COHESITY

GUIDE D'ACHAT

NAVIGUEZ PARMI LES RISQUES LIÉS AUX DONNÉES ET À L'IA AVEC LA BONNE SOLUTION DSPM

Synthèse

Les données sensibles sont désormais distribuées sur vos plateformes cloud, SaaS, bases de données, sauvegardes, infrastructures hybrides, NAS, et plus encore. Vous avez probablement déjà plus de données que vous ne pouvez en gouverner facilement. Mais il est difficile de comprendre où se trouvent vos données les plus sensibles, dans quelle mesure elles sont exposées, qui y a accès et si cet accès est approprié.

Cela crée une situation explosive qui accentue les risques pour l'entreprise au niveau du conseil d'administration. Et le défi s'intensifie : Alors même que les utilisateurs continuent d'accéder à ces données, de les modifier et de les transférer, les agents d'IA font apparaître des risques nouveaux et croissants.

Ces lacunes en matière de sécurité et de protection expliquent pourquoi la gestion de la posture de sécurité des données (DSPM) est devenue une priorité stratégique pour les dirigeants d'entreprise modernes.

89 % **des responsables de la sécurité indiquent que le statu quo en matière de sécurité des données dans leur entreprise est un problème.**

39 % **des responsables de la sécurité indiquent que les technologies héritées sont insuffisantes pour les exigences actuelles.**

60 % **des entreprises manquent de visibilité sur au moins la moitié de leur patrimoine de données.**[1]

[1]Livre blanc Omdia : Réussir la cyber-résilience grâce à une intelligence des données exploitable

Une solution DSPM moderne devrait vous permettre de faire bien plus que simplement gérer vos données d'inventaire. Elle devrait vous aider à réduire activement les risques, à renforcer la cyber-résilience et à répondre aux questions critiques lors de la réponse aux incidents, d'exercices de sécurité ou d'audits :

- Où se trouvent nos données sensibles et de quelles données s'agit-il ?
- Qui ou quoi y a accès ?
- Que devons-nous corriger en premier ?
- Comment réduisons-nous les risques sans ralentir l'innovation et la croissance de l'entreprise ?
- Les données sont-elles protégées et peuvent-elles être récupérées rapidement, en toute sécurité et en toute conformité ?

Pour les responsables de la sécurité, cela signifie passer de la visibilité à une réduction des risques actionnable, avant et après une attaque.

Ce guide s'adresse aux équipes qui évaluent des solutions DSPM, afin que vous puissiez choisir celle qui correspond le mieux à vos besoins.

L'inventaire ne suffit pas.

La véritable question pour l'acheteur n'est pas de savoir si une solution est capable de vous indiquer où se trouvent les données. Il s'agit de savoir si la solution peut identifier et montrer *pourquoi* elles présentent un risque élevé et ce que vous pouvez faire maintenant pour remédier à ce risque.

Ce qu'un DSPM résout

L'une des erreurs les plus courantes chez les entreprises lors de l'évaluation du DSPM est de traiter le DSPM comme un simple outil de découverte. Une solution DSPM fournit bien plus qu'une visibilité. La bonne solution devrait vous aider à résoudre les problèmes liés à la gestion des risques liés aux données.

Voici cinq problèmes que votre solution DSPM devrait vous aider à résoudre :

Problème	Comment le DSPM le résout-il ?
Je ne sais pas où se trouvent mes données sensibles.	De nombreuses entreprises ne sont pas en mesure de dire avec certitude où se trouvent leurs données les plus précieuses ou soumises à une réglementation dans leurs environnements cloud, SaaS et hybrides. Pourquoi ce statu quo ? Les outils traditionnels de sécurité des données cloisonnés en fonction de types de données spécifiques, à certains modèles de déploiement ou à des cas d'utilisation particuliers. Même lorsqu'ils disposent d'un inventaire, celui-ci est souvent incomplet, obsolète ou déconnecté du contexte des risques. Une architecture native du cloud moderne est nécessaire pour suivre le rythme du volume et de la prolifération des données.
Je ne sais pas quoi ou qui accède (ou peut accéder) à mes données.	L'employé type interagit avec environ 36 services cloud par jour, à travers plus de 200 outils de collaboration. Les informations sensibles se propagent sur toutes les plateformes et sont souvent partagées en dehors des contrôles de gouvernance établis. Les données sensibles présentent un risque encore plus grand lorsqu'elles sont surexposées, font l'objet d'autorisations excessives, sont partagées à une échelle trop large, sont stockées au mauvais endroit ou sont accessibles à un nombre d'utilisateurs (y compris non humains) supérieur à celui prévu. Votre solution DSPM devrait vous aider à comprendre quelles données présentent un risque, pas seulement quelles données correspondent à une stratégie de classification.
Je ne sais pas quels risques liés aux données je dois prioriser pour la remédiation.	La plupart des environnements d'entreprise contiennent de grandes quantités de données sensibles. Cependant, tous les risques liés aux données n'ont pas le même degré d'urgence. Les équipes ont besoin d'un moyen de distinguer le bruit de fond des informations pertinentes. La bonne solution doit vous permettre de vous concentrer sur les problèmes susceptibles d'avoir le plus grand impact sur votre activité, en tenant compte de la sensibilité, de l'accès, de l'exposition, de l'environnement et du contexte commercial identifié.
Je ne peux pas remédier aux risques liés aux données rapidement ou automatiquement.	Le contexte des données, associé à une intégration poussée de l'ensemble de la chaîne d'outils de sécurité, est essentiel pour réduire le temps moyen de réponse (MTTR, mean time to respond) lors de la correction des données présentant un risque élevé. Les méthodes traditionnelles de sécurité des données s'appuient largement sur des modèles et des balises, ce qui submerge les équipes d'alertes intempestives qui manquent souvent de crédibilité. Les solutions DSPM doivent favoriser l'action. Les conclusions doivent être compréhensibles, attribuables et traçables. Les équipes de sécurité et informatiques doivent être en mesure d'agir en toute confiance.
Lorsque j'ai besoin de restaurer des données, c'est lent, risqué et coûteux.	Les données secondaires (telles que les sauvegardes) sont essentielles en matière de réponse aux incidents et de restauration. Ces données peuvent également présenter des risques et entraîner des violations potentielles des règles de conformité, auxquels il convient de remédier. Les solutions DSPM modernes devraient renforcer la cyber-résilience et fournir des informations issues de l'analyse des données afin de garantir la mise en œuvre de niveaux de protection adéquats. Les données sensibles doivent être classées par ordre de priorité et récupérées en toute conformité pendant la réponse aux incidents.

À quoi ressemble une situation « idéale »

Avant d'évaluer les fournisseurs, vous devez définir ce que vous entendez par « bon ». Voici cinq domaines dans lesquels une solution DSPM moderne doit exceller :

Déployer rapidement et évoluer sans limites

Une bonne solution de découverte devrait vous permettre d'obtenir rapidement une vue d'ensemble plus complète de votre exposition, sans nécessiter un cycle de mise en œuvre long et fastidieux avant d'en percevoir les avantages.

Les entreprises doivent s'attendre à ce que des centaines de pétaoctets soient analysés en continu, sans que cela n'affecte les performances. Le bon fournisseur offrira une prise en charge étendue dans les environnements clés, y compris les magasins de données cloud, les applications SaaS, les systèmes de fichiers et les bases de données locales, le cas échéant.

Éliminez les angles morts grâce à une découverte et une classification précises

Une phase de découverte rigoureuse permet d'éviter que des résultats de mauvaise qualité ne compromettent l'ensemble des résultats ultérieurs. Si l'outil DSPM passe à côté d'éléments critiques, classe de manière erronée des informations sensibles ou nécessite trop de réglages manuels, les résultats seront moins utiles, voire sans intérêt.

La bonne solution DSPM identifie les angles morts en s'adaptant à votre environnement et en classifiant automatiquement les données (y compris la propriété intellectuelle et les données particulièrement importantes pour votre entreprise).

Hiérarchiser le risque réel, pas le bruit

Le temps est limité : aucune équipe ne peut tout corriger en même temps. Une solution DSPM performante combine les données d'exposition et le contexte pour se concentrer sur les dangers les plus importants. Elle doit donner la priorité aux risques liés à des données hautement sensibles avec des expositions étendues.

Cela nécessite des capacités avancées permettant de mettre en corrélation la sensibilité des données, la finalité métier, les identités, l'activité d'accès et l'exposition afin de mettre en évidence les risques réels pour l'entreprise.

Automatiser la remédiation à grande échelle

Les DSPM modernes doivent aider les organisations à réduire leur exposition, pas seulement à l'observer. Les entreprises devraient rechercher des DSPM qui proposent des mesures correctives prêtes à l'emploi. Par exemple, les solutions de pointe proposent des commandes accessibles d'un simple clic pour révoquer des accès, masquer des données, masquer des données exposées, déclencher des workflows prédéfinis ou acheminer les problèmes directement aux propriétaires des données, le tout avec toutes les informations nécessaires pour résoudre rapidement les problèmes.

Cela est particulièrement important à l'échelle de l'entreprise, lorsque de nombreuses équipes sont impliquées. Les équipes de sécurité identifient souvent le problème, mais sa résolution peut dépendre de différents acteurs, tels que les administrateurs de stockage, les propriétaires des données, les équipes chargées de la gestion des identités ou les parties prenantes métier. Plus une solution facilite cette transition, plus elle a de chances de générer des résultats concrets qui renforcent votre posture de sécurité.

Renforcer la sécurité avant et après les incidents

Nous avons déjà abordé la réduction proactive des risques avant qu'une violation ne se produise. La bonne solution DSPM peut également fournir l'intelligence et le contexte des données nécessaires pour renforcer les efforts de restauration, en veillant à ce que les équipes de sécurité et de protection des données comprennent où se trouvent les données sensibles, quels actifs sont les plus critiques et si les protections appropriées ont été appliquées aux joyaux de la couronne de l'organisation.

En offrant une vision claire des données sensibles et stratégiques pour l'entreprise, votre DSPM doit éclairer et renforcer les stratégies de protection des données qui constituent le fondement de la cyber-résilience. Cela vous aidera à hiérarchiser les données les plus importantes pendant la restauration, à accélérer la réponse aux incidents avec un meilleur contexte et à réduire les coûts et la complexité en identifiant et en éliminant les données obsolètes, redondantes ou de faible valeur.

Le résultat est une boucle de rétroaction continue entre la visibilité, la protection, la réponse et la restauration. Avec une solution DSPM adaptée, vous devriez pouvoir relier ces fonctions entre elles afin de passer d'une approche fragmentée de la sécurité à une stratégie plus globale de sécurité des données et de cyber-résilience de bout en bout.

Kit d'évaluation des fournisseurs

Questions essentielles à poser aux fournisseurs

Les questions suivantes vous aideront à évaluer votre sélection de produits DSPM.

En matière de découverte et de couverture :

- Quels environnements cloud, SaaS, IA, de bases de données et hybrides prenez-vous en charge aujourd'hui ?
- Comment identifiez-vous et classez-vous les données sensibles dans différents types de données ? Combien de temps cela prend-il généralement ?
- Comment gérez-vous les données structurées et non structurées ? Avez-vous une meilleure prise en charge de l'un ou de l'autre ?
- Quel niveau de réglage est requis avant que les résultats ne soient exploitables ?
- Comment aidez-vous les clients à valider la couverture et le niveau de confiance dès le début ?

En matière d'exposition et de contrôles d'accès :

- Comment déterminez-vous si les données sensibles sont surexposées ? Pouvez-vous indiquer quelles identités, quels groupes ou quels utilisateurs ont accès à des données sensibles ?
- Comment identifiez-vous un accès large, excessif ou risqué ?
- Comment reliez-vous le contexte d'accès à la sensibilité des données ?
- Pouvez-vous empêcher que des données sensibles soient saisies ou sortent des modèles et des systèmes d'IA ?
- Pouvez-vous montrer comment votre solution met en évidence les problèmes présentant le plus grand risque ?

Sur la hiérarchisation et la correction des risques :

- Comment classez-vous ou hiérarchisez-vous les résultats ? Quels facteurs influencent la gravité ou la notation des risques ?
- Pouvez-vous montrer comment les équipes passent de nombreux résultats à un plan d'action gérable ?
- Comment votre solution guide-t-elle la correction ?
- Les résultats peuvent-ils être attribués aux bonnes équipes ou aux bons responsables ?
- Les informations peuvent-elles être transmises aux plateformes de protection des données de manière transparente et fournir de meilleurs résultats en matière de sécurité et de restauration ?

Sur le délai de rentabilisation et le déploiement :

- Qu'exige le déploiement initial de notre équipe ?
- À quelle vitesse pouvons-nous nous attendre à des résultats utiles ?
- À quoi ressemblerait notre réussite au cours des 30, 60 et 90 premiers jours ?

Signaux d'alerte à surveiller

Visibilité limitée sur le risque d'accès

L'accès aux données sensibles est le risque le plus important. Si un fournisseur n'est pas en mesure d'indiquer clairement qui (ou quoi) a accès aux données et quels sont les risques encourus, cela constitue une grave lacune.

Les résultats ne sont pas liés au risque et au contexte propres à chaque entreprise.

Chaque entreprise est différente. Le risque lié aux données sensibles ou à la propriété intellectuelle exposée peut varier en fonction des priorités de l'entreprise concernée. Les conclusions doivent s'appuyer sur le contexte appris et les classificateurs afin de fournir des recommandations précises en matière de correction des risques.

Impossibilité de relier les risques liés aux données aux résultats en matière de cyber-résilience

L'optimisation de la posture de risque des données et de l'IA est essentielle pour la cyber-résilience. L'intelligence des données doit servir à mettre en place une stratégie proactive de sécurité des données et à améliorer les résultats en matière de restauration. Les conclusions ne doivent pas être cloisonnées, d'autant plus que la mise en œuvre des mesures correctives implique souvent des équipes pluridisciplinaires.

La valeur dépend d'un effort manuel excessif

Un produit qui nécessite un réglage approfondi, une interprétation particulière ou la conception de processus spécifiques pour le client peut entraîner une augmentation des coûts d'exploitation et une complexité accrue.

Tableau de comparaison des fournisseurs

Utilisez ce tableau pour comparer les fournisseurs côte à côte sur les capacités de base requises pour une stratégie DSPM efficace. Lorsque vous passez en revue chaque ligne, ne vous contentez pas de vérifier si une fonctionnalité existe, mais évaluez également dans quelle mesure elle est mise en œuvre dans la pratique*.

Afin de rendre les comparaisons entre fournisseurs plus cohérentes et objectives, chaque fonctionnalité peut être évaluée à l'aide d'un système de notation simple allant de 0 à 5. Cette approche aide les équipes à aller au-delà d'une simple comparaison consistant à cocher des cases et à évaluer la force relative, la maturité et la facilité d'utilisation pratique de chaque capacité. Un score plus élevé devrait indiquer que cette fonctionnalité est non seulement disponible, mais aussi adaptée aux entreprises, efficace sur le plan opérationnel et qu'elle a fait ses preuves en termes de création de valeur à grande échelle.

Score	Définition
5	Des fonctionnalités de pointe, pleinement opérationnelles, hautement automatisées, évolutives et parfaitement intégrées
4	Capacité solide avec des fonctionnalités éprouvées et des lacunes mineures
3	Une capacité suffisante qui répond aux exigences essentielles, mais qui présente des limites en termes de profondeur, d'échelle ou de facilité d'utilisation
2	Prise en charge basique ou partielle présentant des lacunes notables, nécessitant un travail manuel ou ayant une applicabilité limitée
1	Capacité minimale, fonctionnalité à un stade précoce ou prise en charge très limitée
0	Non pris en charge ou aucune preuve significative fournie

Categorie	Fournisseur 1	Fournisseur 2	Fournisseur 3	Notes
Architecture native du cloud pour un déploiement rapide et sans agent				
Découverte continue des données à grande échelle et à grande vitesse				
Classification des données alimentée par l'IA				
Contextualisation des données				
Risques cartographiés sur les réglementations				
Contrôles d'accès et application adaptables				
Détection et réponse aux données en temps réel				
Alertes contextualisées				
Flux de travail de remédiation intégrés				
Intégration transparente avec les plateformes de protection des données				
Total				

**Les scores doivent être basés sur ce qui est généralement disponible aujourd'hui, et non sur les revendications de la feuille de route. Chaque score doit être validé à l'aide de démonstrations de produit, de références client, de documentation, d'exigences de déploiement et de preuves de la profondeur d'intégration.*

Conclusion

La sélection d'une solution DSPM ne se résume pas à une simple décision concernant les outils. Les enjeux sont trop importants. Les données continuent de se multiplier et de s'étendre à un rythme effréné, et les méthodes manuelles ou les technologies obsolètes ne parviennent pas à suivre le rythme. La bonne solution DSPM vous aidera à clarifier les choses, à mobiliser vos équipes, à réduire les risques et à renforcer à la fois la sécurité des données et la cyber-résilience. Cette solution s'avérera payante à long terme, car elle vous aidera à protéger et à sécuriser les données qui sous-tendent les modèles, les systèmes et les agents d'IA.

En savoir plus sur notre solution DSPM et comment elle peut optimiser vos données et votre posture de risque liée aux données et à l'IA. Ou contactez-nous dès aujourd'hui.

COHESITY

cohesity.com/fr
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

4500066-001-FR 5-2026