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

Publication Date: 12 September 2025

Adam Strange

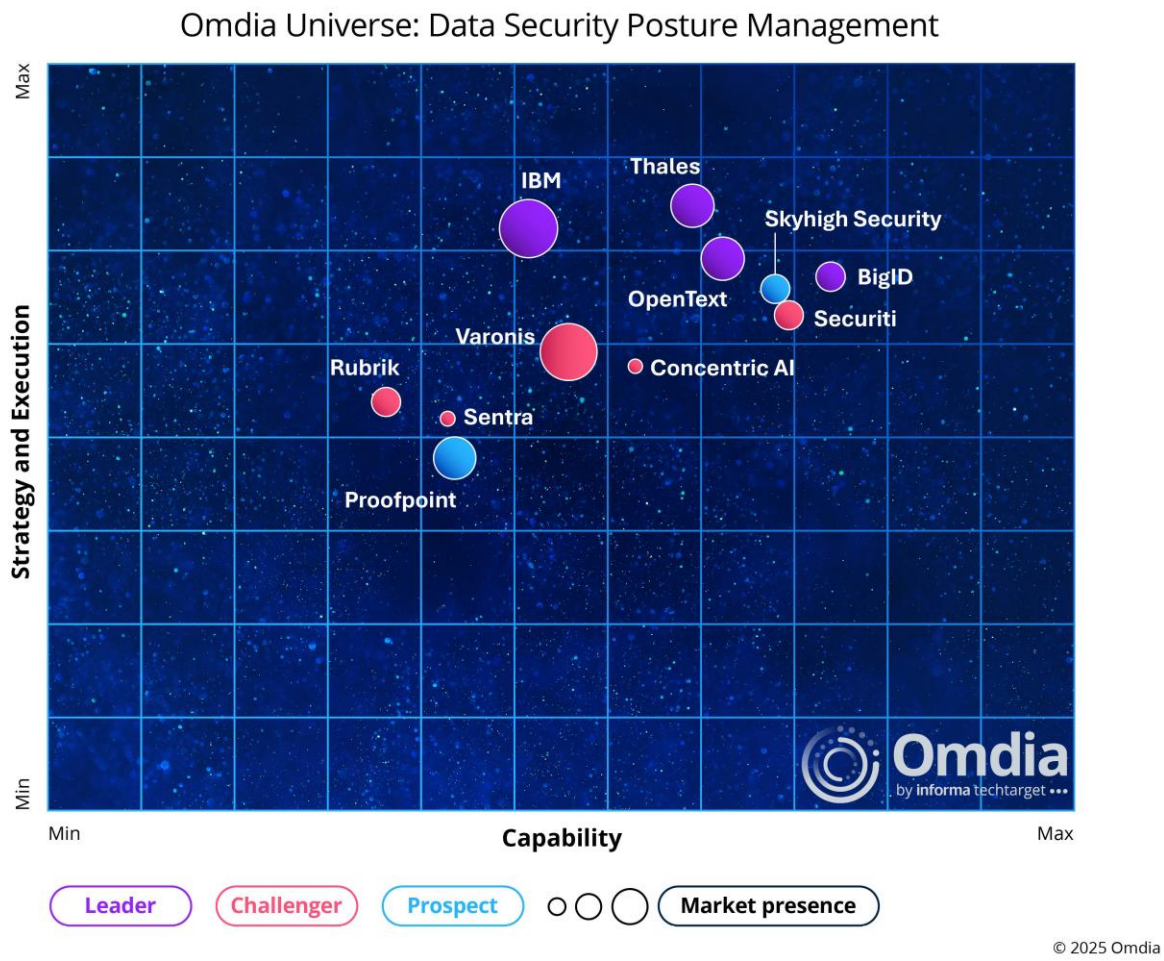
Summary

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.

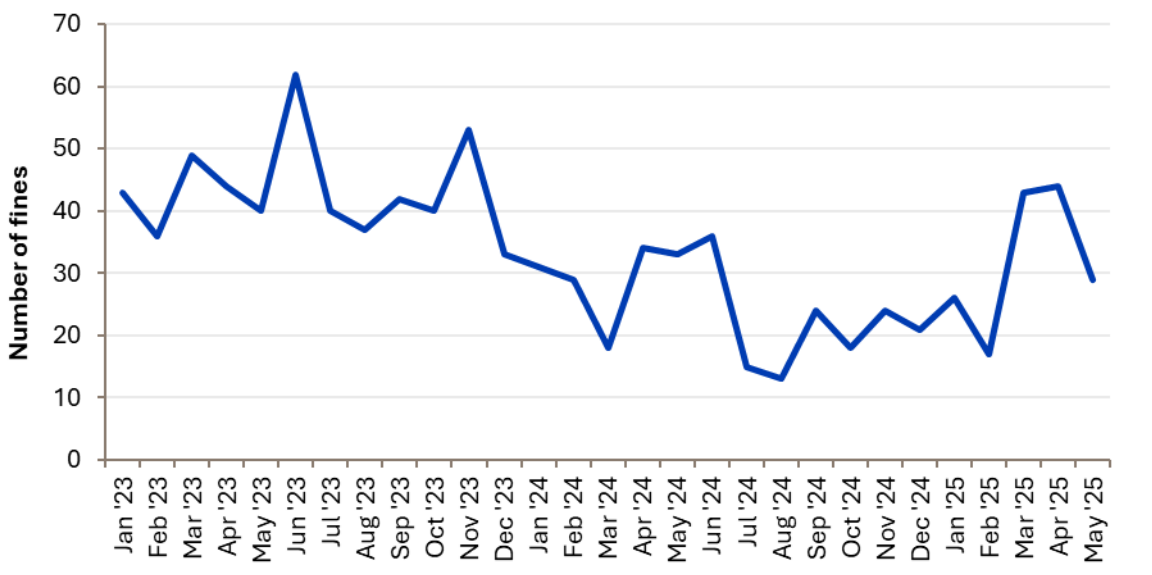
The importance of protecting data cannot be ignored or neglected: there is no sign of the threat landscape reducing. Organizations of all sizes need to maintain maximum levels of vigilance to stop future attacks and data exfiltration. DSPM can help by offering a holistic view, but perpetrators are often 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 CypherTrust 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.

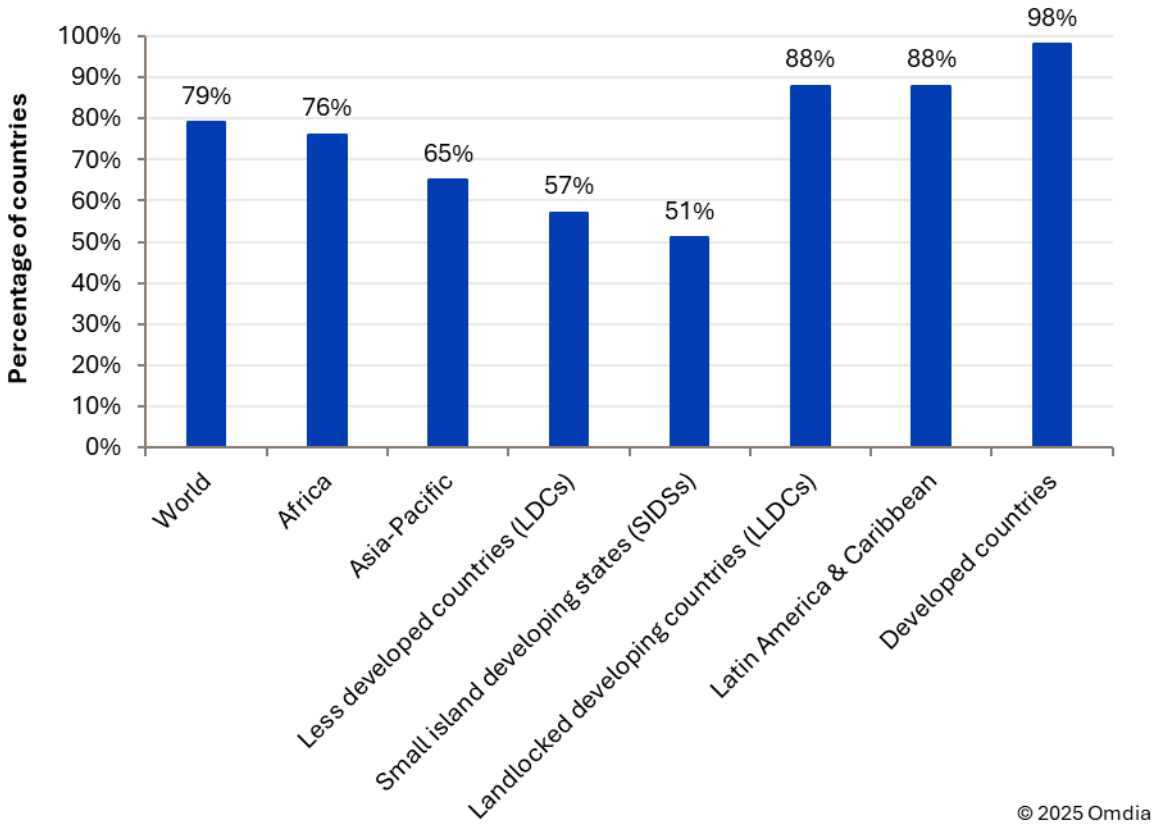
Proofpoint is the latest vendor to enter the DSPM market through its acquisition of Normalyze in October 2024. This acquisition was shrewd and carried through some brand equity from industry commentators. It is a good first step and positions the organization well for the next phase of development. The 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.

BigID (Omdia recommendation: Leader)

BigID should appear on your shortlist if you are looking for an established mid-sized cybersecurity vendor with a broad portfolio that can provide a flexible and responsive service, and if you need scalability through a provider and access to a partner community that can deliver incremental services.

Overview

Since the advent of DSPM as a stated and increasingly recognized proposition within data security, BigID has been a central presence. The organization has very much held its own in a dynamic and competitive marketplace, growing its business, capability, and reputation since the company launched in 2016. Its DSPM proposition was released in 2020 and has grown substantially over the

past five or so years, to currently deliver a wide and highly capable solution set that one might expect from a vendor of greater size and scale.

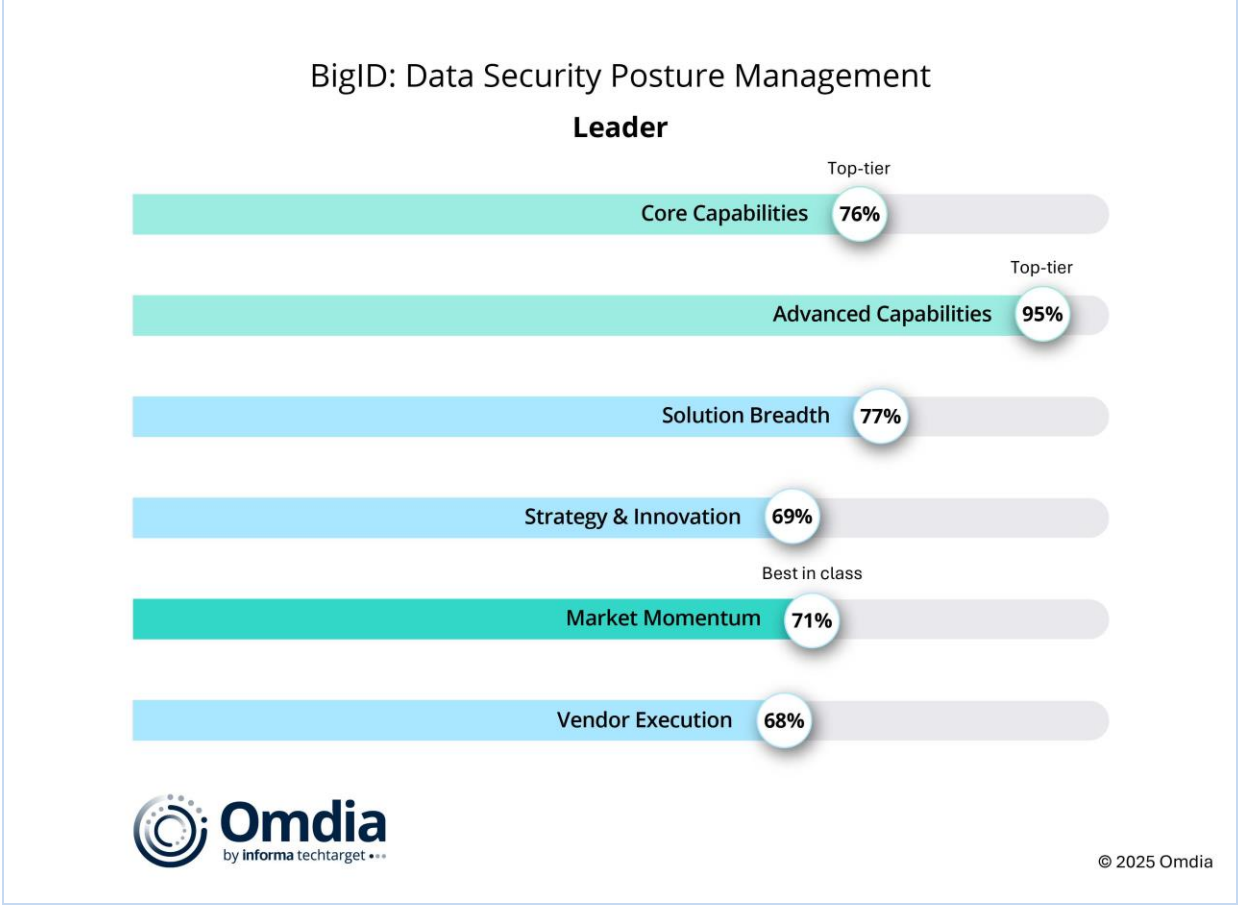
Many of the original DSP vendors can concentrate on the discovery and classification end of the DSPM deliverable, but BigID goes beyond to achieve a Top-tier status in some of its more advanced capabilities, such as posture evaluation, risk assessment, and monitoring. The vendor excels in market momentum, where it is rated as Best in class. Having strong posture management capabilities and good market momentum is a key positive. For vendors able to deliver top-level posture management—the PM piece of DSPM—there are significant opportunities beyond being able to improve data security.

BigID further achieved a Top-tier result for its core technology, enabling it to deliver a comprehensive solution that is well suited to organizations of all sizes. Omdia assessed BigID as having an excellent direction of travel, as it also rates highly for its strategy and execution. This indicates a focused organization investing in its business to maintain a competitive advantage and to deliver a valuable portfolio to its customer base.

Undoubtedly, BigID can help with understanding data, and that includes automatically finding dark data, shadow data, and unknown data with its technology. It can provide protection through access and privilege management and assessment and evaluation of data security posture, using an AI-driven, context-based data remediation layer, making recommendations for better and more informed decisions, reducing data risks, and protecting against unauthorized data exposure.

Omdia sees BigID as a highly capable DSPM vendor that is able to outperform its size to more than match some of its bigger, more established rivals. It can provide an expansive solution irrespective of data location, known or unknown. Its platform is one of the most capable available on the market at the time of writing and is a strong demonstrator of why the company has grown steadily since its foundation to its current valuation of over $1 billion.

Figure 5: Omdia Universe ratings—BigID



Source: Omdia

Strengths

BigID's strengths are in its size and scope. The organization is still relatively small (compared to some of the other vendors in this report), which enables responsiveness and the ability to work quickly with customers to define and implement a precise fit against specific challenges. Additionally, BigID's extensive portfolio, available through its own office and service center network across approximately 20 countries, and its very expansive partner network mean that it is also able to attain larger pieces of business from organizations probably more associated with larger vendors.

Investment and innovation are clear from BigID. The business profits well from the innovation it brings to enabling organizations to manage and protect AI data, an underpromoted aspect of the AI landscape. It has a clear view of its differentiators, specifically the number of connections it can offer with disparate data sources, built-in remediation, and its partner network and a well-defined product roadmap ahead.

Limitations

Overwhelmingly, the proposition from BigID is positive and comprehensive. Its DSPM lacks some data discovery coverage for older flavors of Microsoft Windows operating systems, which may create difficulties in tracking down all forms of legacy data. Furthermore, the classification capability

can be limited if the data is held in some of the lesser-used file extensions outside of the Microsoft Office environment. Generally, however, these are minor points.

BigID's identity management within the DSPM platform covers a good enough grounding of user access controls to provide an effective solution but, importantly, lacks native multi-factor authentication (MFA). In the context of the drive toward more effective login processes or passwordless login, not having MFA support is a gap BigID can address, particularly for users wanting more advanced levels of security or access control.

BigID manages identity for its users through integration with identity providers such as Active Directory and SAML IDPs, including Okta, Ping Identity, and Entra. MFA is supported via SSO integration with these providers; it is not a native capability within BigID. As it is managed in this way, end users looking for vendor consolidation may perceive this as a limitation. By contrast, BigID offers other identity functionality through the delivery of role-based access control (RBAC) and attribute-based access control (ABAC), which are native features of the BigID platform and do not require external integration. Customers can configure BigID to use its own identity store or integrate with Active Directory for RBAC/ABAC, allowing for fine-grained access management, creation of custom roles, definition of scopes, assignment of multiple roles per user, and mapping of roles to imported Active Directory.

Only a small number of vendors can provide comprehensive identity management within a DSPM portfolio, so the presence of limitations in this area will not significantly detract from what is overall a very strong offering. Some work is necessary to fill a few of these gaps for incremental value add.

Concentric AI (Omdia recommendation: Challenger)

Concentric AI should appear on your shortlist if you are looking for a smaller, focused, flexible organization with a very good understanding of the market and subject matter to work with hand in glove.

Overview

With the ever-increasing complexity and diversity of data, which may be stored and used in multiple places, such as residing in cloud or SaaS services or held on-premises across a wide variety of devices and locations, Omdia's research shows organizations are very unlikely to understand the full picture regarding their data. As such, businesses are unsure of the precise value of their data, what risks they face from it, or how to ensure the right data is fully secured. Concentric AI aims to address these issues by identifying exactly what sensitive data is, where it is being accessed or shared outside corporate guidelines, and how much it might be at risk.

Since its launch in 2018, Concentric AI has avoided traditional rule-based mechanisms to discover and analyze data, instead creating aggregated data intelligence, which it enhances from across its customers, using a deep learning as a service capability. This enables data discovery to be semantics-driven and conducted autonomously across multiple data locations—cloud, SaaS, and on-premises—and automates data risk identification and remediation. This is a different approach to other vendors and gains Concentric AI advantage in the marketplace.

Although the vendor originates from among the DSPM pioneers, and as such is still one of the smaller vendors included in this report, it achieved good results in Omdia's assessment for

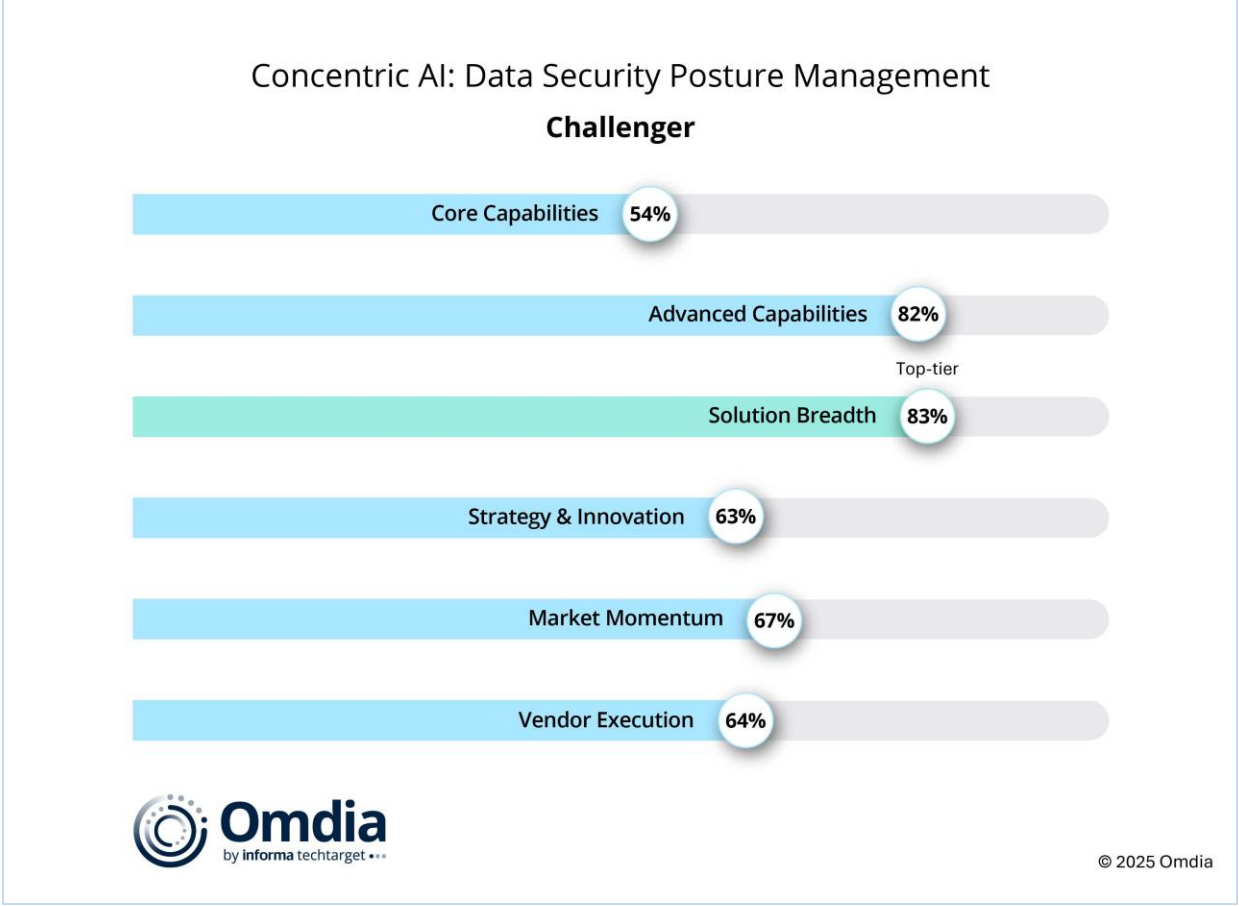
innovation and strategy and vendor execution, which contributed to a very good market momentum score (**Figure 6**). The organization's ongoing focus on innovation, registering multiple patents around its technology, is borne out by the results it secures across its core capabilities, particularly in its advanced offering. These culminate in a Top-tier rating for its overall solution offering. Here is an illustration of an organization working hard, with focus, to secure and grow as a business. Significant recent wins against larger competition highlights this as a strategy that yields results. Concentric AI is another smaller vendor that can unite behind focused, concise messages with responsive delivery, enabling it to compete against larger competition.

As its name suggests, Concentric AI uses AI to address head-on the major challenge for organizations of all sizes: where and what structured and unstructured data is present, across the entirety of locations and usage models, and how to protect it all. Concentric AI's Semantic Intelligence takes advantage of deep learning to automate discovery, classification, risk analysis, and remediation to address the DSPM challenges, particularly for medium to large enterprises with large and complex volumes of data.

Many vendors talk about using AI as if it were a silver bullet or a magical fix to make businesses more productive. The team at Concentric AI collectively has many years of experience with the practical application of ML and an appreciation of the importance of scale and accuracy when dealing with enterprise security challenges, so the vendor places its MIND AI capability at the core of its platform.

Omdia sees opportunities for Concentric AI to stand out from vendors at the smaller end of the DSPM provider spectrum by focusing on what it does and how it operates and being good at it. The investment in innovation is pleasing to see and gives Concentric AI a solid platform from which to take the next steps in growing its business. It is also noteworthy that the vendor can handle on-premises data as well as cloud-based data, which provides further differentiation from more cloud-focused providers in the DSPM space.

Figure 6: Omdia Universe ratings—Concentric AI



Source: Omdia

Strengths

Concentric AI uses context-aware AI for discovery to accurately capture large volumes of data, which it combines using a highly comprehensive data classification tool. In addition, the platform delivers continuous risk monitoring, as well as a comprehensive package of remediation actions (including moving, deleting, archiving, classifying, managing permissions, blocking, masking, and relocating), compliance, and investigation capabilities, which it delivers as a managed service. These capabilities serve as a very effective strategy and route to growth. This is demonstrated by the vendor's impressive growth figures of over 300% year on year overall.

Concentric AI delivers robust capabilities when it comes to access control. Access control policies can be defined directly within its platform and autonomously applied to semantically similar data. The vendor extends the ability to edit permissions on overshared files in addition to editing link permissions within SharePoint, Google Workspace, and OneDrive. It also provides strong functional capabilities when it comes to identifying anomalous user behavior in relation to data.

Concentric AI's strengths particularly lie in clarity, innovation, and delivery (execution), and because it does not overextend itself, it is able to win good business from other larger providers. Its size also serves it well, enabling it to retain focus and quality through its engagement with customers, several of which are happy to underline on the company's website how successful working with Concentric AI can be.

Concentric AI further provides a strong range of additional technologies from outside the more familiar DSPM stable with its offering. Data access governance, risk monitoring and remediation, data loss prevention, and data security for GenAI are all included in its DSPM proposition, offering customers choice and the ability to address wider challenges. Furthermore, the vendor has a clear picture of the road ahead, with innovative and comprehensive enhancements to its existing portfolio outlined for introduction within its future roadmap.

Concentric AI recently announced the acquisition of Swift Security and, as such, has extended its portfolio through the integration of Swift's technology into its Semantic Intelligence platform. This acquisition enhances the existing capabilities of Semantic Intelligence and extends its protection across data at rest, data in motion, and public GenAI applications. With these new features, companies can discover shadow GenAI and gain visibility into the risks associated with each tool, enabling them to make informed decisions about which tools to allow or block. Additionally, they can block or mask sensitive data shared via email, social media, file sharing applications, and public GenAI tools.

Limitations

Although it is good to focus on delivering specific offerings, Concentric AI does not offer all constituent parts of a DSPM platform in-house. The vendor provides data masking functionality but integrates with Microsoft Purview for intelligent encryption. This could leave it exposed when end users want a more comprehensive solution or an organization does not use Purview.

Concentric AI is a smaller organization, retaining offices or service centers in eight countries across North America, EMEA, and Asia & Oceania. Although this could be distinctly beneficial in terms of delivery and focus, the company will need to consider expansion of its physical presence as its strategy continues to bear fruit.

As of mid-2025, Concentric AI has focused on the North American market. This is the largest market and hence offers the largest opportunity. This might be perceived as a limitation by potential end users in other geographies; however, the vendor is investing in go-to-market teams in EMEA and Asia & Oceania, increasing its marketing and expanding its reseller base to address any imbalance.

IBM (Omdia recommendation: Leader)

IBM should appear on your shortlist if you are looking for a large provider that has a comprehensive portfolio of tools and services with a formidable resource pool to enable growth.

Overview

IBM, through its acquisition of Polar Security in May of 2023, now has a fully integrated DSPM solution within its IBM Guardium Data Security Center platform. As one module within a wider platform, IBM's solution is able to deliver significant extension to its core DSPM capability, which in itself is comprehensive. IBM caters to most customer requirements, and what is not addressed at the time of writing will likely be included in forthcoming releases, outlined in a detailed roadmap. The only substantial element missing is identity management, which leaves a gap to be addressed in the future. Currently, Guardium DSPM can provide visibility into potentially unauthorized access to sensitive resources by identifying third parties with access.

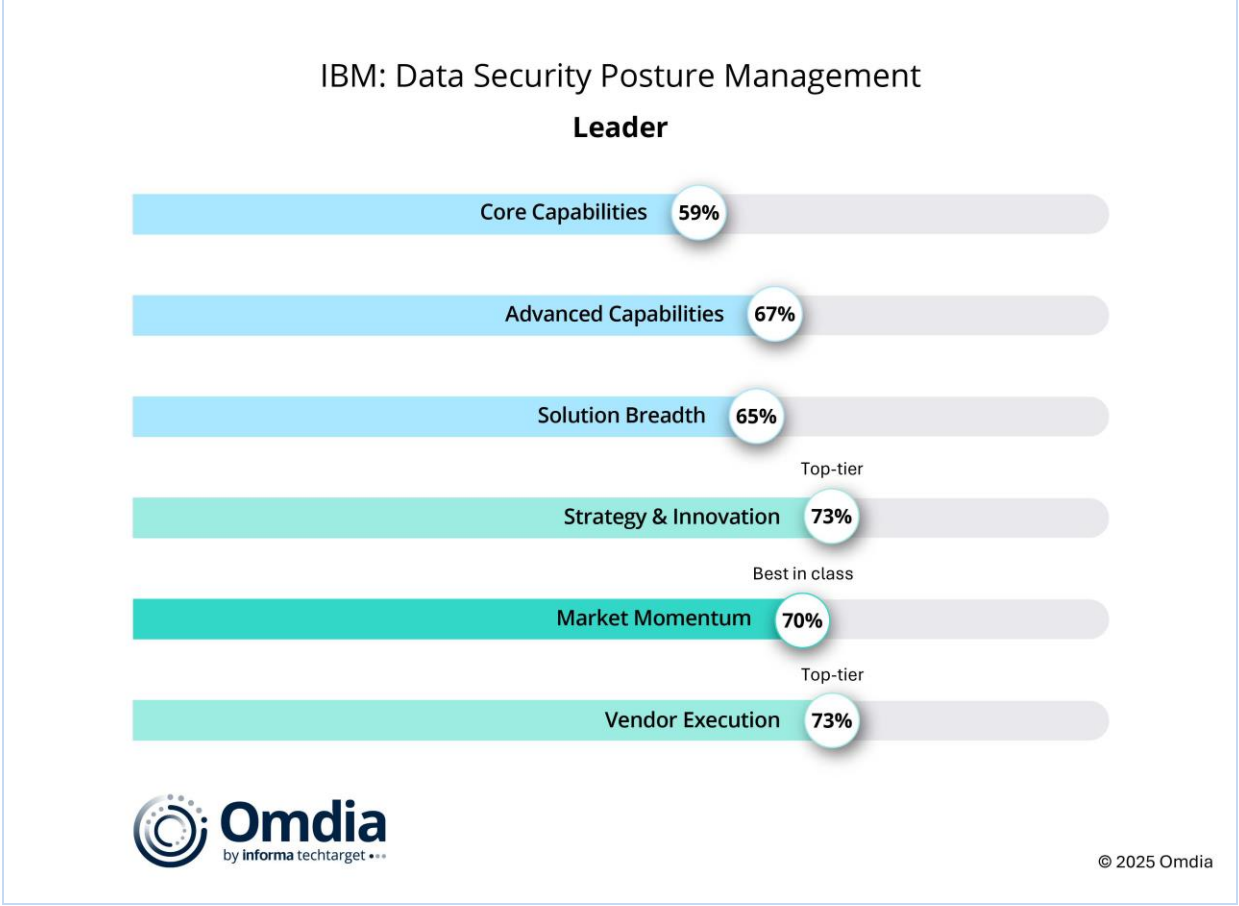
IBM Guardium DSPM aims to be an all-in-one DSPM solution, although the absence of IDM challenges this somewhat. Nevertheless, the vendor still achieves competent ratings for both core and advanced capabilities, and hence solution breadth (**Figure 7**). However, where it lacks some functionality, it achieves much improved scores for strategy and innovation (demonstrated by the comprehensive release program in its roadmap) and execution, which are both Top-tier, for an overall Best in class for market momentum, as would be expected from a vendor with its size, scope, and scale.

IBM focuses on the accuracy of its classification toolset, providing a strong capability in a key area of functionality. Many file types are supported and can be classified, inside and outside the Microsoft domain. Omdia believes those that are not currently supported invariably will be as time progresses. Coupled with its capabilities in data discovery, IBM Guardium DSPM provides a solid foundation from which to protect data through its encryption, tokenization, or data masking tools (which sit outside of the DSPM platform).

IBM Guardium DSPM integrates with key cloud data stores (AWS, Azure, GCP) used by today's leading organizations, together with SaaS applications such as Google Drive, Slack, Microsoft 365 (SharePoint, OneDrive), Jira, Confluence, and more. It supports different file types in a structured or unstructured format.

A key aspect of the IBM DSPM deliverable is its integration within the wider Guardium Data Security Center platform. IBM Guardium DSPM can draw upon much wider data security and compliance features elsewhere in the platform to provide, Omdia believes, an industry-leading capability overall. The proposition is even more substantial when Guardium is viewed within the broader context of the full portfolio of IBM security tools, which contains some 10 distinct product sets in total. Its Guardium platform is equipped to address typical challenges faced by end users, enabling access to an automated data inventory of sensitive data (including shadow data), tracking data movement, maintaining a strong data security posture, and minimizing compliance violations. IBM offers users control over data security and the ability to tailor capability according to evolving needs.

Figure 7: Omdia Universe ratings—IBM



Source: Omdia

Strengths

IBM's strengths come from the integration of its DSPM capability into a much broader platform, giving it the ability to deliver a capable data security proposition and then to further augment with other Guardium Data Security Center solution capabilities, such as IBM Guardium Data Protection, IBM Guardium Vulnerability Assessment, IBM Guardium Data Detection and Response (DDR), and IBM Guardium Data Compliance. The Guardium portfolio also offers broader value with IBM Guardium AI Security and IBM Guardium Quantum Safe. By adopting the full portfolio, end users can enhance data security and ensure compliance while factoring in AI and, importantly, AI security. The entirety of the platform ensures that the first building blocks for quantum computing can be laid down in readiness for the anticipated step change in computing power and performance.

IBM's data classification capability is a key strength. It is comprehensive as it stands, with further enhancements anticipated in the months to come.

IBM's DSPM is seamless in terms of deployment and adoption. This is achieved through an agentless architecture and a unique approach that requires no credentials or passwords to discover and classify sensitive data across environments.

IBM's brand, size, and scale are significant advantages. Located across 170 countries and with nearly 1,500 registered partners, IBM has enormous brand equity and is easily able to transact business

around the globe and at scale. Its resource pool and unrivalled levels of experience and heritage are right at the top of the IT industry, enabling it to deliver against any challenge. It retains a vast portfolio of cybersecurity and broader technology offerings, a large consultancy practice in IBM Consulting, IBM Technology Expert Labs, and a roster of key Guardium business partners that are the main providers helping clients to deploy and gain value from the solutions.

Limitations

While DSPM advocates the right approach, protecting data in its entirety is as large an undertaking as it is necessary. IBM is not alone in being unable to provide every tool at every level necessary to deliver a complete solution.

A lot of the gaps in the IBM capability are perhaps small—a file type not supported in terms of classification, for example—and might be being addressed, but they are nonetheless present as of July 2025. The big gap, however, is the absence of an identity management or enterprise access control capability within the DSPM portfolio. It seems an obvious piece of functionality to provide. Once data is found and its content is understood, classified, and suitably protected, the next step is to control user access. So, the inability to provide the right users—human and non-human—with access to the right data is something that needs to be addressed if IBM is, as it aims to be, an all-in-one DSPM solution.

OpenText (Omdia recommendation: Leader)

OpenText should appear on your shortlist if you are looking for a provider with a rich portfolio of tools and services that brings value beyond the first implementation.

Overview

OpenText may not be as recognizable as some of the others in this assessment, but it has built up a strong portfolio of DSPM capability under its Cybersecurity Cloud platform. OpenText does not actively market its capability as DSPM, which is perhaps why it is not as recognizable a DSPM vendor as some. However, it has built, through a combination of organic growth and acquisition, a strong set of capabilities in this space. Omdia assesses its capability as a Leader.

OpenText was launched in 1991 and has had a reputation for gathering together a stable of technology in the twilight of its lifespan and relaunching it to inject a new lease on life. This may have been the case, but it has acquired more successfully than some and has developed what is now a highly effective and valuable set of tools and capabilities. Indeed, in this assessment, the vendor is among the best propositions analyzed and achieved Best in class for its solution breadth and for its strategy and innovation (**Figure 8**). It also achieved a Top-tier status for its core capabilities and rated very well for advanced capabilities, highlighting that the business is working hard to reinvent itself as a central data and cybersecurity player.

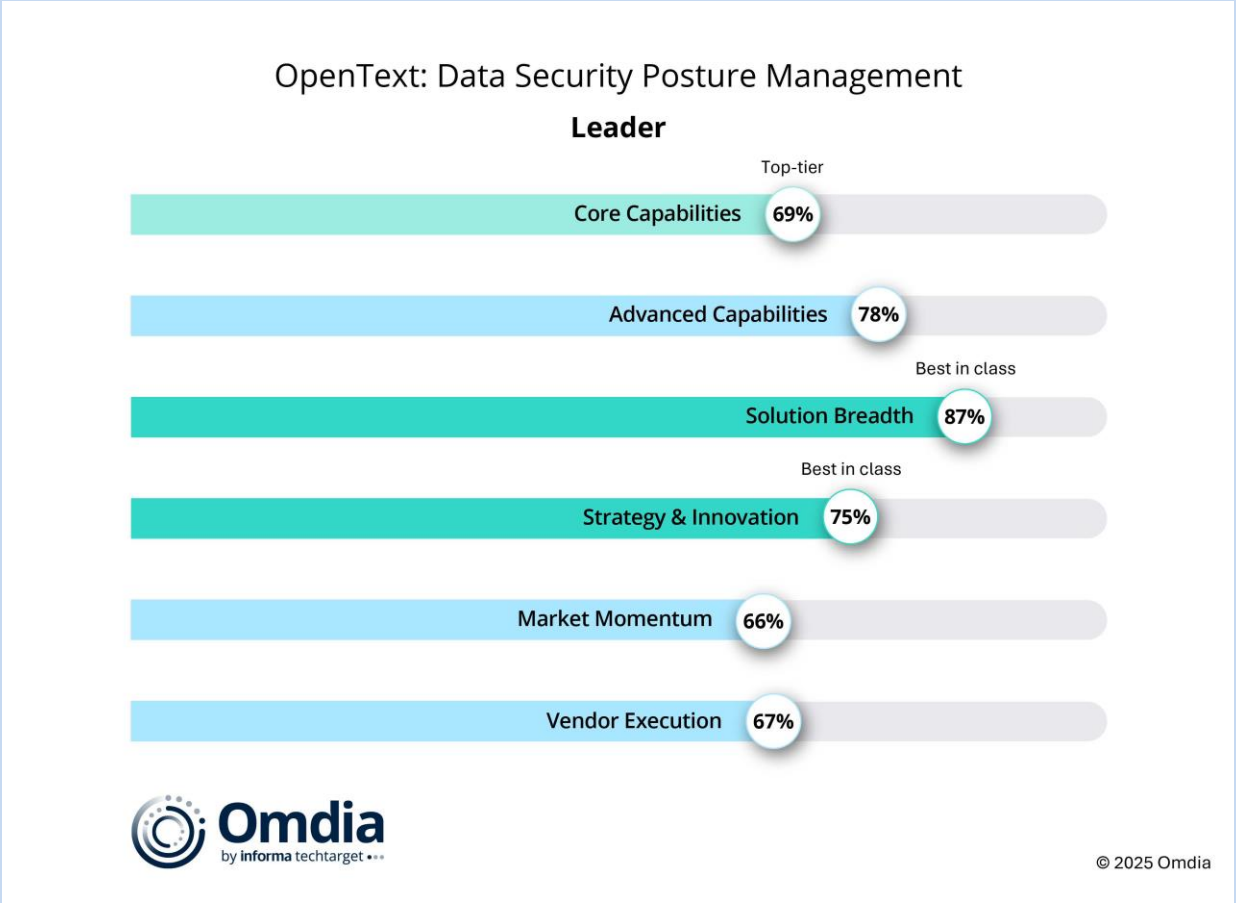
OpenText's portfolio of technologies that would be branded DSPM under other marketing regimes is expansive and thorough. All the major elements of data security (core capability) are provided, and OpenText has invested in its products to support an extensive variety of operating systems (OS) and file types in both discovery and classification. It provides data protection through in-house

encryption, tokenization and data masking, and identity management for the full spectrum of data security functionality under DSPM.

With such a strong showing as far as its technology is concerned, OpenText was able to turn some of its attention to optimally restructuring its business through the second half of 2024 and into 2025 to take maximum advantage. It remains to be seen how the full extent of the restructuring will pan out, but it has momentum to date, all of which secures the vendor as a Leader of this assessment.

OpenText still has some work to do to disassociate itself from legacy perceptions of what the brand could be seen as representing in years gone by. This will take time and involve careful decision-making, investment, and customer engagement. For now, its execution is perhaps still hindered by those historical perceptions. It has, however, the technology to develop fresh brand equity, and assuming the people now resident in influential roles settle in well, the company should maintain its current pathway. OpenText should now be firmly on the list of potential providers for organizations looking to take a step change in the way they protect their data.

Figure 8: Omdia Universe ratings—OpenText



Source: Omdia

Strengths

OpenText's primary strength lies in the breadth and scope of its data security technology offering under the umbrella of its Cybersecurity Cloud. Omdia's assessment is that OpenText provides one of the broadest available. Its portfolio not only delivers all the key components of a DSPM platform, but

it also extends down into the details, providing comprehensive support for a wide range of repositories and file types for its data discovery services and the most commonly used file types for classification, for example. OpenText is able to provide a rock-solid first step on the road toward robust data security.

OpenText is a large organization with offices and service centers in 22 countries, enabling the vendor to capitalize on opportunities as they emerge. It has a large partner base that provides the greater revenue stream (indirect versus direct) and enables the vendor to extend its reach further. It retains balance in its global sales model with most effort devoted to the North American market but has a healthy contribution from other geographic markets, approximately in line with Omdia's assessment of market size for data security (the Americas at 45%, EMEA at 29%, and Asia & Oceania at 25%).

The vendor has a well-defined strategy and a sharp focus by region, organizational size, and buyer persona as its targets for opportunity prospecting. It runs a series of events annually, the largest of which is OpenText World, and forums for customers, partners, and developer access and discussion. All of this facilitates strong community relations and a platform to enable growth.

Limitations

Over the past 6 to 12 months, OpenText has undergone some internal changes aimed at better aligning the organization for future growth. As of mid-2025, this evolution is still settling, and it is not yet clear whether the current structure fully supports the company's ambitions to become a globally recognized cybersecurity leader. While these adjustments are showing positive momentum and moving the business in the right direction, Omdia suspects the vendor has yet to reach the speed or growth it would like to achieve.

Additionally, OpenText suffers from legacy perceptions of the brand and thus with brand recognition. It does not have the recall factor of some of its competitors or, similarly, the understanding of what the brand represents. However, the organization is now on prominent display at trade events and conferences as it works hard to build momentum and brand equity in a competitive market.

Proofpoint (Omdia recommendation: Prospect)

Proofpoint should appear on your shortlist if you are looking for a provider with a strong focus on preventing human-targeted threats and a human-centric stance toward data security.

Overview

Proofpoint is the latest sizable vendor to enter the DSPM market through its acquisition of a DSPM pioneer, Normalyze, which it bought in October 2024. The acquisition brought a respected DSPM provider alongside Proofpoint's existing technologies, such as data email security, data loss prevention (DLP), threat intelligence, and Proofpoint's suite of managed services, for a broad range of capabilities. In Omdia's assessment, it is a new entrant but a prospect worth considering.

Normalyze's DSPM proposition concentrates on data discovery and classification, and from that point of view, Proofpoint adds vital and comprehensive functionality to its portfolio. The vendor can deliver a strong suite of technology in these areas, with little in the way of file types or operating systems left unsupported. It illustrates the investment Normalyze had devoted to its DSPM

proposition and why it had gained praise from industry analysts. Proofpoint made a shrewd acquisition that now sits well within its portfolio of wider tools and services.

However, the proposition does not address the next DSPM stages—protection and control—and in-house encryption, tokenization, data masking, and identity management or access control are absent. Its core competency score (**Figure 9**) is therefore low due to these shortfalls, but a low core competency score should not detract from a high competent discovery and classification capability, which are the core tenets of a successful data security posture. As shown in the chart, the vendor is still able to deliver a good overall solution with the addition of Proofpoint's advanced features, where it achieves a Top-tier rating, as might be expected from a provider with an established managed service capability.

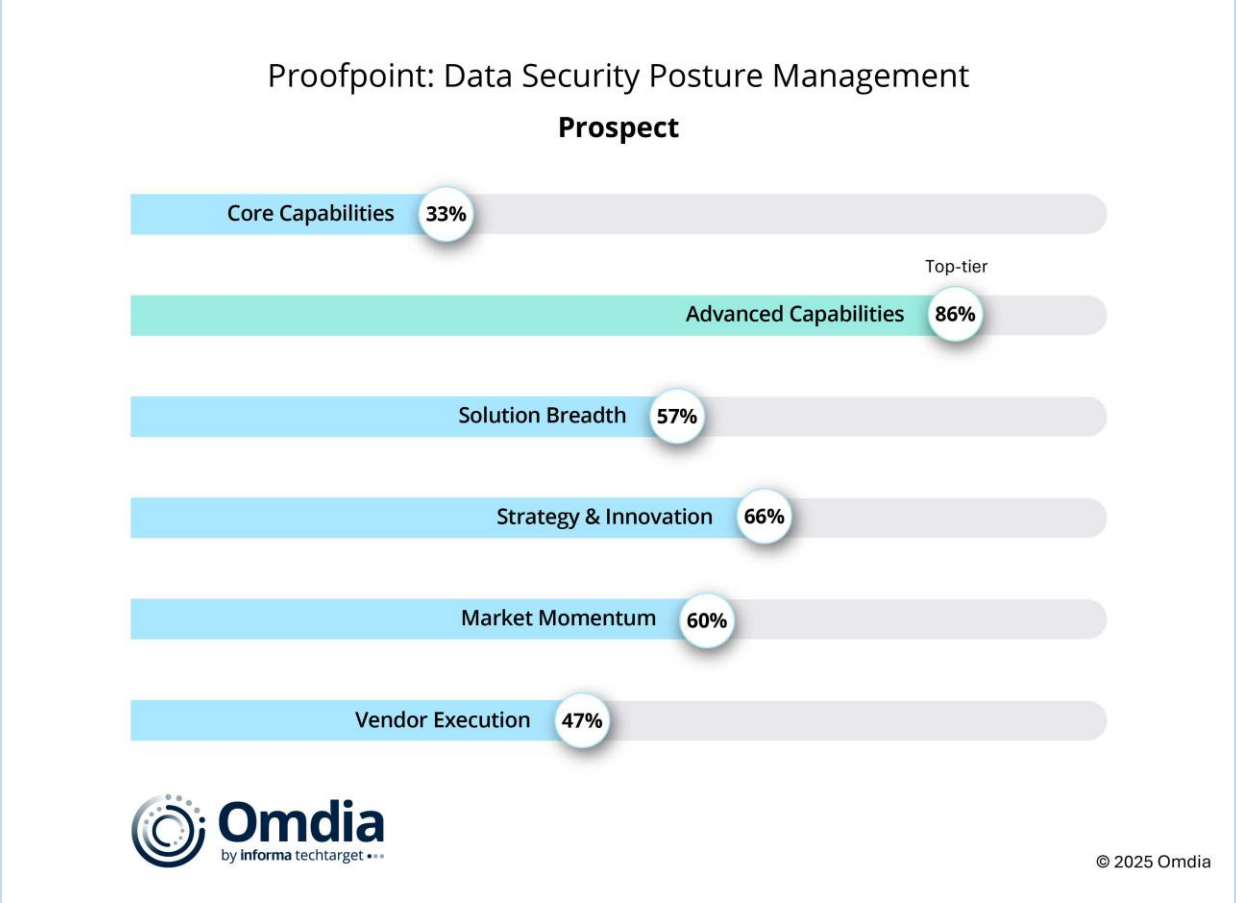
Proofpoint retains a good rating for strategy and level of innovation and should now focus on turning some of its R&D investment into building in some of the innovations currently absent from its DSPM portfolio.

The vendor achieves a solid score for momentum, and its brand has a positive impact here. The Normalyze acquisition is still relatively recent, and as it continues to settle into the organization, Proofpoint will inevitably ramp up its execution levels.

The overall Proofpoint DSPM platform covers a broad range of cloud environments, SaaS applications (currently GDrive, OneDrive, and SharePoint, with plans to add a wide range of additional applications in 2025 and beyond), on-premises DBs, and file shares.

Omdia assesses Proofpoint as having a well-constructed and articulate proposition, defined and focused across five DSPM pillars: data discovery, data classification, data access governance, data risk management, and compliance.

Figure 9: Omdia Universe ratings—Proofpoint



Source: Omdia

Strengths

Proofpoint has a strong brand and a long history in email security. It now adds DSPM capability to its technology and services for a platform that focuses strongly on finding and labelling data. Its DLP solutions will add further control, ensuring only the right data is distributed to the right places. DLP relies on meaningful and detailed classification and labelling, so a strong functionality set in this area is a key strength.

Proofpoint takes a strong human-centric approach to its security offering as a whole. This is a debate that has swung toward and away from the human factor (the employees or users) over the years, but despite the bad press, humans are still very much a part of this equation. True, humans make mistakes. In that sense, they need to be supported by advancements and innovation in technology and effective training (rather than periodic check-box exercises from the business). Proofpoint is well positioned to assist organizations willing to categorize their users as part of the solution more than as part of the problem.

The data discovery and data classification elements of the Proofpoint portfolio are strong, as is the adoption of agentic AI to further enhance this capability. The inclusion of DLP and insider threat management (ITM) capabilities further expands the Proofpoint DSPM offering. The vendor also aims to expand the platform beyond data security to privacy-aware data life cycle management and

privacy management, including Data Subject Access Requests (DSAR) to address GDPR and Personal Information Protection Law (PIPL) audit readiness requirements.

The organization is distributed across 30 countries, with a network of over 300 partners, which includes 23 specialist data security resellers. It has a well-defined strategy and focuses on its identified target market across North America, EMEA, Asia & Oceania and Japan, and Latin America.

Limitations

Overall, Proofpoint has a good DSPM proposition, but for it to claim a full DSPM platform, it needs further functionality in the way data is protected (encryption, tokenization, and data masking). Proofpoint currently provides certain identity-related risk detection capabilities, including monitoring for weak or outdated authentication practices such as accounts without MFA enabled, detection of accounts where passwords have not been changed within a defined period, and identification of dormant or unused accounts. While these features help reduce identity-related exposure, they focus on risk detection rather than full lifecycle identity management.

According to Proofpoint, its DSPM customers do not ask for features such as encryption, tokenization, and data masking as they fall into a broader data security use case outside of posture management. However, from the posture side, its DSPM capability is able to identify if sensitive data is encrypted or not.

As Proofpoint gathers momentum in the DSPM space, the extent to which these areas affect sales will become evident. Other vendors can offer a broader portfolio of tools in the data security space, and all these technologies working in collaboration is where DSPM provides a true advantage. Although it is true that DSPM covers a lot of ground, and customers may not want the full spectrum of capability all in one go, vendors should still be able to offer a broader portfolio. The addition of these complementary and necessary technologies within the Proofpoint stable would enhance the portfolio and allow for swift development of the Proofpoint DSPM offering.

Proofpoint, although a well-recognized brand in the email security space, is not yet as recognized as an out-and-out DSPM vendor. The Normalyze acquisition is still being fully assimilated into the marketing message and digested by the market as a whole. In a competitive marketplace, those not familiar with the recent history could view this as a short-term limitation.

Rubrik (Omdia recommendation: Challenger)

Rubrik should appear on your shortlist if you are looking for a vendor that offers a comprehensive proactive DSPM solution but can also provide wider, reactive capabilities in the event of a breach.

Overview

Rubrik was established in 2014, initially to help organizations stand up against anything that threatened their data via its delivery of a flexible platform for backup and recovery. It entered the DSPM market with its purchase of Laminar in August of 2023, and as such was among the first organizations to spot—and importantly, move—on the opportunity emerging with DSPM.

The vendor has a good proposition in data discovery and classification, where it applies native labeling within its Rubrik Security Cloud (RSC). It can also apply Microsoft's Purview labelling, which can encrypt a file. There is no tokenization offering, and it offers some capability in identity

management around multi-factor identification, federated authentication, existing credential login, and single sign-on. However, toward the more advanced end of the DSPM spectrum (e.g., posture management, monitoring, assessment, incident response planning), the organization delivers an excellent suite of products and services. Additionally, the company offers its considerable strengths in backup and incident recovery through its Cyber Resilience Platform to ensure that in the aftermath of a breach, systems and identities can be restored quickly and effectively.

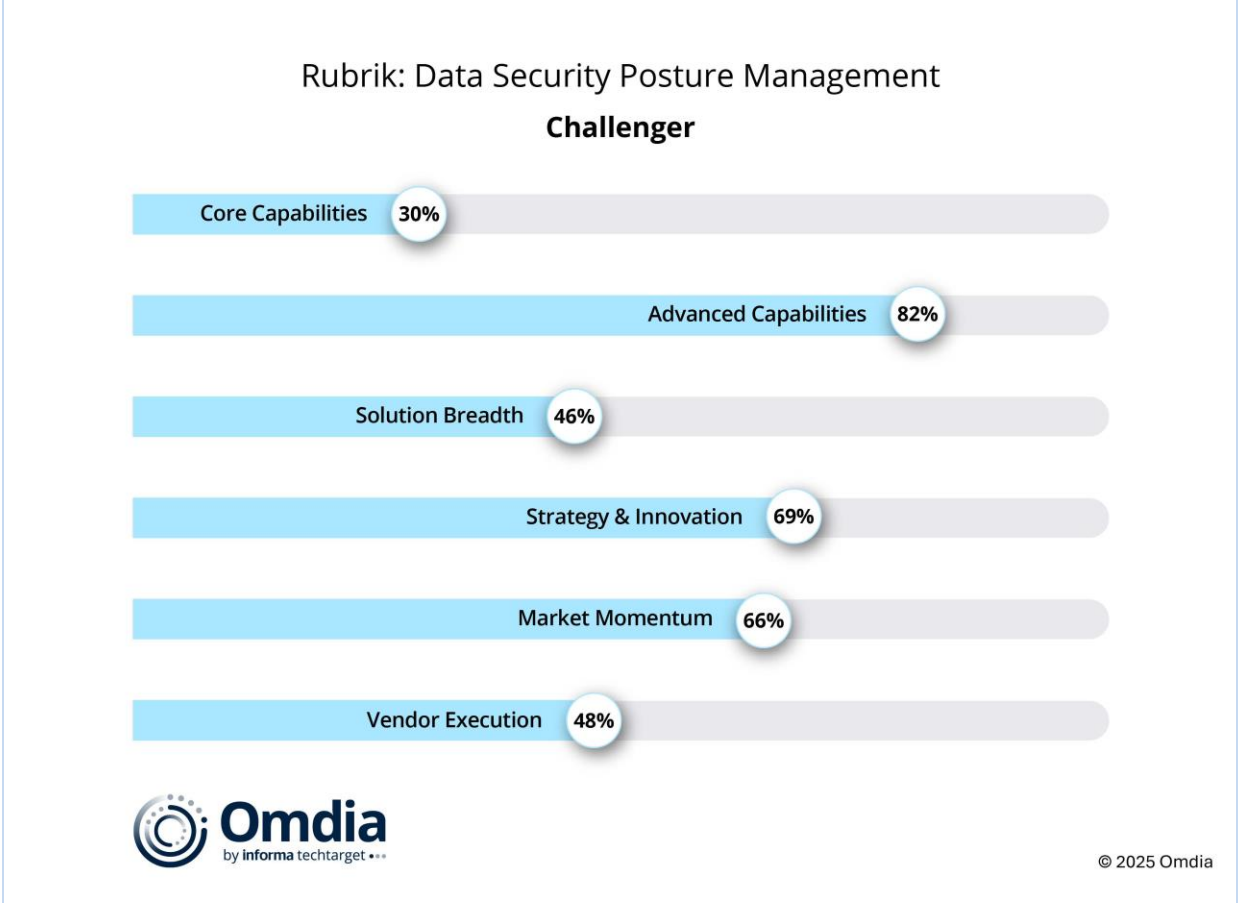
It is worth noting that although DSPM affords a step change in the way data is secured and protected, it is not ever going to offer a 100% failsafe or safety guarantee. It is therefore worth focusing on deploying DSPM to best effect but also accepting that a breach will still occur at some point and that having plans and fully tested measures in place, such as how to get data restored and business operations back up and running with minimal disruption, is also vital. Here, Rubrik has an important advantage over the competition, as it is able to offer proactive DSPM alongside the reactive backup and restore piece when a breach does occur.

Rubrik has a strong partner (and reseller) landscape across many countries and verticals, with its own footprint across 22 countries throughout the US, Europe, and Asia & Oceania, giving it a firm and recognized global presence. It retains a strong roadmap, showing strong levels of innovation. The vendor is able to show precise differentiation from the competition around its DSPM proposition with a strong focus on resilience, monitoring, and remediation as key capability areas.

Importantly, among some of the DSPM offerings, on-premises data is supported along with cloud and SaaS applications, all managed through a true single pane of glass. Often, when DSPM capability is assessed, only cloud-based data is embraced. Here, Rubrik goes beyond what is commonly found for a holistic approach across data, irrespective of its location.

Rubrik has a well-defined and developed strategy, which positions it well to compete with other established brands and the smaller pioneers. As shown in **Figure 10**, though, the organization had middle-of-the-road results for vendor execution. These results are surprising, given positive engagement messages from customer testimonies it has received. Omdia's assessment is the result stems from the vendor's position as a public company and difficulties in providing requested information, rather than its performance. As such, the score in this report should not be taken as a definitive reflection of Rubrik's actual performance. Indeed, the (better) results for strategy and market momentum are a much more accurate indicator, with Rubrik having worked hard to ensure the Laminar acquisition was a good technical and cultural fit for the organization and that, since acquisition, its DSPM proposition now fits well within its broader Data Security Cloud offering.

Figure 10: Omdia Universe ratings—Rubrik



Source: Omdia

Strengths

Rubrik's key strength is in its ability to combine a solid DSPM proposition with its wider data protection and resilience capabilities. DSPM tends to focus on being proactive—taking a robust and holistic approach to keeping the bad actors away from all forms of data that present a risk to the business, were it to be lost. Similar to all other security tools and protocols, it cannot offer absolute guarantees simply because no one knows where the next threat will come from, nor what it might manifest as. All that CISOs or security teams can realistically do is work with what they know about and ensure they build out and maintain the very best security posture they can assemble, in the hope that it will protect according to expectations. DSPM does this, but there are still gaps. Rubrik not only delivers a good DSPM platform but also integrates it into a wider platform to provide the reactive element: what should be done in the event of a breach? This is both an important additional benefit and a key positive.

Rubrik has assimilated the purchase of Laminar into its data security portfolio very well, maintaining the value add that it saw from Laminar in the first place, and it continues to deliver that value across its customer base. Often, the positive elements of an acquired organization become lost in the transition or are irreversibly eroded as companies look for new efficiencies or cost savings. It is a key strength that Rubrik has managed to maintain both the acquired DSPM customer loyalty and its own momentum through the acquisition assimilation process.

Limitations

Rubrik has some weaknesses in its core capabilities. Data discovery is competitive among other flavors elsewhere in the market, as is its classification proposition, although there are some (minor) file types yet to be supported. However, some reliance on Microsoft for encryption and the lack of a tokenization proposition remain gaps that would be beneficial to fill. Identity management is natively offered, but additional capabilities to add functionality would enhance the offering.

Rubrik utilizes Microsoft (Purview), particularly for encryption but also within its classification functionality, specifically for labelling. Purview is an acceptable classification platform and, for the most part, will have technology to address most business challenges. It may not necessarily suit if an organization is looking for specialist or more granular classification. Rubrik may find itself limited in these user cases, or if a customer is not already licensed for or cannot afford either Purview or the wider spectrum of Microsoft data security. Rubrik can, however, deliver labelling natively, so it retains an alternative option if Purview is not available.

The Rubrik brand may not be as recognized as some of the other competitor organizations in the DSPM landscape, and this may be a minor limitation over the short- or midterm. As evidenced at recent trade shows and conferences, together with a prominent profile online, the organization is clearly working hard to build more of a presence and a reputation as a DSPM vendor. The organization has a very good story to tell, not only around its DSPM capability but also its wider resilience, backup, and recovery technologies, so any limitations here should be short-lived.

Securiti (Omdia recommendation: Challenger)

Securiti should appear on your shortlist if you are looking for a specialist DSPM provider able to deliver an extensive portfolio now that will scale to the enterprise level as the business grows.

Overview

Founded in 2019, Securiti was one of the DSPM pioneers. It formally introduced its DSPM offering in 2021 and has since developed its proposition to be among the most comprehensive available. In this analysis, the organization achieved a creditable result for its core technology offering and an exceptional Best in class rating for its advanced features within the posture management end of the DSPM spectrum. Overall, Securiti gained several highly commendable Top-tier results (**Figure 11**), a very good performance given that the organization is still smaller compared to some of the competition and, hence, would be expected to retain a more modest portfolio. Securiti is punching well above its weight when it comes to the scope of what it can deliver.

Securiti has clearly invested in its research and development, with its data discovery capability among the very best in the market. The organization is able to identify data across the full range of locations (e.g., known, unknown (shadow), on-premises, cloud, SaaS). In this landscape, being able to identify the full data estate, in its entirety, known and unknown, is a key advantage.

Securiti's classification offering is also robust, with capable labeling functionality addressing all the widely used file types. Securiti goes on to include support for encryption, using native data system constructs. It provides native tokenization and support for all native data masking types. Identity management is native and comprehensive within its DSPM portfolio. Assessing the overall

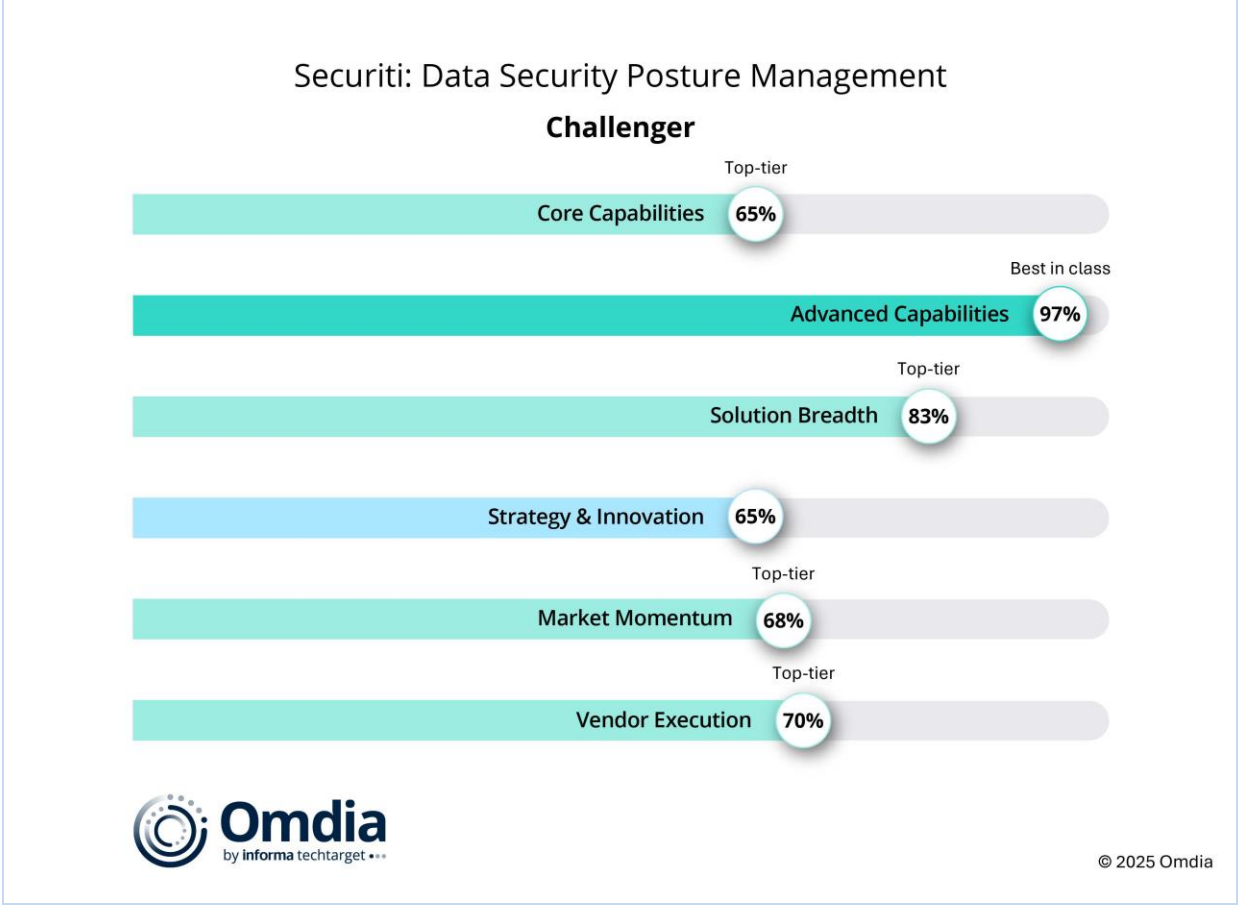
technology deliverable, Securiti delivers a very high standard of functional capability across the data security element of its DSPM portfolio.

When it comes to the more advanced feature set, Securiti excels with its Best in class rating. The organization has assessed what it needs to deliver and has concluded that a focus on the wider posture management domain within DSPM would give it the edge. Although there is one area that still needs to be addressed around posture management itself, and backup and restore specifically, the organization's capabilities around monitoring, risk assessment, analysis, and incident response planning are far more expansive than would be expected from an organization of its size.

Securiti has a direct footprint across nine counties, and with a solid network of partners and over 100 resellers worldwide, the organization maintains a global presence. Perhaps to be expected, the lion's share of the organization's business stems from North America, with EMEA some way behind as its second most important market. It does transact in Asia & Oceania and Latin America, but combined, the contribution only makes up around 10% of the organization's business. The company has a solid customer base throughout and anticipates strong triple-digit annual growth over the next years.

The vendor maintains an innovative approach to its product set, with a number of patents held and pending. It offers a clearly defined roadmap for 2026, turning to AI to refine and expand its functionality and enhance its defensive capabilities. Innovation is therefore much evident, and it is able to offer good differentiation from the competition through its Securiti Data+AI Command Center platform.

Figure 11: Omdia Universe ratings—Securiti



Source: Omdia

Strengths

Securiti's expansive portfolio is its key strength. With its rankings for advanced capabilities and overall solution breadth, few organizations of its size (hundreds of employees, rather than thousands) are able to deliver a comparably broad portfolio. Although there are some (small) gaps in endpoint security functionality (Android and iOS, for example), these are either lower priority or Securiti is broadly able to cover the shortfalls through a platform-based approach, continued innovation (e.g., visualization, understanding, and communication of risk context, data flow intelligence, AI security and governance, data minimization), and the use of AI, such as its Securiti DataCommand Graph as the foundational intelligence layer of the Securiti DSPM platform. These combine to give the organization a highly competitive and attractive offering.

Given the scale and scope of its portfolio, Securiti's size is a strength. A smaller vendor tends to offer greater flexibility, responsiveness, and delivery speed. Having the breadth of solutions available, combined with an accessible and responsive vendor, is a definitive plus. With a wealth of customer success stories and industry accolades prominent on its website, Securiti is evidently able to combine the two to very good effect.

This positions Securiti very well to address the larger enterprise space and customers wanting an extensive, platform-based proposition, as well as the upper end of the mid-sized market, where speed and flexibility are key. Securiti is very well positioned to serve both arenas and to grow

accordingly. With year-on-year growth, Omdia anticipates Securiti will attain a Leader rating in future reports.

Limitations

Size can be both an advantage and a disadvantage. The organization may suffer due to a lack of brand profile and recognition in a competitive market. Securiti has only been trading since 2019, so it lacks the heritage and profile of some of its larger competitors. This could be detrimental as competitors with greater marketing powers seek to gain further prominence. Securiti has not been as obvious as some of its competitors at recent events, such as the RSA Conference, but through a keen focus on its designated target market and leveraging its relationships with global system integration partners, it is cultivating brand equity along alternative routes. With ambitious growth targets, the organization is taking a smaller brand profile in its stride.

If history provides any indication, small organizations that show promise in the DSPM domain are often targets for larger organizations looking to expand their existing data security portfolios or create new ones. Securiti runs this risk as it continues to secure success. From this point of view, some may view its long-term survival as an issue as it continues to grow. So far, the company has grown and developed well, but it needs to be mindful of interest from some of the larger providers in the broader IT market. This may be perceived as a limitation by end-user and partner organizations looking for longevity and the construction of longer-term relationships among their vendor community.

Sentra (Omdia recommendation: Challenger)

Sentra should appear on your shortlist if you are a cloud-centric medium to large organization looking for strong data discovery and classification to provide a foundation for a wider data security platform.

Overview

Sentra was born as one of the DSPM pioneers in 2021. It delivers its DSPM capability, the Sentra Data Security Platform, as a cloud-based service (that is, in SaaS mode). Assessing the deliverables, the organization focuses on discovery and classification at one end of the DSPM spectrum, with accompanying posture management services at the other. Consequently, its score for core capability is in the mid-range (**Figure 12**) but with compensation via advanced capabilities for solution breadth ultimately in the upper mid-range.

The privately owned organization does not declare revenue or growth figures, although it recently announced it closed a $50 million Series B funding round, led by Key1 Capital with participation from existing investors Bessemer Venture Partners, Zeev Ventures, Standard Investments, and Munich Re Ventures. The funding brings Sentra's total investment to more than $100 million, following a more than 300% year-over-year increase in revenue and the addition of multiple new Fortune 500 customers. Omdia sees the organization clearly achieving growth and market momentum, although it is still a comparatively small vendor. As such, delivery across the full range of DSPM functionality is perhaps a challenge. What it does do, it focuses on and does well.

Sentra's platform delivers four key capabilities: discovery, classification, assessment, and remediation.

The vendor provides a multicloud data security platform that works across AWS, Azure, GCP, Oracle Cloud, Snowflake, Microsoft 365/SharePoint, Databricks, and other cloud environments, supporting a growing series of SaaS, IaaS, and DBaaS platforms. It makes no changes to the customer's environment as the data never leaves its location and is designed to have no impact on how well the customer's applications perform.

Sentra's agentless data discovery automatically and continuously discovers data stores without affecting workload performance and without the need to configure the connection to the data store or provide specific credentials. This allows it to find both known and unknown (shadow) data.

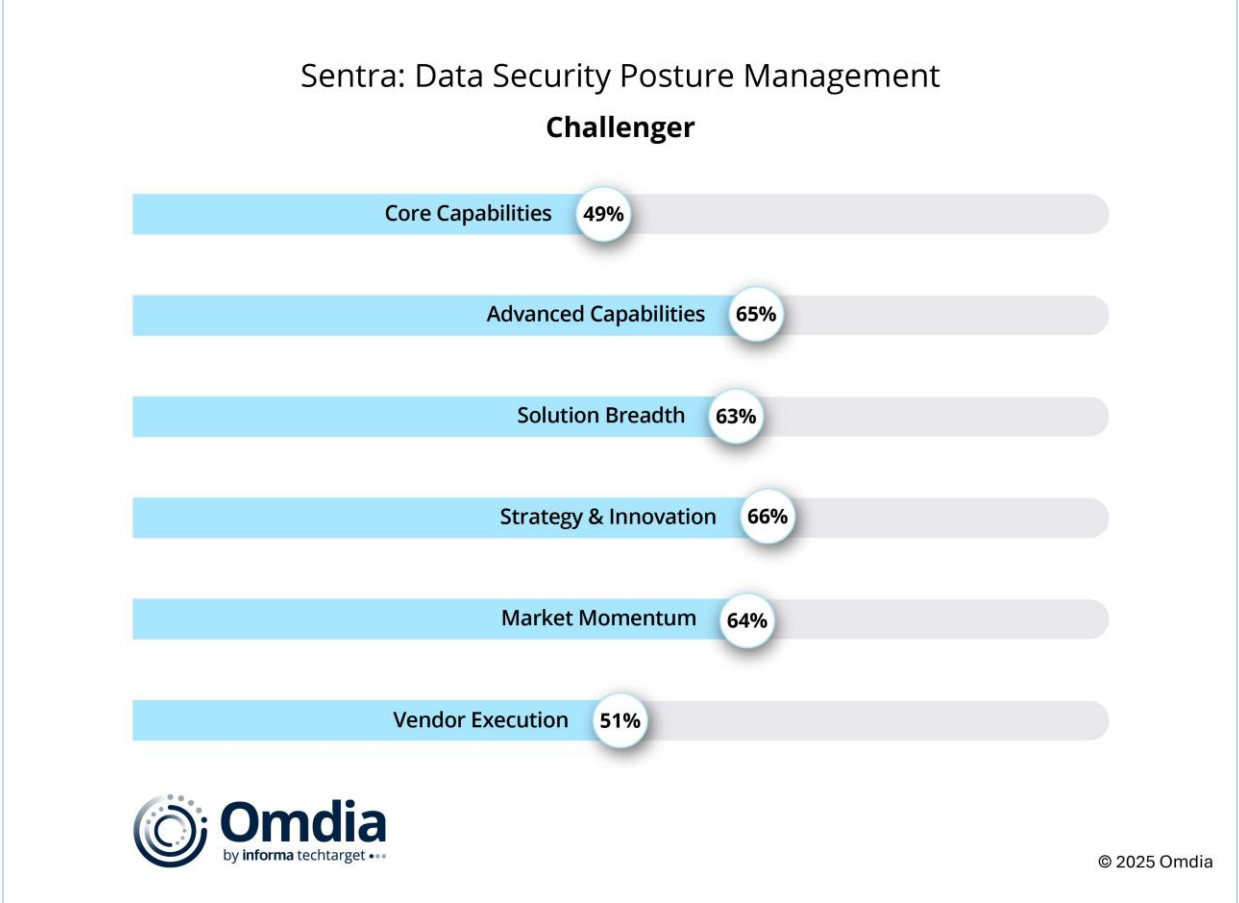
Leveraging ML and metadata clustering, Sentra automatically classifies data, detecting PII, PCI, PHI, information about an organization's intellectual property, or even secrets such as access codes that a developer has unwittingly left in the data. It automatically labels proprietary data, including customer data, HR data, or intellectual property. It can identify toxic combinations of data using a composite data classifier customized to the customer's bespoke concerns.

Sentra assesses the sensitivity of the data against the information it has regarding extant access permissions, user activity in that data store, and any misconfigurations it has detected. Additionally, it accounts for data movement—how the data moves through the customer organization—which involves looking at extract, transform, load (ETL) and extract, load, transform (ELT) tools, as well as data pipelines. The net result of the assessment phase is the allocation of a risk score to each data store, enabling the customer to prioritize the most critical issues and move to the fourth phase, remediation.

The Sentra platform goes on to perform remedial actions, including the reduction or complete removal of access rights, alerting against unusual data movement for further investigation, and deletion of a data store that is deemed surplus to requirements. It integrates with common security tools such as Jira, Splunk, and Slack.

Sentra is focused on the North American market, and it retains customers in EMEA, India, and Australia. Although this is a relatively narrow customer base, the vendor scores well for strategy and innovation because of its focus and defined roadmap. Sentra has a small network of reseller partners, all based in North America, giving it good coverage for the region.

Figure 12: Omdia Universe ratings—Sentra



Source: Omdia

Strengths

Sentra's primary strength is its innovation. It retains the ability to efficiently scan and classify vast amounts of data in cloud environments using novel grouping techniques and AI/ML, while also providing a deep understanding of data access and movement through its Data Authorization Graph, enabling proactive security posture management and threat detection. Sentra simplifies complex data security challenges with highly accurate visibility and actionable insights.

Sentra is further able to automatically discover and identify AI agents, their knowledge bases, and sensitive data assets that they connect to. The vendor is then able to identify which users interact with these agents, the data that is exposed to them by the AI agent, and the risk that this creates. Least privilege access is also enforced to reduce data exposure, together with out-of-the-box policy alerts for unauthorized access, such as public exposure to an AI agent trained on sensitive data.

With its focus on discovery and classification, the vendor facilitates the efficient scanning of petabytes, offering a 100x improvement on the speed of competitors—a key advantage.

Limitations

Sentra is a small organization in this market, with a small customer and partner base that is fundamentally in one geography, albeit the biggest marketplace. The organization is working to build its business quickly and is showing that it is achieving the necessary steps toward this. Right now,

however, its size could be seen as a limitation, particularly for larger organizations looking for more expansive or more defined platform propositions.

Given its size, the organization does not yet deliver across the full spectrum of DSPM propositions. Through its data discovery and data classification, along with the other technologies it delivers as part of its DSPM proposition (DDR, data access governance [DAG], DSAR, and secure AI), the vendor offers a strong alternative perspective. The absence of the more mainstream DSPM components around data protection and identity management/access control could limit sales opportunities, particularly for organizations looking for a comprehensive solution. Sentra partners to address some of the omissions, providing close integration with Microsoft Purview to expand on its core capabilities, for example. Although this naturally requires customers to be licensed for Purview as a prerequisite, Sentra is able to refine Microsoft's out-of-the-box labeling to enhance the Microsoft DLP proposition.

Skyhigh Security (Omdia recommendation: Prospect)

Skyhigh Security should appear on your shortlist if you are a cloud and data-centric organization looking for new approaches toward data protection spearheaded by data discovery and classification.

Overview

Skyhigh Security is one of the later entrants into the DSPM market, launching its proposition in 2025. The company's heritage is much longer, however. Originally, Skyhigh Networks was founded in 2011 by Rajiv Gupta, Sekhar Sarukkai, and Kaushik Narayan to protect an organization's sensitive data by providing visibility, control, and usage of cloud services. On November 27, 2017, McAfee stepped in and announced a definitive agreement to acquire Skyhigh Networks. The deal closed in January 2018. In March 2021, McAfee announced that private equity firm Symphony Technology Group (STG) had acquired its enterprise business for $4 billion. In March 2022, STG relaunched a cloud portfolio, including the former Skyhigh Networks, as Skyhigh Security.

Although a comparatively new entrant, Skyhigh Security delivers a highly creditable DSPM capability in Omdia's assessment, and it achieved a Best in class rating for its advanced features and functionality (**Figure 13**). Overall, it offers a very capable Top-tier solution in terms of core capabilities, solution breadth, and vendor execution.

The Skyhigh Security data discovery functionality is good, but there are gaps compared to some of the competition when it comes to structured data in some databases. Oracle, SQL, and DB2 ,for example, are not supported.

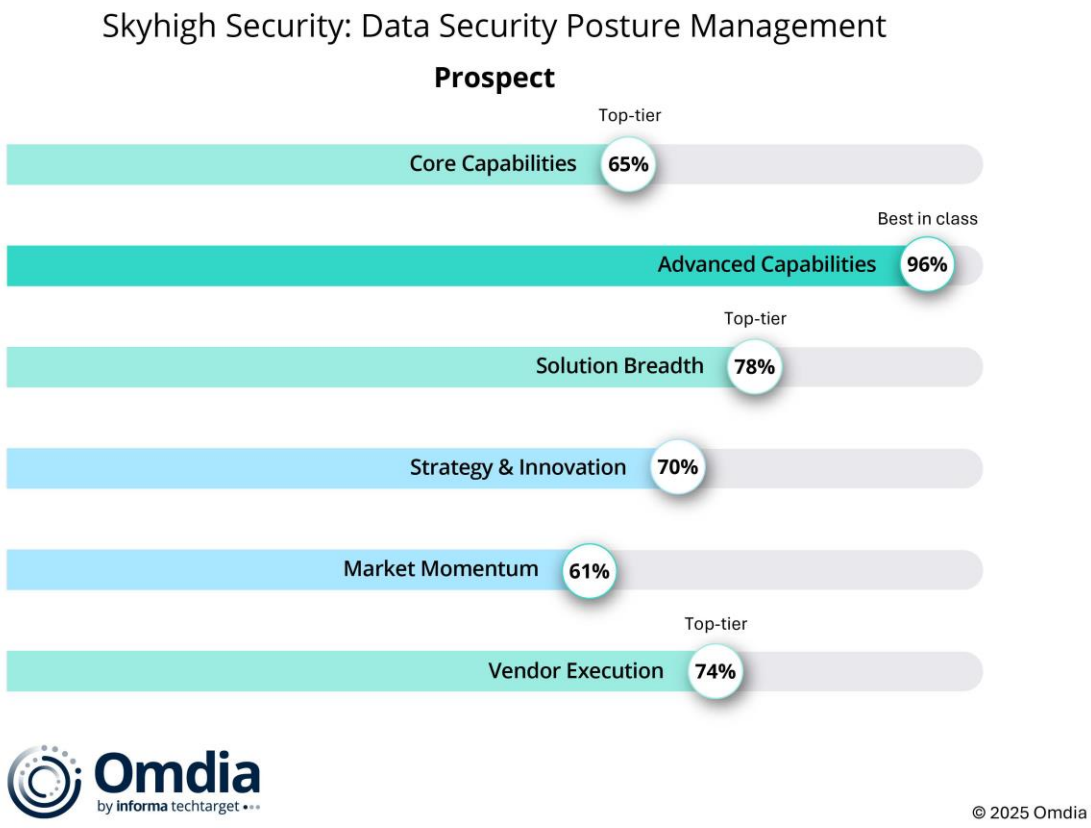
However, Skyhigh Security takes a differentiated approach by fingerprinting this data, enabling discovery not only at rest but also in motion. Skyhigh Security's classification capability is comprehensive, with excellent support across a wide range of file types and operating systems.

Like several others, Skyhigh Security's core capabilities focus on data discovery and classification without defined in-house encryption and have limited tokenization, data masking, and identity management. The vendor's investment is clear at the posture management end of its portfolio, where the company offers a very comprehensive mix of tools and services.

The vendor achieves good results with strategy and innovation and, together with its Top-tier execution rating, registers a satisfactory market momentum for a vendor with a newer proposition. It has a strong focus on where it feels opportunities will emerge and a balanced approach to global markets, with offices and service centers across 14 countries. As would be expected, the company targets, though not exclusively, the North American market. Its go-to-market model leans toward a strong direct model, yet it still retains a higher number of partners than a direct model would suggest.

Overall, Skyhigh Security emerges very positively from this assessment and is a strong prospect moving forward. It offers an expanse of capabilities more associated with a larger or more established vendor, highlighting how the organization positions itself well in a crowded market.

Figure 13: Omdia Universe ratings—Skyhigh Security



Source: Omdia

Strengths

Skyhigh Security's premier strength is in its posture management tools and services. This advanced functionality is key to maintaining the levels of data security standards required by any business. Data has to be secure at all times—currently and in the future. Having the right tools is a critical first step, but any organization must ensure that what is put in place today is future-proofed moving forward. Skyhigh is able to deliver a top-level capability in this department.

Skyhigh offers a strong capability in discovery and classification, and although the vendor does not score as high as some in the core capability section overall, it has a very good proposition in these two areas.

The vendor has invested in integrating commendable levels of innovation into its DSPM proposition. Technologies such as exact data matching, indexed document matching, ML auto classifiers, optical character recognition (OCR), and large file processing all provide suitable strengths. The vendor also provides visibility and control of data in shadow IT, over 40 sanctioned web, email, and private apps. Closed-loop remediation is provided, as well as real-time inline prevention for data in motion and near-real-time prevention for data at rest. The vendor has clearly spent some time thinking through key attributes to offer to its customer base.

Skyhigh Security offers a range of capabilities and, as such, provides broad functionality across key areas. For end users looking for comprehensive solutions or platforms—one-stop shop provisioning—Skyhigh Security could be a very suitable option.

Limitations

Skyhigh Security's comparatively late entry into the DSPM market may hold it back in an environment not only populated by DSPM vendors that have been in from the start but also now by much more familiar and sizable players that have added DSPM to their broader portfolios. It is a competitive market and one where smaller players run a considerable risk of acquisition as soon as they show promise, as has been highlighted by a number of previous instances. Skyhigh Security needs to be mindful of the competition, their buying power, and the vendor's attractiveness as an M&A target.

A key limitation at the product level is the inability to autonomously remediate every risk tied to sensitive data. Although an SSE-driven DSPM excels at providing visibility, context, and actionable insights, it generally lacks the permissions or mandate to fix all issues directly. To bridge this, Skyhigh Security could integrate with privileged access management (PAM) or CIEM solutions to extend remediation capabilities.

A direct model is among the minority of vendor go-to-market strategies out there today, and the organization may find itself restricted in terms of coverage with this approach. Partners provide a vast extension to in-house sales teams in addressable market coverage and in discovering revenue generation opportunities. Skyhigh Security may be limited in securing all the required opportunities without a more partner-centric model. The organization retains a large partner base, which it employs across the rest of its business. Extension of this model to the DSPM business would inevitably benefit the vendor and is under evaluation.

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.

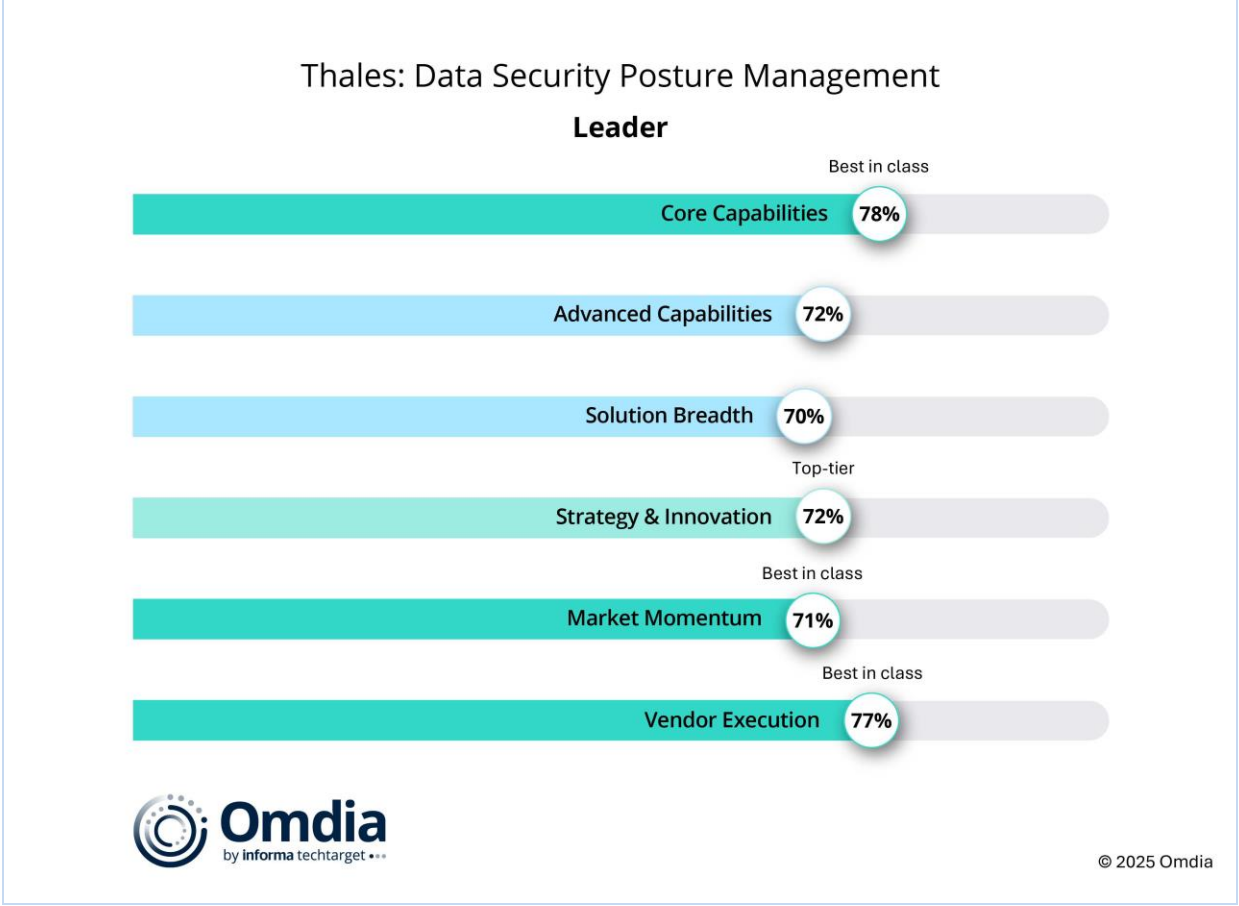
Thales has a roadmap to address this, but some functionality is currently lacking. There are comprehensive encryption, tokenization, and data masking capabilities, as well as the necessary remediation piece that providers in this category can lack natively. As expected from an experienced provider, the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

Varonis (Omdia recommendation: Challenger)

Varonis should appear on your shortlist if you are looking for an experienced vendor with an emphasis on assessing and managing data security posture.

Overview

Varonis was founded in 2005, giving it more heritage than some of the vendors it competes with. It launched its DSPM proposition in 2022, contributing its own brand authority to what was then a fledgling technology. The vendor's cloud native Unified Data Security Platform operates continuously to discover and classify critical data, removing identified exposures and detecting threats in all their various guises with AI-powered automation.

Varonis offers a comprehensive solution in its Data Security Platform, with a highly competitive offering within its discovery and classification tools. The proposition lacks comprehensive in-house encryption, however, deferring to third parties in some cases, but can offer FIPS 140-2 Level 2 and 3, especially for Microsoft Exchange and SQL Server. Data masking within databases is provided

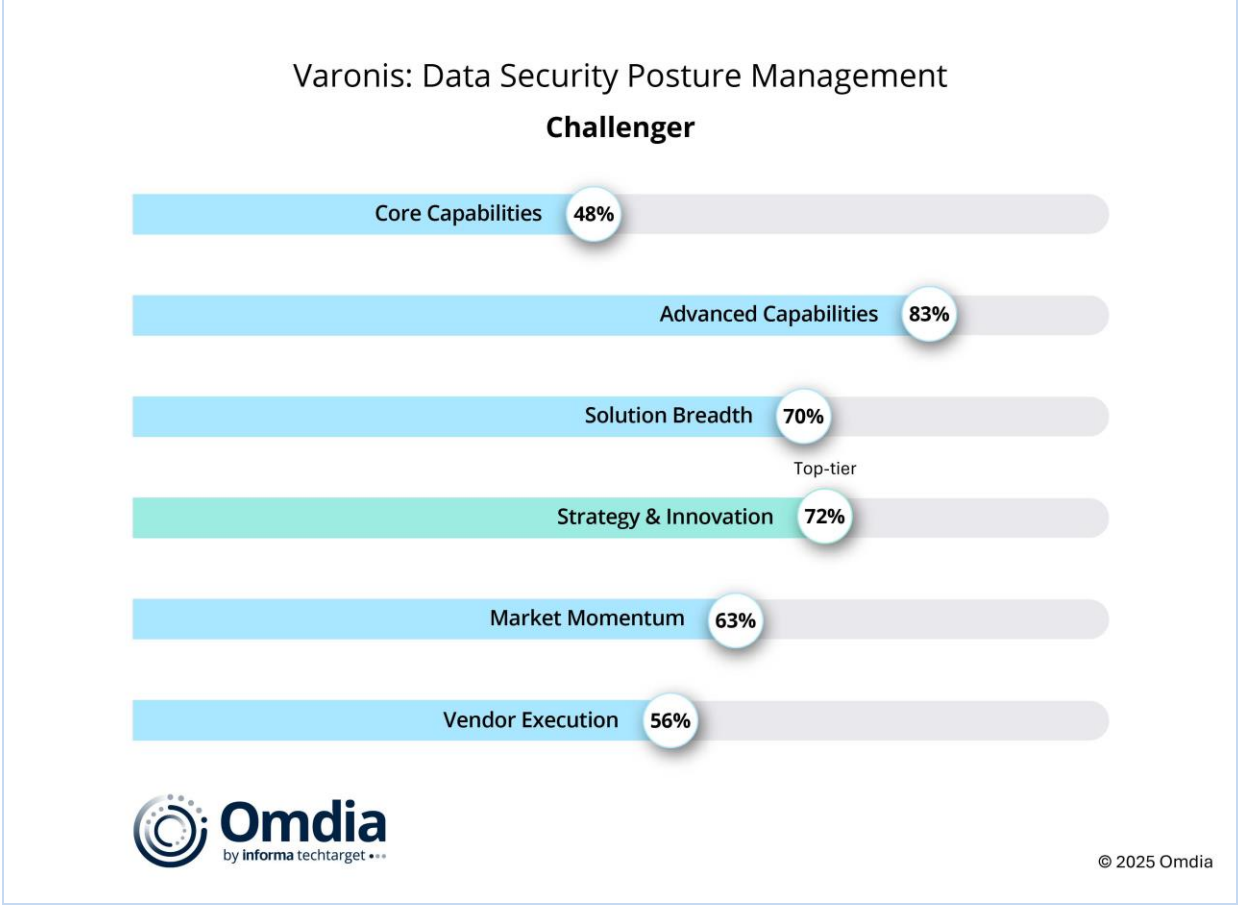
natively, while it partners with third parties for format preserving tokenization. Varonis provides some identity management, such as MFA and centralized identity management.

Varonis achieves a very creditable rating (**Figure 15**) for its more advanced DSPM features (posture management, analysis, monitoring, and response planning in particular), and although it has a few minor gaps, it is generally very strong across the board—a combination which gained it a Top-tier rating for the strategy and particularly innovation. Combining core and advanced features, the vendor provides a competitive and well-thought-out platform.

Varonis has offices and support centers across 13 countries and operates a wholly indirect model through a network of over 2,000 partners. Its customer base extends across all regions and geographies, in a balanced approach that prioritizes North America but retains a healthy base in EMEA, commensurate with the region's relative market size.

The Varonis Unified Data Security Platform is where the organization's DSPM proposition is located, although interestingly, the organization structures discovery and classification separately outside its DSPM definition on its website. Nevertheless, the platform also delivers wider integrated capabilities in user and entity behavior analytics (UEBA), identity protection (again defined as separate from DSPM), data access governance (DAG), DLP, and more, all powered by its Athena AI engine. The addition of DLP in particular is substantially beneficial. The Varonis DSPM proposition needs to be considered in this wider context, and this is a plus for the organization, illustrating the detailed thought process outlined above.

Figure 15: Omdia Universe ratings—Varonis



Source: Omdia

Strengths

Varonis offers its DSPM platform as part of a wider portfolio, which itself sits amid a much boarder portfolio of cybersecurity capabilities. Although it is not alone in the market from this point of view, it is nevertheless a strength to have a platform (an integrated set of products and functionality) available. Having a DLP capability is also a significant advantage because, once classified, a DLP tool stops unauthorized distribution internally and externally where policy is contravened. DLP has to operate with effective classification and vice versa for a robust data security proposition.

Varonis has a long heritage in the data security space and advocates a data-first approach. Data has long been seen as just a part of the overall cybersecurity equation and is often ignored as focus is given over to robust defenses to keep bad actors out. Omdia is patently aware that this strategy is insufficient in today's threat landscape. Data now needs specific protection, and sensitive data even more so. Varonis offers customers the peace of mind that protection of their most critical assets—their data—is its first and foremost consideration. This viewpoint is not always top-of-mind for vendors.

Varonis has a large patent ownership and patent pending pipeline, together with a rich, defined product roadmap. These elements go together to highlight the innovation the organization is applying to ensure its products continually deliver optimal capabilities to meet end users' needs throughout its customer base.

The Varonis website is rich in quotes, case studies, and feedback from customers. Customer testimony is a definite strength. Despite the anonymization of many of the case studies, enough have been published, along with the quotes elsewhere on the site, to indicate that customers are happy with the company's service and execution. (Note: This is somewhat contradicted by the rating for execution illustrated in Figure 15. The rating above is based on submitted data. For reasons of legitimate non-disclosure, Varonis has not provided information, which has resulted in the score seen.)

Limitations

A focus on the North American market, as it is the largest, is a good strategy, but the vendor runs the risk of placing too much emphasis on this area. Its revenue streams are nevertheless large, but expanding its relatively small installed base in Asia & Oceania, in particular, would yield further opportunities and pipeline. Organizations in less covered geographies may feel the vendor is focused elsewhere. For a vendor of Varonis's size, some organizations looking for Varonis' own expertise or that want to work with local Varonis representatives may see having only 13 local offices as a limitation. However, Varonis's 100% channel model should provide adequate compensation for this.

The vendor has a comprehensive solution, although with some adjustments to the website details, the proposition would receive better representation. The vendor could avoid possible confusion around what is and what is not DSPM, given some of the key elements of a DSPM platform—discovery and classification, especially—sit outside of the DSPM description on the company's platform overview. Possible limitations could be associated with this.

Lastly, Varonis works with third parties to provide elements of its technology (e.g., encryption, tokenization). Some end users, on a path toward vendor consolidation, may have reservations regarding new, multivendor propositions. A channel model helps with the overall engagement, and a reseller or systems integrator would, in all probability, provide the primary interface with the client, establishing a single point of contact and avoiding a multivendor management scenario.

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

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, TechTarget and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com