Guide du RSSI pour une sécurité des données à l'épreuve du temps grâce à une solution DSPM optimisée par l'IA

2025

Table of Contents

Naviguer dans l'environnement moderne de la sécurité des données

La croissance exponentielle et la dispersion des données sur de multiples plateformes ont accru la complexité, les coûts et les risques pour de nombreuses entreprises. Les responsables de la sécurité sont désormais confrontés à des défis importants pour comprendre et contrôler en profondeur leurs données critiques. Cette complexité est davantage accrue par l'adoption rapide de l'IA qui disperse davantage les données, rendant les entreprises plus vulnérables aux risques liés aux données et à la conformité.

Pour atténuer efficacement les risques de sécurité et garantir une conformité rigoureuse, les équipes chargées de la sécurité des données ont besoin d'outils innovants offrant une vision globale et en temps réel de l'ensemble de leurs données. La gestion de la posture de sécurité des données (DSPM) s'est imposée comme l'approche moderne de référence, permettant aux responsables de la sécurité des données d'atteindre cette visibilité et cette compréhension continues grâce à l'IA et à l'automatisation.

Cet e-book explore le potentiel transformateur de la gestion de la posture de sécurité des données (DSPM), permettant aux responsables de la sécurité et à leurs équipes de protéger proactivement les données sensibles. Conçu spécifiquement pour les professionnels de haut niveau en sécurité et gestion des risques, il fournit des informations exploitables pour gérer les complexités de l'environnement moderne de la sécurité des données. Ce guide complet vous permet de renforcer la sécurité des données de votre entreprise tout en explorant les tendances critiques. Il aborde les défis urgents et dévoile des stratégies innovantes, soulignant ainsi le rôle indispensable de la gestion de la posture de sécurité des données (DSPM) lors de la sécurisation de vos actifs de données à l'ère dynamique de l'IA.

L’impératif du RSSI : maîtriser la sécurité des données à l’ère de l’IA

Pour les responsables de la sécurité des systèmes d’information (RSSI), l’adoption rapide de l’IA et des technologies cloud pose un dilemme majeur. Tout en offrant des opportunités sans précédent de réduction des coûts, d’amélioration des résultats commerciaux et de gains de productivité remarquables, cette transformation numérique introduit simultanément un environnement complexe de défis en matière de sécurité des données.

Environnement de données en peine explosion

Le cœur du problème réside dans l’explosion des données d’entreprise. Les informations précieuses et sensibles ne sont plus confinées ; elles sont de plus en plus fragmentées et réparties dans des environnements divers : écosystèmes d’IA, SaaS, PaaS, déploiements multicloud, architectures cloud hybrides et infrastructures sur site traditionnelles. Cette prolifération est stupéfiante : l’IDC prévoit une croissance annuelle composée des données de 21,2 % qui devrait atteindre plus de 221 000 exaoctets d’ici 2026.

Gérer la complexité et les risques

Cet environnement complique considérablement la tâche des RSSI, qui doivent désormais gérer la sécurité des données dans un environnement de données en constante expansion et éphémère. Les données sont constamment créées, partagées et stockées dans des centaines de systèmes et d’applications divers au sein de l’entreprise, ce qui rend la protection complète des données extrêmement difficile.

Principaux risques liés à la sécurité des données à l’ère de l’IA :

- **Risques de vulnérabilité et de non-conformité :** la dispersion et la fragmentation des données accroissent considérablement le risque de violations de données et de non-conformité réglementaire. Garantir le respect des réglementations en constante évolution en matière de gouvernance et de protection des données (RGPD, CCPA, etc.) représente un défi de taille.
- **Menace liée aux données ROT (redondantes, obsolètes ou triviales) :** la prolifération incontrôlée des données fantômes (copies de données inconnues ou non autorisées) et des données inutilisées (données périmées ou oubliées) crée des vulnérabilités critiques. Celles-ci entraînent souvent d’importantes failles de sécurité et augmentent la surface d’attaque de façon exponentielle.
- **IA générative et défis liés à la sécurité des LLM :** l’essor de l’IA générative et des grands modèles de langage (LLM) engendre une nouvelle vague de risques hautement spécialisés. Parmi ceux-ci figurent l’IA fantôme, les fuites de données (exposition involontaire d’informations sensibles), les problèmes de droits d’accès au sein des systèmes d’IA et de nouvelles possibilités d’infractions réglementaires. Une sécurité renforcée de l’IA et une gouvernance rigoureuse des données des LLM sont donc essentielles.

Pour relever ces défis aux multiples facettes en matière de sécurité des données, les RSSI doivent adopter une approche stratégique et proactive, axée sur une gouvernance des données robuste, des solutions de protection des données avancées et des cadres de sécurité complets basés sur l’IA afin de protéger les informations sensibles à l’ère du numérique.

Risque de perte de données précieuses

Face à la multiplication des attaques ciblées et à un environnement réglementaire en constante évolution, il est devenu crucial que les RSSI priorisent la sécurité de ces environnements. Environ 44 % des entreprises ont subi une violation de données dans leur environnement cloud au cours des 12 derniers mois.[1] Une telle violation peut avoir de graves conséquences, notamment la perte de données, l’atteinte à la réputation et des pertes financières. À mesure que les menaces liées à l’IA et aux attaques dans le cloud gagnent en complexité, le rôle du RSSI devient plus critique que jamais.

Pour gérer ces risques et garantir le respect des réglementations, les responsables de la sécurité doivent maîtriser parfaitement leurs environnements

1. Magazine Infosecurity, **« Cloud Breaches Impact Nearly Half of Organizations »** (Les violations du cloud touchent près de la moitié des entreprises), 25 juin 2024
2. **Rapport d’IBM sur le coût d’une violation de données, 2025**

4,44 M US$

Coût moyen mondial d’une violation de données en 2025[2]

de données. Cependant, le volume, la variété et la rapidité des données compliquent souvent leur sécurisation. Les responsables ne disposent souvent pas de réponses à ces questions :

- Où sont les données ?
- Quels magasins de données contiennent des données précieuses ou sensibles ?
- Qui, quoi ou quels outils d'IA ont accès à ces magasins ?
- Comment les données sont-elles accessibles ou partagées avec des outils d'IA ?
- Quelle est la valeur des données ?
- Comment les données sont-elles traitées et quel est l'impact sur la conformité réglementaire ?

Au-delà des limites : pourquoi la sécurité des données traditionnelle échoue à l'ère de l'IA

L'environnement de la sécurité des données a profondément changé. Face à la montée des menaces, la réponse classique de nombreux RSSI et de leurs équipes a consisté à accumuler une multitude d'outils de sécurité disparates. Or, ces outils traditionnels se révèlent de plus en plus inadaptés, incapables de fournir les informations et les protections essentielles requises dans le contexte actuel.

Défis non relevés de la sécurité de l'IA

Une lacune majeure des solutions existantes réside dans leur incapacité à appréhender les comportements spécifiques, les nouveaux modes de défaillance et les exigences particulières de gouvernance des données des technologies émergentes. Plus précisément, elles ne parviennent pas à protéger les grands modèles de langage (LLM), les agents d'IA génératives et autres modèles fondamentaux. Ces nouveaux risques liés à l'IA exigent une approche fondamentalement différente.

Impératif d'un nouveau paradigme de sécurité

Face à l'émergence de nouvelles menaces, il est indispensable d'adopter une approche globale et intégrée de la gouvernance et de la sécurité des données à l'ère de l'IA. Nous parlons d'un changement de paradigme : la sécurité de l'IA n'est plus une simple considération secondaire, mais un élément central de votre stratégie globale de cybersécurité.

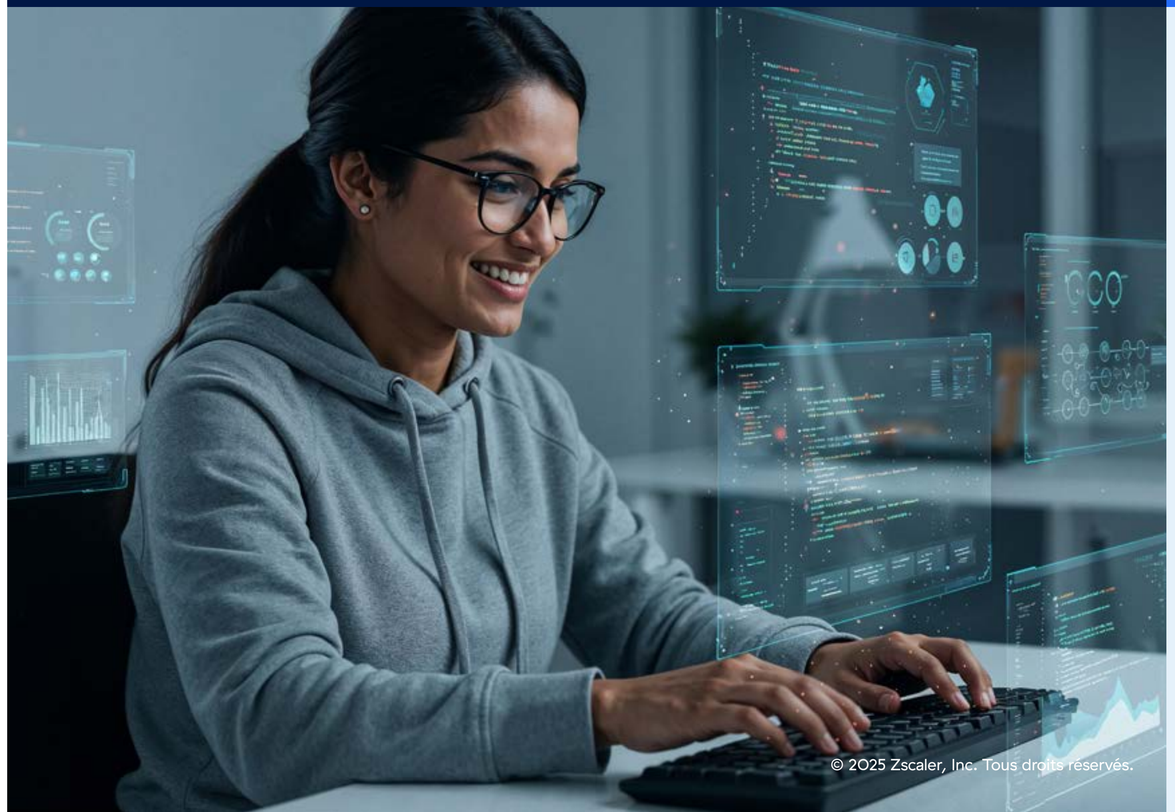
Optimisation des investissements dans un contexte budgétaire restreint

Face à ces défis, les budgets de sécurité, de plus en plus serrés, contraignent les responsables à évaluer et optimiser leurs investissements de manière critique. L'accent est désormais mis sur la réduction de la complexité opérationnelle et la minimisation des coûts, tout en renforçant les défenses en cybersécurité et en comblant les failles critiques. Paradoxalement, cet investissement stratégique implique souvent l'utilisation de solutions de sécurité sophistiquées basées sur l'IA. Ces outils avancés ne constituent pas seulement une réponse à une partie du problème ; ils permettent une meilleure visibilité, une détection des risques plus rapide et une réponse aux incidents plus efficace, renforçant ainsi l'ensemble de votre posture de sécurité face aux menaces de l'ère de l'IA.

3. **Rapport d'IBM sur le coût d'une violation de données, 2025**

97 %

des entreprises ayant signalé une violation de données liée à l'IA ne disposaient pas de contrôles d'accès à l'IA adéquats.[3]



Adopter une solution DSPM : l'impératif moderne de la sécurité des données basée sur l'IA

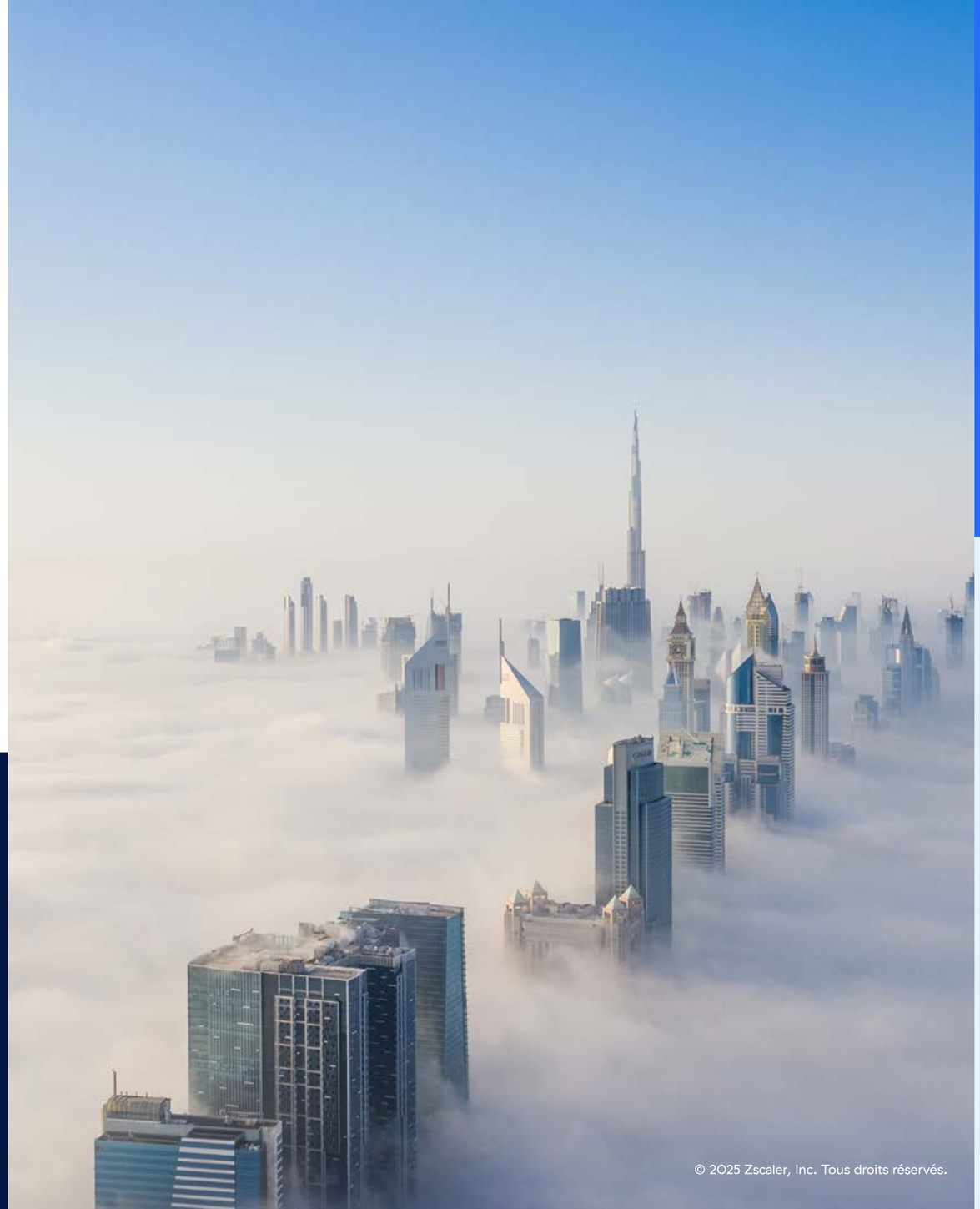
Face aux risques sans précédent liés à l'IA et aux limites reconnues des outils de cybersécurité traditionnels, une approche véritablement moderne de la sécurité des données n'est pas seulement bénéfique, elle est essentielle. C'est là que la gestion de la posture de sécurité des données (DSPM) apparaît comme une solution essentielle et indispensable.

La DSPM offre le contexte et l'automatisation nécessaires pour gérer habilement les complexités des environnements de données modernes. En adoptant une méthodologie tournée vers l'avenir, les RSSI peuvent mieux comprendre leurs données, garantir le respect des réglementations et réduire les risques liés à l'utilisation de l'IA.

4. Ibid.

1,9 M US$

Économies moyennes réalisées par les entreprises qui utilisent l'IA et l'automatisation en matière de sécurité de façon intensive[4]



Comment les RSSI peuvent améliorer la posture de sécurité des données grâce à une solution DSPM intégrée

Les RSSI peuvent exploiter l'IA, l'AA et la corrélation des risques efficacement pour améliorer leur posture de sécurité des données de diverses façons :

Répondre aux préoccupations concernant l'IA fantôme, les données fantômes et les données inutilisées

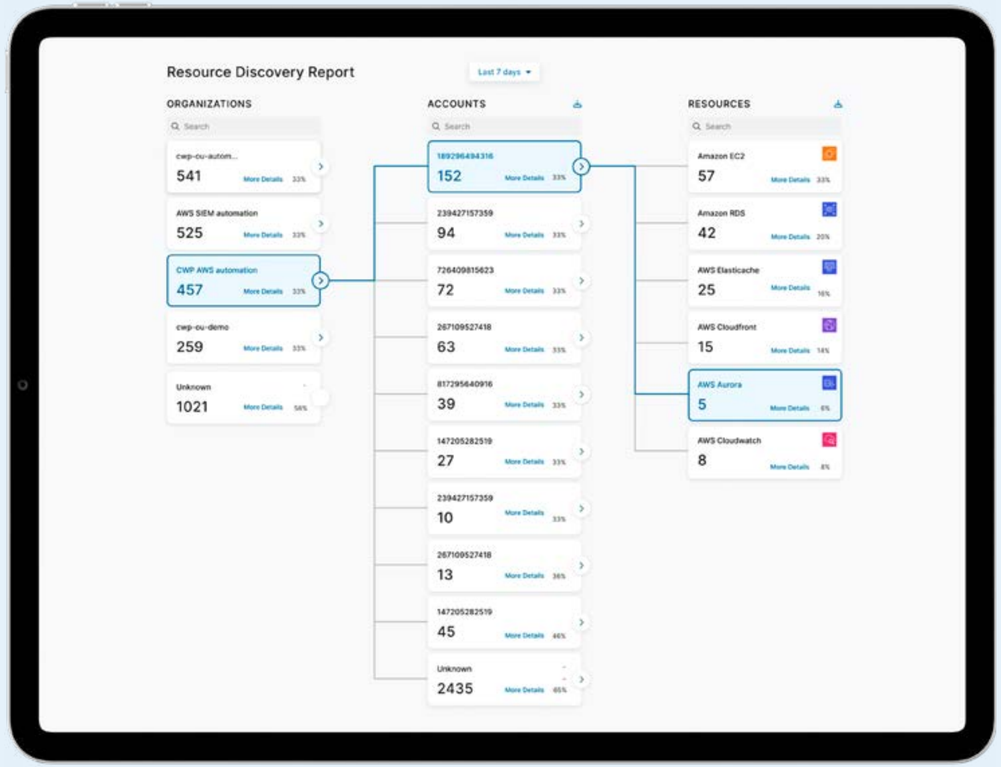
Données fantômes
Les données fantômes et les données inutilisées présentent des risques de sécurité importants, car elles échappent souvent aux protocoles de sécurité informatique et aux cadres de gouvernance des données. Selon IBM, 35 % des violations de données impliquent des données fantômes, et ces violations entraînent un surcoût moyen de 16 %. De plus, l'identification et le confinement des violations impliquant des données fantômes prennent respectivement 26,2 % et 20,2 % de temps en plus[5]. Les données fantômes peuvent se trouver dans des fichiers non structurés, des bases de données structurées, le stockage cloud ou sur des appareils personnels sans surveillance adéquate, tandis que les données inutilisées, sans gestion de cycle de vie, peuvent devenir un problème. Les solutions DSPM exploitent l'IA pour découvrir en permanence les magasins de données, améliorant ainsi la visibilité globale sur l'environnement des données. L'IA peut aider à cataloguer les données sombres (« dark data ») et les données fantômes, augmentant ainsi la visibilité sur les données. Elle alerte également les équipes chargées de la sécurité des risques potentiels et minimise les risques de violation. Elle peut surveiller les irrégularités et les schémas dans l'accès aux données, détecter les anomalies et anticiper les failles de sécurité potentielles.

IA fantôme
L'IA fantôme, à l'instar de l'informatique fantôme, désigne principalement l'utilisation d'outils d'IA non autorisés pour interagir avec des données sensibles d'entreprise, une pratique pouvant avoir des conséquences importantes sur la sécurité et la conformité des données. À mesure que ces outils d'IA deviennent plus accessibles et performants, les employés les adoptent sans supervision informatique. Bien que cela puisse paraître inoffensif, cela peut engendrer des risques en cascade que les cadres de sécurité traditionnels ne peuvent pas contrer par la simple interdiction des outils d'IA.

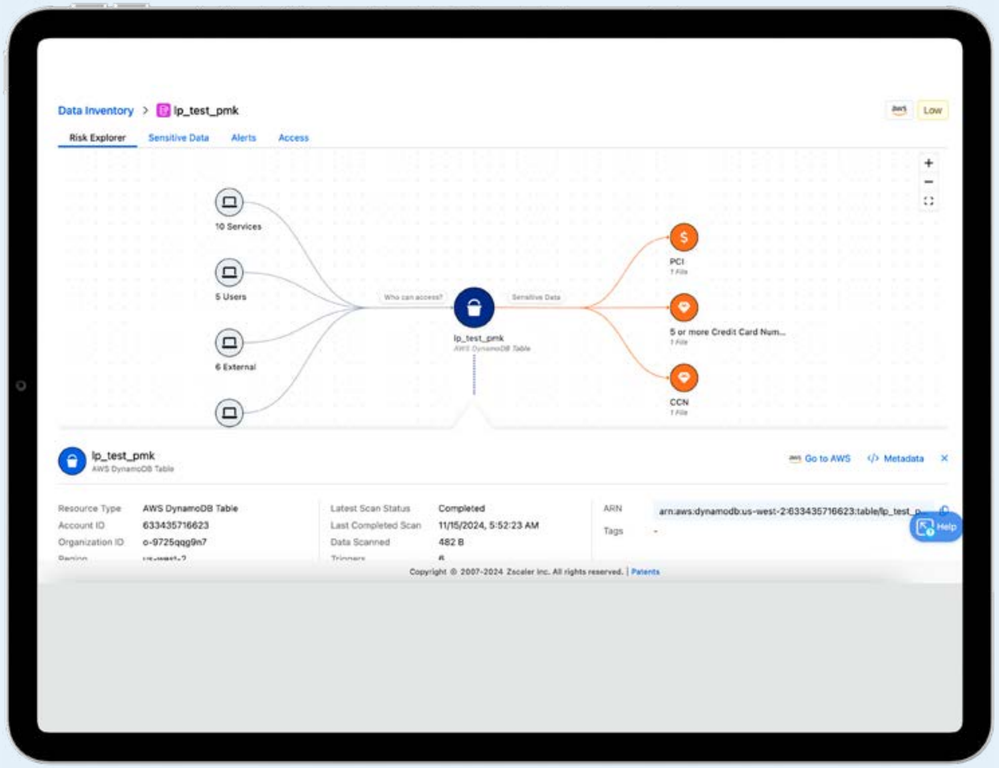
Grâce à la DSPM, les entreprises peuvent tirer profit de l'IA. Plutôt que de bloquer ou d'interdire les outils d'IA, les entreprises peuvent gérer les risques liés à l'IA fantôme grâce à la gestion de la posture de sécurité des données (DSPM) tout en tirant parti des avantages de l'IA.
La fonctionnalité de sécurité de l'IA intégrée de la DSPM aide les équipes à obtenir une visibilité et un contrôle de bout en bout sur les données et les modèles d'IA afin de protéger les entreprises de manière proactive contre les risques liés à l'IA Cette solution vous permet de :

- Bénéficiez d'une vue complète de vos modèles, agents et services d'IA.
- Identifier et sécuriser les données d'entraînement de l'IA contre l'empoisonnement, les erreurs de configuration et l'exposition
- S'aligner sur les cadres de conformité de l'IA, nouveaux et émergents

Avec la DSPM, les responsables de la sécurité peuvent transformer le chaos de la sécurité en innovation contrôlée, en fournissant une découverte de données unifiée, une évaluation contextuelle des risques et une gouvernance automatisée pour chaque interaction avec l'IA.



5. Ibid.



Classification des données optimisée par l'IA

Une classification efficace des données est un aspect fondamental d'une sécurité robuste des données. Il est essentiel de cartographier de manière proactive les données sensibles et les risques associés afin d'éviter toute exposition potentielle due à des erreurs de configuration ou à des pratiques dangereuses. Les approches conventionnelles, qui reposent souvent sur des procédures manuelles ou une reconnaissance de schémas simpliste, peuvent générer un nombre élevé de faux positifs et une allocation sous-optimale des ressources de sécurité. Souvent, les entreprises s'appuient fortement sur des solutions basées sur les expressions régulières, une approche rigide et lourde en raison des faux positifs qui s'avère fragile et inefficace. Même les approches actuelles basées sur des produits ponctuels ne parviennent pas à intégrer la classification au sein d'une plateforme centralisée et unifiée, ce qui entraîne des alertes incohérentes et une visibilité cloisonnée, notamment lorsque les données circulent dans l'écosystème d'une entreprise.

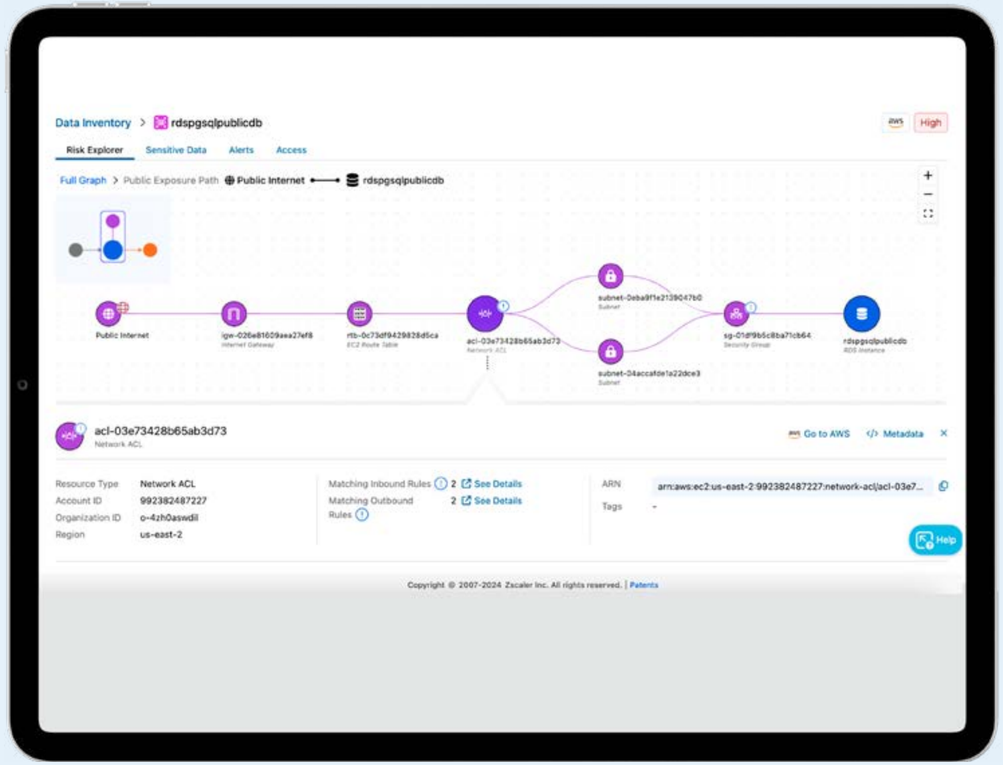
Les responsables de la sécurité peuvent tirer parti de la DSPM grâce à la classification LLM optimisée par l'IA. Cette solution permet d'améliorer les opérations liées aux flux de travail traditionnels basés sur les expressions régulières, offrant une visibilité et une flexibilité exceptionnelles tout en sécurisant les données sensibles connues et inconnues comme jamais auparavant. Contrairement aux techniques dépendantes des mots-clés, la classification LLM permet une identification de contenu plus approfondie. Elle utilise un traitement avancé du langage pour la classification des données afin de comprendre l'intention et le contexte du contenu, sans nécessiter de schémas ou de mots-clés prédéfinis. Cela permet aux entreprises non seulement d'améliorer leurs pratiques existantes, mais aussi de découvrir et de sécuriser de nouveaux types de données sensibles auparavant négligées ou indétectables.

Gestion proactive des risques

Pour contrôler les risques et garantir la conformité, les responsables de la sécurité doivent disposer d'un moyen proactif pour gérer leur posture de sécurité des données. L'une des applications les plus intéressantes de l'IA en matière de sécurité des données est l'approche proactive de la sécurité et l'analyse prédictive. En analysant et en corrélant les données, les algorithmes d'IA peuvent prévoir les risques de sécurité potentiels. Cette approche proactive permet aux entreprises de garder une longueur d'avance sur les menaces et les risques critique.

La DSPM exploite l'IA et des techniques de corrélation avancées pour identifier les schémas et les tendances dans les données susceptibles d'indiquer des incidents de sécurité imminents. En outre, l'IA peut être utilisée pour hiérarchiser les magasins de données en fonction de leur valeur (degré de risque), garantissant ainsi que les efforts de sécurité sont dirigés vers les ressources les plus critiques. En automatisant de nombreux processus de sécurité, l'IA réduit également la charge de travail des professionnels de la sécurité, permet une approche proactive de la sécurité et améliore l'efficacité opérationnelle globale.

Par exemple, la corrélation avancée de Zscaler DSPM peut établir des liens de manière proactive et détecter les risques cachés, permettant ainsi de prioriser les efforts de sécurité sur les données les plus critiques.



49 %

des entreprises investissent dans la sécurité après une violation de données.[6]

6. Rapport d'IBM sur le coût d'une violation de données, 2025

Rationaliser la conformité grâce à la gouvernance des données en temps réel

Le respect de la conformité aux réglementations et aux protocoles de sécurité internes changeants constitue une pierre angulaire de l'IA et de la sécurité des données, du RGPD à la SEC. Aujourd'hui, les entreprises doivent composer non seulement avec les réglementations établies, telles que le RGPD et la loi HIPAA, mais aussi avec les cadres émergents ciblant spécifiquement l'IA, notamment la loi européenne sur l'IA, la norme NIST AI 600 et bien d'autres. La sécurité des données et le risque de non-conformité partagent un lien indissoluble, s'influençant profondément et façonnant la trajectoire d'une entreprise. Les violations de données peuvent déclencher des sanctions pour non-conformité, entraînant de graves répercussions, des amendes élevées et une atteinte à la réputation d'une entreprise. À l'inverse, le respect des réglementations peut servir de bouclier, en protégeant l'IA et les données contre les vulnérabilités et les menaces de sécurité.

De nombreuses réglementations se résument à savoir où se trouvent les données sensibles, à limiter les personnes pouvant y accéder et à surveiller en permanence les risques. Bien que cela puisse paraître simple, la complexité de l'IA et des environnements de données peut faire de cette tâche un véritable défi. En outre, les réglementations évoluent constamment, sous l'effet des nouvelles technologies, de l'évolution des préoccupations relatives à la confidentialité et de l'interconnexion croissante de l'économie mondiale.

Ce terrain réglementaire en constante évolution exige une vigilance et une adaptation constantes de la part des entreprises qui souhaitent rester conformes. Les approches traditionnelles de conformité, caractérisées par des vues fragmentées, des évaluations manuelles et des réponses réactives, peinent à apporter clarté et efficacité.

La DSPM peut rationaliser les processus de conformité grâce à des capacités de conformité et de gouvernance des données en temps réel. La solution DSPM offre aux entreprises une vue d'ensemble de leur état de conformité en matière de données, des analyses complètes, des outils d'évaluation comparative, des mesures correctives et des rapports leur permettant de remédier rapidement aux lacunes en matière de conformité. Ceci est particulièrement important dans les secteurs fortement réglementés, où une compréhension claire de l'état des données et de l'atténuation des risques est essentielle. Des étapes de correction guidées aux flux de travail automatisés, le tableau de bord de conformité permet aux équipes de sécurité d'agir rapidement et efficacement. L'application de l'IA dans la gouvernance des données garantit que les entreprises peuvent répondre aux exigences réglementaires tout en maintenant des mesures de sécurité robustes.

63 %

des entreprises ne disposent pas de politiques de gouvernance en matière d'IA.[7]

7. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls

Assurer un accès sur la base du moindre privilège

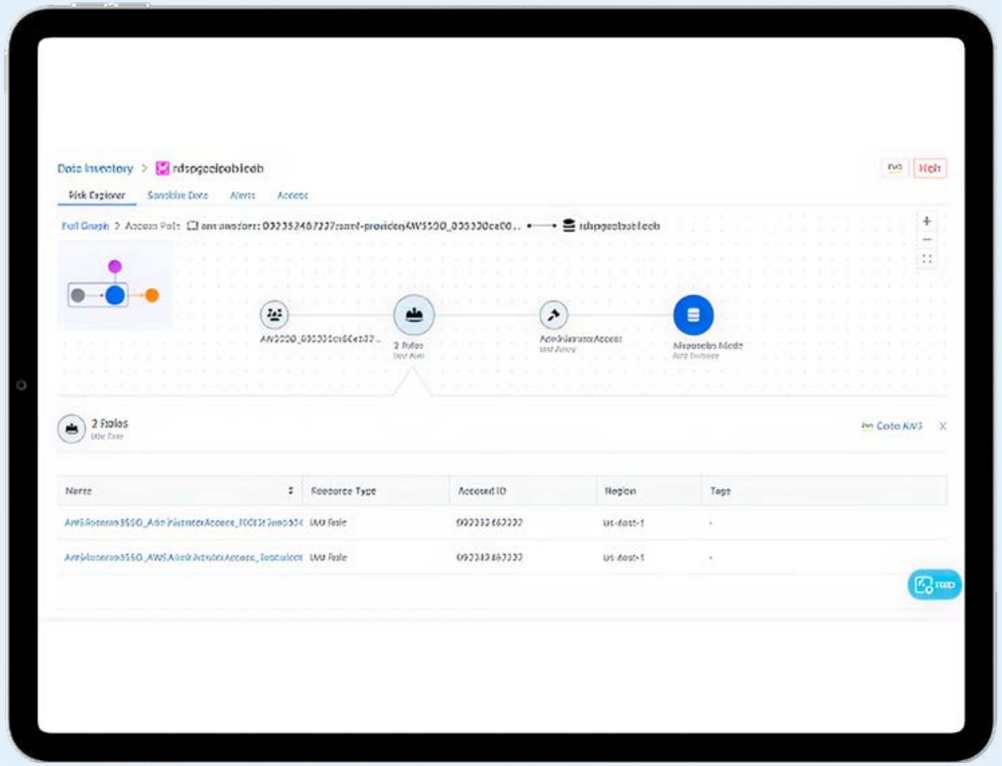
Compte tenu du volume considérable d'utilisateurs, d'applications et de ressources, les environnements de données présentent un risque important en termes de contrôles d'accès inadéquats, de prolifération des identités et de stockage orphelin. Environ 90 % des entreprises ont subi des violations de données liées à l'identité, entraînant des incidents de sécurité coûteux.

De plus, les modèles d'IA et les outils basés sur les LLM introduisent des risques supplémentaires liés à l'accès non autorisé aux données. Les principaux risques comprennent la divulgation involontaire ou non autorisée de données sensibles, l'exfiltration de données (lorsque des données sensibles sont volées via les résultats de l'IA) et les attaques sophistiquées, où des identités compromises exploitent les systèmes d'IA pour obtenir un accès non autorisé.

C'est pourquoi garantir un accès aux données selon le principe du moindre privilège est un axe fondamental de la sécurité des données. La gouvernance liée à l'accès aux données présente davantage de défis en raison de la prolifération des données, de la multiplication des autorisations et de la complexité des architectures d'IA et multicloud. Néanmoins, elle demeure un élément essentiel de la sécurité des données, car la divulgation non autorisée de données sensibles constitue généralement la première étape d'une attaque sophistiquée.

La DSPM propose une approche unifiée de la gouvernance de l'accès aux données, avec une surveillance continue de la sécurité des données et du comportement des utilisateurs. La DSPM examine les rôles, les autorisations et les attributs liés à la gestion des identités et des accès aux données afin d'identifier rapidement les voies d'accès risquées aux bases de données. La DSPM prend en charge les données structurées, non structurées et réparties sur les environnements sur site, multicloud et SaaS. Ainsi, les entreprises peuvent identifier et traiter de manière cohérente les risques d'accès et appliquer des politiques d'accès à travers une infrastructure de données et un écosystème d'IA diversifiés. En exploitant des informations détaillées concernant les schémas d'accès et les vulnérabilités potentielles, les équipes de sécurité des données peuvent appliquer plus efficacement l'accès sur la base du moindre privilège. Cette approche réduit le risque d'accès non autorisé et améliore la sécurité globale de l'environnement de données.

8. Enquête menée par Security Today : **90 % des entreprises ont subi un incident lié à l'identité l'année dernière**, 5 juin 2024.



90 %

des entreprises ont subi un incident lié à l'identité.[8]

Optimiser les coûts de stockage et de consommation

Les équipes de gestion des données doivent optimiser les coûts de stockage et de consommation en identifiant les données dupliquées ou négligées qui peuvent être supprimés ou transférés vers des solutions de stockage plus économiques. Les méthodes classiques s'avèrent souvent insuffisantes pour identifier et gérer ces données, ce qui engendre des dépenses de stockage superflues.

Les solutions DSPM peuvent répondre à ce problème en fournissant des informations sur les magasins de données dupliqués ou inutilisés, et permettre aux entreprises de prendre des mesures appropriées. Par exemple, Zscaler DSPM fournit une vue complète des magasins de données dupliqués ou inutilisés, permettant aux équipes d'identifier les données qui peuvent être supprimées ou migrées en toute sécurité.

Grâce à des perspectives basées sur l'IA, les entreprises peuvent restreindre les dépenses de stockage excessives et assurer la bonne gestion et la protection des informations sensibles.

Appliquer des politiques unifiées sur tous les environnements de données

Avec les méthodes traditionnelles, le maintien de politiques de sécurité des données cohérentes dans divers environnements est un défi considérable. Les solutions DSPM peuvent surmonter ce problème par leur approche unifiée de la sécurité des données dans des contextes multicloud, permettant aux entreprises d'appliquer des politiques uniformes sur tous les environnements de données.

Zscaler DSPM propose une stratégie unifiée pour la sécurité des données. Cette solution donne aux entreprises les moyens d'établir des politiques uniformes sur tous les environnements de données, assurant une surveillance complète des données cloud tout en rationalisant le processus d'identification et de résolution des risques. En s'appuyant sur des informations alimentées par l'IA/AA, les entreprises peuvent réduire le risque de violation des données et mieux respecter les règles de protection des données.

Réponse rapide aux incidents

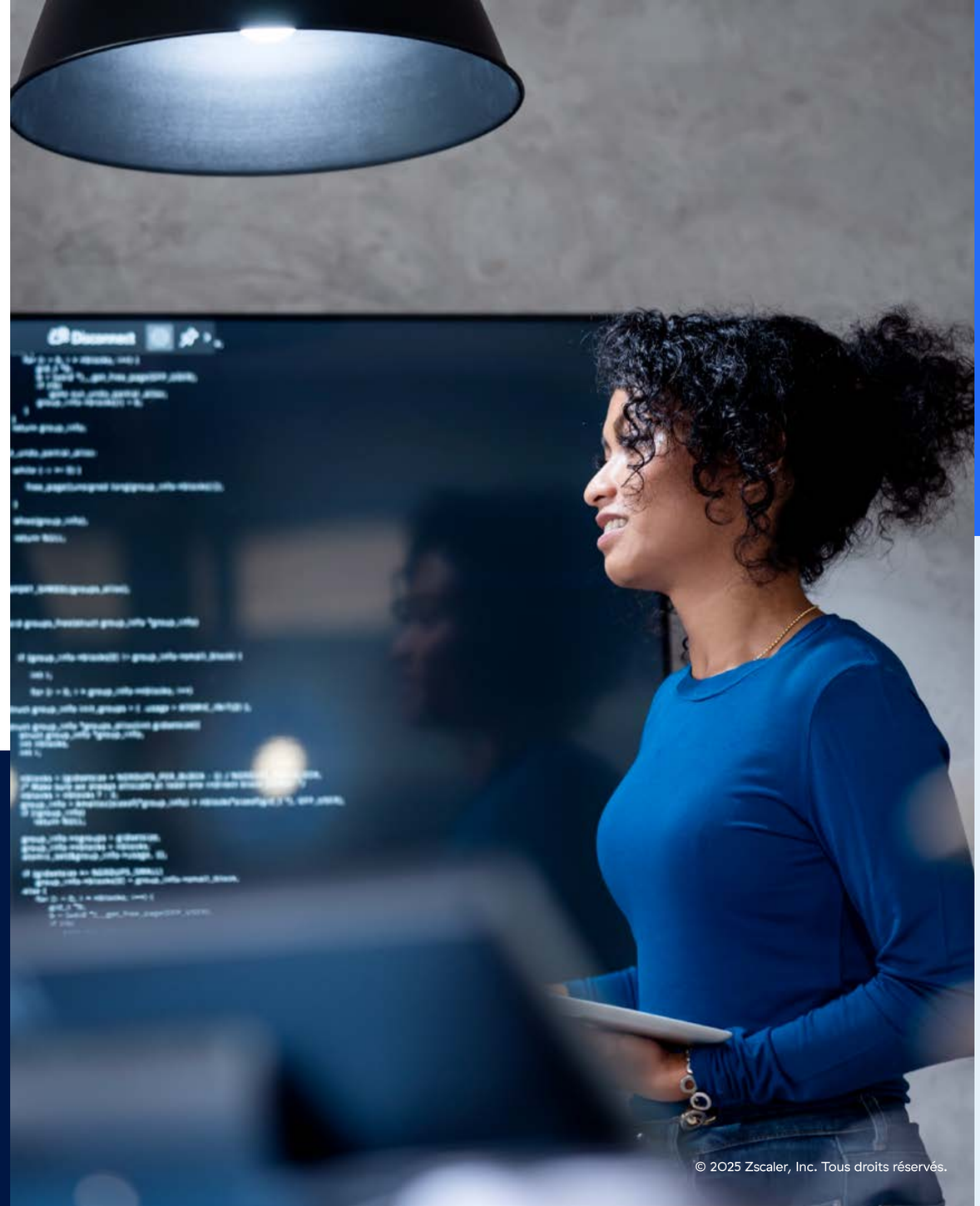
L'identification et l'atténuation des risques sont des tâches fondamentales qui incombent aux professionnels de la sécurité des données. La vitesse à laquelle les menaces évoluent exige des réponses en temps réel. Les méthodologies conventionnelles peuvent toutefois s'avérer inefficaces face à un environnement de menace dynamique basé sur l'IA. L'automatisation de la sécurité optimisée par l'IA est la réponse à ce défi.

La gestion de la posture de sécurité des données (DSPM) permet de surveiller en permanence les données, de détecter les anomalies et de répondre aux menaces. Les solutions DSPM renforcent l'atténuation des risques grâce à une corrélation sophistiquée des risques et à une intelligence d'accès adaptative. Certaines solutions DSPM, comme Zscaler DSPM, intègrent les renseignements sur les menaces provenant de Zscaler ThreatLabz, un processus de correction guidé et rigoureux, ainsi qu'une mise en œuvre accélérée de la sécurité. Grâce à une corrélation des menaces sophistiquée optimisée par l'IA, les entreprises peuvent identifier les risques latents et les vecteurs d'attaque clés, ce qui leur permet de concentrer leurs efforts sur les risques les plus critiques.

9. Statista, **Délai moyen d'identification et de confinement des violations de données dans le monde de 2017 à 2024**, consulté le 9 décembre 2024

194 jours

Délai moyen d'identification d'une violation de données[9]



Sécurité renforcée de l'IA

Les entreprises adoptent les applications d'IA à un rythme effréné. Malheureusement, des applications comme l'IA générative et les grands modèles de langage (LLM) ont entraîné des risques importants de fuites de données et de non-conformité. Un rapport récent indique que 13 % des entreprises ont signalé des violations de leurs modèles ou applications d'IA[10], ce qui fait apparaître l'IA comme cible de choix.

Les entreprises qui intègrent l'IA générative dans leurs opérations doivent prendre des mesures afin d'empêcher que des données sensibles soient utilisées par inadvertance au sein de ces modèles. Les équipes de sécurité doivent s'attacher en priorité à signaler, étiqueter et classer les données pour garantir que les équipes interfonctionnelles exploitent l'IA générative de manière responsable.

La DSPM renforce le contrôle et la protection des données dans les environnements d'IA générale grâce à ses fonctionnalités intégrées d'IA-SPM. En identifiant et en catégorisant les données avec précision, la DSPM empêche la transmission d'informations sensibles aux modèles de langage (LLM), réduisant ainsi les risques de fuites de données et de non-conformité. La DSPM privilégie une approche axée sur les données, en se concentrant sur la sécurisation des informations qui alimentent l'IA plutôt que sur la seule infrastructure. En découvrant, en classant et en surveillant en permanence les données tout au long de leur cycle de vie, la DSPM contribue à atténuer les risques de sécurité spécifiques à l'IA, tels que l'empoisonnement des données, la divulgation de données sensibles et le vol de modèles.

L'adoption d'une solution DSPM dotée de capacités AI-SPM intégrées peut permettre aux entreprises d'instaurer la confiance dans leurs applications d'IA. Ce faisant, elles protègent non seulement leurs données importantes, mais rendent également les applications d'IA plus fiables et plus sûres.

10. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls

Exploiter la DSPM pour sécuriser un environnement de données diversifié

L'utilisation stratégique de la DSPM est primordiale dans la quête d'une sécurité des données plus solide. Ces technologies offrent le contexte et l'automatisation nécessaires pour gérer efficacement les subtilités des environnements de données modernes. Grâce à une démarche proactive, les responsables de la sécurité peuvent mieux sécuriser les données sensibles, assurer la conformité et atténuer les risques associés aux technologies progressives telles que l'IA générative.

« D'ici 2026, plus de 20 % des entreprises déploieront la technologie DSPM en réponse à l'urgence d'identifier et de localiser des référentiels de données jusqu'alors inconnus, et d'atténuer les risques de sécurité et de confidentialité associés. »

Analyse Gartner, « Innovation Insight: Data Security Posture Management », Brian Lowans, Joerg Fritsch, Andrew Bales, 28 mars 2023

Zscaler DSPM

Zscaler DSPM est la plateforme de protection des données entièrement intégrée la plus complète au monde qui sécurise les données structurées et non structurées sur les services SaaS, les environnements de cloud public (AWS, Azure, GCP), les architectures sur site et les terminaux.

Cette solution procure une visibilité granulaire sur vos données cloud, classe et identifie les données et les accès, et contextualise l'exposition des données et la posture de sécurité, permettant aux entreprises et aux équipes de sécurité de prévenir et de corriger les violations de données dans le cloud à grande échelle.

Zscaler DSPM adopte une approche unifiée basée sur l'IA pour garantir une gestion des données optimale sur tous les supports de stockage, y compris les environnements IaaS, SaaS, sur site, les terminaux, etc. Intégrée nativement à la plateforme de sécurité des données Zscaler, elle vous permet de comprendre et de contrôler pleinement toutes vos données sur une seule et même plateforme.

La plateforme de sécurité des données Zscaler utilise un moteur DLP unique et unifié pour offrir une protection des données cohérente et de premier ordre sur tous les canaux. En suivant tous les utilisateurs sur tous les sites et en régissant les données en mouvement et au repos, elle garantit une protection homogène des données sensibles et le respect de la conformité.

Pour plus d'informations, consultez zscaler.com/fr/dp/dspm.

Effectuez une visite interactive du produit DSPM.

Pourquoi la DSPM a-t-elle sa place dans votre stratégie de protection des données ?

Regarder le webinaire à la demande ⟶

Scannez le code QR pour accéder à diverses ressources DSPM utiles :

zscaler™ | Experience your world, secured.™

À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation numérique pour améliorer l'agilité, l'efficacité, la résilience et la sécurité de ses clients. La plateforme Zscaler Zero Trust Exchange™ protège des milliers de clients contre les cyberattaques et la perte de données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Adossé à plus de 150 data centers dans le monde, Zero Trust Exchange™, basé sur SSE, constitue la plus vaste plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **zscaler.com/fr** ou suivez-nous sur X (ex-Twitter) **@zscaler**.

+1 408 533 0288 **Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/fr**