Cybersecurity INSIDERS

The 2024 DSPM Adoption Report

CYERA

Introduction

With 90% of the world's data being created in the last two years, and the total amount of data set to reach 181 Zettabytes in 2025, IT and security teams are under pressure to help their business leverage data to support key business initiatives, without exposing its data to risk. The challenges of identifying, monitoring, and protecting sensitive information have intensified. Many organizations struggle with fragmented tools and limited data discovery, as well as manual and weak classification accuracy that fail to scale, leading to data security blind spots that expose critical data to risks. This new reality has paved the way for a new security category to dramatically rise in popularity. Data Security Posture Management (DSPM) has become vital for providing continuous visibility, automatic classification, and security posture of sensitive data spread across growing SaaS, IaaS, PaaS, and existing on-premises environments.

This 2024 DSPM Adoption Report is based on a comprehensive survey of 637 IT and cybersecurity professionals that reveals how organizations are approaching DSPM, the challenges they face, the effectiveness of their current solutions, and their adoption plan over the next 12 months. Through this survey, we uncover the critical needs and priorities of enterprises when it comes to securing their data across various environments.

Key Survey Findings

- **DSPM Adoption on the Rise:** DSPM is becoming the fastest-growing security category with 75% of organizations saying they will adopt DSPM by mid-2025. This is a faster rate of adoption than that of Security Service Edge (SSE) solutions, Extended Detection and Response (XDR), and Cloud Security Posture Management (CSPM). This rapid adoption reflects the recognition that DSPM is crucial for managing data security risks in modern, multi-environment infrastructures, especially given the vital role that data plays within the business.
- **Visibility Gaps Weaken Security Postures:** An overwhelming 83% of respondents believe that a lack of visibility into data is weakening the overall security posture of their organizations. This underscores the need for tools that provide comprehensive and real-time visibility into sensitive data across all environments.
- **The Data Discovery and Data Classification Gap:** A staggering 87% of enterprises find their current data discovery and classification solutions lacking, with only 13% considering them very effective. This underscores a critical deficiency in data security practices, emphasizing the urgent need for more precise and automated solutions to safeguard sensitive information.
- **Challenges in Detecting and Responding to Exposures:** More than 60% of organizations do not feel confident in their ability to detect and respond to data security and privacy exposures. This highlights a critical gap that must be addressed through enhanced monitoring, automated response capabilities, and better alignment between detection tools and security strategies.
- **Core DSPM Features:** Real-time data monitoring (43%), data discovery (38%), and data classification (35%) are seen as the core features that enterprises should prioritize in any DSPM proof of value engagement. These features are essential for providing the visibility and control needed to secure sensitive data effectively, as real-time monitoring and integration with discovery and classification have been historically lacking.

We would like to extend our gratitude to Cyera for their insights and valuable contributions to this report. Their expertise in the data security space has been instrumental in creating this important research.

As organizations continue to navigate the complexities of data security, we hope this report, which is generated by the responses of your peers, provides valuable insights and practical guidance for strengthening your data security posture. By addressing the challenges outlined and prioritizing the key features and strategies discussed, we are confident that your organization will be well-equipped to manage the risks associated with sensitive data in the years ahead.

Best,

Holger Schulze

Founder, Cybersecurity Insiders

Today’s Biggest Data Security Challenges

Data security remains a top priority for organizations as they navigate an increasingly complex threat landscape. Data security is top of mind for organizations due to the rapidly increasing frequency and cost of data breaches. This growing financial and business impact, along with the complex regulatory landscape and the expanding use of cloud and AI technologies, makes it essential for organizations to enhance their data security posture. The primary challenges around data security today, as reflected in the report, highlight the tension between ensuring robust data protection and managing data access and visibility within diverse environments.

The results reveal that 57% of respondents view excessive data access—often stemming from overprivileged accounts—as a pressing concern. Overprivileged access to data, along with the lack of visibility into sensitive data—cited by 50% of respondents as a significant challenge—are the two greatest data security challenges today. This validates the need for a stronger correlation between identity and data access, ensuring that only the right individuals have access to the right data at the right time. Managing exceedingly large amounts of data was also cited by 46% of respondents, reflecting the growing difficulties in maintaining control over expanding data sets, particularly in hybrid and cloud environments.

What are the primary challenges around data security today?

57% Excessive data access, overprivileged accounts

50% No visibility into the sensitive data that exists in the environment

46% Data management, managing large amounts of data

43% Need to deal with sensitive personal data

Given these findings, organizations should prioritize implementing solutions that enhance visibility and control over sensitive data without stifling business operations. Focusing on technologies that enable granular data discovery, coupled with automated policy enforcement, can help mitigate the risks associated with both overprivileged access and poor data management. Moreover, maintaining a comprehensive and real-time view of sensitive data will allow organizations to proactively address security gaps and avoid the pitfalls of excessive or restrictive access controls.

Additional responses include: Data accuracy given incomplete data visibility, which can lead to incorrect conclusions 39% | Concerns over restrictive data access - overly-constrictive controls 35% | Lack of visibility or control over how SaaS services transfer and use sensitive data 33% | Other 1%

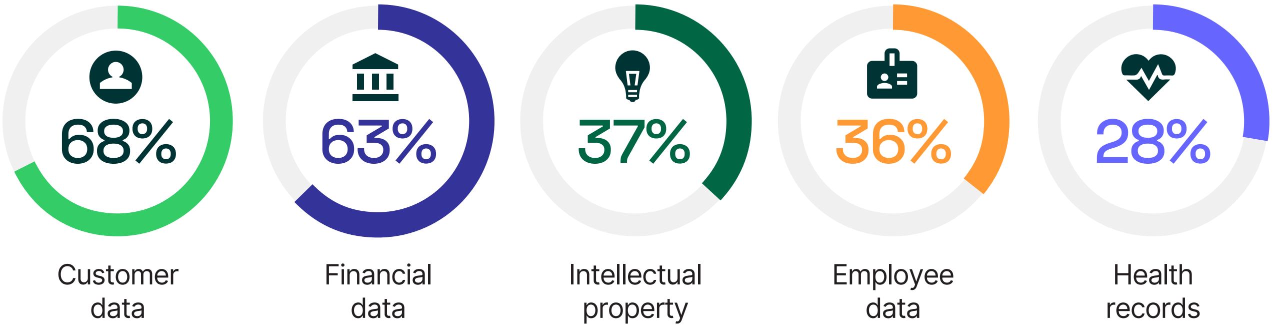
Critical Data at Risk

Because data breaches have far-reaching consequences, understanding which types of data organizations are most concerned about is crucial for shaping effective security strategies.

The survey reveals that customer data, at 68%, and financial data, at 63%, are by far the top concerns for IT and cybersecurity professionals, reflecting the value and high stakes associated with the compromise of these types of information.

Customer data is the most valued, as it directly impacts customer trust and brand reputation. Financial data follows closely, given the potential for immediate monetary loss and regulatory repercussions. Intellectual property, cited by 37% of respondents, underscores the importance of safeguarding proprietary information which can protect a company's competitive edge within the market. Interestingly, employee data and health records are still significant concerns at 36% and 28% respectively, highlighting the breadth of data types that organizations must protect.

Which types of data are you most concerned about being compromised?



Organizations should ensure that their security posture is tailored to protect these critical data types, with an emphasis on technologies that offer robust encryption, access controls, and continuous monitoring. As customer and financial data are the top priorities, implementing data-centric security measures that focus on these areas can help prevent breaches and mitigate the impact should they occur. Additionally, aligning data security measures with the specific risks associated with each type of data—such as intellectual property or employee information—will create a more resilient and adaptive security framework.

Additional responses include: Operational data 22% | Partner data 19%

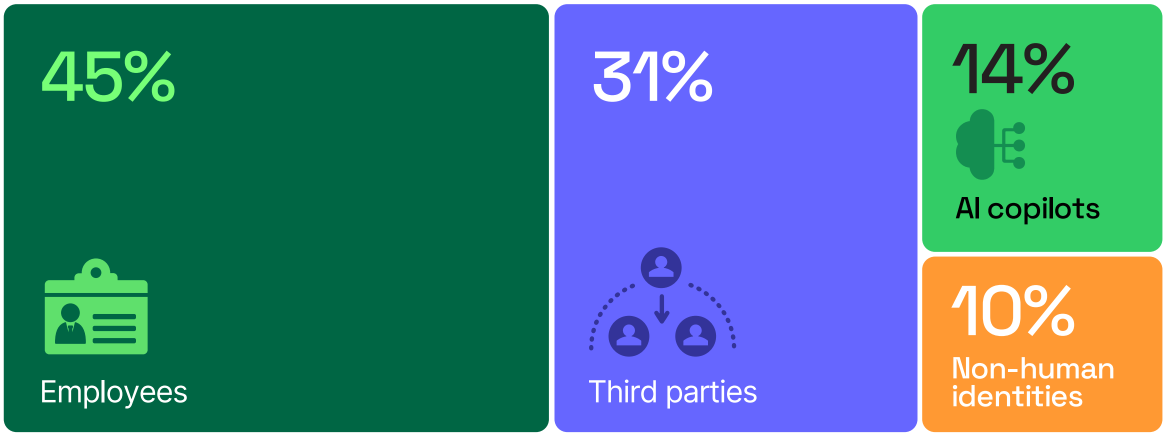
Insider and Third-Party Risk

Understanding which entities pose the greatest data security risks is crucial for organizations as they seek to protect sensitive information from both internal and external threats.

The survey results reveal that employees, at 45%, are seen as the most significant concern, highlighting the ongoing challenge of insider threats. This is particularly critical as employees often have extensive access to sensitive data as part of their daily job, and often switch roles throughout their tenure at an organization, making them a potential weak point in an organization's security posture.

Third parties, including partners, contractors, and auditors, follow at 31%, underscoring the risks associated with external relationships. As organizations increasingly rely on third-party services, the potential for data exposure grows, making it essential to manage and monitor these interactions carefully. The risk grows exponentially as "Nth party" users, the third-parties of third parties, will often require access to company data as well. The rising concerns around AI copilots (14%) and other non-human identities (10%), such as IoT devices, combining for 24%, point to the new challenges posed by emerging technologies, which can introduce vulnerabilities if not properly secured.

What entity are you most concerned about from a data security perspective?



To address these concerns, organizations should adopt a comprehensive data security strategy that includes visibility into what sensitive data is accessible by insiders, rigorous third-party data access visibility and control, and proactive measures to secure AI and IoT technologies' access to data. By doing so, they can reduce the likelihood of data incidents from both existing and emerging threats, ensuring that sensitive information remains protected.

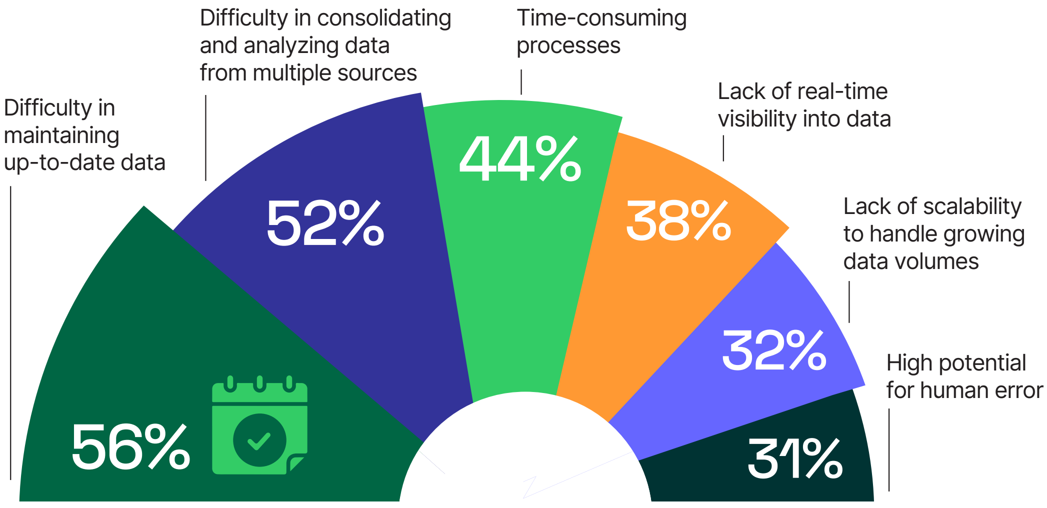
Data Discovery Roadblocks

Discovering and managing sensitive data is the foundation of any successful data security program or strategy because it directly impacts an organization's ability to protect its most critical digital assets. Without effective data discovery organizations face significant risks, including high exposure to data security risks, non-compliance with regulations centered around data, and the inability to mitigate the impact of data incidents in a timely manner.

The report reveals that organizations face numerous challenges in this area, which can impede their ability to protect sensitive information and respond to emerging threats. The most significant challenge, cited by 56% of respondents, is the difficulty in maintaining up-to-date data. Lack of continuous data discovery exacerbates this issue, making it difficult for teams to stay current with the ever-changing data landscape. Additionally, 52% of participants report challenges in consolidating and analyzing data from multiple sources, a problem that is often compounded by the lack of support across heterogeneous environments—cloud, SaaS, DBaaS, and on-premises. This creates significant barriers to obtaining a unified view of data across these diverse platforms.

Time-consuming processes and the lack of real-time visibility into data, noted by 44% and 38% of respondents respectively, further emphasize the inefficiencies that hinder effective data security. These issues not only slow down response times but also increase the risk of missing critical security events. Moreover, the lack of scalability (32%) and the high potential for human error (31%) indicate that many organizations are struggling to keep pace with the growing volume of data and the intricacies involved in managing it securely.

What challenges do you experience with your current data discovery methods?



To overcome these challenges, organizations should invest in advanced data discovery capabilities that offer automation, real-time visibility, and scalability across heterogeneous environments. These solutions must also support a mix of structured, unstructured, and semi-structured data. By doing so, they can reduce the manual effort involved, minimize the risk of errors, and ensure that their data security posture remains strong as data environments grow and evolve.

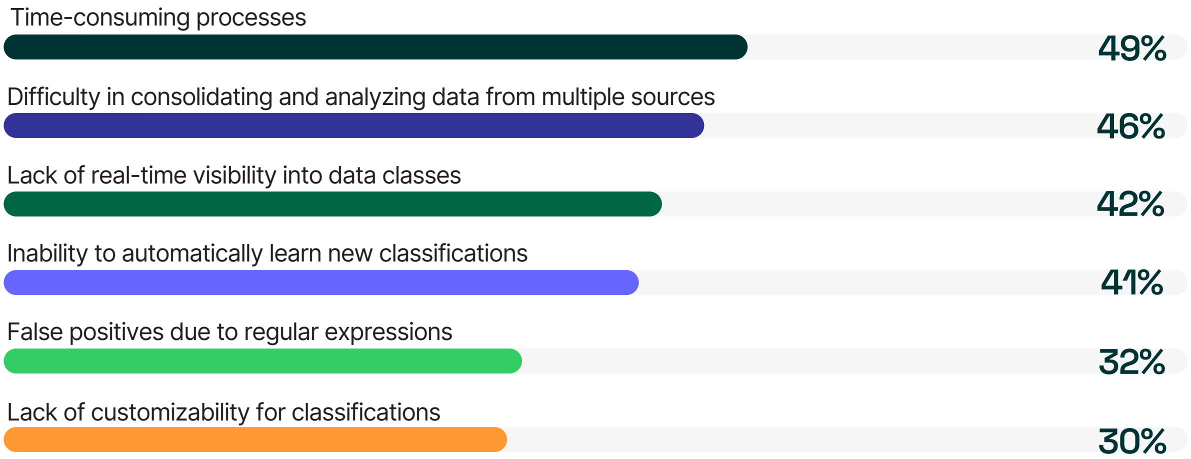
Data Classification Hurdles: Automation Is Key

Following data discovery, the next critical step in a robust data security strategy is data classification, enabling organizations to identify and prioritize the protection of their most sensitive information. However, the report reveals significant challenges organizations face with their current data classification methods, which can severely undermine the effectiveness of their overall data security strategy.

The most pressing issue, identified by 49% of respondents, is the time-consuming nature of data classification processes. This challenge is largely due to the lack of automation and a continued reliance on manual methods, which slows down the process and increases the risk of leaving sensitive data exposed for longer than necessary. Similarly, 46% of participants report difficulties in consolidating and analyzing data from multiple sources, reflecting the complexities of managing classification across diverse environments, such as cloud, SaaS, DBaaS, and on-premises systems.

A lack of real-time visibility into data classes, cited by 42% of respondents, further exacerbates these challenges, making it difficult for organizations to maintain an up-to-date understanding of their data landscape. The inability to automatically learn new classifications, noted by 41%, highlights a significant gap in adaptability, which is crucial in dynamic data environments. False positives due to regular expressions (32%) and a lack of customizability (30%) also present barriers, potentially leading to misclassified data and inefficient protection measures.

What challenges do you experience with your current data classification methods?



To address these challenges, organizations should consider adopting advanced data classification tools that offer automation, real-time visibility, and adaptive learning capabilities. These capabilities can be found within DSPM solutions that use Large Language Models (LLMs) to classify data that is unique to the organization or a particular industry. By integrating these features, companies can streamline the classification process, reduce the reliance on manual efforts, and ensure that their data is accurately classified and protected according to its sensitivity. Additionally, enhancing customizability and reducing reliance on rigid regular expressions will allow for more precise and context-aware classifications, ultimately strengthening the organization's data security posture.

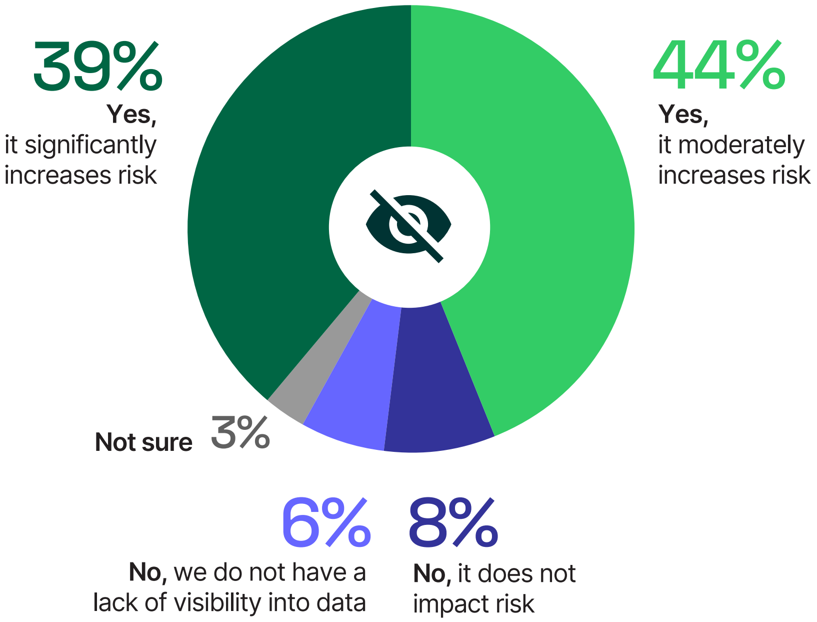
Impact of Data Visibility on Security Posture

Data visibility is a cornerstone of a strong security posture, as organizations must know what data they have, where it resides, and how it is being accessed in order to protect it effectively.

The survey results underscore the critical nature of data visibility, with 83% of respondents acknowledging that a lack of visibility into data is weakening the overall security posture of enterprises. This reflects widespread concern about the risks associated with blind spots in data management.

Specifically, 39% of participants believe that insufficient data visibility significantly raises their security risk. This finding aligns with earlier concerns about overprivileged access and the difficulty in managing large amounts of data, emphasizing how these gaps in visibility can lead to vulnerabilities that are easily exploited by malicious actors. Only a small percentage (8%) believe that data visibility does not impact risk, suggesting that most organizations recognize the importance of having a clear and comprehensive view of their data.

Do you believe that a lack of visibility into data currently impacts your organization's overall security posture?



For organizations, it's essential to prioritize tools and processes that enhance their ability to locate, monitor, and manage sensitive data. Implementing continuous data discovery, combined with real-time monitoring, can help close the visibility gaps that currently expose organizations to unnecessary risk. By improving visibility, companies can strengthen their security posture and reduce the likelihood of data breaches or unauthorized access.

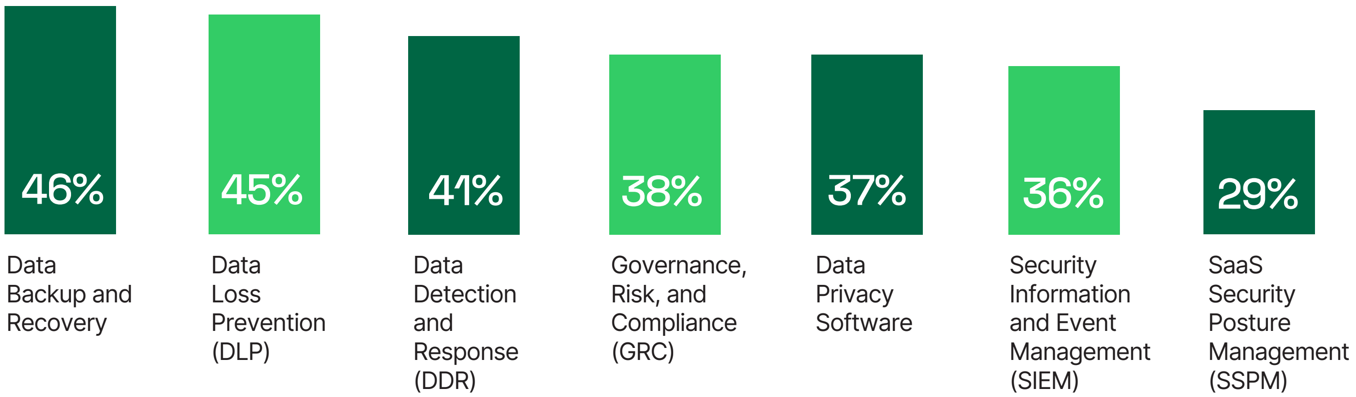
Current Methods for Data Inventory and Discovery

Effective data inventory and discovery are essential for maintaining a robust security posture, yet the survey results reveal that organizations are still relying on a diverse array of tools, many of which do not integrate seamlessly with one another. This fragmented approach can hinder the ability to stay up-to-date with changes in data and complicate efforts to analyze data across the environment, ultimately impacting overall data security.

The most commonly used methods include Data Backup and Recovery (46%) and Data Loss Prevention (DLP) solutions (45%). While these tools play crucial roles in protecting and recovering data, they often function independently, leading to silos that limit visibility and coordination across the organization. Data Detection and Response (DDR) is also widely used (41%), further confirming that teams are employing multiple specialized tools to address various aspects of data security.

Governance, Risk, and Compliance (GRC) at 38% and Data Privacy Software at 37% reflect the growing emphasis on regulatory compliance and privacy concerns, yet these tools also may not fully integrate with other discovery methods. Security Information and Event Management (SIEM) systems, used by 36% of respondents, provide valuable insights but often lack the comprehensive data visibility needed for effective discovery across hybrid environments. The use of newer approaches like SaaS Security Posture Management (SSPM) and Cloud Security Posture Management (CSPM), at 29% and 23% respectively, indicates a move toward cloud-focused solutions. Even so, it's important to note that unlike DSPM, SSPM and CSPM are not focused on data security, but rather the infrastructure or applications posture itself.

What methods or tools do you currently use for data inventory and discovery?



For organizations to overcome the challenges of tool fragmentation, it is critical to adopt solutions that integrate data inventory and discovery across environments. By focusing on platforms that offer comprehensive and unified data visibility, companies can streamline their discovery processes, reduce data silos, and ensure that they are fully equipped to manage and protect their data effectively in an increasingly complex landscape.

Additional responses include: Data Access Governance (DAG) 24% | Cloud Security Posture Management (CSPM) 23% | Data Security Posture Management (DSPM) 19% | Other 3%

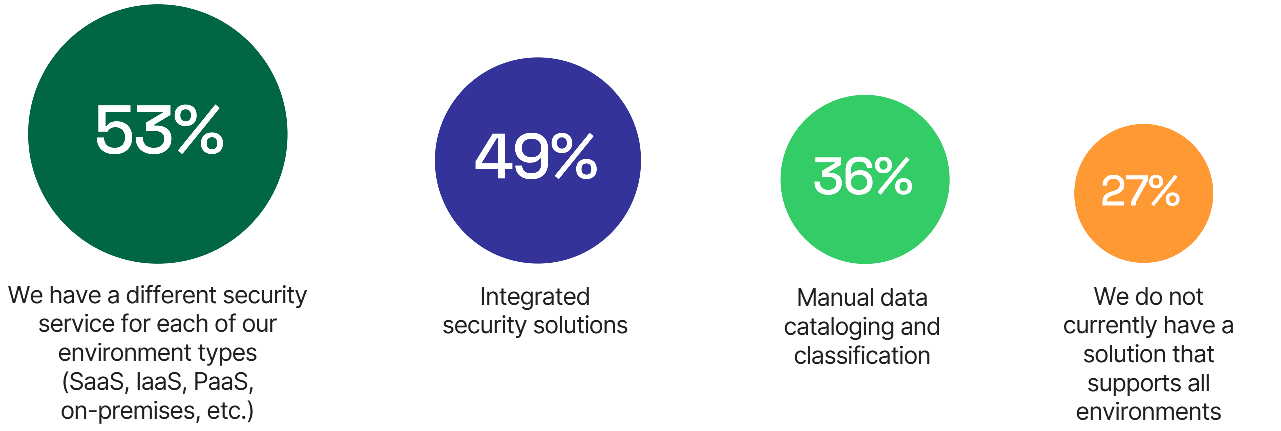
Methods for Gaining Visibility into Sensitive Data

Achieving comprehensive visibility into sensitive data across diverse environments is a growing challenge for organizations, especially as they manage data in cloud, on-premises, and hybrid settings. The survey results highlight the varied approaches that companies are taking to address this challenge, yet they also reveal significant gaps that undermine data security efforts.

Over half of the respondents (53%) indicate that they rely on different security services for each of their environment types, such as SaaS, IaaS, PaaS, and on-premises. This fragmented approach complicates data visibility and increases the likelihood of blind spots across the enterprise. While 49% of organizations have adopted at least some form of integration across security solutions, which offer a more unified view of data, it's clear that many companies still struggle to consolidate their security efforts across diverse platforms.

Additionally, a concerning 36% of respondents continue to rely on manual data cataloging and classification processes. This reliance on manual methods not only increases the risk of human error but also slows down the ability to respond to security threats quickly. Compounding this issue, 27% of organizations report that they do not currently have a solution that supports visibility across all environments, further exposing them to risk.

What methods do you currently use to gain visibility into sensitive data across different environments?



For organizations to strengthen their data security posture, it's critical to move away from siloed and manual approaches. Adopting integrated solutions that provide comprehensive visibility across all environments will help reduce gaps and improve the efficiency of data protection efforts. By streamlining data discovery and classification, companies can ensure they have a clear and real-time view of their sensitive information, regardless of where it resides.

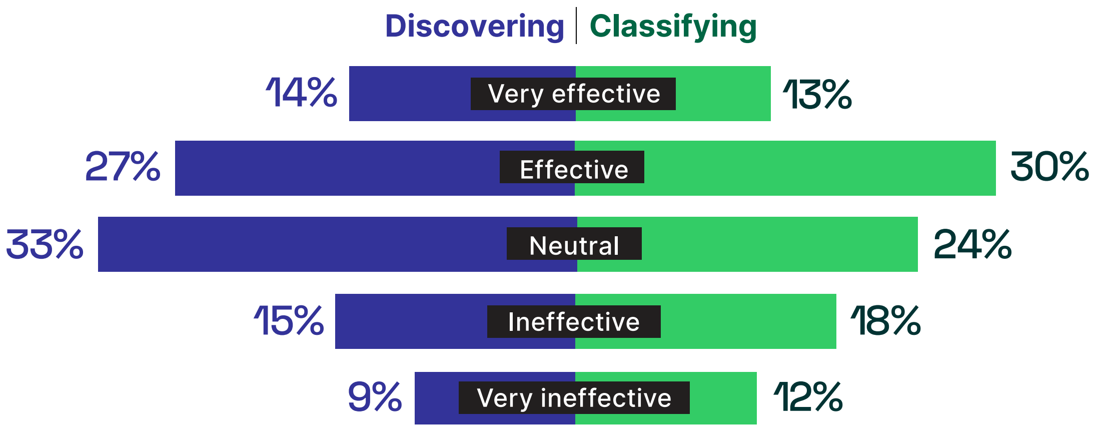
Effectiveness of Data Discovery and Classification

Understanding the effectiveness of data discovery and classification tools is essential for organizations aiming to protect their most critical sensitive data. The survey results reveal a mixed picture, highlighting both progress and ongoing challenges in these key areas.

When it comes to data discovery solutions, only 14% of respondents believe their discovery tools are very effective, meaning that 86% of organizations do not have complete confidence in their discovery capabilities. In comparison, data classification methods receive similarly low favorable ratings. Only 13% of respondents consider their classification tools to be very effective. This means that 87% of enterprises do not believe their classification methods are at the highest level of effectiveness, highlighting a need for better data classification solutions.

The fact that only a fraction of enterprises consider their existing discovery and classification solutions to be very effective underscores a critical gap in data security. Even when organizations can discover their critical data, they may struggle to classify it effectively, which undermines broader data protection efforts. This widespread lack of confidence suggests that many companies need to rethink and upgrade their data security repertoire.

How effective are your current methods or tools in discovering and classifying the most critical sensitive data within your environment?



To address these gaps, organizations should focus on integrating their data discovery and classification services, ensuring that once data is discovered it can be accurately and efficiently classified. The key should be to prioritize DSPM solutions that can provide data discovery at scale and within an appropriate time frame (days, not months or years), and combine this with classification that has high precision and automation for continued posture assessment. Investing in tools that enhance automation and reduce manual efforts will help shift more organizations from neutral or ineffective ratings to positive ones. By improving both discovery and classification, companies can better safeguard their most sensitive data and strengthen their overall security posture.

Additional responses include: We do not discover data today 2% | We do not classify data today 3%

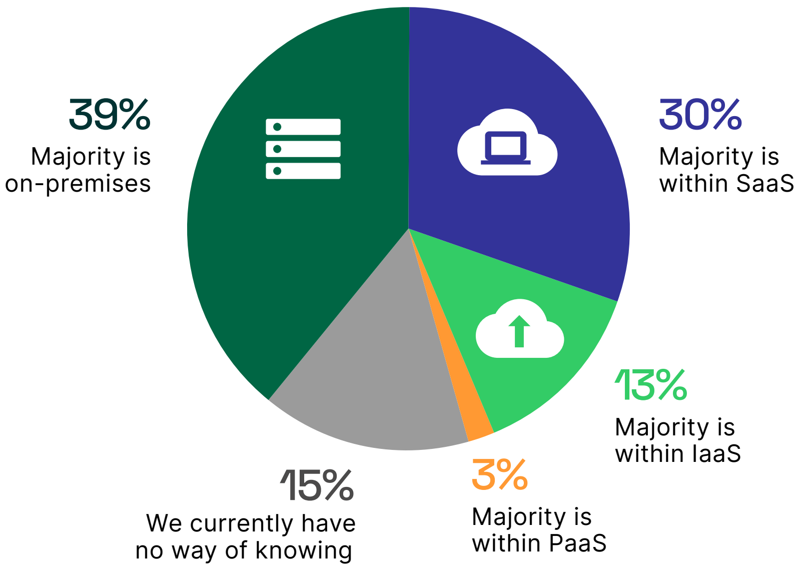
Location of Sensitive Data

In today's corporate environments, sensitive data is not confined to a single location but is scattered across a complex mix of on-premises systems, SaaS platforms, and cloud infrastructures. This dispersion makes it increasingly difficult for organizations to maintain comprehensive visibility and control over their most critical data, intensifying the need for robust security solutions that can operate seamlessly across all environments.

Nearly 40% of respondents report that the majority of their sensitive data remains on-premises, highlighting the continued need for strong on-premises data security. Next, 30% of organizations indicate that their sensitive data primarily resides within SaaS environments, reflecting the growing dependence on cloud-based applications. However, this shift also introduces new challenges in managing and securing data across multiple SaaS providers.

Alarmingly, 15% of organizations admit they have no way of knowing where their sensitive data is located, significantly increasing their exposure to potential breaches. An additional 13% report that the majority of their data resides in IaaS environments, further complicating the data management landscape.

Where does the majority of your sensitive data exist today?



This broad distribution of data across corporate systems underscores the necessity for comprehensive data security solutions that offer unified visibility and control across the entire data landscape. Without such tools, organizations risk leaving critical data undiscovered and unprotected, especially when they lack a clear understanding of where that data exists. Implementing integrated and scalable solutions will be key to overcoming these challenges and ensuring data security across all environments.

Critical Activities to Monitor for Data Security

Maintaining a strong data security posture requires vigilant monitoring of key activities that could indicate potential threats or vulnerabilities. The survey results reveal a clear prioritization of what professionals consider the most critical activities to keep under surveillance, with unauthorized and overprivileged access events emerging as top concerns.

Unauthorized access attempts are viewed as the most critical activity to monitor, with 58% of respondents highlighting this as a priority. This focus on unauthorized access aligns with the broader concern about protecting sensitive data from breaches, whether due to external attacks or insider threats. Closely related, 55% of participants emphasize the importance of monitoring overprivileged access for humans, reflecting the risks associated with granting excessive permissions that can lead to unintended data exposure or misuse.

Interestingly, overprivileged access for non-human identities—such as automated processes, bots, or IoT devices—is also seen as crucial, with 42% of respondents prioritizing it. This concern surpasses the need to monitor traditional activities like data removal (40%), usage patterns related to sensitive data (36%), and even industry compliance violations (31%). The emphasis on non-human identities underscores the evolving threat landscape where automation and connected devices are introducing new security risks if not properly managed.

Data exfiltration attempts are another high-priority activity, cited by 56% of respondents. Additionally, changes in data access permissions (49%) and data transfer and sharing activities (41%) are recognized as critical areas to monitor, as they can signal potential security breaches or policy violations.

What activities do you consider most critical to monitor in order to maintain a strong data security posture?

58%	Unauthorized access attempts
56%	Data exfiltration attempts
55%	Overprivileged access for humans
49%	Changes in data access permissions
42%	Overprivileged access for non-human identities
41%	Data transfer and sharing activities
40%	Data being removed or deleted
36%	Usage patterns of sensitive data

Given these findings, organizations should prioritize DSPM solutions that offer data detection and monitoring capabilities that provide comprehensive visibility into both human and non-human access events. Implementing tools that can detect unauthorized access, flag overprivileged accounts, and track changes in data permissions will be essential in maintaining a strong security posture. Moreover, the focus on non-human identities indicates a growing need for security measures that can address the unique risks posed by automation and connected devices in today's data environments.

Additional responses include: Industry compliance violations 31% | Configuration changes in data stores 22%

Challenges in Managing Data Security Posture

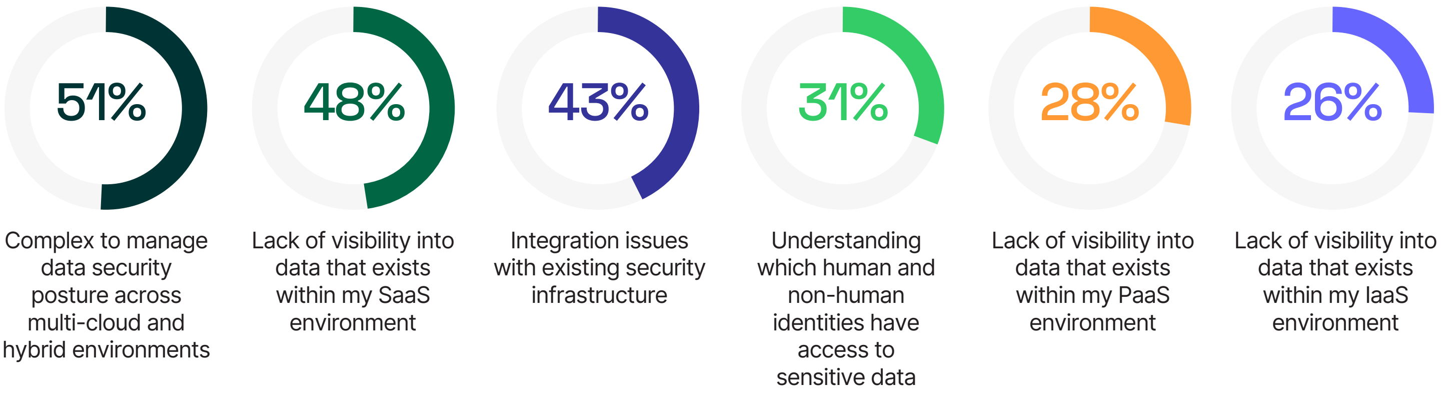
Managing data security posture across complex environments is increasingly challenging for organizations, especially as they navigate multi-cloud and hybrid architectures.

A majority of respondents (51%) report that managing data security posture across multi-cloud and hybrid environments is a top challenge. This complexity often stems from the need to coordinate security efforts across various platforms, each with its own unique risks and requirements. Closely following this, 48% of participants cite a lack of visibility into data within their SaaS environments, highlighting how difficult it can be to maintain control over data that resides outside of traditional on-premises systems.

Integration issues with existing security infrastructure is another critical concern, affecting 43% of respondents. These integration challenges can create friction between new and legacy systems, further complicating the already intricate task of managing data security. This lack of cohesion adds unnecessary complexity, which can stall or even derail data security projects if not addressed effectively.

Understanding which human and non-human identities have access to sensitive data is also a significant challenge, with 31% of respondents identifying it as an area of concern. As organizations adopt more automated processes and connect to IoT devices, keeping track of who—or what—has access to sensitive data becomes increasingly difficult.

What challenges do you face in managing your data security posture?



This reality—where understanding data security posture across hybrid cloud and SaaS environments is fraught with challenges—can lead to stalled or failed data security initiatives if not carefully managed. Organizations must prioritize solutions that provide comprehensive visibility and seamless integration across all environments. By doing so, they can reduce complexity, enhance control, and ensure the success of their data security efforts in a rapidly evolving landscape.

Additional responses include: Limited automation for data incident remediation processes 25% | Lack of visibility into data that exists within my on-premises environment 23% | Lack of monitoring into data events that matter 22%

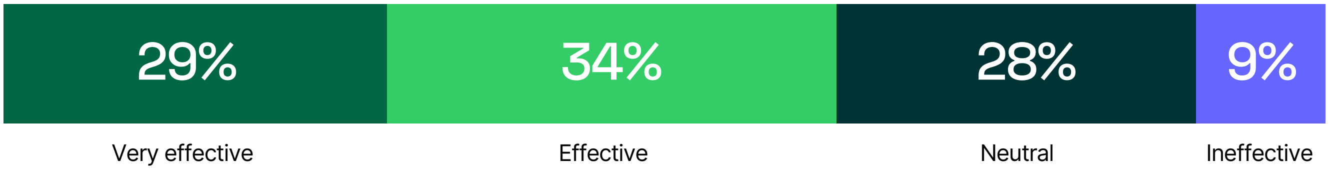
Effectiveness of Data Security Posture Management

As organizations increasingly turn to Data Security Posture Management (DSPM) tools to protect their sensitive data, the survey results reveal promising insights into the effectiveness of these solutions.

Among those who have adopted DSPM, the majority—63%—report that these tools have been either effective or very effective in identifying and mitigating security risks associated with data. This positive feedback highlights the value that DSPM brings to an organization's overall security strategy.

However, 28% of respondents remain neutral, likely reflecting experiences with early DSPM solutions, or "DSPM 1.0" tools, that may lack comprehensive support across multiple environments or struggle with scalability and precision. These limitations can prevent organizations from fully realizing the benefits of DSPM, leading to less confidence in the solution's effectiveness.

If you are using a DSPM tool today, how effective is your current data security posture management in identifying and mitigating security risks associated with data?



To maximize the effectiveness of DSPM, organizations should focus on solutions that not only scale across diverse environments—such as SaaS, IaaS/PaaS, and on-premises—but also provide precise, actionable insights into data security risks. By advancing beyond early iterations of DSPM and adopting modern, more robust and scalable tools, companies can manage and mitigate data security threats more effectively.

Future Investment in Data Security Posture Management

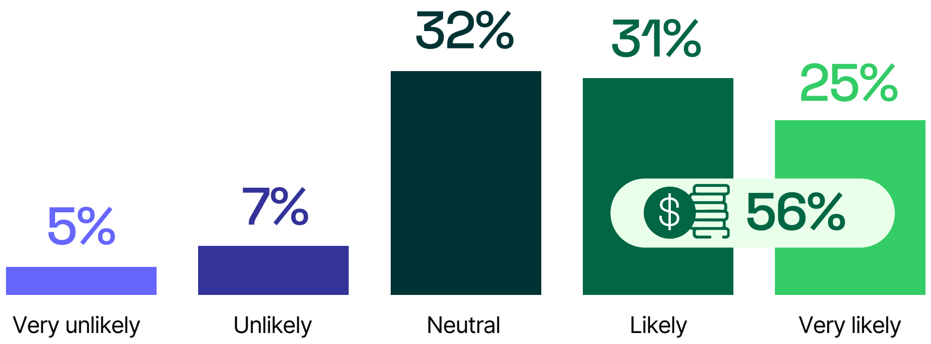
As the importance of securing sensitive data continues to rise, the survey results indicate a strong trend toward the adoption of Data Security Posture Management (DSPM) solutions.

Currently, 19% of enterprises have already implemented DSPM, and by mid-2025, 75% of organizations are expected to have adopted this technology. This positions DSPM as the fastest-growing security category globally.

When looking at future investment plans, 56% of respondents are either likely or very likely to invest in a DSPM solution within the next 12 months. This enthusiasm underscores the recognition that DSPM is becoming a critical component of modern data security strategies.

Only a small fraction of respondents are unlikely (7%) or very unlikely (5%) to invest in DSPM, which suggests that the majority of organizations understand the value DSPM provides, even if they have not yet taken the steps to adopt it.

How likely are you to invest in a DSPM solution in the next 12 months?



As DSPM continues to evolve and address the challenges of data security across various environments, more enterprises are likely to make it a cornerstone of their data security program.

Expected and Observed Benefits of DSPM

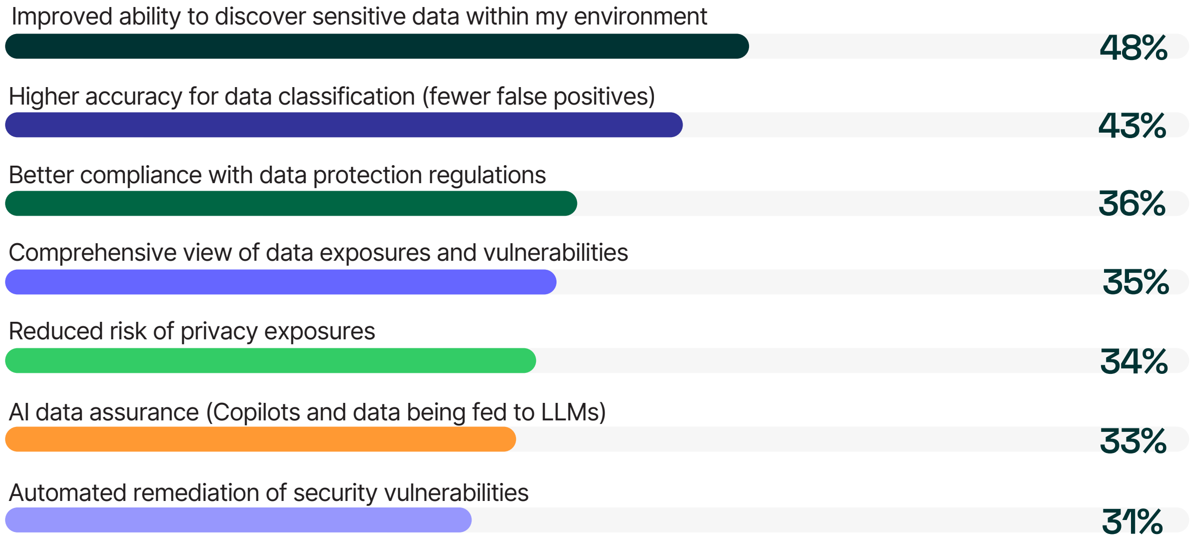
As organizations increasingly adopt Data Security Posture Management (DSPM) solutions, the anticipated benefits reflect the growing need for more effective and accurate data security practices. The survey results reveal that security professionals are most excited about DSPM's ability to enhance data discovery and improve precision in data classification—two areas where previous solutions have often fallen short.

Nearly half of the respondents (48%) expect or have already observed an improved ability to discover sensitive data within their environments. This benefit is particularly valuable given that many earlier discovery solutions lacked comprehensive support across all environments, leading to significant blind spots. By addressing these gaps, DSPM tools enable organizations to gain a more complete understanding of their data landscape, and with higher levels of confidence and automation.

Additionally, 43% of respondents are enthusiastic about DSPM's potential to boost accuracy in data classification, reducing the occurrence of false positives. In the past, high rates of false positives have been a major pain point for data security leaders, creating unnecessary noise and making it difficult to focus on genuine threats. DSPM's enhanced precision in classification offers a solution to this frustration, allowing for more efficient and effective data protection.

Beyond discovery and classification, other significant DSPM benefits include better compliance with data protection regulations (36%) and a more comprehensive view of data exposures and vulnerabilities (35%). The ability to reduce the risk of privacy exposures (34%) and enable the confident use of data for AI purposes (33%) also highlight DSPM's evolving role in addressing modern security challenges, such as ensuring that data fed to AI models is secure and compliant.

What benefits are you expecting/have you observed from using a DSPM solution?



Additional responses include: None - I do not plan to adopt a DSPM solution 11% | Other 2%

Core DSPM Features: What Matters Most

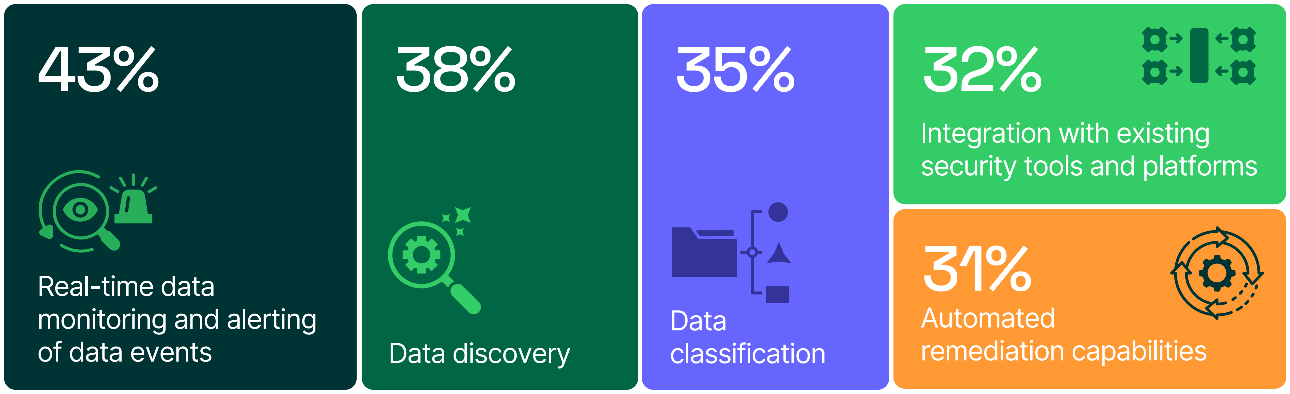
When it comes to Data Security Posture Management (DSPM), organizations are clear about what they need most: near real-time data monitoring, data discovery, and data classification. These three features emerged as the top priorities in the survey, highlighting their critical role in strengthening data security and forming the foundation of any DSPM solution.

Real-time data monitoring and alerting of data events, prioritized by 43% of respondents, is seen as the most crucial feature. This focus reflects the need for immediate visibility into data activities, allowing organizations to detect and respond to threats as they happen. However, the true value of real-time monitoring is fully realized only when it's paired with robust data discovery (38%) and data classification (35%) capabilities. The integration of these features is essential, as monitoring alone is insufficient without a clear understanding of what sensitive data exists and how it should be classified.

This gap—where real-time data monitoring often operates in isolation from discovery and classification—highlights why these three features should be the primary focus in any DSPM proof of value engagement. Without the ability to correlate real-time events with accurate discovery and classification, organizations risk missing critical insights that could prevent data breaches.

Other important features include integration with existing security tools (32%) and automated remediation capabilities (31%). These functionalities ensure that DSPM can seamlessly fit into the broader security infrastructure and take proactive steps to address vulnerabilities. Continuous risk assessment (30%) and comprehensive reporting (28%) are also valued, offering ongoing visibility into security posture and detailed insights for decision-making.

Which features do you consider most important in a DSPM solution?



Ultimately, real-time monitoring, data discovery, and classification stand out as the core needs that organizations should prioritize when evaluating DSPM solutions. Ensuring that these features work in sync will empower security teams to maintain a more effective and resilient data security posture.

Additional responses include: Continuous risk assessment and vulnerability detection 30% | Comprehensive reporting and analytics 28% | Policy management and enforcement 14% | Other 4%

Evaluation Considerations When Choosing a DSPM Solution

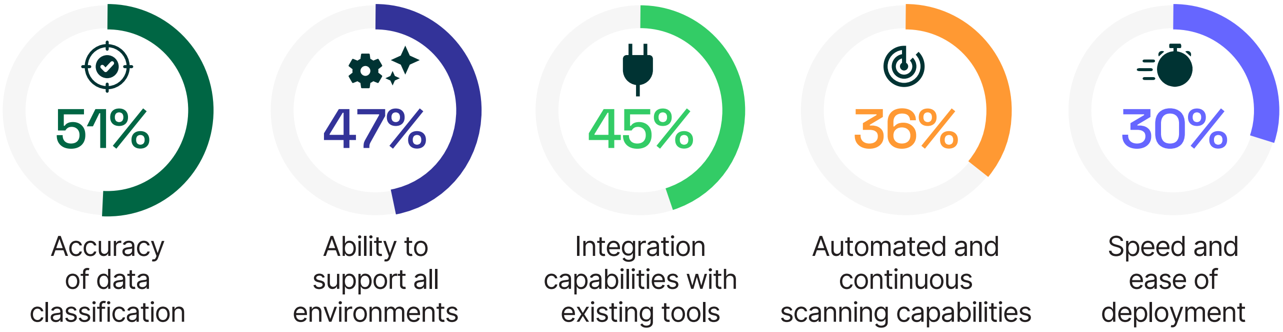
Selecting the right Data Security Posture Management (DSPM) solution is crucial for organizations aiming to safeguard their sensitive data effectively. The decision-making process is complex, as it directly impacts the organization's ability to discover, classify, protect, and manage data across diverse environments. Given the rapidly evolving threat landscape, choosing a DSPM solution that aligns with an organization's unique security needs is of paramount importance.

Precision stands out as the top priority for security professionals, with 51% of respondents identifying the accuracy of data classification as their primary consideration. This focus on precision is critical, as accurate classification forms the foundation of any effective data security strategy. Without it, organizations cannot properly identify and protect their most sensitive information, leaving critical gaps in their security posture and making it difficult to focus existing security personnel on the data that matters most.

Following closely, 47% of respondents prioritize the ability to support all environments. With data scattered across on-premises systems, cloud platforms, and SaaS applications, comprehensive coverage is essential. Security leaders understand that a DSPM solution must seamlessly handle data across all environments to provide the visibility and control necessary to mitigate risks. Integration capabilities with existing tools are also highly valued, with 45% of respondents citing this as a key evaluation. In an increasingly complex security ecosystem, the ability for DSPM to send signals and work in tandem with other security technologies is of paramount importance. This ensures that data security is not siloed but rather integrated into the broader security framework, enhancing overall effectiveness.

Other important factors include automated and continuous scanning capabilities (36%), which help maintain up-to-date data security in real time, and the speed and ease of deployment (30%), which can significantly impact the success and adoption of a DSPM solution. Cost and return on investment (23%) and compliance mapping (19%) are also important, though they take a backseat to the more pressing concerns of accuracy, coverage, and integration.

What key considerations do you evaluate when choosing a DSPM solution?



Ultimately, when data security leaders are considering a DSPM vendor, precision in classification, support across all environments, and strong integration capabilities should be at the top of their evaluation criteria to ensure that a DSPM solution can effectively manage sensitive data and align with the broader security strategy of the organization.

Additional responses include: Cost and return on investment 23% | Compliance mapping and support 19% | Other 3%

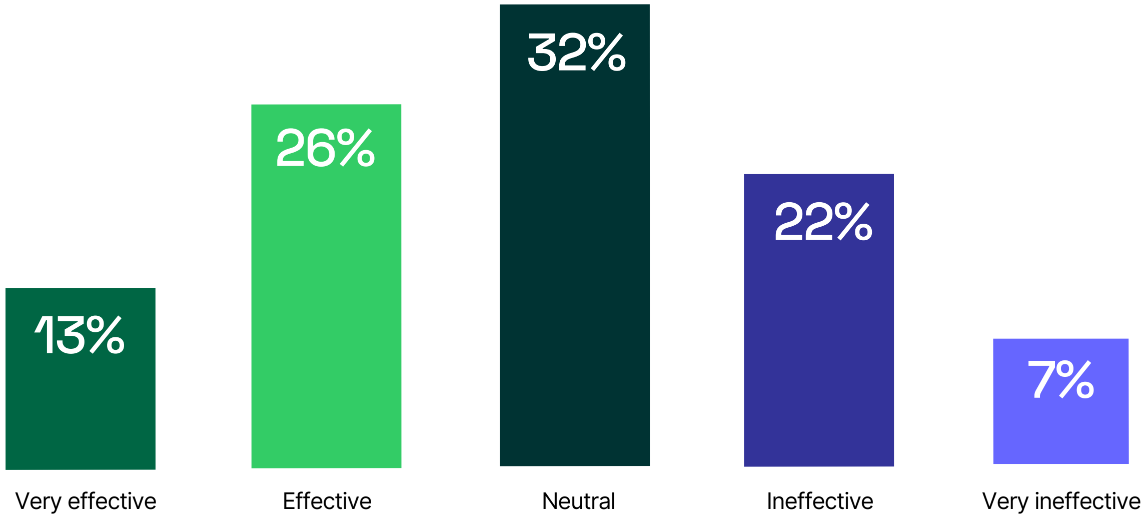
Effectiveness in Detecting and Responding to Data Security Exposures

The ability to detect and respond to security and privacy exposures of sensitive data is a critical aspect of maintaining a strong data security posture.

Given the increasing frequency and sophistication of cyber threats, organizations must be confident in their ability to protect their most valuable assets. However, only 13% of respondents believe their organization is very effective at detecting and responding to data security and privacy exposures, with an additional 26% considering themselves effective. This means that 61% of organizations do not feel they have a strong ability to manage these crucial tasks.

This lack of confidence is concerning, as it suggests that a significant number of organizations may be leaving sensitive data vulnerable to breaches and other security or privacy incidents.

How effective is your organization in detecting and responding to security and privacy exposures of sensitive data?



For organizations to improve their effectiveness, it's essential to invest in solutions that provide comprehensive data visibility, automated issue identification, and ongoing risk monitoring.

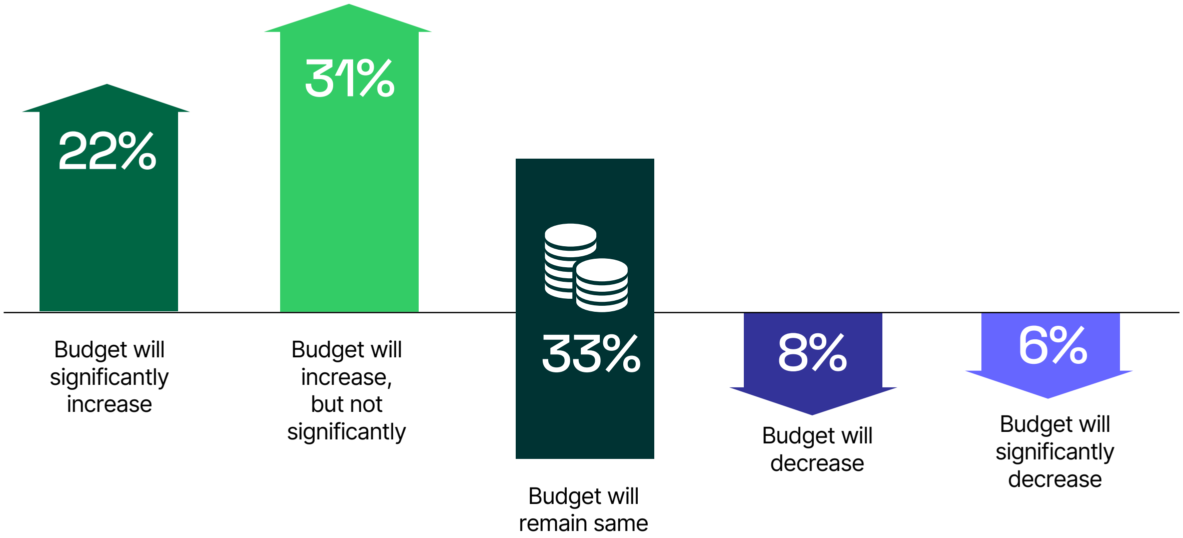
Data Security Budgets: A Priority for the Year Ahead

As organizations continue to face a dynamic and challenging threat landscape, the allocation of resources toward data security remains a critical priority. The survey results reflect this focus, with a significant portion of respondents expecting their data security budgets to either increase or remain stable over the next 12 months.

Specifically, 22% of respondents anticipate a significant increase in their data security budget, while an additional 31% expect a more moderate increase. This indicates that over half of organizations recognize the need for continued investment in data protection, reinforcing the importance of maintaining and enhancing their security posture.

Meanwhile, 33% of respondents expect their budget to remain the same, further highlighting that data security continues to be a priority, even in organizations where spending levels are not expected to rise. Notably, only 14% believe their data security budget will decrease, underscoring the widespread understanding that cutting back on security investments could leave organizations vulnerable to escalating threats.

In the next 12 months, how do you expect your data security budget to change?



Overall, these findings demonstrate that data security remains at the forefront of business priorities. As companies allocate their budgets for the coming year, it is clear that most will continue to invest in safeguarding their sensitive information, ensuring they are well-prepared to defend against evolving risks.

Essential DSPM Best Practices for Elevating Data Security

To get the most out of your Data Security Posture Management (DSPM) efforts, it's crucial to adopt proven best practices that enhance data protection and streamline operations. By focusing on continuous discovery, automatic classification, and integration across diverse IT environments, these practices ensure a comprehensive data security posture management.

1 **Ensure Continuous Data Discovery:** With 83% of respondents identifying visibility gaps as a security weakness, continuous data discovery across all environments is crucial. This minimizes blind spots and helps identify and protect sensitive data more effectively.

2 **Prioritize Classification:** 87% of enterprises do not believe their classification methods are at the highest level of effectiveness. Automating this process improves speed and reduces manual errors. Selecting a solution with unsupervised AI-powered classification can address the need for learned classifications missed by RegEx, enhancing precision and reducing false positives.

3 **Implement Real-Time Monitoring:** Real-time monitoring is critical for quick threat detection. As 43% of respondents prioritize this feature, ensure your DSPM solution includes robust alerting to mitigate risks as they arise.

4 **Integrate with Existing Security Tools:** Integration across existing IT security platforms is key for cohesive security strategies. With 45% of organizations prioritizing this, ensure your DSPM solution seamlessly connects with your current tools to enhance overall security.

5 **Focus on Scalability Across Environments:** Managing data security across multi-cloud and hybrid environments is challenging, with 51% citing it as a concern. Choose a DSPM solution that scales effectively across all environments to maintain consistent protection.

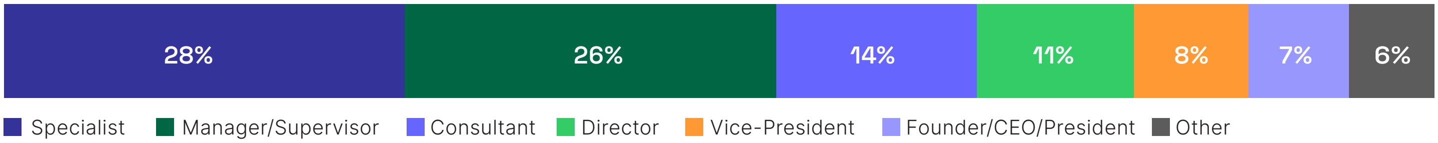
6 **Develop a Budget Line Item for DSPM Budget:** 53% of IT and security organizations will be increasing their data security budget. Given that DSPM is new, you may not be able to fund the solution by using an existing line item. Prioritize setting aside a DSPM budget when meeting with your business stakeholders (which should include the data team, security team, privacy team, and IT team) to ensure that you can implement DSPM within your security plans.

7 **Identity Data Access:** Managing who has access to what data is a fundamental aspect of DSPM. Implementing strict data access controls, with a focus on least privilege and zero trust principles, ensures that only authorized users can access sensitive data, reducing the risk of insider threats and unauthorized access.

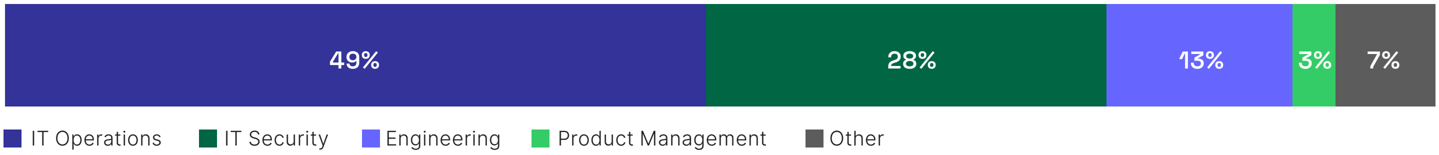
Methodology & Demographics

The 2024 DSPM Adoption Report is based on an extensive survey of 637 cybersecurity professionals conducted in August 2024. The study explored how organizations are approaching DSPM, the challenges they face, the effectiveness of their current solutions, and their adoption plan over the next 12 months. The respondents encompass technical executives and IT security practitioners, providing a balanced representation of organizations of diverse sizes across a wide range of industries.

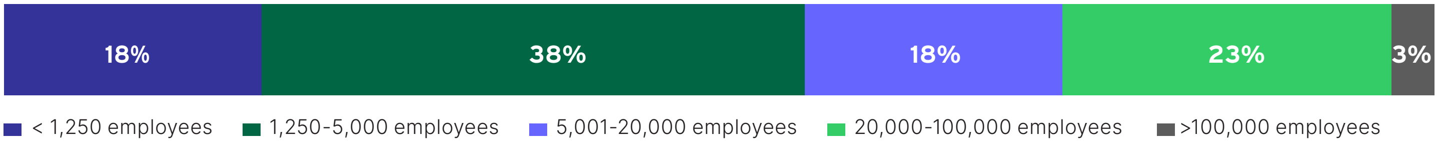
JOB TITLE / LEVEL OF SENIORITY



DEPARTMENT



COMPANY SIZE



CYERA

Data is the fastest-growing attack surface in the world. Founded in 2021, Cyera, which has raised $460M in total funding and is valued at $1.4bn, is a pioneer in the data security space. Cyera empowers security leaders at Paramount Pictures, Mercury Financial, and others to quickly discover their data attack surface, classify data with high precision, comply with data regulations and privacy standards, and monitor, detect, and quickly remediate data risk.

What makes Cyera unique is its agentless design that deploys in just five minutes across any environment - and its unsupervised, AI-powered classification engine that auto-learns unique classifications and delivers 95% classification precision. These insights are then combined with the data security company's Identity capabilities. Cyera can discover human and non-human identities (i.e., AI copilots), assign trust levels to them, assess their level of access to sensitive data, and determine the context in which the identities can access that data. These platform capabilities are complemented by Cyera's proactive data risk assessment, 24×7×365 data monitoring, and Data Incident Response services. These services make Cyera's data security experts readily available to Cyera's customers.

With Cyera, security leaders can focus on enabling their businesses to safely use data in all the ways they see fit —now and in the future.

To learn more about Cyera, visit **www.cyera.io**

Cybersecurity

INSIDERS

Cybersecurity Insiders brings together 600,000+ IT security professionals and world-class technology vendors to facilitate smart problem-solving and collaboration in tackling today's most critical cybersecurity challenges.

Our approach focuses on creating and curating unique content that educates and informs cybersecurity professionals about the latest cybersecurity trends, solutions, and best practices. From comprehensive research studies and unbiased product reviews to practical e-guides, engaging webinars, and educational articles - we are committed to providing resources that provide evidence-based answers to today's complex cybersecurity challenges.

Contact us today to learn how Cybersecurity Insiders can help you stand out in a crowded market and boost demand, brand visibility, and thought leadership presence.

Email us at **info@cybersecurity-insiders.com** or visit **cybersecurity-insiders.com**