Enterprise Strategy Group by TechTarget

BRIEF

SEPTEMBER 2024

Streamlining Data Security Posture Management (DSPM) Implementations

Todd Thiemann, Senior Analyst

Abstract: DSPM comprises technology and processes that continuously monitor and assess an organization's data security controls across all infrastructure, including on-premises data centers and private and public cloud environments. Recent data resilience research by TechTarget's Enterprise Strategy Group revealed some interesting findings when it comes to DSPM solution deployment and top use cases. While DSPM tools are relatively quick to deploy compared to other security technologies, organizations need to consider the people, process and technology when implementing DSPM and ensure they strategically plan an approach that will meet future needs to support scale and innovation, including usage of AI and generative AI (GenAI).

Overview

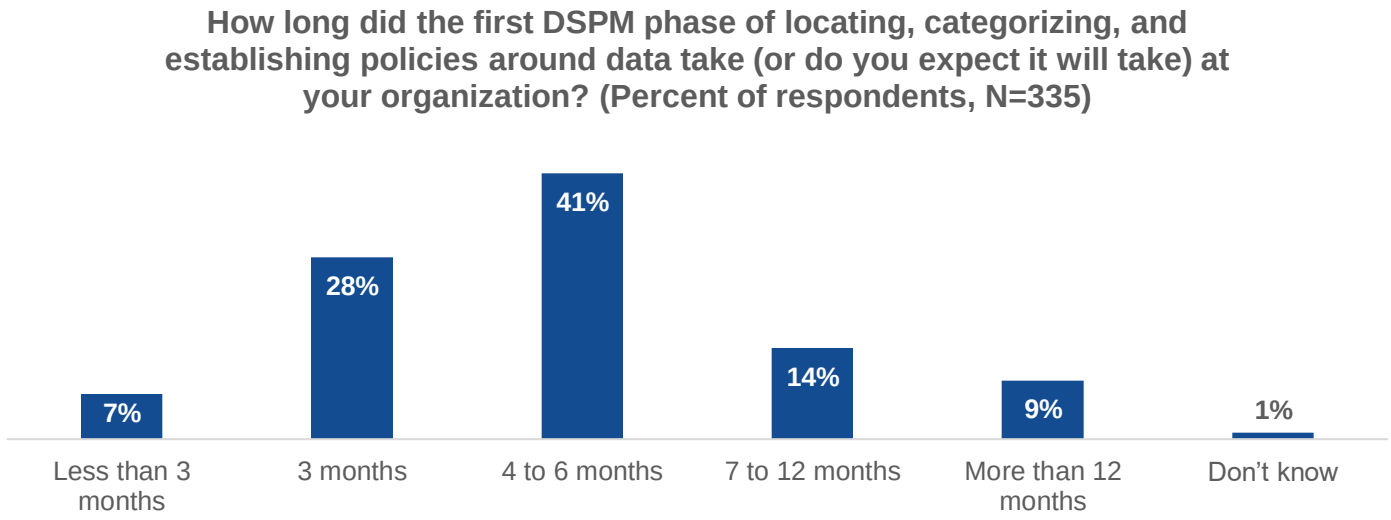
Enterprise Strategy Group completed a data resilience survey of 370 respondents at midmarket (i.e., 100 to 999 employees) and enterprise (i.e., 1,000 or more employees) organizations in North America. As part of that research, respondents revealed that the initial stage of DSPM deployment took approximately three to six months.[1]

Analysis

DSPM deployments involve a combination of technology, people, and processes to discover and categorize data stores to identify weaknesses, prioritize risks, and ensure data remains protected from evolving threats on an ongoing basis. The scale of operations varies across enterprises as one might expect, but on average the initial phase of locating, categorizing, and establishing policies takes four to six months for most enterprises (see Figure 1). DSPM projects involve a variety of constituents and can touch complex environments residing both in the cloud and on premises.

[1] Source: Enterprise Strategy Group Complete Survey Results, *Data Resilience Emerges: The Collision of Data Discovery, Protection, Security, and Governance*, August 2024. All charts and research references in this brief come from these complete survey results.

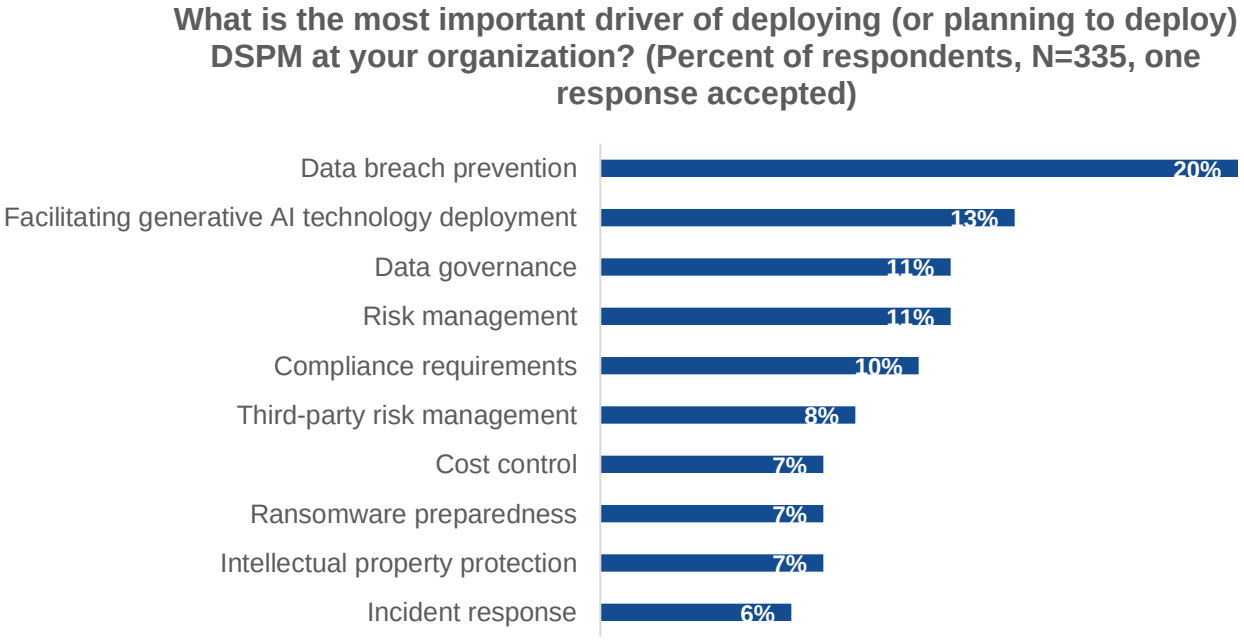
Figure 1. Duration of Initial Phase in DSPM Deployment



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Enterprises deploy DSPM to address a number of issues. As shown in Figure 2, the most prevalent use case is preventing a potential data breach (20%), followed by facilitating the deployment of GenAI technology (13%). Enterprises want to know where their sensitive data is stored and categorize what is inside of their data stores so they can take steps to avoid potential data leakage and loss. In the case of GenAI, locating and categorizing data used to inform large language models can help avoid potentially sensitive information making its way into a model and subsequently being inadvertently leaked.

Figure 2. Primary Drivers for DSPM Deployment



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Achieving DSPM Deployment Success

Ensuring that you have clear objectives and a strong project plan will accelerate DSPM deployment and optimize project success. What follows are the typical steps that Enterprise Strategy Group has observed in successful DSPM implementations. Every organization is different, and the order and exact elements of the below steps will vary depending on your organization.

1. Stakeholder Alignment

- **Engage key stakeholders.** Start by aligning key stakeholders, including governance, risk, and compliance (GRC) personnel, data teams, cloud architects, and security teams. Ensure that everyone understands the objectives, benefits, and their roles in the DSPM deployment process.
- **Define goals, definitions, and metrics.** Collaboratively establish the goals of the DSPM initiative, such as reducing data exposure, achieving compliance, and improving overall data security posture. Arrive at what data is sensitive to the business and data classification definitions. Agree on key performance indicators to measure success.
- **Secure executive buy-in.** Present a clear case to executives, highlighting the importance of DSPM in mitigating data risks, achieving regulatory compliance, and supporting business goals. Ensure top-down support for resource allocation and prioritization.
- **Assign roles and responsibilities.** Clearly define the responsibilities of each team. GRC will focus on compliance and policy alignment, data teams will manage data classification and ownership, and security teams will oversee the implementation of security controls and monitoring.

2. Assess Current Data Environment

- **Inventory data stores.** Begin by cataloging all data stores across your environment, including cloud, on-premises, SaaS, IaaS, PaaS, and hybrid systems. DSPM tools can help in this effort, particularly in identifying any unmonitored “shadow data” to which IT and security teams lack visibility.

3. Identify Exposed Data Stores and Begin Mitigating Risks

- **Discover exposed data.** Use DSPM tools to scan and identify data stores that are exposed to potential threats, such as those lacking encryption or with open-access permissions.
- **Scan for misconfigurations.** Regularly scan your environment for misconfigurations in data stores, access controls, and security settings.
- **Mitigate exposure and automate remediation.** Implement immediate corrective actions, such as applying encryption, restricting public access, and ensuring proper authentication mechanisms. Use DSPM tools to automatically correct misconfigurations or flag them for immediate attention by the relevant teams.

4. Identify Data Stores With Critical Data

- **Valuable and sensitive data discovery.** Locate data stores containing critical and sensitive data, including cardholder data (PCI DSS), protected health information, personally identifiable information, and data covered by GDPR.
- **Monitor access patterns.** Regularly monitor these stores for unusual access patterns that could indicate potential security breaches.

5. Classify Data

- **Data classification.** Categorize data based on sensitivity and compliance requirements of your organization. For example, use classifications like public, internal, sensitive, and restricted.
- **Automate classification.** Consider implementing automated tools that can classify data in real time as it enters your environment, reducing manual effort.

6. Determine Necessary Security Controls Based on Classification

- **Apply security controls.** Implement security measures such as encryption, tokenization, or masking based on the data's classification level.
- **Continuous monitoring.** Set up continuous monitoring for all data stores to detect unauthorized access or changes in data classification.

7. Identify and Delegate Data Owners

- **Assign ownership.** Designate data owners who are responsible for managing access and ensuring compliance with security policies for each data store.
- **Document responsibilities.** Clearly define the roles and responsibilities of data owners to avoid confusion and ensure accountability.

8. Identify Users with Access to Sensitive/Restricted Data

- **Access review.** Regularly audit who has access to sensitive and restricted data to ensure it aligns with their role and responsibilities.
- **Justify access.** Determine if access is necessary for their job function. If not, remove or restrict access.

9. Restrict Access to Need-to-know and Least Privilege

- **Enforce least privilege.** Ensure that users only have access to the data they need for their job, following the principle of least privilege.
- **Implement role-based access control.** Use RBAC to manage user permissions and restrict access based on job roles.

10. Segment Data Types to Control Sprawl of Restricted Data

- **Data segmentation.** Segment data into different categories based on sensitivity, regulatory requirements, and business value that might require special treatment or controls.
- **Isolate critical data.** Place sensitive and high-value data in isolated environments or segments with stricter security controls.

11. Determine Necessary Security Controls Based on Classification

- **Apply security controls.** Implement security measures such as encryption, tokenization, or masking based on the data's classification level.
- **Continuous monitoring.** Set up continuous monitoring for all data stores to detect unauthorized access or changes in data classification.

12. Implement Continuous Compliance Checks

- **Automate compliance audits.** Schedule regular audits to ensure ongoing compliance with industry regulations (e.g., PCI DSS, GDPR, HIPAA) and internal policies.
- **Generate compliance reports.** Use DSPM tools to generate real-time compliance reports that can be shared with stakeholders and auditors.

13. Enable Observability by Establishing Alerts and Incident Response

- **Set up alerts.** Configure your DSPM solution to trigger real-time alerts for any suspicious activity, such as unauthorized access attempts or data exfiltration.
- **Incident response plan.** Develop and implement an incident response plan that specifies actions to take in the event of a security breach.

14. Evaluate and Iterate

- **Regular assessments.** Periodically assess the effectiveness of your DSPM implementation and adjust as needed to address new threats or business changes.
- **Feedback loop.** Establish a feedback loop with key stakeholders to continuously improve DSPM strategies and tools.

15. Do an Ongoing Validation of Classification and Remediation Steps

- **Continuous classification review.** Regularly review and validate the accuracy of data classification to ensure that all sensitive data is properly identified, especially as data evolves or new types of data are introduced.
- **Remediation validation.** Continuously validate that remediation steps taken to secure or remove sensitive data are effective. This includes verifying that access controls are enforced, encryption is properly applied, and data is securely deleted or archived as needed.
- **Audit and feedback loop.** Implement an ongoing audit process to assess the effectiveness of your classification and remediation strategies. Collect feedback from stakeholders to identify any gaps or areas for improvement.
- **Automated validation.** Utilize your DSPM solution to regularly validate that classification and remediation protocols are being followed correctly, ensuring compliance and security standards are consistently met.

16. Educate and Train Teams

- **Ongoing training.** Provide regular training sessions for IT, security, and data teams to stay updated on DSPM practices, tools, and the latest threats.
- **Cross-team collaboration.** Encourage collaboration between data owners, security teams, and compliance officers to ensure consistent data protection practices.

Conclusion

Understanding and improving your data security posture helps avoid breaches and enable a smoother and safer deployment for new initiatives like GenAI applications. Successful DSPM deployments involve a combination of people, process, and technology. Given that DSPM touches on multiple organizational functions within the enterprise including security, IT, and data governance, ensuring alignment and engagement on an ongoing basis enables you to get the most value from your DSPM investment.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com