomaly detection and more precise blocking to reduce false positives.
- Thales allows customers to respond natively through actions such as system patching, user isolation, and policy updates, or rely on automated workflows to ensure consistent and auditable responses. Thales enables this through broad integrations with ticketing systems, SIEMs, XDR, DLP, CNAPP, and a catalog of over 2,000 pre-built integrations, including cross SOAR orchestration.
- To support GenAI initiatives, Thales can create an inventory of AI models to audit their access patterns and profile LLMs to detect anomalous behavior. Thales provides additional protection for LLMs using RAG with Thales's CipherTrust Transparent Encryption to provide a seamless and robust security framework for LLM use cases.
- Thales's latest product releases, the Data Risk Intelligence and File Activity Monitoring, are a strategic move that strengthens its DSF layer as it significantly enhances its capability in providing visibility, control, and intelligence for sensitive unstructured data as well as data at rest. Its roadmap signals its intention to enhance its end-to-end coverage by improving DevSecOps integration and adding more GenAI security use cases. The company is also set to deepen its data protection techniques by delving into the encryption field to develop quantum-resistant encryption and zero-loss encryption.

Thales (continued)

GROWTH

- Thales is the Growth Index leader on the Frost Radar™ thanks to its unmatched global footprint, diversified customer base, extensive channel ecosystem, and a growth rate that remains largely in line with the overall market's.
- The company delivers its DSP globally to enterprises across the BFSI, manufacturing, and retail/eCommerce sectors. Its long-standing presence in the highly regulated cybersecurity and defense technology space positions it to address complex data security needs across different regions, sizes, and sectors. This is amplified by its acquisition of Imperva, allowing Thales to leverage Imperva's mature customer base in applications and web security to further extend its DSP reach.
- Platform pricing is flexible and scalable. It has been designed this way to allow the company to address diverse data security needs in modern enterprises. Thales also offers a volume-based licensing framework that allows per-unit pricing to decrease as the number of licenses increases, offering cost efficiencies at scale.
- Thales offers its DSP through a fair mix of direct sales and a network of 6,700 technology, service provider, and OEM partners. The direct sales approach allows Thales to leverage its broad portfolio that extends into defense and aerospace to cross-sell or upsell its DSP while the network of channel partners enables the company to reach a broader customer segment across regions, sizes, and sectors.
- Backed by decades of experience across cybersecurity markets, Thales has built 11 SOCs globally and experienced multilingual support teams. This operational depth ensures that its DSP customers can expect fast responses and consistent support across regions—a critical advantage for those that operate in highly regulated environments.

Thales (continued)

FROST PERSPECTIVE

- Following its acquisition of Imperva, Thales has carved out a distinct narrative in the DSP market where it converges two historically separate domains: centralized encryption and key management with real-time visibility and analytics in the same platform. The convergence allows Thales to create an architectural depth where data remains protected at its core through robust encryption, masking, and tokenization techniques even if perimeter or identity-based defenses are compromised. To maintain this position, Thales must continue to ensure that the integration between the CDSP and DSF layer functions cohesively while also simplifying platform complexity to ensure consistent user experience.
- Data protection-based cryptography and coverage of all data types is expected to remain a central piece of Thales CipherTrust DSP in the coming years, with its roadmap indicating continuous investments in deepening encryption techniques.
- The latest feature releases suggest that Thales is strengthening its visibility and analytics as well as initiatives around AI posture and quantum computing so that its DSP is more complete. This commitment reiterates Thales's position as the ideal vendor for customers that prioritize in-depth data protection techniques, and the company can solidify its position by including proactive capabilities. Native data lineage tracking to trace data flow and transformation is set to be available soon.
- Thales benefits from being a trusted partner to BFSI, defense, and government sectors across multiple offerings in its portfolio, creating massive growth opportunities for the company. It also benefits from having direct access to Imperva's broad customer base, allowing more cross-selling opportunities. However, the company needs to be more aggressive in pushing its DSP to its non-core customer segments, especially as the market becomes more competitive.

Zscaler

INNOVATION

- Zscaler's DSP builds on its DLP heritage with the DLP serving as the core engine orchestrating decisions across multiple control points, such as cloud, SaaS applications, endpoints, and personal devices. This ensures consistent enforcement of discovery, classification, and protection across different environments using a single policy framework, effectively streamlining management. Built on its cloud-native Zero Trust Exchange, this means customers can leverage its core DLP strength first and gradually extend coverage to broader data lifecycle framework and, consequently, avoid a rip-and-replace trap.
- Zscaler utilizes an LLM-based classification to analyze data context and usage patterns, which allows the company to identify sensitive data without relying on keyword searches or explicit labeling. As a result, discovery and classification is more accurate while also reducing false negatives as it is less dependent on manually defined keywords and can find sensitive data that might be formatted differently.
- For customers that utilize O365, Zscaler provides integration with Microsoft Labelling to automatically classify and tag sensitive data at rest. These tags can be updated when changes are made and its DLP, meanwhile, can use these tags to enforce the suitable policies and actively prevent data exfiltration.
- Zscaler also provides a workflow automation module that allows DLP administrators to perform forensic analysis, communicate with other employees about best practices, and implement suitable policy actions to resolve incidents through a single console. With this single console, data loss incident triage becomes simpler, reducing costs and accelerating response times.

Zscaler (continued)

INNOVATION

- Customers can monitor their user-level risk exposure through Zscaler's User Risk Report that generates risk score based on anomalous behaviors, DLP violations, interactions with high-risk web categories, and unsanctioned use of applications. This allows them to closely monitor and determine the effectiveness of policy configurations, identify risky users, and configure policies to defend against threats as well as anomalous behaviors from users and devices. Risk scores are also visualized through a graph, which makes information easily understandable even for non-technical people.
- While its DLP is the primary enforcer of its policy actions, Zscaler also provides integrations with SIEM and SOAR to allow customers to align with broader enterprise orchestration workflows, which is extremely helpful for complex, multidomain incidents.
- Zscaler offers robust controls to mitigate GenAI risks across public AI services, private AI instances, Microsoft CoPilot, and enterprise chatbots. It provides full visibility into AI services, agents, models, and shadow AI usage, with its inline proxy able to block unauthorized AI services and monitor user prompts to block sensitive data from being sent to a prompt. Because of this, customers can ensure safer AI initiatives in their enterprises.
- Zscaler has introduced several updates, such as the advanced classification technology to reduce false positives, in the last 12 months to strengthen the value proposition of its DSP. Its product roadmap signals its focus to improve their capability around monitoring and securing data at rest, adding more GenAI-specific controls and enhancing its reporting capabilities and dashboards.

Zscaler (continued)

GROWTH

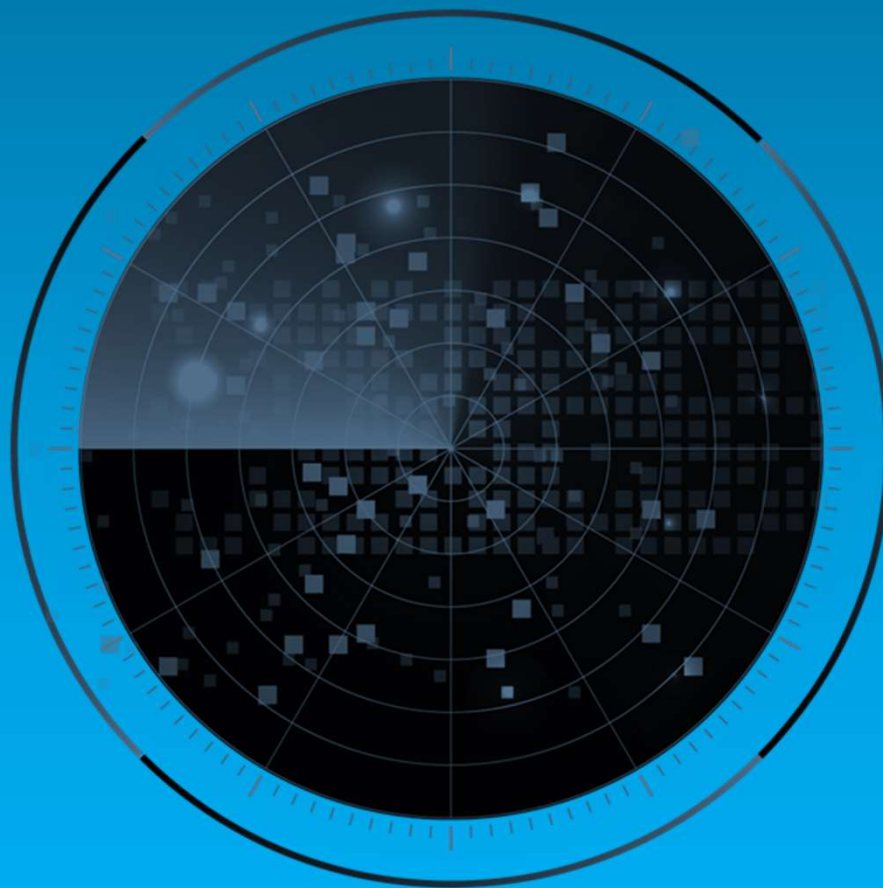
- Zscaler is one of the Growth Index leaders on the Frost Radar™, thanks to its increasing market share and exponential growth rate year after year. The company centers its growth strategy by extending its DLP foundation into a platform-like architecture and including capabilities such as DSPM and access governance, positioning itself as a protection-first DSP.
- Its zero trust, cloud-native architecture known as the Zero Trust Exchange connects users, applications, and data through the same policy layer. This made it easier for Zscaler to cross-sell or upsell its DSP to its broad customer base for other product segments, such as SASE and CASB.
- The company's well-established footprint has helped it push its DSP globally, with North America holding the most revenue in 2025, followed by EMEA. It targets enterprises around the world, skewing slightly toward larger enterprises.
- Its pricing model is designed to scale up or down based on a customer's size and data footprint and focus more on how customers adopt and operationalize data security services over time. This provides customers with the flexibility to choose a pricing package that fits their budgets and addresses their most urgent needs.
- Zscaler provides comprehensive training and incentives to its channel partners, which account for most of its data security deals. The robust channel partner program has motivated many partners to strengthen customer relationships, which has resulted in Zscaler achieving an NPS score that is double the average for SaaS companies. Because of the high satisfaction rate, there is a strong sense of brand loyalty, with many CISOs choosing Zscaler repeatedly.

Zscaler (continued)

FROST PERSPECTIVE

- Zscaler's approach of leveraging DLP as the core engine while extending into the broader DSP makes sense given its cloud-native Zero Trust Exchange architecture that enforces least-privilege by default and allows seamless integration of advanced modules. The modular approach allows Zscaler to leverage its mature DLP strengths without falling into the common rip-and-replace trap that many vendors face when modernizing architectures.
- Zscaler plans to strengthen its platform by improving monitoring and protection of data at rest, adding more GenAI-specific controls, as well as enhancing reporting and dashboards for holistic coverage across all data states. The next phase of innovation for Zscaler to strengthen its value as a holistic DSP can include deepening its intelligence layer to improve policy precision and reduce alert noise; providing deeper attack-path analysis to help security teams to understand potential routes of data exposure; and supporting policy enforcement simulation and data lineage to trace the flow and transformation of data across different environments.
- Zscaler's data security business significantly benefited from its strong foothold in SSE and SASE, where it can position its DSP as a natural extension of those offerings, allowing for massive growth opportunities and accelerated customer adoption through cross-selling or upselling. While this is commercially effective, it has led to its DSP being slightly overshadowed by its reputation as a leading access and network provider. The company can consider strengthening its brand identity in data security through clearer messaging and ecosystem visibility to capture stand-alone demand for DSP.

Best Practices & Growth Opportunities



Best Practices

1

Having a centralized policy and intelligence engine is a force multiplier for a DSP. It can ensure coherence and consistency for every data security decision because the engine would continuously aggregate insights across data, identities, and behaviors, which then ensures that enforcement decisions are not made in isolation but are context-aware and aligned with broader business logic. Vendors should invest in deepening the intelligence layer to minimize policy fragmentation in different environments.

2

Vendors should continuously map capabilities across the data lifecycle to identify gaps and prioritize investments in those gaps to enhance the DSP and make the platform more holistic. For example, vendors that identify classification as a weakness should leverage LLMs or other advanced classification methods to improve accuracy; vendors that identify remediation as a gap can consider deepening native capability or expanding third-party integrations.

3

Flexible deployment options ensure that a DSP can operate in any environment or regulatory constraint without enterprises having to compromise architecturally. Successful vendors in this space provide on-premises, hybrid, and cloud deployment options, signaling the ability to address diverse needs in different sectors, sizes, and maturity levels.

Growth Opportunities

1

SMBs as well as the Asia-Pacific and Latin American regions have been underserved, but the development of increasingly stringent data regulations and digital transformation initiatives will accelerate the demand for DSPs because data is increasingly distributed in various systems. Those data need to be discovered and classified correctly to ensure compliance with the latest regulatory obligations to avoid blind gaps as well as regulatory penalties.

2

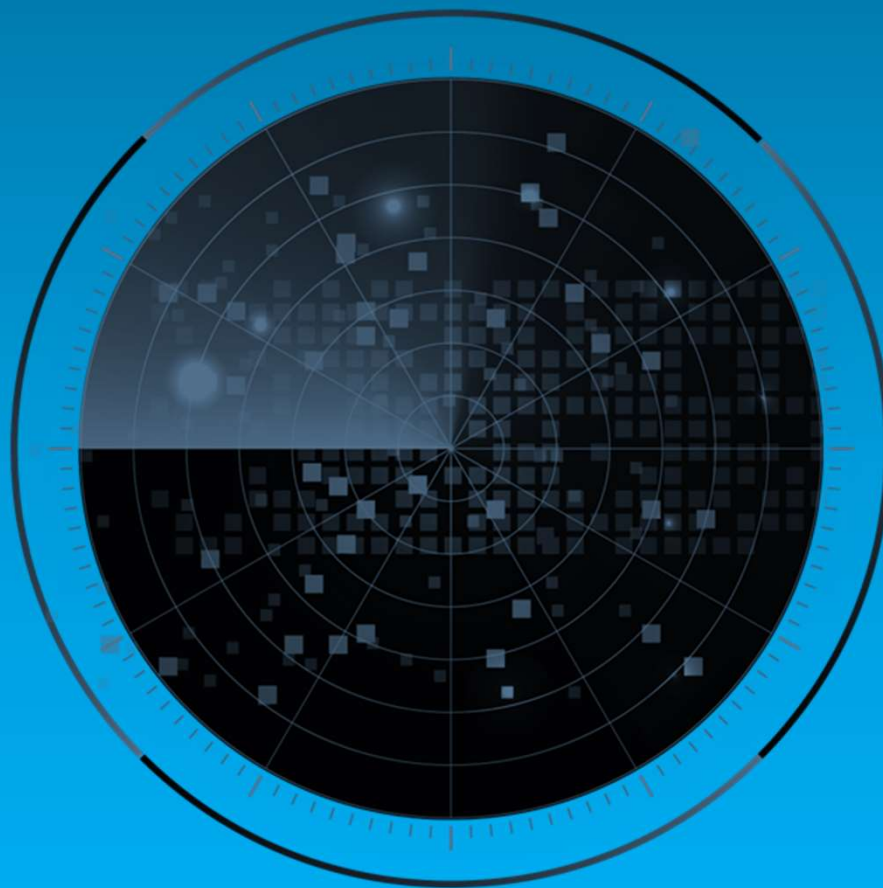
A DSP's data lineage capabilities mean that it can provide visibility into how data, identities, and access are interacting with one another. DSP vendors should consider extending its data lineage to not only show how data flows and transforms but analyze possible attack paths to simulate how an attacker might travel in a customer's environment to reach sensitive data. DSP vendors would greatly benefit from this addition because it transforms a DSP into a more proactive solution.

3

Many enterprises start with capabilities that address their most urgent use case before gradually expanding to include more capabilities. DSP vendors would benefit from ensuring that their platforms seamlessly plug into existing SIEM, SOAR, ITSM, and data pipeline systems and that incremental, modular expansion does not disrupt ongoing operations. This approach would align vendors with many enterprise realities, where architectural overhauls are viewed as impractical and risky.

F R O S T  S U L L I V A N

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.

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.

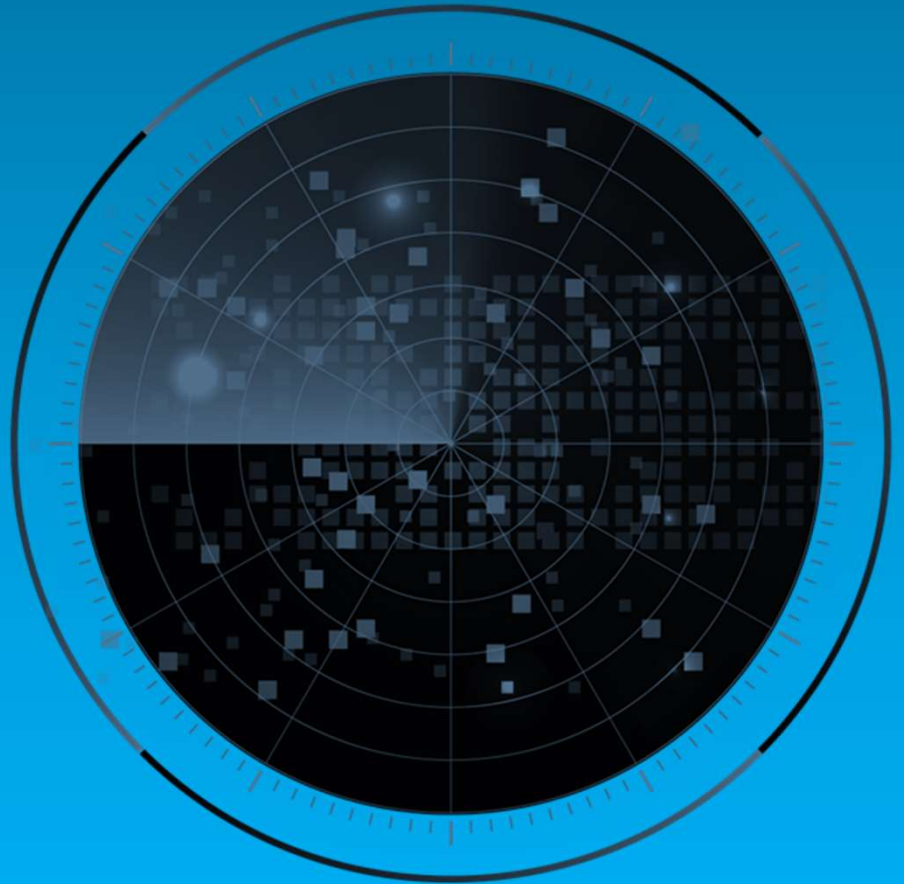
II4**MEGA TRENDS LEVERAGE**

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.

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



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.

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**

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**

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**

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.

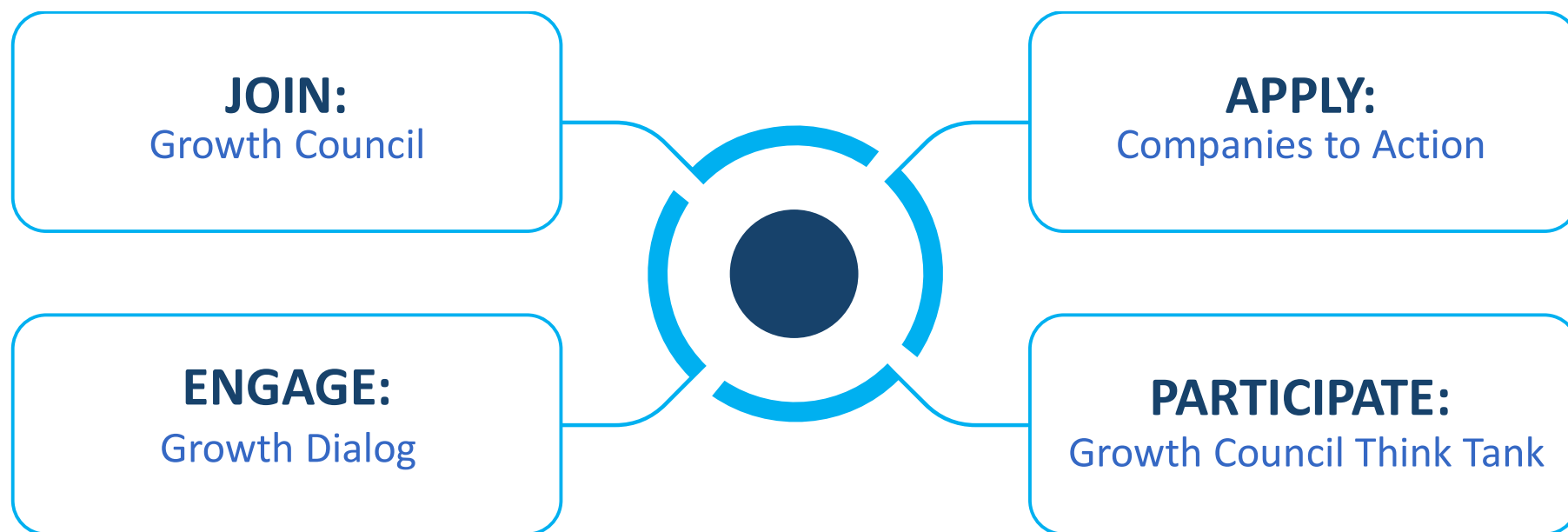
LEVERAGING THE FROST RADAR™

- 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™**

Next Steps



Does your current system support rapid adaptation to emerging opportunities?

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, write to: permission@frost.com

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