A Buyer's Guide to Data Security Posture Management

2025

Bonus:
Vendor evaluation template

Contents

An Overview of Data Security Posture Management (DSPM)

In an era where data breaches and cyber threats are escalating, Data Security Posture Management (DSPM) has emerged as a critical component of modern data security strategies. While organizations are increasingly aware of the importance of protecting their data, many are still grappling with the complexities of managing data security across diverse and dynamic environments.

According to Gartner, "by 2026, more than 20% of organizations will deploy DSPM technology, due to the urgent requirements to identify and locate previously unknown data repositories and to mitigate associated security and privacy risks." [1]

Here's why DSPM is not just a good idea, but a necessity for businesses today:

Accelerating Data Initiatives

DSPM serves as a critical enabler for data initiatives, including cloud migrations, mergers and acquisitions (M&A), and the adoption of large language models (LLMs). Understanding and classifying data as it's being created and used ensures that these initiatives are more secure and effective.

For instance, during cloud migrations, DSPM can help identify valuable or sensitive data that needs to be protected, ensuring compliance and reducing the risk of data breaches. Similarly, in M&A scenarios, DSPM provides clarity on data assets and risks, facilitating smoother integrations. The adoption of LLMs, which rely heavily on vast datasets, benefits from DSPM by ensuring that the data fed into these models is secure and compliant, thereby enhancing the overall quality and trustworthiness of the insights generated.

Enabling Least Privilege Access

DSPM facilitates the ability to grant business users, third parties, and other external stakeholders access to data they would otherwise be restricted from due to improper data classification and access controls. By accurately discovering, classifying, and monitoring data, DSPM ensures that data is organized and protected according to its sensitivity and business value. This lets security and data teams implement least privilege access, ensuring users and machines only have access to the data they need for their specific roles. Consequently, business users can securely access the necessary data to drive innovation and productivity, while minimizing the risk of data breaches and ensuring compliance with regulatory standards. Through precise data classification and access governance, DSPM enhances data sharing capabilities while maintaining robust security protocols.

Comprehensive Data Visibility

One of the core benefits of DSPM is its ability to provide comprehensive visibility into an organization's data landscape. This includes not just where data is stored, but how it is accessed, used, and moved across various environments. By offering detailed insights into data flows and interactions, DSPM enables organizations to identify and address potential security gaps that might otherwise go unnoticed.

Proactive Risk Management

Most organizations don't understand what data they have or how it might be exposed. "**83% of organizations** having experienced at least **one breach** related to access issues in the last 18 months." [2] DSPM tools go beyond mere data discovery; they actively assess and manage the security posture of data. This involves continuous monitoring and evaluation of data security risks, taking into account factors such as data sensitivity, access patterns, and potential vulnerabilities. By proactively identifying risks, DSPM allows organizations to implement targeted measures to mitigate them before they can be exploited.

Automating Continuous Governance

With regulatory requirements becoming more stringent globally, ensuring compliance has become a significant challenge for organizations. DSPM solutions help streamline compliance efforts by automating the discovery and classification of valuable or sensitive data, mapping it against relevant regulations, and providing actionable insights for maintaining compliance. This not only reduces the burden on IT and security teams but also minimizes the risk of regulatory fines and reputational damage.

Increasing Data Utilization

Modern DSPM solutions are designed to scale with an organization's growth and adapt to its evolving data security needs. Whether dealing with on-premises data centers, cloud environments, or hybrid infrastructures, DSPM provides a unified approach to managing data security. This scalability and adaptability are crucial for organizations looking to maintain robust data security practices amidst expanding and increasingly complex data requirements.

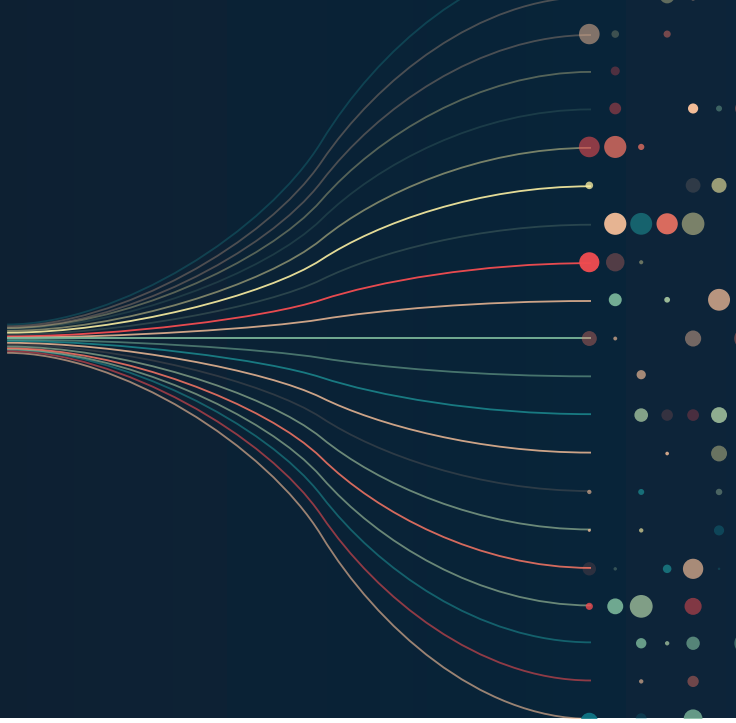
Enhancing Broader Security Strategies

While DSPM is a specialized tool, it integrates seamlessly with broader data security strategies and platforms. This integration enhances the overall security posture by providing a cohesive and coordinated approach to data protection. By aligning DSPM with other security measures, such as endpoint protection, network security, and identity management, organizations can achieve a more holistic and effective defense against data breaches and cyber threats.

DSPM is an indispensable element of a comprehensive data security strategy. It provides the visibility, risk management, compliance support, and scalability needed to protect data in today's complex digital landscape. As organizations continue to navigate the challenges of data security, DSPM stands out as a vital tool for safeguarding their most valuable asset – their data.

Benefits of DSPM

- **Enhance Data Visibility and Control:** Ensure comprehensive discovery, classification, and monitoring of valuable or sensitive data across diverse environments (multi-cloud, on-premises, hybrid, SaaS), including shadow data or shadow AI.
- **Enable Data Initiatives:** Allow organizations to confidently pursue initiatives involving LLMs and other advanced data projects.
- **Accelerate Risk Management and Remediation:** Rapidly prioritize security risks with accurate classification, monetary value assessment, and AI-driven anomaly detection to identify unusual access patterns.
- **Increase Value of Existing Tools:** Augment or replace traditional data security tools, breaking down silos in complex data landscapes.
- **Optimize Consumption and Costs:** Identify and manage duplicate or abandoned data to reduce storage costs by moving to more affordable backups or deleting unnecessary data.
- **Respond to Business Demands:** Securely provide access to data lakes and generative AI capabilities, ensuring no security gaps are introduced.
- **Ensure Compliance and Governance:** Achieve and maintain compliance with evolving regulations like GDPR, HIPAA, and CCPA through automated mappings and continuous monitoring.
- **Facilitate Least Privilege Access:** Simplify the implementation of least privilege access for users and machines, even in PaaS environments with unstructured data.
- **Improve Incident Response:** Enhance incident response capabilities with automated detection and rapid response mechanisms for identified vulnerabilities.
- **Boost Operational Efficiency:** Streamline operations by reducing manual data security tasks through automation and AI-driven processes.
- **Support Data-Driven Decision Making:** Provide accurate, real-time insights into data security posture to inform strategic decision-making.



Drivers for DSPM

IT teams frequently face significant hurdles when embarking on large initiatives due to inaccurate data classification and improper access controls. These foundational issues can lead to project failure or abandonment because the critical first step—discovering and classifying data—was not adequately addressed. Without a clear understanding of what data exists, where it resides, and who has access to it, organizations cannot effectively secure their data, comply with regulatory requirements, or leverage their data assets to achieve strategic objectives. Here's a look at how these challenges impact various key initiatives:

Overall Data Security Posture

Organizations often aim to enhance their data security posture by replacing outdated data security tools that are incapable of addressing the complexities of modern data environments, including multi-cloud, on-premises, hybrid, and SaaS. However, without accurate data classification and access controls, these efforts can be futile.

Sustainable Zero Trust Model

Implementing a Zero Trust architecture requires strict verification for every access request, along with a clear understanding of data access privileges. If data classification and user access controls are not correctly established from the outset, Zero Trust cannot be effectively implemented, leading to a fundamental breakdown of the Zero Trust principle, "never trust, always verify."

Responsible Use of AI Across the Enterprise

Monitoring and controlling the use of valuable or sensitive data by AI systems to ensure data privacy and security is not compromised requires accurate data classification. Without it, AI systems may inadvertently use critical data inappropriately, leading to privacy breaches and security risks.

Proactive Anomaly Detection and Breach Prevention

To detect unusual data access patterns and prevent potential breaches using AI-driven anomaly detection, organizations must have a precise inventory of their data assets. Without accurate data classification, anomaly detection systems cannot differentiate between legitimate and suspicious activities, leading to false positives or missed threats.

Continuous Data Privacy and Regulatory Compliance

Updating data and access governance strategies to meet compliance standards such as NIST, GDPR, HIPAA, GLB, CCPA, or SEC requires precise data classification. Compliance efforts depend on the ability to identify and protect sensitive data in accordance with regulatory requirements. Misclassified data can lead to non-compliance, resulting in fines and reputational damage.

Complex Data Projects

Complex data projects, including data lake access, mergers, acquisitions, or cloud migration or data consolidation projects, hinge on accurate data classification. Misclassified data can lead to integration challenges, data loss, and security breaches during these projects.

Access to Data Lakes (e.g., Snowflake) – DSPM enables precise control over who can access valuable or sensitive data stored in data lakes, ensuring compliance and security It can also facilitate the efficient use of data lakes by ensuring that data is classified and easily retrievable for other sophisticated analytics and business intelligence purposes.

Mergers and Acquisitions (M&A) – DSPM facilitates accurate data classification for seamless integration of data assets from merging entities, minimizing the risk of data incompatibility and loss. It can also identify and secure valuable or sensitive data early in the process, reducing the risk of exposing critical or unknown information during the merger or acquisition.

Cloud Migrations – DSPM can accurately classify data suitable for cloud migration, ensuring that critical data is adequately protected and ensure that data migrated to the cloud complies with relevant regulatory requirements, reducing the risk of non-compliance.

Data Consolidation – DSPM plays a crucial role in helping merge various datastores through comprehensive data discovery and accurate classification. DSPM prevents any data from being abandoned or overlooked during the consolidation process so IT teams avoid paying for unused or redundant storage and leverage cheaper, more efficient storage options.

Scaling Security Operations

Scaling security operations to manage growing security needs without proportionally increasing headcount is possible with automation and AI. However, these technologies rely on accurate data classification to function effectively. Misclassified or unidentified data can lead to automation errors, security gaps, and inefficient resource allocation.

Secure Development Life Cycle (SDLC) Enhancements

Integrating security into the SDLC, particularly in DevOps and DevSecOps environments, requires accurate data classification to identify valuable or sensitive data early in the development process. Without proper classification, developers may inadvertently expose information, leading to security vulnerabilities.

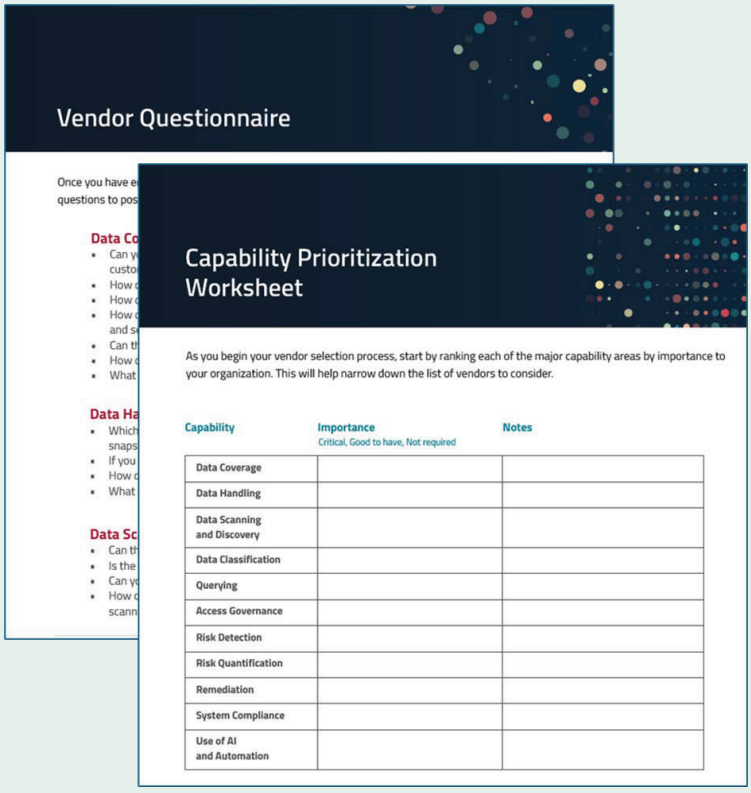
Data Consumption and Cost Optimization

Data hygiene projects aimed at cleaning up, backing up, and eliminating unnecessary data help reduce cloud costs and minimize attack surfaces. Accurate data classification is essential for identifying which data is critical, redundant, or obsolete. Without this step, organizations risk mismanaging their data, resulting in increased costs and security vulnerabilities.

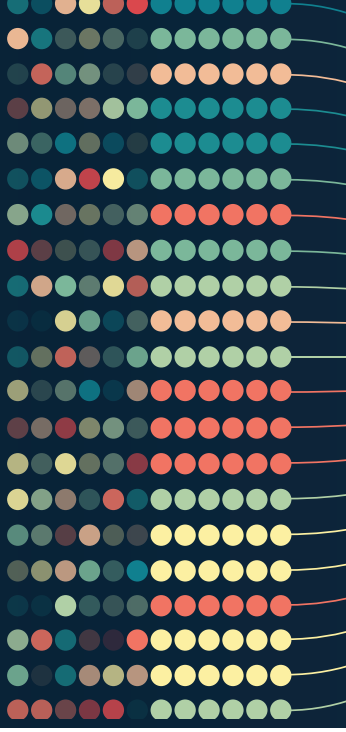
Evaluation Readiness

If you are ready to start building your DSPM key capabilities

click here to go right to the Buyer Worksheets



Key Considerations for Vendor Selection



Before deciding on which vendors to evaluate, there are some important decision points you should discuss internally. Below are the most critical topics and questions will help guide your vendor selection process.

1. How Much Data Do You Have?

Understanding the volume of data your organization handles is crucial when evaluating DSPM solutions. Large volumes of data require scalable solutions that can manage extensive datasets without compromising performance. When discussing with vendors, ask about their capacity to handle your data volume and their approach to scaling.

Questions to Ask Vendors:

- What is the maximum data volume your solution can handle?
- How do you ensure performance and accuracy at scale?
- Can your solution scale dynamically as our data grows?

2. What Are Your Environments?

The environments in which your data resides—cloud, on-premises, hybrid, SaaS, PaaS—affect which DSPM solution is suitable for your needs. Some vendors specialize in cloud environments, while others offer comprehensive coverage for multiple environments. Ensuring compatibility with your specific setup is essential for effective data security.

Questions to Ask Vendors:

- Does your solution support multi-cloud, on-premises, hybrid, SaaS, and PaaS environments?
- How do you manage data security across diverse environments?
- Are there limitations or specific requirements for any environment?

3. Platform or Standalone

Choosing between a standalone DSPM solution and one integrated into a larger platform involves considering the breadth of coverage and potential single points of failure. Standalone DSPM solutions often offer more specialized features and flexibility, whereas integrated solutions may suffer from legacy limitations and deployment challenges.

Questions to Ask Vendors:

- Is your DSPM solution standalone or part of a larger platform?
- How does your solution avoid single points of failure?
- What are the deployment and scaling challenges associated with your solution?

4. Drivers for DSPM

Identify whether your evaluation focuses on specific use cases (e.g., regulatory compliance, cloud migration, data governance) or aims to improve overall security posture. Different DSPM solutions may excel in different areas, so aligning the solution with your primary use cases ensures it meets your specific needs. For a list of example use cases that DSPM supports, **see page 33.**

Questions to Ask Vendors:

- What use cases does your solution best support?
- Can you provide examples of how your DSPM solution has addressed specific challenges?
- How flexible is your solution in adapting to new use cases?

5. Data Handling

Consider how you want the DSPM solution to handle your data—whether through snapshots processed in the vendor's environment, a sidecar approach maintaining control, or vendor scans where data never leaves your control. The choice impacts data security, compliance, and the importance of data lineage. For more details about the various data handling approaches, **see page 13.**

Questions to Ask Vendors:

- How does your solution handle data processing and storage?
- Do you offer a sidecar approach or in-place scanning?
- How does your solution ensure data lineage and control?

6. Continuous or Point-in-Time Scanning

Evaluate whether the DSPM solution offers continuous monitoring or point-in-time scans. Continuous monitoring provides proactive security by detecting and addressing issues as data is created and used, whereas point-in-time scans may leave gaps in data protection between scans.

Questions to Ask Vendors:

- Does your solution provide continuous monitoring or periodic scans?
- How frequently are point-in-time scans conducted?
- What are the benefits of your approach to monitoring?

7. Data Variety

The ability of a DSPM solution to handle large volumes and a variety of data types is crucial. Some solutions may require extensive setup and configuration before scanning, while others offer machine learning capabilities to adapt and improve over time, reducing the need for manual intervention.

Questions to Ask Vendors:

- What setup and configuration are required before the first scan?
- Does your solution use machine learning to adapt and improve accuracy?
- What is your accuracy rate? Or your false positive/false negative rate?

8. Budget

Budget considerations include the cost implications of different data handling methods, which was covered in topic #5. Processing data in the vendor's environment can be expensive, so it's important to understand the cost impact and compare it to other options where scanning is done where the data lives.

Questions to Ask Vendors:

- What is the cost structure for your DSPM solution?
- How does data processing in your environment impact the overall cost?
- Are there flexible pricing models based on usage?

9. Onboarding

Effective onboarding involves collaboration between security and data teams. Some vendors may bypass important stakeholders with their methods, leading to potential security gaps. Ensure the solution facilitates shared responsibility and integrates smoothly with existing teams and processes.

Questions to Ask Vendors:

- How do you approach onboarding and integration?
- Does your solution require collaboration between security and data teams?
- How do you ensure a smooth onboarding process?

10. Licensing and Support

Licensing flexibility and support are critical. Consider vendors that offer elastic use of DSPM, adjusting based on your needs, rather than rigid multi-year licenses. Additionally, look for white-glove deployment services tailored to your environment rather than a one-size-fits-all approach.

Questions to Ask Vendors:

- What licensing options do you offer?
- Can your licensing model adjust based on usage?
- Do you provide white-glove deployment services tailored to our environment?

DSPM Solution Criteria

When evaluating DSPM vendors, it's essential to understand how each vendor delivers on the following critical capabilities. These capabilities are considered table stakes for any comprehensive DSPM solution.

Data Coverage

DSPM should comprehensively cover structured, unstructured, and semi-structured data across diverse environments, including major cloud providers (AWS, GCP, Azure), SaaS platforms (Snowflake, Salesforce, Workday), and on-premises databases and file shares. The solution must continuously monitor and discover new data stores, notifying security teams of any at-risk data.

What to look for:

- Detailed visibility into data access, including who or what is accessing the data and when, including granular insights into data access patterns to identify potential risks and ensure proper governance.
- DSPM performs security scans within the native data environment so that valuable or sensitive data is never moved or copied outside its original location for security analysis.
- Data lineage: Understanding the lifecycle of data and its movement through the organization is essential for assessing risks.

Data Handling

DSPM should support various data environments and storage types, ensuring all data, including backups, are properly managed. Effective data handling involves identifying duplicate or abandoned data, optimizing storage costs and maintaining data lineage.

What to look for:

- Detailed visibility into data access, including who or what is accessing the data and when, including granular insights into data access patterns to identify potential risks and ensure proper governance.
- DSPM performs security scans within the native data environment so that valuable or sensitive data is never moved or copied outside its original location for security analysis.
- Data lineage: Understanding the lifecycle of data and its movement through the organization is essential for assessing risks.

Data Scanning and Discovery

DSPM must continuously scan and discover all data stores, providing comprehensive visibility across the entire data landscape. This includes identifying new and shadow data stores, ensuring no data is left unclassified or unmanaged.

What to look for:

- Comprehensive data mapping for automated discovery and correlation what data an organization has, where it resides, and the associated risks.
- DSPM should leverage scanning technology that identifies data attributes in a single pass with maximum accuracy, reducing false positives and negatives.
- DSPM should discover attack paths to critical data that weigh data sensitivity against identity, access, vulnerabilities and configurations.

Data Classification

DSPM should automatically and accurately classify data based on sensitivity, regulatory requirements, and business value. This ensures that valuable or sensitive data is correctly identified and protected, facilitating compliance and risk management.

What to look for:

- DSPM should be able to classify valuable or sensitive data and map it to regulatory frameworks, tracking data lineage to understand where it came from and who had access to the data.

Querying

The solution should offer easy-to-use querying capabilities that do not require data science expertise. Systems must be self-learning, tuning alerts based on user actions, and enabling flexible, accurate data queries for security teams.

What to look for:

- AI-Driven "Ask Me Anything" Queries: DSPM should simplify querying with open Google-like searches that provide instant, intelligent responses to user queries about threats, complemented by AI-crafted remediation steps.
- DSPM provides APIs enabling users to send text or files for immediate on-the-fly sensitivity assessment.

Access Governance

DSPM must provide continuous access governance, ensuring only authorized users can access specific data. It should identify and manage user roles, resources, and privileges, detecting excessive or inappropriate access rights to minimize risk.

What to look for:

- DSPM analyzes IAM roles, permissions, and access logs to quickly identify who has what type of access to a given data store and enforce least privilege access.
- DSPM provides a comprehensive overview of attack path and user access data as a graph, allowing users to better understand and detect risks.

Risk Detection

The solution should detect potential vulnerabilities and attack paths affecting sensitive data. This includes building custom risk detection rules, visualizing attack paths, and integrating with third-party ticketing systems for streamlined risk management.

What to look for:

- DSPM identifies suspicious activity including data exfiltration and potential account takeover by continuously baselining user activity and identifying abnormal behavior.
- DSPM discovers attack paths to sensitive data, prioritizing risks based on data sensitivity, identity, access, vulnerabilities, and configurations.
- DSPM solutions that integrate with Data Detection and Response (DDR) for automated threat mitigation capabilities.

Risk Quantification

DSPM must assess and quantify risks associated with data stores, providing a clear understanding of potential impacts. This involves using AI-driven analytics to prioritize risks and guide remediation efforts effectively.

What to look for:

- DSPM estimates the cost of breach for each data store, helping teams prioritize their security efforts around what matters most.
- DSPM continuously improves classification accuracy and remediation recommendations based on user feedback and actions.

Remediation

The platform should offer AI-driven remediation plans, integrating with existing ticketing and routing tools to address vulnerabilities promptly. This includes automated responses and detailed remediation steps to mitigate identified risks.

What to look for:

- DSPM connects with DevSecOps workflows to remediate risks, particularly as they appear early in the application development lifecycle.
- DSPM integrates with leading SOAR engines and third-party ticketing, notification, and automation services (e.g., ServiceNow, Slack, Jira).
- DSPM provides AI-generated, human-validated remediation steps in a checklist for data and security teams.

System Compliance

DSPM ensures that data management practices adhere to relevant regulations and standards. This involves regular audits and reporting to demonstrate adherence. Also, ensure the vendor complies with customer-defined data purge and retention policies. Check that the vendor has clear policies for the lifecycle management of data.

For In-Environment Scanning:

- Coordination: Seamless coordination between security, data, and operations teams to comply with data access requirements.

For Snapshot and Extract Methods:

- Security Practices: Ensure the vendor follows stringent security practices for data handling.
- Encryption: Verify that data is encrypted during transfer and storage.
- Data Purge and Retention Policies: Ensure the vendor complies with customer-defined data purge and retention policies.
- Data Lineage: Ensure the vendor provides detailed records of data lineage to track data flow and transformations.
- Audit Trails: Verify the presence of comprehensive audit trails to support compliance and forensic investigations.
- Compliance Certifications: Ensure the vendor adheres to relevant regulatory standards (e.g., GDPR, HIPAA, NIST) and undergoes regular third-party audits.
- Customer Access and Oversight: Ensure customers have access to monitor data handling processes and receive regular compliance and security reports.

Use of AI and Automation

The solution should leverage AI and automation to enhance data security processes, from automated data discovery and classification to predictive risk assessment and anomaly detection. AI-driven capabilities improve efficiency, accuracy, and proactive threat management.

What to look for:

- DSPM has specialized API for LLM security so teams can conduct real-time sensitivity analysis of data going into and out of LLMs, while providing full governance and visibility into your data usage. These APIs can be easily integrated into existing customer workflows, helping keep costs down and increasing security for services like Microsoft CoPilot.
- DSPM system should offer scanning capabilities for identifying valuable or sensitive data being used in Large Language Models (LLMs) like Microsoft Copilot or ChatGPT to ensure that AI-generated content does not expose sensitive company information.
- The system should also secure cloud-based AI deployments in AWS Bedrock and Azure OpenAI by detecting any sensitive data being fed into the foundational or custom models.

Decision Criteria At-A-Glance

Below is a brief description and the decision criteria of each capability, which should help determine their relative importance to your organization. Consider using the Buyer's Worksheet at the end of this guide to define which capabilities are most critical and why.

Capability	Description	Decision criteria
Data Coverage	Data coverage refers to the DSPM solution's ability to scan data across all environments, including cloud, on-premises, hybrid, SaaS, and PaaS.	▪ If data only lives in a single cloud, most DSPM solutions can address that environment ▪ For multi-cloud, ensure that the vendors have coverage for SaaS and cross-cloud capabilities ▪ For mixed environments of on-prem, PaaS, SaaS and cloud, the number of vendors with that coverage is limited so ask questions around your specific sources and request a coverage roadmap ▪ If data exists in virtualized environments, ask how the solution scans and classifies in place or if snapshots must be taken ▪ Specialized APIs for LLM models that can be used to conduct real-time sensitivity analysis of data going into and out of LLMs, while providing full governance and visibility into your data usage. These APIs can be easily integrated into existing customer workflows, helping keep costs down and increasing security for services like Microsoft CoPilot Note: Some vendors get around coverage limitations by taking snapshots of customer data and moving it over to their environment, reducing the dependency on multi-environment capabilities, but creating a break in a data lineage.

Capability	Description	Decision criteria
Data Handling	Data coverage refers to the DSPM solution's ability to scan data across all environments, including cloud, on-premises, hybrid, SaaS, and PaaS.	▪ Support for real-time, continuous data scanning ▪ Scanning done within customer environment or snapshot and extract method ▪ Ability to handle large volumes of data without performance degradation
Data Scanning and Discovery	Data scanning involves the ability to continuously monitor and analyze data to identify sensitive information and potential security risks. Effective data scanning should be automated and scalable to handle large volumes of data. Data discovery is the process of identifying and cataloging all data assets within an organization. This capability is crucial for understanding where sensitive data resides and how it is used.	▪ Automated scanning processes that minimize manual intervention (scan with minimal inputs initially) ▪ Ability to tune scanning results without coding ▪ Specific scanning capabilities for identifying sensitive data being used in Large Language Models (LLMs) ▪ Unsanctioned / shadow AI or LLMs ▪ Set-it-and-forget it scanning or requiring scheduling ▪ Complete identification and cataloging of all data assets within the organization ▪ High accuracy in discovering and identifying sensitive data ▪ Scan processing speeds
Data Classification	Data classification involves categorizing data based on its sensitivity and importance. This process helps prioritize data protection efforts and ensures that the most critical data receives the highest level of security.	▪ High accuracy in classifying data ▪ Ability to classify data at a granular level based on sensitivity, value or importance ▪ Flexibility to customize classification criteria to fit organizational needs ▪ Automated data classification processes to reduce manual effort ▪ Automated data tagging integration with external data sources ▪ Continuous awareness/learning of classification rules/system based on user actions
Querying	Querying capabilities allow users to search and retrieve specific data based on various criteria. This feature is essential for quickly accessing critical information and generating insights.	▪ Capability to support and execute complex queries based on custom criteria ▪ AI-powered querying for open questioning ▪ Quick and efficient retrieval of queried data ▪ Easy-to-use querying interface accessible to both technical and non-technical users
Access Governance	Access governance involves managing and controlling who has access to data. This capability ensures that only authorized users can access sensitive information.	▪ Comprehensive audit trails for tracking data access and ensuring accountability ▪ Visualizations of access across multi-environments based on data

Capability	Description	Decision criteria
Risk Detection	Risk detection identifies potential threats and vulnerabilities within data environments. This involves monitoring data activities to detect anomalies and suspicious behavior.	▪ Capability to deploy a wide range of patterns and ▪ Advanced detection of unusual data access patterns using machine learning and AI ▪ Use of historical data to establish baseline models of normal behavior ▪ Supervised learning to trained on labeled data where anomalies are already identified ▪ System-discovered deviations from the norm (leveraging techniques like z-score, moving averages, and Gaussian distribution, decision trees, random forests) ▪ Detection accuracy achieved with user identity, location, and historical behavior, threshold adjustment, feedback loops, and anomaly scoring)
Risk Quantification	Risk quantification involves assessing the potential impact of identified risks on the organization. This includes evaluating the likelihood and potential damage of security incidents.	▪ Detailed assessment of the potential impact of identified risks ▪ Effective prioritization of risks based on their potential impact and likelihood ▪ Clear and actionable visualizations of risk quantification and breach impact
Use of AI and Automation	The use of AI in DSPM enhances data security through automated analysis, pattern recognition, and predictive capabilities. AI can identify and respond to larger data volumes and variety at scale and identify threats more efficiently than human-driven or manual processes.	▪ AI capabilities across a range of areas including data identification, data masking, anomaly detection, behavioral analysis, risk assessment, user behavior, data flow, querying, remediation, resource utilization and performance tuning
Remediation	Once the system identifies vulnerable data stores containing valuable or sensitive data, it provides actionable steps to mitigate the risks associated with those vulnerabilities.	▪ AI-generated remediation plan tailored to address the specific vulnerabilities identified ▪ Post-remediation steps automatically validated (no human action required) ▪ Self-learning system continuously improves remediation recommendations based on user feedback and actions ▪ Integration with workflow and ticketing tools

Capability	Description	Decision criteria
System Compliance	Compliance ensures that data management practices adhere to relevant regulations and standards. This involves regular audits and reporting to demonstrate adherence.	**For In-Environment Scanning** ▪ Seamless coordination between security, data and operations team to comply with data access requirements **For Snapshot and Extract methods** ▪ Ensure the vendor follows stringent security practices for data handling ▪ Verify that data is encrypted during transfer and storage. **Data Purge and Retention Policies** ▪ Ensure the vendor complies with customer-defined data purge and retention policies ▪ Check that the vendor has clear policies for the lifecycle management of data **Data Lineage** ▪ Traceability: Ensure the vendor provides detailed records of data lineage to track the data flow and transformations ▪ Verify the presence of comprehensive audit trails to support compliance and forensic investigations **Compliance Certifications** ▪ Ensure the vendor adheres to relevant regulatory standards (e.g., GDPR, HIPAA, NIST) ▪ Check if the vendor undergoes regular third-party audits to validate their compliance practices **Customer Access and Oversight** ▪ Ensure customers have access to monitor data handling processes ▪ Regular reporting: Verify that the vendor provides regular compliance and security reports to the customer

In addition to DSPM-centric capabilities, there are requirements you may want to add to your evaluation criteria:

- **Regions serviced:** find out the geographical regions where the solution is hosted and the implications for data residency and compliance.
- **System logs:** ask about system activity log capture as well as error logging and capture.
- **Scale-out and scale-up options:** find out what each vendor does to increase performance and any licensing implications, including record limits.
- **Frequency of releases and upgrade level of effort:** ask vendors to provide an overview of the typical effort for recurring maintenance or periodic upgrades to a new version, including manual recompilation or reconfiguration needs, as well as the QA and benchmarking process for each release of the solution.
- **Security and user management:** require vendors to explain their support for third-party. authentication and authorization technologies, support for single sign-on capabilities, how their solution restricts user access to view, read, or modify individual data elements and rows of data, and specifics on encryption of data in transit and at rest.
- **System reporting/analytics:** beyond the DSPM-specific visualizations and reporting, capture system reporting/analytics capabilities and support for third-party tools.

Implementation Considerations for DSPM Solutions

Below are the essential steps and considerations for a successful DSPM onboarding, including potential challenges and ways to overcome them.

Steps to Successfully Implement a DSPM Solution

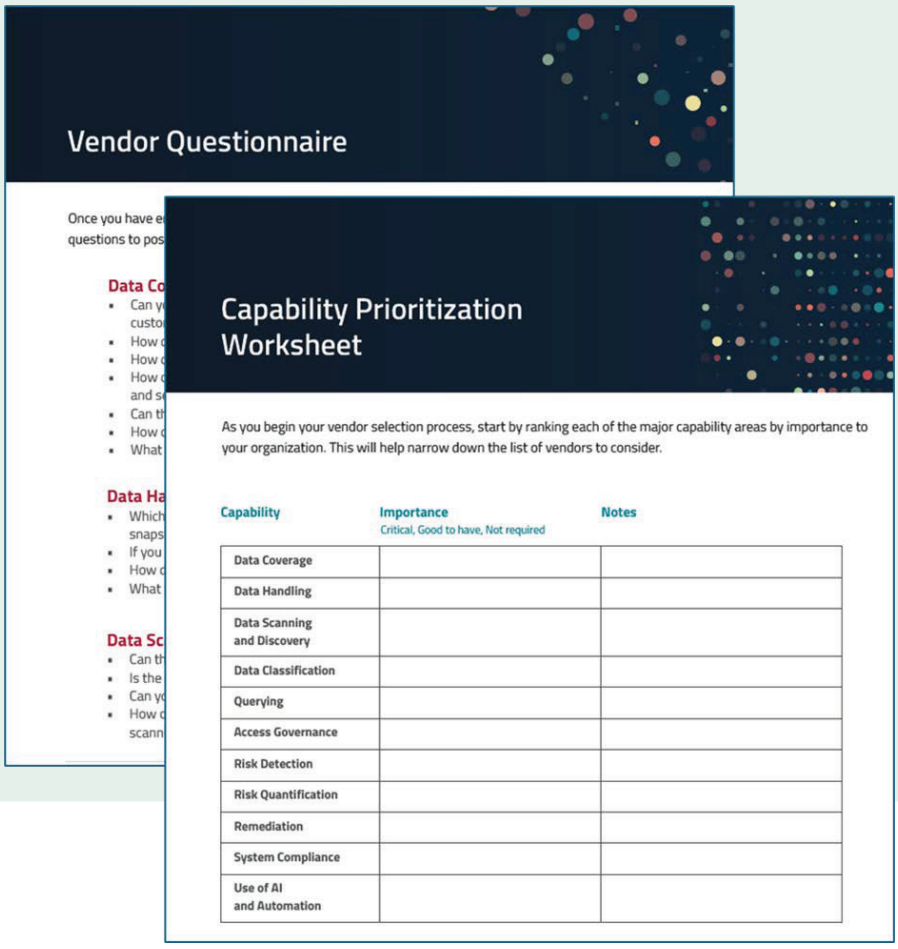
1. **Objective Setting:** Clearly define the goals of implementing a DSPM solution. Common objectives include enhancing data visibility, improving compliance, and reducing security risks.
2. **Scope Definition:** Determine the scope of the DSPM implementation. This includes identifying which data stores, environments (cloud, on-premises, hybrid), and types of data (structured, unstructured) will be included.
3. **Initial Scan:** Perform an initial data discovery to identify all data stores across your environment. This includes both known and shadow data stores.
4. **Classification:** Classify data based on sensitivity and regulatory requirements. Accurate classification is crucial for effective risk management and compliance.
5. **Access Analysis:** Analyze access controls to determine who has access to sensitive data. This involves reviewing IAM roles, permissions, and user activity logs.
6. **Least Privilege Enforcement:** Implement least privilege access policies to minimize unnecessary data access and reduce potential attack surfaces.
7. **Custom Risk Rules:** Develop custom risk detection rules that align with your organization's specific security requirements and environment.
8. **AI-Driven Remediation:** Test AI-generated remediation plans to address identified vulnerabilities. These plans should include actionable steps that can be implemented promptly.
9. **Integration with Existing Tools:** Integrate the DSPM solution with your existing tools, such as SOAR platforms, ticketing systems (e.g., ServiceNow, Jira), and notification services (e.g., Slack, email).
10. **Audit and Reporting:** Implement regular audits and generate compliance reports to demonstrate adherence to regulatory and internal standards.

11. **Feedback Loop:** Establish a feedback loop to continuously improve data classification accuracy and remediation effectiveness based on user feedback.
12. **Training and Support:** Provide ongoing training and support to ensure that security teams are well-versed in using the DSPM solution effectively.

This is a representative set of key steps, some of which take place concurrently. Additional steps are required if vendor utilizes an Extract and Scan method. Other steps vary by use case.

Evaluation Readiness

If you are ready to start building your DSPM key capabilities
click here to go right to the Buyer Worksheets



Potential Implementation Pitfalls and How to Overcome Them

Roadblocks to Access Data

Pitfall: Many organizations do not have a comprehensive inventory of their data assets, leading to gaps in data discovery and classification. In other cases, there is a lack of alignment between the team who needs to implement DSPM and the teams who are responsible for the data.

Solution: Conduct a thorough initial scan to identify all data stores across your environment, including shadow data and forgotten databases. Use a DSPM solution that provides continuous monitoring and discovery to keep your data inventory up to date.

- **Stakeholder Engagement:** Engage with stakeholders across the organization to ensure necessary permissions are granted for data access and scanning.
- **Clear Policies:** Establish clear data access policies to streamline the approval process and ensure compliance with data privacy regulations.

Inadequate Budget or Resource Allocation

Pitfall: Often, organizations fail to allocate sufficient budget or resources for DSPM implementation, treating it as an afterthought rather than a critical project.

Solution: Ensure that DSPM implementation is prioritized as part of larger strategic initiatives such as cloud migration, M&A, or adopting new data technologies. Allocate dedicated resources, including time, budget, and personnel, to the DSPM project to ensure successful deployment and integration.

- **Strategic Resource Allocation:** Acknowledge that implementing DSPM is a crucial part of larger initiatives such as cloud migration, M&A, or adopting new data technologies. Allocate dedicated resources for the DSPM implementation to ensure it gets the attention it requires.
- **Minimal Initial Inputs:** Choose a DSPM solution that can start with minimal inputs and iterate from there. A smart system should not require extensive documentation and definitions up front but can begin scanning and refining its processes based on initial findings.
- **Automation and Efficiency:** Leverage the automation capabilities of the DSPM solution to reduce the manual workload. Automated data discovery, classification, and risk assessment can significantly reduce the strain on your team.

Resistance to Change

Pitfall: Organizational inertia and resistance to adopting new technologies or processes can hinder DSPM implementation. This can often occur when the organization feels they have already invested in data security products that should provide DSPM capabilities or they are deeply invested in a platform from a vendor that does not offer DSPM.

Solution: Engage stakeholders early and communicate the benefits of DSPM clearly. Provide training and support to ensure that all team members understand how to use the new system and its importance to overall data security.

Overly Complex Configuration

Pitfall: Some DSPM solutions require extensive setup and configuration, which can delay implementation and reduce effectiveness.

Solution: Choose a DSPM solution that offers automated, easy-to-use configuration options. Look for systems that can start scanning with minimal inputs and refine their processes based on initial findings, reducing the burden on your team.

Lack of Integration with Existing Systems

Pitfall: Failing to integrate DSPM with existing security tools and workflows can lead to fragmented data security efforts.

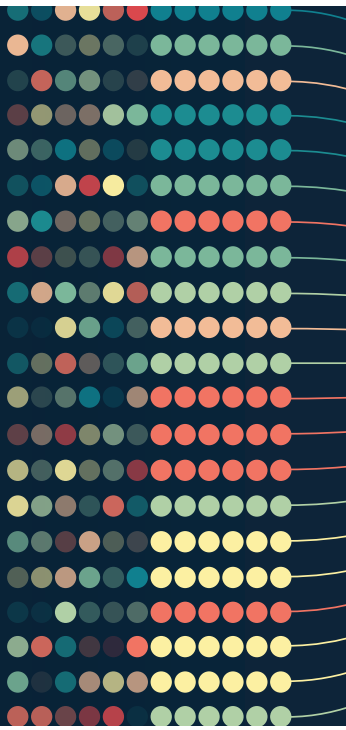
Solution: Ensure that your DSPM solution supports integration with your existing security stack, including SOAR platforms, ticketing systems, and notification services. This will enable seamless workflows and a more cohesive security strategy.

Insufficient Focus on Compliance

Pitfall: Neglecting regulatory compliance requirements can result in fines and reputational damage.

Solution: Use DSPM to automatically map data to relevant regulatory frameworks and continuously monitor compliance. Ensure that the solution provides detailed compliance reports and audit trails to demonstrate adherence to regulations.

Measuring the ROI of DSPM: Key Performance Indicators (KPIs)



Reduction in Data Breaches

- **KPI:** Measure the number and severity of data breaches before and after DSPM implementation.
- **Metric:** Percentage decrease in data breaches, reduction in the number of compromised records, and decrease in financial losses due to breaches.

Improved Data Visibility and Control

- **KPI:** Track the improvement in data visibility across the organization.
- **Metric:** Number of previously unknown data stores discovered, percentage of data stores classified, and reduction in shadow data.

Enhanced Compliance Posture

- **KPI:** Assess compliance with regulatory standards and internal policies.
- **Metric:** Number of compliance violations identified and resolved, time taken to prepare for audits, and reduction in compliance-related fines.

Efficiency of Security Operations

- **KPI:** Evaluate the efficiency gains in security operations due to DSPM.
- **Metric:** Reduction in time spent on manual data discovery and classification, number of automated remediation actions taken, and increase in security incidents handled per month.

Risk Reduction

- **KPI:** Measure the effectiveness of risk detection and mitigation.
- **Metric:** Number of risks identified and mitigated, average time to detect and respond to risks, and reduction in potential breach impact (financial and reputational).

Cost Savings

- **KPI:** Calculate the cost savings from optimized data management and reduced risk.
- **Metric:** Savings from eliminating redundant or unnecessary data, savings delivered by archiving non-essential data to cost-effective cloud storage, and overall return on investment (ROI) from reduced breach costs and operational efficiencies.

By tracking these KPIs, organizations can effectively measure the ROI of their DSPM implementation, demonstrating the value of enhanced data security and compliance to stakeholders and ensuring continuous improvement in their data security posture.

Capability Prioritization Worksheet

As you begin your vendor selection process, start by ranking each of the major capability areas by importance to your organization. This will help narrow down the list of vendors to consider.

Capability	Importance Critical, Good to have, Not required	Notes
Data Coverage		
Data Handling		
Data Scanning and Discovery		
Data Classification		
Querying		
Access Governance		
Risk Detection		
Risk Quantification		
Remediation		
System Compliance		
Use of AI and Automation		

Vendor Questionnaire

Once you have engaged with the vendors who appear to address your most critical needs, here are 100 questions to pose to help determine fit.

Data Coverage

- Can you provide a list of the environments you cover today? For each, indicate if you have customers with those environments being scanned in production.
- How does your solution manage data across multiple cloud providers?
- How does your solution handle data in hybrid environments?
- How does your solution ensure comprehensive data coverage across structured, unstructured, and semi-structured data?
- Can the solution cover data stored in on-premises, cloud, and hybrid environments?
- How does your solution handle the discovery of shadow data stores?
- What does your roadmap look like in terms of new data coverage/environments?

Data Handling

- Which data handling models does your solution use (e.g., in-environment scanning, sidecar or snapshot and extract)?
- If you use snapshots for data coverage, how does this affect data lineage?
- How does your solution ensure data security during handling?
- What measures are in place to maintain data integrity and compliance during data handling?

Data Scanning and Discovery

- Can the solution handle large volumes of data without performance degradation?
- Is the scanning process automated or require manual administration?
- Can your solution scale to handle our data volume?
- How often does your solution scan data environments? Does the solution provide continuous scanning or periodic scans?

- Does the solution provide a complete inventory of all data assets?
- How accurate is the data discovery process in identifying valuable or sensitive data?
- How quickly can the solution discover and catalog data assets?
- How comprehensive is your data discovery process?
- What methods do you use to ensure accurate data discovery?
- How long does it typically take to complete data discovery?
- Can your solution discover cloud-native structured data stores (e.g., Postgres, MySQL, Redshift)?
- Can your solution discover cloud-native unstructured data stores (e.g., S3, Azure Blob, MS OneDrive)?
- Can your solution discover cloud-native block storage (e.g., EBS volumes)?
- Can your solution discover data in PaaS data stores (e.g., Snowflake)?
- Can your solution discover data in SaaS environments (e.g., Google Workspace, Microsoft 365)?
- Can your solution discover embedded databases deployed directly on cloud compute instances?
- Does the solution continuously discover new data stores?
- Can the solution scan hard-to-reach data stores, such as those in private VPCs or on-premises datastores?

Data Classification

- How granular is the data classification (e.g., by sensitivity, regulatory requirement)?
- Can the classification criteria be customized to fit organizational needs?
- Is the classification process automated, reducing the need for manual tagging?
- Can your solution automatically and continuously classify discovered data stores?
- Can the solution classify data by analyzing actual content in data stores (vs. object/table/column names)?
- Can the solution classify data immediately and accurately without customer-defined rules, and can it be customized as needed?
- Can the solution map data to industry-standard frameworks (e.g., GDPR, PCI DSS, HIPAA)?
- Can the solution configure data sampling parameters to minimize compute costs?
- Can the classification parameters be customized to support unique customer data criteria?
- Can the solution uniquely identify data that appears within user-configurable proximity to other data classification values?
- Can the solution assess the monetary impact associated with the breach of a data store based on the sensitivity of the data involved?

Querying

- Can the solution support complex queries based on various criteria?
- How quickly can the solution retrieve and present queried data?
- Is the querying interface user-friendly and accessible to non-technical users?
- How flexible is your querying capability?
- What is the average response time for queries?
- Is the querying interface easy to use for all team members?

Access Governance

- How does the solution manage and control data access?
- Does the solution provide detailed audit trails of data access?
- How does the solution ensure consistent enforcement of access policies?
- Can the solution identify all users, roles, and resources with access to cloud data stores?
- Can the solution track the level of privileges associated with each user, role, and resource?
- Can the solution detect external (cross-account) users and roles with access to cloud data stores?
- Can the solution detect the level of exposure of resources within SaaS data stores?
- Does the solution provide detailed access and privilege visibility for all users across all cloud data stores?
- Can the solution identify inactive privileges by tracking the last accessed date?

Risk Detection

- How well does the solution detect potential threats and vulnerabilities?
- Can the solution identify unusual data access patterns?
- How quickly does the solution respond to detected risks?
- What types of risks can your solution detect?
- How effective is your anomaly detection capability?
- What is the response time for detected risks?
- Can the solution detect potential attack paths that could lead to a breach of valuable or sensitive data?
- Can the solution check detected risks against industry benchmarks and compliance standards?
- Can the solution build custom queries to detect and find potential data security risks unique to an organization's cloud environment?
- Can the solution build custom risk detection rules that combine valuable or sensitive data, access, risk, and configurations?
- Can the solution identify risks based on activity and/or events?
- Can the solution detect anomalous behavior indicators associated with potential data exfiltration and account takeover threats?
- Can the solution associate the monetary value of data stores with detected risks?

Risk Quantification

- How does the solution assess the potential impact of identified risks?
- Does the solution help prioritize risks based on their potential impact?
- Are the risk quantification results presented in a clear and actionable format?

Remediation

- What specific remediation actions does your DSPM solution support?
- How does your solution generate and implement remediation plans?
- What integrations with ticketing and routing tools do you have?

- How do you ensure data security during the remediation process?
- Can you provide examples of successful remediation cases?
- Can the solution provide detailed remediation steps for each risk?

System Compliance

- Does the solution support compliance with all relevant regulations (e.g., GDPR, HIPAA)?
- How does the solution help prepare for regulatory audits?
- Are compliance reports generated automatically, and are they customizable?
- Can the solution categorize risks, report data compliance gaps, and map results to industry compliance benchmarks?
- Can the solution provide an executive dashboard and export meaningful information to data officers?
- Can the solution provide graph-powered guidance to visualize and query attack paths to valuable or sensitive data?
- Does the solution offer role-based access control?

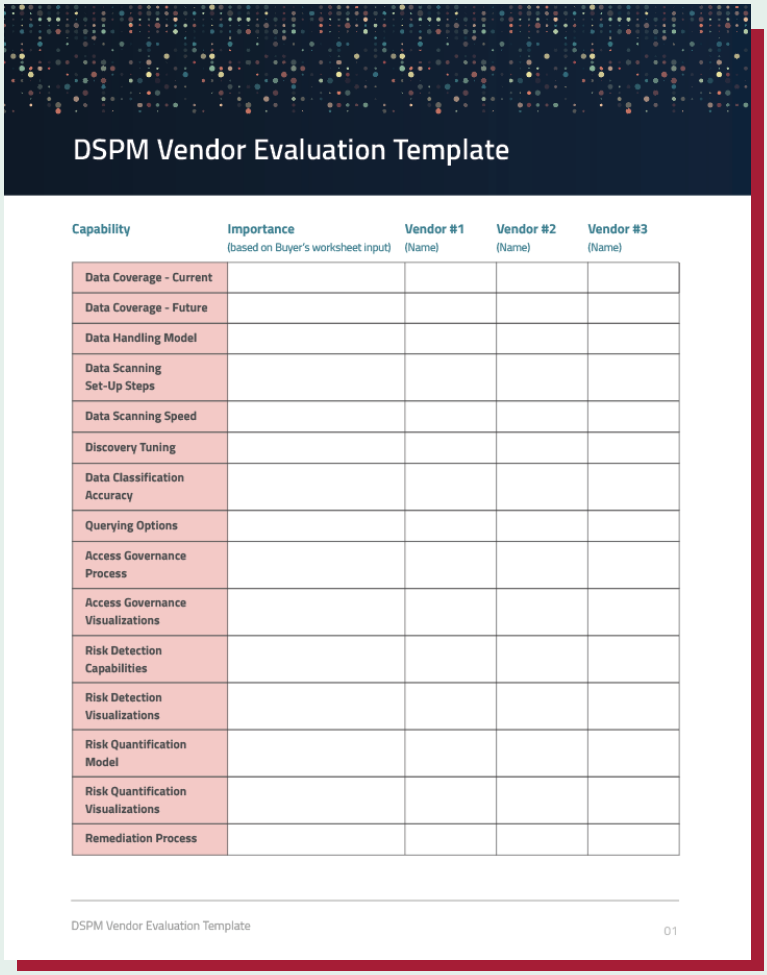
Use of AI and Automation

- Does the solution use AI to automate data security processes? If so, explain.
- Can the AI predict potential threats and vulnerabilities?
- How does AI improve the efficiency of data security measures?
- How do you use AI to automate data security processes?
- How does AI improve the efficiency of your solution?
- Does the solution support SSO authentication?
- Does the solution provide documented and accessible API enabling integration with
- external tools?
- Can the solution trigger notifications and workflows to external third-party tools?

Onboarding

- How easy and well-documented is the onboarding experience, and can it be completed with minimal assistance?
- Can the solution integrate with IaaS, PaaS, and SaaS without requiring
- How quickly can the solution provide risk and compliance insights after onboarding?

DSPM Vendor Evaluation Template



DSPM Vendor Evaluation Template

Capability	Importance (based on Buyer's worksheet input)	Vendor #1 (Name)	Vendor #2 (Name)	Vendor #3 (Name)
Data Coverage - Current				
Data Coverage - Future				
Data Handling Model				
Data Scanning Set-Up Steps				
Data Scanning Speed				
Discovery Tuning				
Data Classification Accuracy				
Querying Options				
Access Governance Process				
Access Governance Visualizations				
Risk Detection Capabilities				
Risk Detection Visualizations				
Risk Quantification Model				
Risk Quantification Visualizations				
Remediation Process				

DSPM Vendor Evaluation Template 01

Download Here

Use Cases and Additional Resources

While DSPM is a foundational solution supporting many use cases, here are several stories of actual DSPM implementations within specific industries or business environments. Names of organizations and vendors have been anonymized to eliminate bias.

Enhancing Overall Data Security Posture

TechCorp, a mid-sized technology company, faced challenges in managing their data security across a hybrid environment of on-premises and multiple cloud platforms. Their legacy data security tools, designed for on-premises monitoring, were inadequate for the dynamic nature of modern cloud environments. TechCorp's security team was struggling to maintain visibility and control over their data assets, leading to potential security gaps and compliance risks.

To address these issues, TechCorp decided to implement a DSPM solution. The DSPM tool provided comprehensive data discovery and classification across their entire data landscape, including AWS, Azure, and on-premises servers. Within weeks, TechCorp's security team had a complete inventory of all their data assets and their associated risks.

The DSPM solution automated the classification of valuable or sensitive data, mapping it to relevant regulatory frameworks such as GDPR and HIPAA. This automation reduced the manual workload on the security team and ensured that all valuable or sensitive data was appropriately protected. Additionally, the tool's continuous monitoring capabilities provided real-time alerts on any unauthorized access or potential vulnerabilities.

With the enhanced visibility and control provided by the DSPM solution, TechCorp's security team could proactively manage their data security posture. They replaced their outdated security tools with the DSPM platform, which offered better integration with their cloud environments and streamlined their compliance efforts. As a result, TechCorp significantly reduced their risk of data breaches and improved their overall security posture.

Implementing a Zero Trust Architecture

HealthcareInc, a leading healthcare provider, recognized the need to implement a Zero Trust architecture to ensure stringent verification for every access request. Their primary challenge was gaining a clear understanding of who could access their sensitive patient data and ensuring that only authorized users had the appropriate access.

HealthcareInc selected a DSPM solution to support their Zero Trust initiative. The DSPM tool began by discovering and classifying all valuable or sensitive data across their cloud and on-premises environments. This included patient records, billing information, and other sensitive healthcare data.

The DSPM solution's access governance capabilities provided detailed visibility into who had access to what data. The tool identified over-privileged users and roles with excessive access rights, which were promptly addressed by the security team. The DSPM platform also integrated with HealthcareInc's existing identity management system, allowing for seamless enforcement of least privilege access policies.

By continuously monitoring data access patterns, the DSPM solution detected any anomalies or unusual access requests in real-time. This proactive approach enabled HealthcareInc to quickly respond to potential security threats and ensure that only verified users could access sensitive data.

With the DSPM tool in place, HealthcareInc successfully implemented their Zero Trust architecture. The solution provided the necessary insights and controls to manage data access securely, significantly reducing the risk of unauthorized access and data breaches.

Anomaly Detection and Breach Prevention

FinTech Solutions, a financial services company, was concerned about the increasing frequency of data breaches in the industry. They wanted to enhance their ability to detect unusual data access patterns and prevent potential breaches using advanced anomaly detection technologies.

FinTech Solutions implemented a DSPM solution with AI-driven anomaly detection capabilities. The tool started by conducting a thorough data discovery and classification process, identifying all valuable or sensitive financial data across their cloud and on-premises environments.

Once the initial scan was completed, the DSPM solution continuously monitored data access patterns, using machine learning algorithms to establish a baseline of normal activity. Any deviations from this baseline, such as unusual access requests or large data transfers, triggered real-time alerts.

One afternoon, the DSPM tool detected an unusually high volume of data being accessed from a privileged account. The security team was immediately notified and investigated the incident. They discovered that the account had been compromised by an external attacker attempting to exfiltrate valuable or sensitive data.

Thanks to the prompt alert from the DSPM solution, FinTech Solutions was able to stop the data exfiltration in progress and secure the compromised account. The tool's detailed audit logs provided valuable insights into the incident, helping the team understand how the breach occurred and implement measures to prevent similar attacks in the future.

By leveraging the anomaly detection capabilities of their DSPM solution, FinTech Solutions significantly improved their breach prevention efforts. The proactive monitoring and real-time alerts enabled them to detect and respond to potential threats swiftly, minimizing the risk of data breaches.

Scaling Security Operations

RetailChain, a global retail company, was experiencing rapid growth and expansion into new markets. With this growth came an increasing volume of data and a corresponding rise in security challenges. RetailChain needed a way to manage their growing security needs without proportionally increasing their headcount.

RetailChain implemented a DSPM solution to scale their security operations efficiently. The DSPM tool began by discovering and classifying all data across their diverse environments, including multiple cloud platforms and on-premises data centers.

The solution's automation capabilities played a crucial role in scaling RetailChain's security operations. Automated data discovery and classification reduced the manual workload on their security team. The tool also provided AI-driven risk assessment and anomaly detection, enabling the team to focus on high-priority security issues.

To further enhance efficiency, the DSPM solution integrated with RetailChain's existing security orchestration, automation, and response (SOAR) platform. This integration allowed for seamless automation of remediation workflows. When a security alert was triggered, the DSPM tool automatically generated and assigned remediation tasks to the appropriate team members, streamlining the incident response process.

With the DSPM solution in place, RetailChain's security team could manage a larger volume of data and security events without needing to hire additional staff. The automation and AI capabilities of the DSPM tool improved the team's efficiency and effectiveness, enabling them to scale their security operations to meet the demands of their growing business.

Secure Development Life Cycle (SDLC) Enhancements

DevOpsTech, a software development company, wanted to integrate security into their Secure Development Life Cycle (SDLC), particularly in their DevOps and DevSecOps environments. Their goal was to identify and remediate security issues early in the application development process.

DevOpsTech selected a DSPM solution to enhance their SDLC. The tool was integrated into their development pipeline, providing continuous data discovery and classification throughout the development

lifecycle. This integration allowed the security team to monitor data security from the initial stages of development through deployment.

The DSPM solution's automated classification capabilities ensured that valuable and sensitive data was identified and protected during development. The tool also provided detailed visibility into data access and usage, allowing the security team to enforce least privilege access policies for developers and other stakeholders.

When the DSPM tool detected potential security risks, such as critical data exposure or improper access permissions, it generated real-time alerts and remediation recommendations. These alerts were integrated with DevOpsTech's existing issue tracking system, ensuring that security issues were promptly addressed by the development team.

By incorporating the DSPM solution into their SDLC, DevOpsTech significantly enhanced their security posture. The continuous monitoring and automated risk assessment capabilities allowed them to identify and mitigate security issues early in the development process, reducing the risk of data breaches and improving overall application security.

Performing Data Hygiene

EduData, an educational institution, was facing challenges with managing their growing volume of data. They needed to clean up, back up, and eliminate unnecessary data to reduce cloud costs and minimize attack surfaces.

EduData implemented a DSPM solution to streamline their data hygiene efforts. The DSPM tool began by conducting a comprehensive data discovery process, identifying all data assets across their cloud and on-premises environments. This included both active and abandoned data stores.

The solution's classification capabilities allowed EduData to identify critical data that needed to be retained and protected. The tool also detected duplicate and unnecessary data, providing recommendations for data clean-up and optimization.

Using the DSPM solution, EduData automated their data hygiene processes. The tool generated actionable insights and recommendations for data clean-up, such as archiving old data, deleting duplicates, and optimizing storage costs. These recommendations were integrated into EduData's existing data management workflows, allowing for seamless execution.

With the DSPM solution in place, EduData successfully cleaned up their data environment, reducing cloud storage costs and minimizing their attack surface. The automated data hygiene processes ensured that their data was well-managed and secure, enabling them to focus on their core educational mission

Addressing Data Privacy and Compliance Requirements

HealthPlus, a healthcare provider, needed to update their data and access governance strategies to meet

stringent compliance standards such as GDPR, HIPAA, and CCPA. Ensuring the privacy and security of patient data was a top priority for the organization.

HealthPlus implemented a DSPM solution to address their data privacy and compliance requirements. The tool began by discovering and classifying all sensitive patient data across their cloud and on-premises environments. This included electronic health records, billing information, and other valuable or sensitive data.

The DSPM solution's compliance mapping capabilities allowed HealthPlus to automatically map their data to relevant regulatory frameworks. The tool provided detailed insights into compliance gaps and generated actionable recommendations for remediation.

With the DSPM solution, HealthPlus automated their compliance monitoring processes. The tool continuously monitored data access and usage, providing real-time alerts for any potential compliance violations. The solution also generated customizable compliance reports, ensuring that HealthPlus was always audit-ready.

By leveraging the DSPM solution, HealthPlus significantly improved their data privacy and compliance posture. The automated compliance monitoring and reporting capabilities reduced the burden on their security team and ensured that patient data was protected in accordance with regulatory standards.

Managing Complex Data Projects

MegaBank, a multinational financial institution, was undertaking a major merger and acquisition (M&A) project. The success of this project depended on accurately discovering and classifying data assets from both organizations involved in the merger.

MegaBank implemented a DSPM solution to manage their complex data project. The tool began by discovering and classifying data across both organizations' environments, including cloud, on-premises, and hybrid data stores. This comprehensive data discovery process provided MegaBank with a complete inventory of all data assets involved in the merger.

The DSPM solution's classification capabilities allowed MegaBank to identify and protect valuable or sensitive data, such as financial records and customer information. The tool also provided insights into potential data security risks and compliance gaps, enabling the security team to address these issues proactively.

Throughout the M&A project, the DSPM solution continuously monitored data access and usage, ensuring that critical data was protected and compliance requirements were met. The tool's integration with MegaBank's existing security tools allowed for seamless automation of remediation workflows, ensuring that any identified risks were promptly addressed.

By leveraging the DSPM solution, MegaBank successfully managed their complex data project. The comprehensive data discovery and classification capabilities provided the necessary insights and controls

to ensure the security and compliance of their data assets throughout the merger process.

Enabling Responsible Use of AI Across Enterprise

TechInnovate, a leading technology company, was adopting large language models (LLMs) to enhance their AI capabilities. However, they needed to ensure that the valuable or sensitive data used in their AI systems was properly classified and protected to prevent data breaches and comply with regulatory requirements.

TechInnovate implemented a DSPM solution to enable the responsible use of AI across their enterprise. The tool began by discovering and classifying all data used in their AI systems, including training data for LLMs like ChatGPT and Microsoft Copilot.

The DSPM solution's classification capabilities ensured that critical data was identified and protected before being used in AI models. The tool also provided insights into potential data privacy and security risks, enabling the security team to address these issues proactively.

The DSPM solution integrated with TechInnovate's AI platforms, providing real-time sensitivity analysis of data going into and out of their LLMs. This integration allowed TechInnovate to monitor and control the use of valuable or sensitive data by their AI systems, ensuring that data privacy and security were not compromised.

With the DSPM solution in place, TechInnovate successfully enabled the responsible use of AI across their enterprise. The comprehensive data discovery and classification capabilities provided the necessary insights and controls to ensure that their AI systems were secure and compliant, enhancing the overall quality and trustworthiness of their AI-generated insights.

Performing Data Clean-Up

EduTech, an educational technology company, was dealing with an extensive amount of data, including backups that were created from a primary data set but the initial data set was deleted. These orphaned backups were consuming storage space and increasing costs unnecessarily.
EduTech decided to implement a DSPM solution to address their data clean-up needs. The DSPM tool began by discovering all data assets across their cloud and on-premises environments, including active data, backups, and shadow data stores.

The solution's classification capabilities allowed EduTech to identify valuable or sensitive data that needed to be retained and protected. The tool also detected duplicate and unnecessary data, including orphaned backups that were no longer needed.

Using the DSPM solution, EduTech automated their data clean-up processes. The tool generated actionable insights and recommendations for data clean-up, such as archiving old data, deleting duplicates, and optimizing storage costs. These recommendations were integrated into EduTech's existing data management workflows, allowing for seamless execution.

With the DSPM solution in place, EduTech successfully cleaned up their data environment, reducing cloud storage costs and minimizing their attack surface. The automated data clean-up processes ensured that their data was well-managed and secure, enabling them to focus on their core educational mission.

Source: Big Data statistics

Resources and Citations

1. Gartner® research, "Innovation Insight: Data Security Posture Management." Published 28 March 2023 by analysts Brian Lowans, Joerg Fritsch, Andrew Bales, ID G00784502. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.
2. Tenable State of Cloud Security Maturity report
3. 2024 GigaOm Radar for Data Security Posture Management
4. Gartner Innovation Insight: Data Security Posture Management
5. Omdia: On the Radar: Normalyze Scans Clouds to Manage Data Security Posture
6. GigaOm Radar for Data Security Platforms
7. ESG Report: 2023 Cloud Data Security
8. Top Takeaways from the Gartner® Innovation Insight: Data Security Posture Management
9. 77+ Surreal Big Data Statistics To Map Growth in 2024
10. Gartner Predicts Solid Growth for Information Security, Reaching $287 Billion by 2027

proofpoint.

Contact Us

Phone: +1.408.517.4710

Web: proofpoint.com/us/contact

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 85% of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com

Connect with Proofpoint: X | LinkedIn | Facebook | YouTube

DISCOVER THE PROOFPOINT PLATFORM →