

Zscaler Data Security Posture Management (DSPM)

© 2024 Zscaler, Inc. Tous droits réservés.

Descriptif de la solution

Présentation — Sécuriser les données dans l'ère du cloud

La sécurisation de volumes importants de données d'entreprise en environnements multicloud n'est pas avare en défis : gestion de la complexité et du périmètre de la protection des données, gestion des menaces internes, violations des données, accès des tiers et des fournisseurs, risques liés à la chaîne collaborative, ainsi que la conformité aux réglementations applicables aux données. Les entreprises peinent à répertorier, classer, contrôler et protéger les données critiques, mais aussi à les mettre à l'abri de diverses menaces. Cette complexité est accentuée par une dissémination des données et une diversité des rôles et autorisations dans les multiples environnements hébergeant ces données.

Environnements complexes	Référentiel de données	Attaques ciblées et sophistiquées	Accès surprivilégié
82 % des violations impliquent des données stockées dans le cloud[1]	175 Zo de données devraient être stockées dans le cloud d'ici 2025[2]	4,88 M USD : le coût moyen mondial d'une violation de données en 2024[3]	80 % des entreprises ont subi des piratages d'identité[4]

Malheureusement, les solutions traditionnelles de protection des données n'ont pas été conçues pour les environnements multicloud dynamiques. Parallèlement, les outils autonomes de DSPM sont cloisonnés, ce qui n'offre pas un niveau d'intégration satisfaisant avec l'arsenal existant dédié à la protection des données. Les entreprises ont besoin d'une nouvelle approche plus unifiée pour sécuriser leurs données dans le cloud.

Zscaler concrétise la sécurité des données dans des environnements multicloud grâce à une solution de gestion de la posture de sécurité des données (DSPM), étroitement intégrée et sans agent logiciel.

Qu'est-ce que la DSPM ?

« La DSPM (Data Security Posture Management) procure une visibilité sur la localisation des données sensibles, les entités accédant à ces données, leurs modalités d'utilisation, ainsi que sur la posture de sécurité des données stockées ou des applications. » — Gartner

La DSPM est parfois qualifiée de sécurité « data first », à l'inverse du modèle de protection proposé par d'autres technologies et pratiques de cybersécurité. Plutôt que sécuriser les appareils, les systèmes et les applications qui hébergent, déplacent ou traitent les données, la DSPM se recentre sur la protection des données en elles-mêmes, et se veut complémentaire des autres solutions qui forment le stack de sécurité d'une entreprise.

Plus précisément, la DSPM implique une surveillance, une évaluation et une optimisation continues des fonctions de sécurité pour protéger les données sensibles sur les plateformes multicloud. En automatisant l'identification des données sensibles, des vulnérabilités potentielles, des erreurs de configuration ou de tout manquement aux règles de conformité, la DSPM traite de manière proactive le risque d'exposition des données. Ce faisant, la DSPM aide à renforcer la posture globale de sécurité des données, à minimiser le risque de piratage et à répondre aux exigences de conformité réglementaire.

1. https://www.informationweek.com/cyber-resilience/data-breaches-just-keep-piling-up
2. https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/
3. https://www.ibm.com/reports/data-breach
4. https://www.darkreading.com/cybersecurity-operations/identity-related-breaches-last-12-months

© 2024 Zscaler, Inc. Tous droits réservés.

Pourquoi la DSPM ?

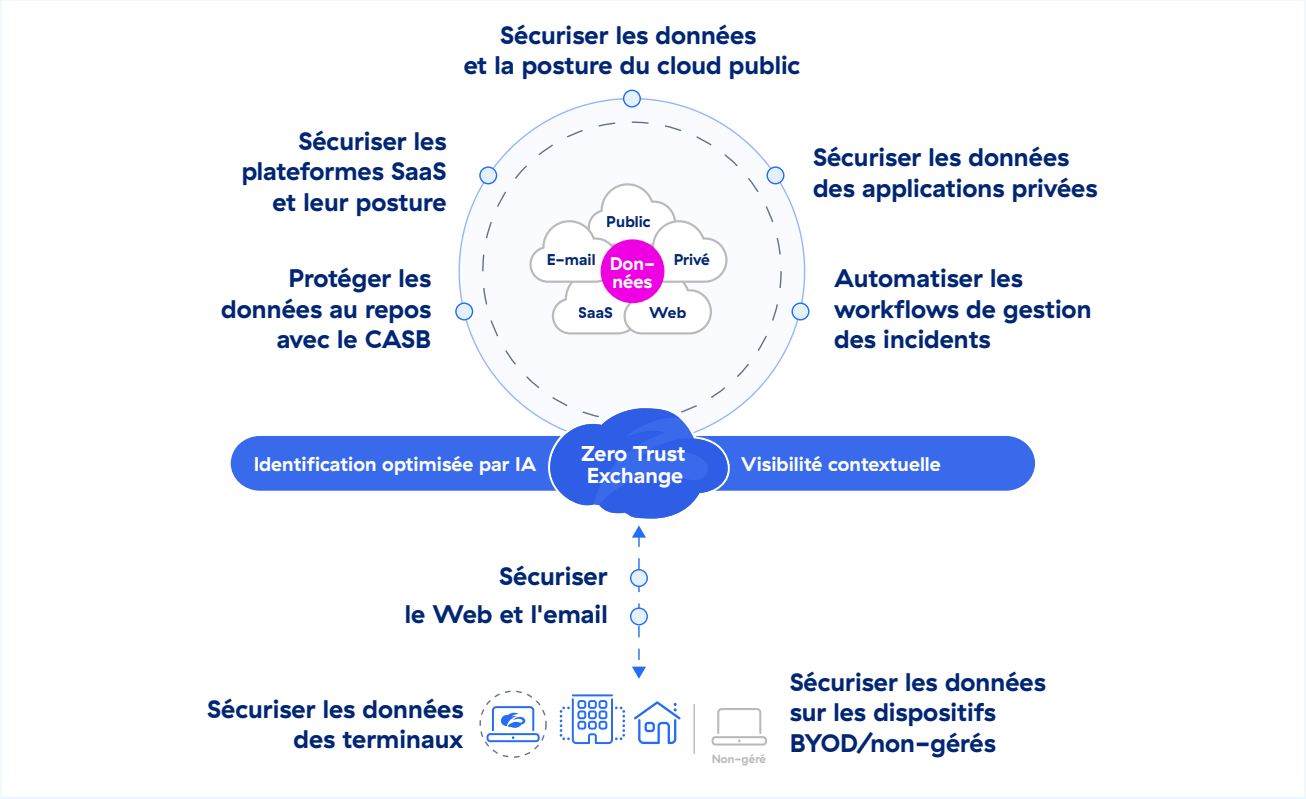
L'objectif principal des outils de DSPM est d'évaluer et de gérer le statut de sécurité d'un environnement de données d'une entreprise en localisant les point faibles, en surveillant les paramètres de sécurité et en identifiant les menaces potentielles qui pèsent sur les données sensibles. La DSPM va au-delà de la simple politique pour examiner les données elles-mêmes.

En analysant et en catégorisant les données, la DSPM aide les entreprises à identifier précisément les données sensibles et la manière dont elles sont utilisées. Cette technologie permet également de hiérarchiser les problèmes identifiés et d'éviter une multiplication d'alertes qui pourraient amener à négliger ces problèmes.

Les principaux cas d'utilisation pratiques de la DSPM portent sur la détection des vulnérabilités de sécurité (telles que le chiffrement) dans les environnements cloud, l'application des politiques d'accès, la gestion des alertes et les capacités d'investigation lors d'incidents.

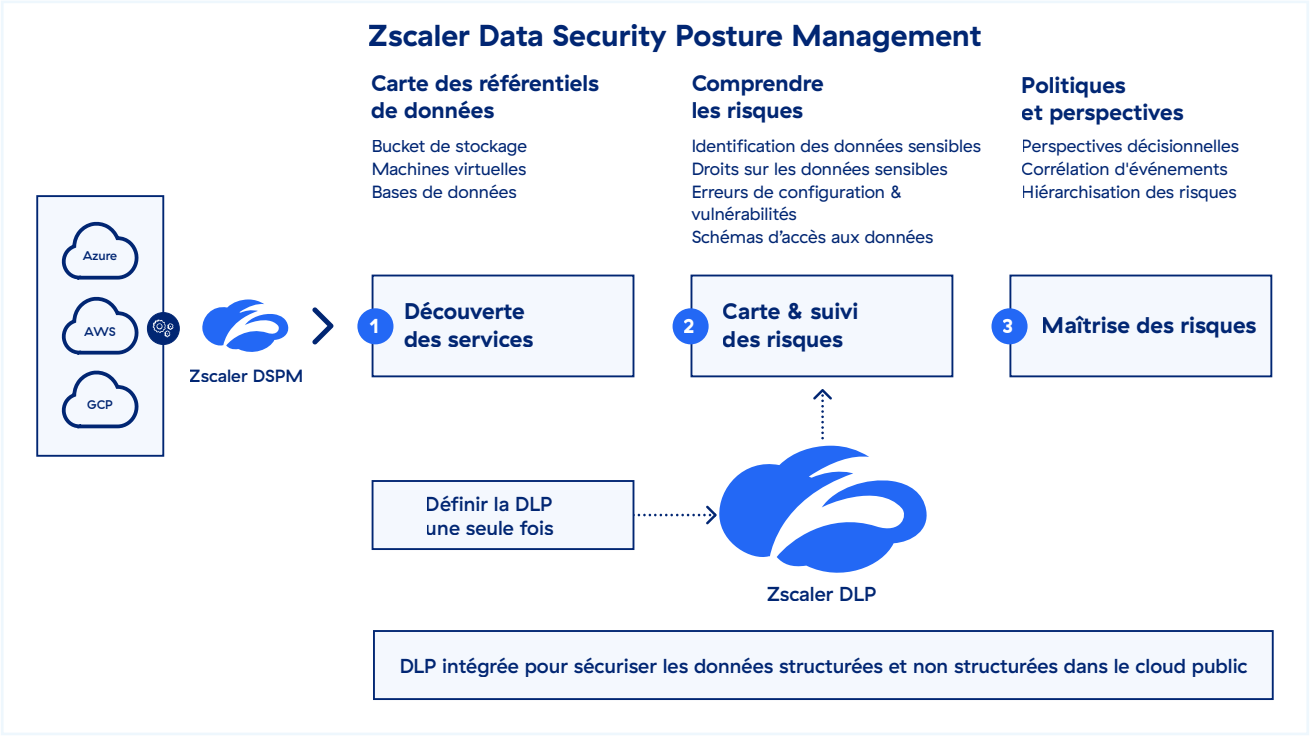
Au cœur de Zscaler DSPM

Zscaler AI Data Protection est une plateforme intégrée pour une protection intégrale des données. Elle sécurise à la fois les données structurées et non structurées sur un vaste périmètre : services SaaS, environnements de cloud public (AWS, Azure, GCP), applications privées, messagerie électronique et terminaux.



Composante de la plateforme Zscaler, Zscaler DSPM étend une sécurité des données robuste au cloud public. Elle procure une visibilité granulaire sur les données cloud, catégorise les données et les accès et contextualise l'exposition des données et la posture de sécurité. Autant d'atouts qui permettent aux équipes de sécurité de prévenir et de corriger à grande échelle les violations de données dans le cloud.

© 2024 Zscaler, Inc. Tous droits réservés.



Avec son moteur DLP unifié, Zscaler DSPM offre une protection des données cohérente sur tous les canaux. En suivant tous les utilisateurs sur tous les sites et en régissant les données en cours d'utilisation ou au repos, la solution assure une protection homogène des données et la mise en conformité.

Panel fonctionnel de Zscaler DSPM

Identification, classification et inventaire des données
Les méthodes d'analyse traditionnelles sont onéreuses et exigent des efforts considérables pour aboutir à des résultats satisfaisants. En se contentant d'un simple accès aux ressources dans les environnements cloud (AWS, Azure et GCP), Zscaler DSPM analyse les référentiels de données, détecte les données sensibles et catégorise les données avec précision. La solution simplifie les tâches suivantes :

- **Identification de toutes les données :** Zscaler DSPM surveille en permanence les environnements cloud pour découvrir automatiquement de nouveaux référentiels et entrepôts de données à mesure qu'ils sont déployés. Cette approche favorise un vrai gain de temps et élimine toute zone d'ombre sur les données.
- **Classification précise des données :** Zscaler DSPM utilise des moteurs DLP et des dictionnaires prédéfinis pour classifier les données. La solution procure une visibilité sur le type de données sensibles stockées dans les ressources cloud, la région, les fichiers contenant des données sensibles, le degré de risque associé aux données sensibles, etc. Elle offre une certaine flexibilité aux entreprises pour créer ou répliquer les politiques existantes.
- **Inventaire précis des données :** Zscaler DSPM crée également une carte et un inventaire précis des ressources de données, ce qui permet aux équipes de sécurité de localiser les données sensibles, d'identifier ceux qui y ont accès et de comprendre la manière dont elles sont utilisées.

Avec Zscaler DSPM, les équipes de sécurité améliorent la visibilité sur les données au sein de l'infrastructure cloud. La gestion et la sécurité des données gagnent en efficacité au sein des environnements multicloud qui englobent des couches complexes de SaaS, PaaS, IaaS et de bases de données.

© 2024 Zscaler, Inc. Tous droits réservés.

Cartographier et suivre l'exposition des données

Les services et les configurations cloud changent fréquemment, ce qui peut aboutir une exposition des données. Ces failles de sécurité doivent impérativement être corrigées avant que des acteurs malveillants ne les exploitent. Zscaler DSPM détecte les ressources exposées publiquement tout comme les vulnérabilités ou les erreurs de configuration dans les différentes composantes (groupe de sécurité du réseau, équilibreur de charges, réseau virtuel, etc.) associés à ces ressources de données. Il en résulte de solides avantages :

- **Analyse de l'exposition :** déterminez le niveau exposition publique, les erreurs de configuration et les vulnérabilités des référentiels de données et des services qui y font appel.
- **Évaluation des risques :** définissez un niveau de risque global en corrélant impact et probabilité. Les risques sont classés en trois catégories : élevé, moyen ou faible.
- **Hiérarchisation des risques :** aidez les équipes de sécurité à évacuer les informations non pertinentes et à hiérarchiser les incidents en fonction selon des critères de risque et de gravité.
- **Corrélation avancée des menaces :** corrélez les menaces, les facteurs de risque et les chemins d'attaque furtifs afin de minimiser les risques.
- **Veille sur les accès adaptatifs :** bénéficiez d'une vue granulaire, basée sur les risques et orientée utilisateur, sur tous les chemins d'accès aux données et paramètres de configuration critiques.

Maîtrise des risques

Zscaler DSPM simplifie la gestion des risques grâce à des mesures correctives guidées et basées sur des éléments de contexte : les équipes de sécurité peuvent ainsi résoudre les problématiques et incidents à la source, en amont de tout dommage. Les fonctionnalités suivantes sont proposées :

- **enquêtes et réponses efficaces** pour aider les équipes de sécurité à appréhender rapidement les causes profondes potentielles d'un événement lié à la sécurité des données.
- **correction guidée approfondie** pour apporter aux équipes pluridisciplinaires des workflows automatisés et de conseils pertinents et ainsi traiter les risques liés à la sécurité des données.
- **sécurité plus rapide** qui permet aux équipes de configurer des alertes personnalisées en temps réel afin de suivre l'évolution des données et de leur environnement, et ainsi accélérer les enquêtes et la prise en charge des risques.
- **intégration homogène** avec les outils et plateformes ITSM, SIEM ou ChatOps existants pour améliorer les alertes, les opérations de remédiation, l'accompagnement et les workflows.

Évaluer Zscaler DSPM

Demander une démo
Découvrez Zscaler DSPM en action lors d'une démonstration guidée.

Demander une démo

Téléchargez le guide d'achat dédié au DSPM
Découvrez les 5 principaux critères pour choisir une solution DSPM adaptée à votre entreprise.

Télécharger le guide

Pour plus d'informations, rendez-vous sur : zscaler.com/fr/dp/dspm.

© 2024 Zscaler, Inc. Tous droits réservés.

Annexe

Glossaire

- Gestion de la posture de sécurité des données (DSPM)
- Plateforme de protection des applications cloud natives (CNAPP)
- Gestion de la posture de sécurité cloud (CSPM)
- Gestion des droits d'accès à l'infrastructure cloud (CIEM)

À lire également

Scannez le code QR pour accéder aux ressources de la DSPM.

Sessions en replay

- Conférence : Session Zenith Live '24, « Zscaler DSPM : Sécuriser les données cloud avec une plateforme entièrement intégrée »
  Découvrez l'expérience DSPM d'Inter&Co.
- Webinaire : « Pourquoi la DSPM a-t-elle sa place dans votre stratégie de protection des données ? »

zscaler™ | Experience your world, secured.™

À propos de Zscaler
Zscaler (NASDAQ : ZS) accélère la transformation digitale de ses clients pour qu'ils gagnent en agilité, efficacité, résilience et sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et les pertes des données, en connectant de manière sécurisée les utilisateurs, les appareils et les applications, quelle que soit leur localisation. Adossée à plus de 150 data centers dans le monde, Zero Trust Exchange est la plus vaste plateforme cloud de sécurité et SSE active en mode inline. Pour en savoir plus, rendez-vous sur **zscaler.com/fr** ou suivez-nous sur Twitter**@zscaler**.

©2024 Zscaler, Inc. Tous droits réservés. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ et les autres marques commerciales répertoriées sur zscaler.com/fr/legal/trademarks sont soit 1) des marques déposées ou marques de service, soit 2) des marques commerciales ou marques de service de Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs.

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