OMDIA UNIVERSE

Publication date:
09 Sep 2025

Author(s):
Adam Strange, Principal Analyst, Data Security

Omdia Universe: Data Security Posture Management (DSPM), 2025

Omdia
by informa techtarget

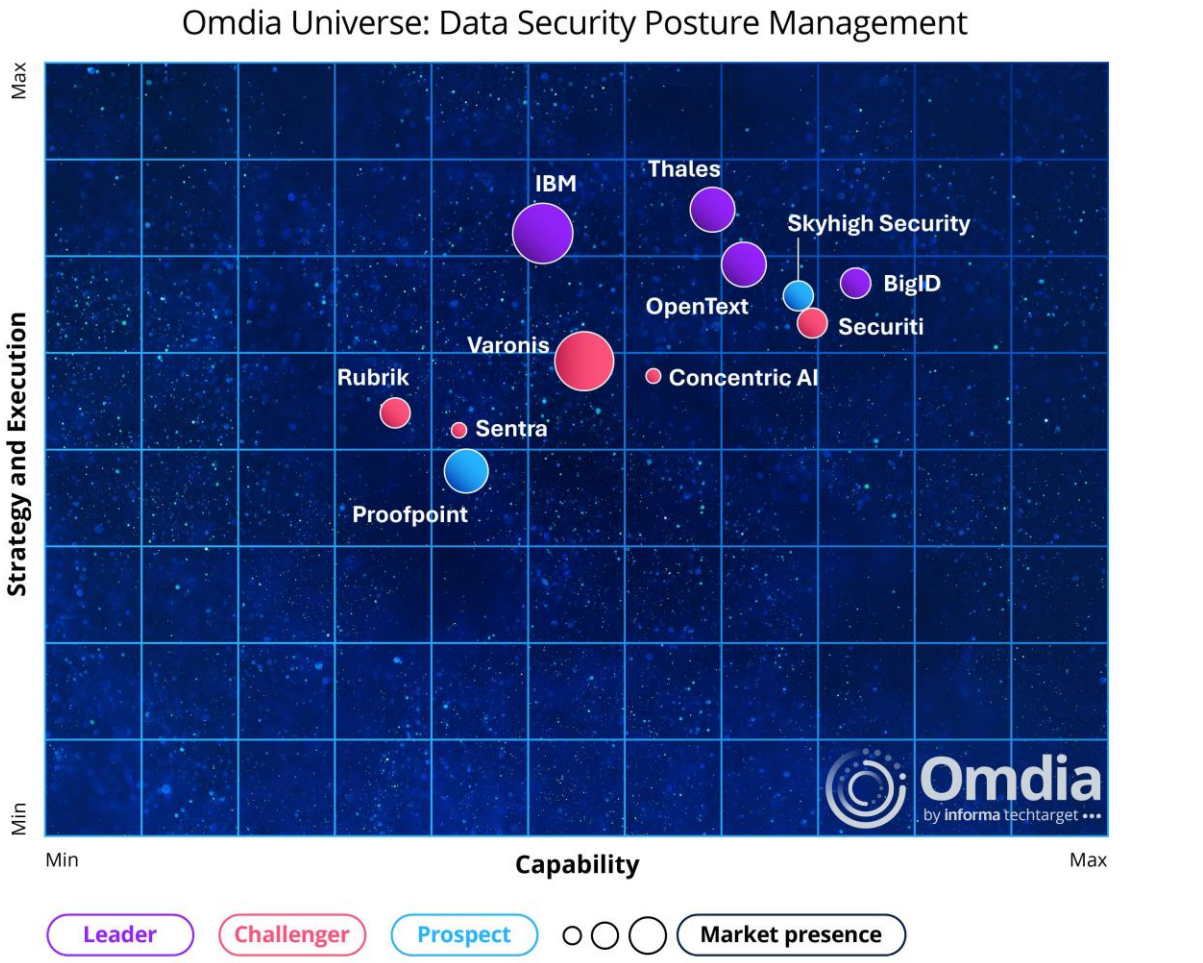
Summary

Catalyst

Data security posture management (DSPM) arguably emerged into mainstream cybersecurity thinking after the RSA Conference in 2023. It represented a step change in the mindset most organizations were taking around data security, advocating a more holistic approach toward not only understanding and protecting data, but also ensuring the measures put in place (the posture) on day 1 were just as robust and resilient on day 100 and beyond. Since then, DSPM has matured and evolved as smaller pioneers were acquired by larger, more established vendors keen to add holistic data security to their existing portfolios.

This report offers a unique assessment of the DSPM market, collating vendor data into graphical representations of each brand, its technology and capability, strategy, execution, and market momentum. Omdia trusts this report will enable participating vendors to assess strengths and address gaps in strategy and deliverables.

Figure 1: The Omdia Universe for DSPM



Source: Omdia

Omdia view

Over the last three years, Omdia has observed the continued evolution and maturity of the data security landscape, driven by four main factors:

- The threat landscape is ever-advancing and evolving, with the ability to penetrate defenses at a concerning rate.
- Operational data privacy regulations have been enacted worldwide, with regulators now willing and able to take the required steps to enforce them.
- Organizations have an underlying need to protect themselves better against data loss as a whole, ensuring their business-critical assets (their data) can facilitate growth from a secure location.
- Automated intelligence, which includes artificial intelligence (AI), particularly generative AI (GenAI) and agentic AI, accesses vast amounts of unknown or unsanctioned data, exposing organizations to significant risk. On the other hand, used wisely, AI has considerable potential to reduce data security workloads substantially and enhance data protection.

Data security has shifted from being a bit-part player among a broader cybersecurity discussion to become a standalone discipline, assuming its logical place as the foundation of a wider, multi-tier cybersecurity posture. If organizations can map out and understand their data landscape, they can apply suitable measures to defend it, and as such, attempt to reduce the risk of significant sanctions or penalties from regulators. From there, the necessary wider, multi-layer defensive protocols can be built out from much firmer foundations.

With such a critical role in the broader cybersecurity landscape, there was a need to adopt a more holistic approach to protecting data. The response from a number of small data-centric pioneers in early 2Q23 was DSPM.

Since the first half of 2023, Omdia has seen significant activity in the DSPM market. Omdia research indicates an overwhelming 80% of IT decision makers are either using, adopting, or planning a DSPM implementation (up from the still substantial 73% of respondents to the same survey in 2024). Further, the continued acquisition of the pioneer DSPM vendors by the likes of IBM, Thales, Palo Alto Networks, Proofpoint, and others shows industry recognition of the importance of DSPM's holistic approach and the value in having the capability added to existing data and cybersecurity portfolios.

Similar to the growth of data security as a whole, there are substantial factors dictating the growth behind DSPM as it grows in substance, awareness, and credibility.

- In the face of an ever-growing threat landscape, DSPM is the logical (and necessary) evolution of data security. Because data is intrinsically linked to every aspect of business operations, it makes sense to adopt both the more stringent protection measures DSPM advocates and the holistic approach it delivers.
- Data privacy legislation, which mandates better protection around data storage and usage, is increasingly enacted and enforced worldwide. Additionally, there are real and heavy financial and custodial penalties for unauthorized data exfiltration or loss.
- Cloud adoption is continuing to gather pace, with all the new remote data stores requiring visibility, controls, and governance to maintain security standards. Compliance needs to

extend across data irrespective of its location, and DSPM offers a robust way to manage data assets wherever they are located.

Analyzing the DSPM universe

Not surprisingly, as DSPM has evolved as a deliverable, so has the definition of what does and what does not represent a DSPM platform, as well as where DSPM stops and a wider data security platform begins.

Some vendors are already assimilating DSPM functionality into wider portfolios and employing data security platform terminology rather than the DSPM acronym, while others will offer core capabilities in the data discovery and data classification space, combined with other services under a DSPM umbrella.

Although DSPM is arguably already morphing into the next stage of its evolution, for the purposes of this report, Omdia defines DSPM into two capability areas: data security and posture management.

Data security (core capabilities)

- Data discovery: The ability to find all data irrespective of type and location, across all on-premises or cloud locations, SaaS applications, storage devices, operating systems, or operational status (in use or shadow data)
- Data classification: Capability to understand the relative sensitivity of a document and be able to apply visual and metadata labelling for controlled usage
- Encryption: Once data has been found and classified, it can be applied to data at or exceeding a prescribed base level of sensitivity
- Tokenization: Where full encryption is not required, or as an alternative to encryption and key management, sensitive data can be replaced with non-sensitive tokens
- Data masking: A further obfuscation measure that involves replacing data with fictitious, though realistic, equivalent values
- Identity management: Privilege provisioning and removal, together with access management of human and non-human identities to predominantly controlled or sensitive data

Posture management (advanced capabilities)

- Security posture evaluation: Consideration and evaluation of a variety of factors that influence the effectiveness of a security posture, currently and into the future
- Monitoring and analysis: The process of continual observation to identify potential weaknesses in data security defenses
- Risk assessment: The process of threat identification, the assessment of associated risk to resident data, and suggestions for remediation efforts
- Security control assessment: The evaluation of security controls to establish whether they have been effectively implemented and are operating as planned

- Compliance monitoring: Monitors against defined data privacy legislation, such as the General Data Protection Regulation (GDPR), to ensure operational standards conform to prescribed standards
- Incident response planning: The adoption of documented response plans, processes, and remediation actions in the event of a cybersecurity incident or authorized breach
- Continuous monitoring: The process of continuous monitoring of data security defenses to ensure they are offering the required levels of security currently and into the future

Strategy and market execution

Omdia assesses vendor solutions across additional criteria as follows:

- Vendor execution assesses the vendor's broader impact on relationships with partners and the ecosystem, the go-to-market strategy, options for deploying the solution, licensing flexibility, depth of customer support, and evidence of return on investment (ROI).
- Strategy and innovation assess evidence of innovation in the solution, competitor differentiation, a focus on industry verticals, support for the industries, and more.
- Market momentum assesses the relevance of the vendor's portfolio to data security issues, and how well the solutions are integrated. It also assesses market penetration and market reach.

Market dynamics

The DSPM market continues to evolve at a robust pace as organizations devote more time, budget, and effort toward protecting data.

It is debatable which of the threat landscape drivers, along with the introduction of AI agents and machine learning (ML), are most impactful, but Omdia notes the overwhelming and critical need to do more to protect data, in the context of malicious actors appearing to attack with impunity. Indeed, as AI technology falls into the hands of these actors, the effectiveness of attacks will likely increase.

Recent breaches in UK retail alone indicate there are still vulnerabilities in cyber or data security strategies, and this is, in turn, an opportunity for vendors. End-user organizations need the expertise and advice that accompanies the development of security tools, and those who step in to impart this knowledge are in a strong position. Customer-centricity is key, and vendors need to realize they are equally exposed if their customers experience breaches. While at this point they will not be fined, revenue streams will inevitably suffer.

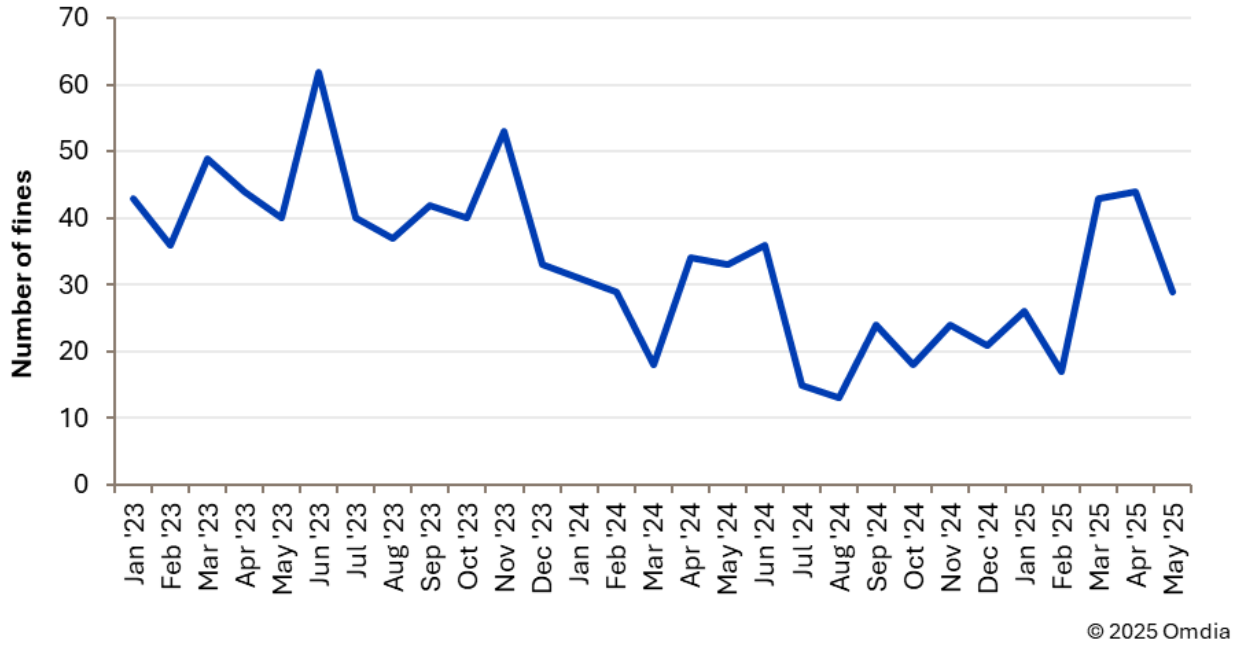
The importance of protecting data cannot be ignored or neglected: there is no sign of the threat landscape reducing. Organizations of all sizes need to maintain maximum levels of vigilance to stop future attacks and data exfiltration. DSPM can help by offering a holistic view, but perpetrators are often skilled and determined. Insider threats should also be actively considered, with rigorous enforcement of least privilege access applied to restrict users to appropriate data only. Even then, measures to block unauthorized access or anomalous behavior must be fully employed.

Regulatory compliance—the second key driver for the DSPM market—has forced organizations to consider data security much more specifically. DPSM provides tools such as data discovery, data classification, encryption, and access controls to ensure that the standards of protection around data

defined by regulators are adhered to. Ultimately, the standards defined by GDPR, the California Privacy Rights Act (CPRA), and a host of others worldwide are a positive step to help protect and secure data and should be embraced across organizations of all sizes and industries.

Those who do not protect their data accordingly run a substantial risk of heavy fines. According to the GDPR enforcement website, tracked by CMS Law, the number of penalties under GDPR alone totals 2,435 and amounts to over €6.2 billion ($7.3 billion) as of June 2025. Recent heavy fines levied at social media companies predominantly by Ireland's Data Protection Commission have disproportionately increased the total fines. However, the fines per month are still on average well into double digits, as shown in **Figure 1**.

Figure 2: GDPR fines by month



Source: GDPR Enforcement Tracker Report 2025, CMS.Law; Omdia

Widespread adoption of cloud services is another prime driver for DSPM. There is nothing fundamentally wrong with adopting a cloud-based infrastructure; indeed, from a data discovery point of view alone, tracking down all the organizational data in a cloud-based environment is many times simpler than doing so on-premises. The challenge expands when organizations adopt hybrid and multicloud environments, mixing cloud services with on-premises infrastructure. Inevitably, this increases complexity, creating new data security challenges.

DSPM functionality offers visibility and control across these diverse environments, enabling organizations to manage data sprawl, identify data exposure risks, and enforce consistent security policies.

Interest grows from the larger players

With any new technology that has experienced profound development, larger vendors will begin to show interest initially and then become actively involved if they feel there is opportunity. This has certainly been the case within DSPM.

This interest may be appealing to small vendors looking to partner to extend market reach; however, it also brings acquisition into frame. Acquisition might be a positive outcome for DSPM investors looking to maximize return from a sale to a larger vendor, but for vendors looking to build out their businesses organically, the prospect of being acquired looms large in the DSPM space.

Since 2023, IBM, Thales, Rubrik, CrowdStrike, Proofpoint, Palo Alto Networks, and Tenable have all acquired DSPM pioneer organizations, significantly shifting the needle away from smaller startup vendors to a market that larger players are now beginning to dominate. As shown in **Figure 3**, in this analysis, three of the four vendors achieving Leader recognition are large dominant providers. Although size does not necessarily guarantee leadership, DSPM has attracted big players with substantial budgets and powerful brand momentum.

There are still numerous candidates for acquisition in the DSPM space, and inevitably, more of the pioneers will be integrated into wider, larger, existing portfolios. Although DSPM continues to develop in profile and capability, most vendor solutions in the market still have gaps. For instance, there is still a need to add reactive remediation technology that is ready to respond if—or, more probably, when—an attack does happen. So, marrying the classic functionality of a DSPM proposition with an extended and/or complementary capability from an established provider is a clear commercial opportunity.

Figure 3: Vendor rankings in the DSPM universe

Vendor	Product(s) evaluated
Leaders	
BigID	BigID Next for DSPM
IBM	Guardium Data Security Center
OpenText	OpenText Data Security Platform
Thales	Thales CipherTrust Data Security Platform for DSPM
Challengers	
ConcentricAI	Semantic Intelligence
Rubrik	Rubrik DSPM
Securiti	Securiti Data+AI Command Center
Sentra	Sentra Data Security Platform
Varonis	Unified Data Security Platform
Prospects	
Proofpoint	Proofpoint Data Security Posture Management
Skyhigh Security	Skyhigh DSPM

Source: Omdia

Market leaders

There are four Leaders in Omdia's assessment of the DSPM market: BigID, IBM, OpenText, and Thales.

BigID delivers the broadest portfolio of capabilities overall, and Omdia has rated it as Best in class for market momentum. The vendor has grown from among the DSPM pioneers to become a significant player and can compete very effectively with other larger vendors.

IBM was the first major brand to acquire DSPM capabilities when it purchased Polar Security in May of 2023. Fully integrated into IBM's Guardium suite and now in its second iteration, Guardium offers a very strong platform, augmented by IBM's wide and comprehensive cybersecurity portfolio.

OpenText attained Best in class scores for strategy and solution breadth, indicating a comprehensive, well-constructed set of technologies for a compelling proposition overall. After a degree of restructuring, the vendor now offers a well-integrated cybersecurity cloud platform.

Thales achieved Best in class ratings in core technology, market momentum, and vendor execution for an excellent overall result. Having bought Imperva in 2024, Thales integrates its DSPM capabilities into its CipherTrust data security platform, bringing data discovery, classification, data protection, and centralized management for keys and secrets into a single platform. Able to further leverage its existing identity and access management and hardware security module (HSMs) capabilities, Thales has grown strongly over recent years and now offers an industry-leading data security platform.

Market challengers

The Challengers category in this report includes five vendors: Concentric AI, Rubrik, Securiti, Sentra, and Varonis.

Concentric AI, Securiti, and Sentra all originate from the original pioneering DSPM stable, and although they are not the largest of providers, all are achieving a good pace of growth in a competitive market.

Concentric AI, for a smaller organization, delivers a comprehensive set of advanced posture management tools and services, for a Top-tier solution breadth ranking overall. It has the flexibility and responsiveness to meet customer needs quickly and efficiently, and its momentum score provides a good barometer for this. Coupled with a strong focus on innovation and patent registration, Concentric AI has a competitive proposition that has enabled the vendor to achieve wins against bigger competition to build a growing reputation in the DSPM market.

Securiti rated very commendably in this analysis, with an expansive DSPM proposition and a Best in class ranking for its advanced capabilities. Across the other categories, it achieves some highly commendable results, given its smaller relative size against some of its competition, and Omdia expects the vendor will climb into the Leader category for future reports.

Rubrik's DSPM largely stems from its acquisition of Laminar, which it has successfully integrated with its pre-existing backup and recovery portfolio. This enables the vendor to offer the proactivity of DSPM and the reactivity of remediation in the event of a breach. Rubrik rated very well for its advanced capabilities and achieved strong scores for strategy and innovation and market momentum. Some additions to its core technology portfolio would further increase its overall ratings.

Sentra is another perhaps less well-known brand—although it is making moves to change that. Its size presents limitations in the overall breadth and scope of its solution, but the vendor compensates by adhering to a well-defined strategy with good innovation. Its scores across all categories indicate a well-balanced and efficient organization. Following over 300% year-on-year growth and rapid Fortune 500 adoption, Sentra has surpassed $100 million in total funding, illustrating how well positioned it is to meet growing end-user demand for its data security solutions.

Varonis is an experienced vendor in the data security space and has crafted its DSPM proposition from a data-centric point of view, with care and attention to map precisely against customer needs. In Omdia's assessment, it achieved Top-tier status for strategy and innovation and scored well for its advanced features and solution breadth.

Market prospects

Within the market prospects category are Proofpoint and Skyhigh Security.

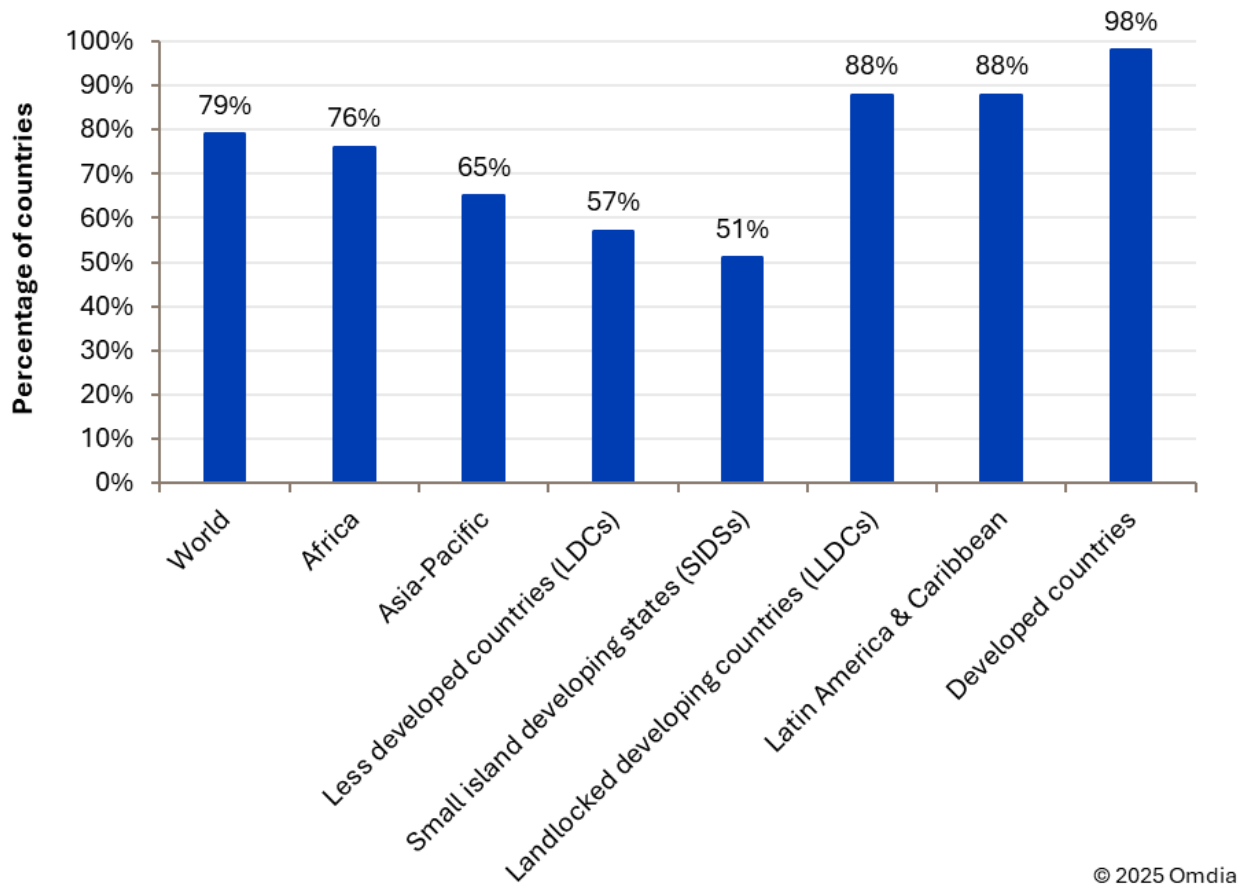
Proofpoint is the latest vendor to enter the DSPM market through its acquisition of Normalyze in October 2024. This acquisition was shrewd and carried through some brand equity from industry commentators. It is a good first step and positions the organization well for the next phase of development. The vendor has some areas to address across its overall portfolio, but it registered a Top-tier status for advanced capabilities with some good overall ratings in other categories.

Skyhigh Security recently increased its profile as a DSPM vendor. The organization scored well across the assessed areas and achieved Best in class for its advanced capabilities and three Top-tier ratings elsewhere. Omdia expects the vendor to become highly competitive if its current trajectory and momentum are maintained. For current purposes, although its portfolio looks admirable, its size and longevity result in a Prospect status—nevertheless, it is an organization to watch closely moving forward.

Opportunities

Large-scale opportunity exists for vendors within the DSPM market. The current threat landscape will likely become more intense as the weaponization of AI becomes more widespread. Even without the use of AI, attackers remain committed, diligent, and plentiful. It is therefore safe to say all organizations need to do more to protect their data, and DSPM represents a logical and effective way forward. For organizations that do not invest in data security, the regulatory and compliance landscape is only headed in one direction, and those who insist on plowing a furrow independent of the regulations will, at some point, be held to account. The majority of countries have now enacted or have data privacy legislation in the draft stage. **Figure 4** shows adoption on a global basis.

Figure 4: Percentage of countries with legislation in privacy and data protection



Source: UNCTAD, Omdia

Enforcement will inevitably vary, but in general, the trend is to penalize heavily for noncompliance. Chief among these is unauthorized data exfiltration, but some of the most hefty fines, under GDPR at least, have been for misappropriation of stored data. Security is crucial when it comes to data, but usage and process are also important considerations. Some countries have yet to deliver substantial fines for noncompliance, but the trend is increasing in significance for CISOs and will become the norm. Better ways for data to be protected are, therefore, critical considerations within the wider cybersecurity equation and, as such, now represent a substantial opportunity for vendors offering DSPM solutions.

In addition to the regulatory mandate, it is simply good business practice to increase defenses around data. However, the significant challenge becomes how to find it all at the outset. Because it is impossible to adequately protect what you do not know you have, DSPM offers CISOs an important way forward in identifying the broader extent of the data landscape, and the more automated the toolset, the better. Here, AI can step in to provide valuable assistance in tracking down large volumes of data, known and unknown. Once found, data (business-critical or otherwise) should be controlled and protected in direct relation to the risk it presents to the business, were it to be lost or stolen. Again, there is a significant opportunity for DSPM vendors that can articulate the more effective stance DSPM offers to finding, understanding, and protecting the data.

Thinking broadly, DSPM can deliver a number of key components to fundamentally improve the way data can be protected, and its future would therefore seem buoyant, if not assured. There is undeniably an ongoing opportunity, with CISOs and IT security professionals either looking to or being mandated toward reinforcing security around their data; DSPM would seem a lucrative path to follow for vendors able to provide these enhancements.

Omdia's research shows that a large proportion of IT decision makers anticipate increases in their data security budgets for 2026, so finances are not expected to be a limitation next year. End users are clearly showing an appetite for further security around their data, and this represents an opportunity for vendors willing to position themselves as both partners sharing and taking on customer challenges and providers of vital value-added services.

Threats

The DSPM market faces several threats, including many shared with the wider data security and IT universes. DSPM is equally susceptible to insider threats, the evolving threat landscape, and the general unavailability of well-trained resources, for example, as other areas of cybersecurity. A lack of resources has been a problem for several years and is only now being addressed, not through an influx of trained people but with the increase in automation and AI. DSPM must also be adaptable and flexible enough to keep pace with new and sophisticated advances emerging from cybercriminals. Maintaining a robust posture is fundamental, but DSPM focuses on ensuring defenses hold now and into the future.

DSPM, being broadly a platform of integrated tools and services, can be as complex as it is comprehensive. Poor adoption due to a lack of buy-in (and as such, incomplete coverage) is a concern, and Omdia's research shows that while the direction of travel is overwhelmingly toward adoption, a significant number (20%) have ruled out the umbrella approach. Lack of comprehensive buy-in from users can hinder the adoption of new processes, increasing the risk of data breaches and compliance failures. DSPM initiatives can therefore fail if they do not involve all relevant stakeholders, leading to missed vulnerabilities and overrestrictive controls. If a DSPM solution does not integrate with all relevant systems, for example, or does not account for all data types, it may leave gaps in security coverage.

Due to the expansiveness of DSPM, managing data security across diverse cloud and on-premises environments (public, private, and hybrid) is a significant obstacle, and ensuring a DSPM infrastructure is tightly and scalably integrated with legacy security infrastructure is also a critical challenge. Many organizations struggle to find solutions that seamlessly integrate across environments and offer continuous scalability.

Data discovery (the tracking down of all resident data irrespective of location and age) remains a decidedly awkward problem to resolve. Most data discovery tools will find data where they are told where to look, but few, if any, go out and hunt down absolutely every piece of data in every location, known and unknown. Accurate data discovery is crucial for the success of DSPM. Currently, most tools just about do enough. Moving forward, the utilization of AI in this domain is critical as data volumes continue to expand.

Operating hand in hand with discovery is classification. Without finding data, it is impossible to understand it or classify (label) it to then control its use. Many early technologies offered simple solutions (typically four labels: restricted, sensitive, confidential, public, or words to that effect) to what is actually a many-layered challenge. Classification has to be accurate (avoiding false positives), meaningful, and enforceable.

AI introduces new complexities to IT and the DSPM infrastructure specifically. The use of AI by adversaries will intensify, and a DSPM infrastructure needs to keep up, but there is also the potential for ill-thought-out deployment of AI to lead to toxic combinations of misconfigurations or specifically targeted attacks on the AI infrastructure. These combinations can amplify risks and require a clear and focused approach to identifying them and then deploying suitable remediation measures. It will vary by region, but security leaders are concerned that AI will exacerbate these issues, making it more difficult to prioritize remediation efforts. Omdia's research still shows a significant number of IT decision makers (45%) harbor reservations about data security in the context of AI deployments.

Looking more inwardly, a threat to smaller DSPM vendors undeniably comes from larger vendors, as is typically the case throughout IT in general. The volume of acquisitions already seen in the DSPM market clearly shows that the established players have noticed and want to act upon the opportunity.

While acquisition is not a threat to the broad DSPM market, it does effect change. Currently, the pattern is one vendor buying another, so Omdia is not seeing consolidation into a single or reduced number of stables. Acquisition is nevertheless a risk if a smaller vendor has decided to stand alone and both strives for and delivers successful, autonomous business growth as the prescribed direction of travel.

Market outlook

Currently, the future looks bright for DSPM. Its arrival has been timely, and it has certainly gained much traction since it emerged into an already crowded market of xSPMs and acronyms. Some organizations were already championing a more holistic approach to data security, and momentum was already growing. The advent of the specific DSPM terminology, however, enabled vendors to define this vision more clearly, enabling CISOs to better understand the specifics of the subject area. Now, with numerous vendor offerings in the market and the marketing budgets from the larger players behind it, DSPM has both critical mass and momentum.

Regulators, malicious actors, and the basic need for better business hygiene around data security mean there is and will remain a growing need to better understand and protect data, and this is where DSPM can provide a trump card. Its mandate is to provide a more holistic, integrated, and effective means to secure data in all its various types and classifications. DSPM offers a considerable step in a more effective direction when it comes to data security.

Because DSPM is still a relatively young market, Omdia does not yet provide a detailed market size analysis, and reporting elsewhere in the market is variable. The market figures shown here are based on available open source data and are not specific as to what tools are and are not included.

The market size for DSPM tools has been and is experiencing significant growth. Publicly available statistics suggest a market value of $1.20 billion in 2024, growing to reach $4.15 billion by 2033, with a compound annual growth rate (CAGR) of 15.1%.

However, this overall figure seems low and the CAGR high when compared with Omdia's own reporting of some of the DSPM component parts. Data discovery and data classification would represent this figure alone under Omdia's data security market reporting.

Omdia estimates the encryption, tokenization, and data masking markets to be worth circa $5 billion for 2024 and identity management to be another $10 billion. Omdia estimates the monitoring, posture evaluation, and risk assessment elements of DSPM to be worth another $8 billion at the end of 2024. When totalled, this represents an estimated overall market size in the region of $24.3 billion for 2024.

Omdia asserts a CAGR for DSPM of around 5–7%, yielding a market of circa $25.5 billion at the end of 2025, rising to $34.5 billion by 2030.

As expected, North America is a key region, currently holding the largest share of the DSPM market at 41.2%, with EMEA (29%) and Asia & Oceania (24.8%) showing strong growth potential.

Vendor analysis

Vendor accolades

Within the vendor analysis section, two types of accolades can be awarded to vendors:

- The **Best in class** accolade is awarded to the vendor(s) with the highest score (highest outright, tied highest, or within <1% of the highest score) for each of the scoring categories that make up this Omdia Universe topic:
  - Core capabilities
  - Advanced capabilities
  - Solution breadth
  - Strategy and innovation
  - Market momentum
  - Vendor execution
- The **Top-tier** accolade is given to vendors falling within the upper tercile (top third) of the scores within the comparison group, for each of these same scoring categories.

Thales (Omdia recommendation: Leader)

Thales should appear on your shortlist if you are looking for a comprehensive data security platform from a single vendor.

Overview

As a global technology leader for the defense, aerospace, and cyber and digital sectors, Thales entered the DSPM market in late 2023 with its acquisition of Imperva, which was known for its Data Security Fabric (DSF) platform and its early foray in DSPM with the initial offering of Cloud Data Security in 2021. Thales expanded its cybersecurity portfolio to offer a highly complementary combination of solutions to help organizations protect applications, data, and identities with its CipherTrust Data Security Platform.

Omdia assesses the Thales DSPM proposition as a Leader, and with three Best in class ratings for core technology, momentum, and execution and one other Top-tier rating, the vendor has grown significantly over the last three years to become one of the premier DSPM and cybersecurity providers. It has managed to achieve what many of the defense companies have so far failed to do with their own cyber ventures—to become a recognized provider that can compete with established and experienced IT vendors on their own turf.

Thales provides one of the most comprehensive DSPM propositions in this assessment, and when combined with its existing enterprise-level encryption, key management, hardware security models (HSMs), and identity management tools and services, its proposition becomes even more compelling.

In a portfolio that extends across all but one of the standard DSPM domains, there are still some gaps. Some elements are still on the roadmap, and others remain to be addressed. Discovery is comprehensive, with support across a broad range of file types, databases, and OSs. The company's classification toolset is not as comprehensive compared to some other providers, with a number of file types yet to be supported.

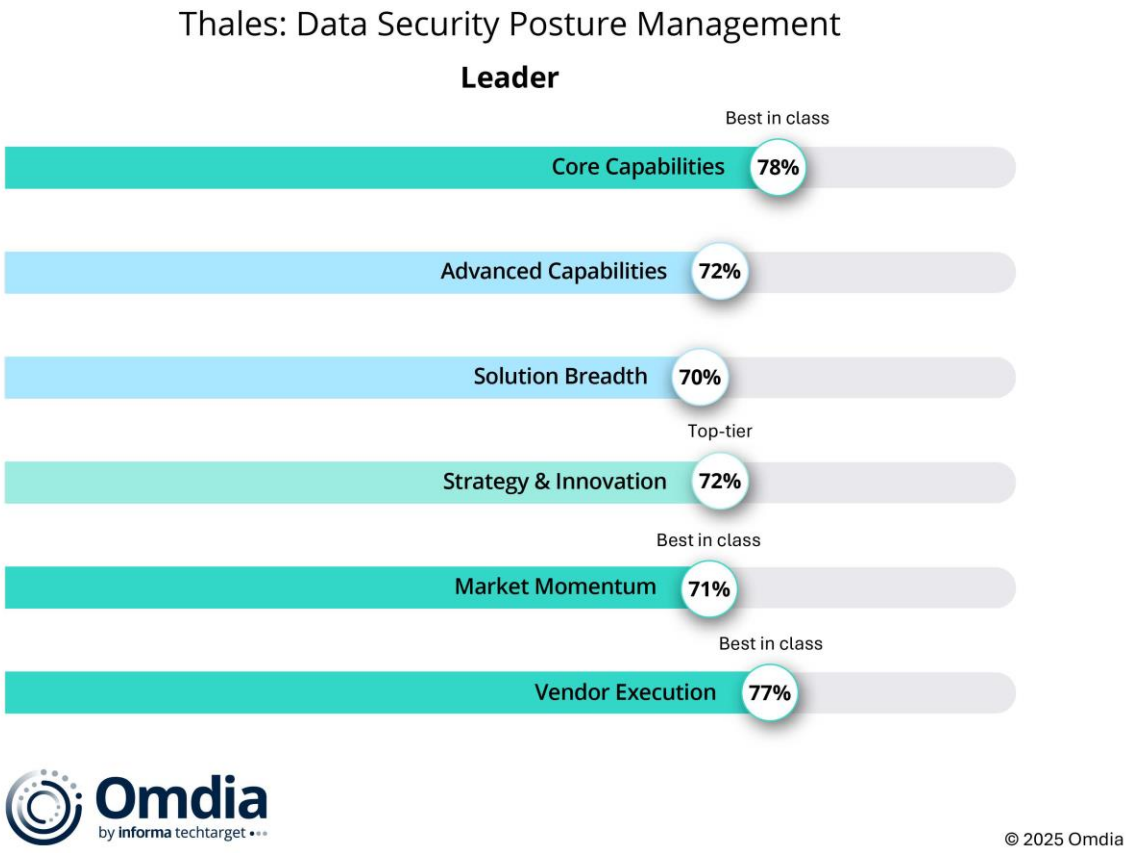
Thales has a roadmap to address this, but some functionality is currently lacking. There are comprehensive encryption, tokenization, and data masking capabilities, as well as the necessary remediation piece that providers in this category can lack natively. As expected from an experienced provider, the IDM proposition is strong.

Outside the core capability, Thales delivers a broad suite of posture management offerings. The organization provides very good capability across posture management itself, risk assessment, analysis, and monitoring; however, the DSPM portfolio lacks incident response planning. Thales addresses this by providing metrics and information to support incident planning, as well as playbooks to take automated actions against incidents from its wider cybersecurity portfolio. Overall, the assessment for its DSPM proposition as a whole is highly competitive when compared to other current vendor propositions. The swift introduction of its roadmapped functionality will deliver further value to this already strong platform.

Thales also provides robust propositions when it comes to its go-to-market approach (**Figure 14**), providing the organization not only with a compelling technology proposition but with a strategy, execution, and momentum unmatched among the other competitors in this report.

Furthermore, Thales has a global reach, operating in 140 countries through its network of 196 offices and support centers, within which are 11 security operations centers (SOCs), enabling it to scale appropriately. The vendor has a mature network of over 6,500 partners globally and has strategic partnerships in place with key industry technology partners such as Google, Microsoft, and Amazon, industry MSPs, and other industry leaders. Thales has a long history of supporting enterprises, including Fortune 100 organizations, where it focuses on building customer-centric business value and the development of a thorough understanding of each specific environment and delivery need. Additionally, Thales remains at the forefront of technological advancements, laying the foundation for advancing work in digital skills and delivery of cybersecurity and next-generation technologies.

Figure 14: Omdia Universe ratings—Thales



Source: Omdia

Strengths

Thales has composed an exceptional data security offering, but when viewed in the context of its wider CipherTrust platform, a key strength emerges. Not only is there the considerable scope and scale of its DSPM toolset but also the benefits of integration with a wider product set. Thales takes the steps of unifying data discovery, classification, data protection, and granular access controls with centralized key management, all on a single platform. In Omdia's assessment, some organizations can match or even surpass its technology portfolio, but include the go-to-market activity, and a DSPM solution from Thales is second to none.

Thales is unique in the IT market with its defense heritage. It has borne out its cybersecurity capability from the group's wider underlying DNA of knowing exactly what it takes to defend organizations, individuals, and even countries. Cybersecurity is an extension into a new combat domain—land, air, sea, and now cyber—and customers should trust in Thales' ability to use its fundamental knowledge of how to protect an environment to their advantage. In a market full of nuanced (and typically momentary) marketing messages around minor technological differentiation, the association with the defense group gives Thales cybersecurity a distinct edge. Unique selling points or propositions (USPs) are hard to come by in IT and often do not last very long. Here, Thales can enjoy benefits and longevity.

From a product point of view, Thales DSPM sets itself apart by not only identifying an organization's most critical data but also continuously tracking and analyzing every activity involving that data. While

traditional solutions typically focus on basic responses such as allowing, blocking, or deleting files, Thales offers an extensive range of advanced, precise, and tailored remediation strategies. Granular entitlements for refined access control, robust encryption to secure data at rest and in motion, sophisticated tokenization for secure data substitution, dynamic masking that obscures sensitive data seamlessly, and proactive real-time alerts to rapidly highlight emerging risks are all key strengths.

Rather than simply locking doors, Thales DSPM acts as an intelligent, vigilant security ecosystem—continuously aware of exactly where critical assets reside, monitoring who accesses them, and instantly deploying targeted protective measures tailored to the specific threat based on context. This is DSPM in its truest sense.

Limitations

Given its existing capabilities, Thales DSPM does not score as highly as might be expected in the advanced category. This is largely due to the absence of incident response planning under the DSPM umbrella. Thales compensates elsewhere, so this is only a small inhibitor.

Within the core components of DSPM, the only area that could be viewed as a limitation is the classification pillar. It is not as functionally comprehensive as other classification offerings, and a number of core pieces of functionality around labelling are only on the roadmap rather than in general availability. Equally, a number of unsupported file types are currently unable to be classified, which is an issue for organizations wanting comprehensive classification of all documents and records.

Omdia sees Thales's defense credentials as a strong asset, reflecting deep expertise in security and resilience. Some organizations may prefer to work with companies outside the defense sector. However, Omdia believes the advantages of partnering with Thales—including its proven track record and robust capabilities—will outweigh such considerations.

Appendix

Methodology

Omdia approached all 11 vendors included in the report to provide input into this study. The subsequent analysis is based on responses from those vendors to a bespoke questionnaire, collating the information they provided into a positional Universe diagram of strategy and execution versus capability, with a "bubble" to represent market presence. Furthermore, Omdia subdivided the data into a series of vendor-aligned charts to represent the assessed performance and provide comparisons against the criteria mentioned above.

The best performing vendors in each criterion are awarded "Best in class," and those who also performed well are awarded "Top-tier" status. Vendor contributions were voluntary. The vendors that do not appear either declined to participate or did not complete the response questionnaire in time before publication.

Omdia Universe

Omdia's rigorous methodology for the Universe product involves the following steps:

- Omdia analysts perform an in-depth review of the market using Omdia's market forecasting data and Omdia's enterprise insights survey data.

- Omdia creates a matrix of capabilities, attributes, and features that it considers to be important now and in the next 12–18 months for the market.
- Vendors are interviewed and provide in-depth briefings on the current solutions and future plans.
- Analysts supplement these briefings with other information obtained from industry events and user conferences.
- The Universe is peer reviewed by other Omdia analysts before being proofread by a team of dedicated editors.

Further reading

Market Landscape: Data Security Posture Management (DSPM) (March 2024)

Cybersecurity Decision-Maker Survey 2024: Data Security (August 2024)

Author

Adam Strange, Principal Analyst, Data Security

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com