L’essentiel de Zscaler™ Data Security

L’ESSENTIEL

Avantages de la plateforme de sécurité des données :

AUTOMATISATION DES FLUX DE TRAVAIL
Répondre plus rapidement aux incidents et former les utilisateurs aux comportements adéquats grâce à l’automatisation intégrée des flux de travail.

CLASSIFICATION PILOTÉE PAR L’IA
Avec la classification LLM, vous pouvez retrouver du contenu par intention, et pas seulement par mots-clés, pour une protection plus intelligente.

SÉCURITÉ ROBUSTE DES DONNÉES D’IA
Favorisez la productivité sécurisée de l’IA grâce à un contrôle complet des données partagées avec Public AI, Microsoft Copilot et les outils d’IA privés.

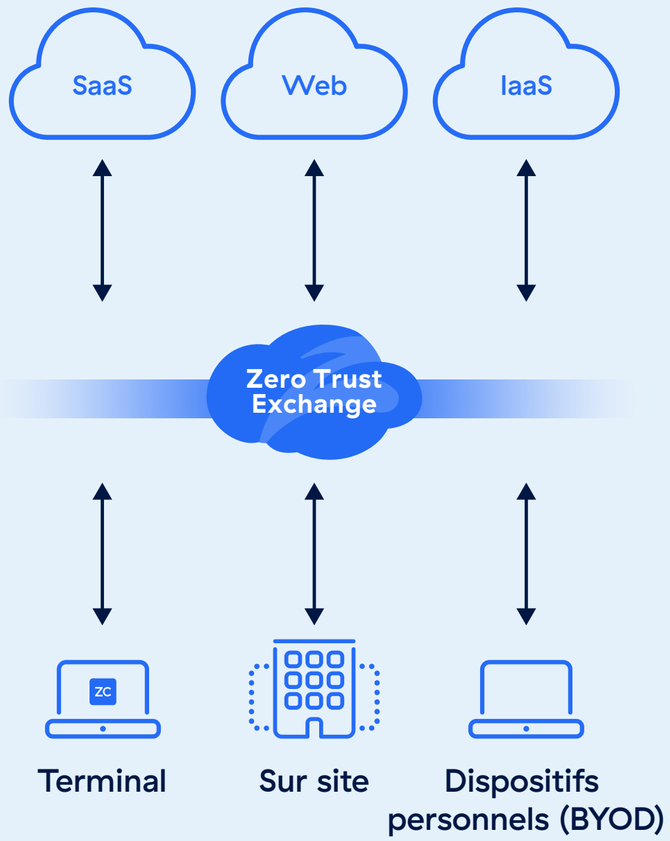
AUTOMATISATION DES FLUX DE TRAVAIL
Répondre plus rapidement aux incidents et former les utilisateurs aux comportements adéquats grâce à l’automatisation intégrée des flux de travail.

Zscaler Data Protection offre une sécurité intégrée contre toutes les sources de perte de données :

Classification LLM optimisée par l’IA

Les données sensibles étant dispersées dans des clouds et des écosystèmes fragmentés, leur identification et leur sécurisation sont essentielles afin de créer une base solide pour la protection des données.

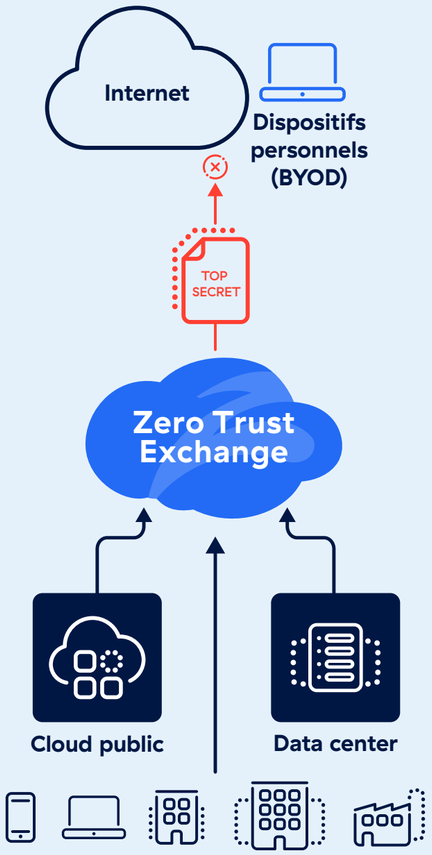
La classification optimisée par l’IA de Zscaler simplifie ce processus, en vous permettant de localiser les données sensibles où qu’elles se trouvent. En s’appuyant sur la classification LLM avancée, il détecte les données en fonction de l’intention, éliminant ainsi le besoin de recherches par mots-clés traditionnelles. En s’appuyant sur la classification LLM avancée, elle détecte les données en fonction de l’intention, éliminant ainsi les recherches traditionnelles par mots clés.



Prévenir les pertes de données vers le Web et via les dispositifs personnels (BYOD)

Les utilisateurs qui accèdent à Internet et à des destinations à risque met en péril les données d'entreprise. Les appliances traditionnelles ne peuvent pas suivre les utilisateurs hors du réseau ni sécuriser leur trafic Internet.

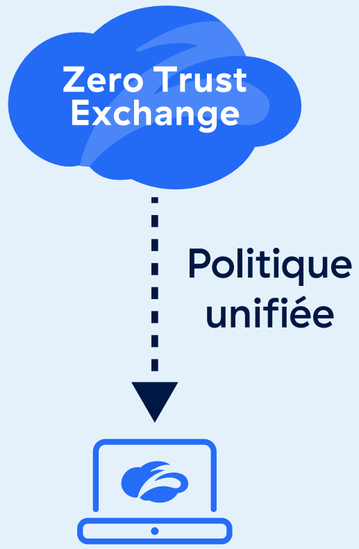
Zscaler est une plateforme cloud native et évolutive, qui inspecte l'ensemble du trafic, partout. Une politique de DLP unique protège les données sur le Web, les applications SaaS et privées, et s'accompagne de techniques de classification avancées telles que EDM, IDM et OCR. Tirez parti de l'isolation du navigateur pour diffuser en toute sécurité des données sous forme de pixels vers les dispositifs personnels (BYOD) non gérés.



Sécurisez les données des terminaux

Les utilisateurs qui accèdent à Internet et à des destinations à risque met en péril les données d'entreprise. Les appliances traditionnelles ne peuvent pas suivre les utilisateurs hors du réseau ni sécuriser leur trafic Internet.

Zscaler est une plateforme cloud native et évolutive, qui inspecte l'ensemble du trafic, partout. Une politique de DLP unique protège les données sur le Web, les applications SaaS et privées, et s'accompagne de techniques de classification avancées telles que EDM, IDM et OCR. Tirez parti de l'isolation du navigateur pour diffuser en toute sécurité des données sous forme de pixels vers les appareils personnels (BYOD) non gérés.

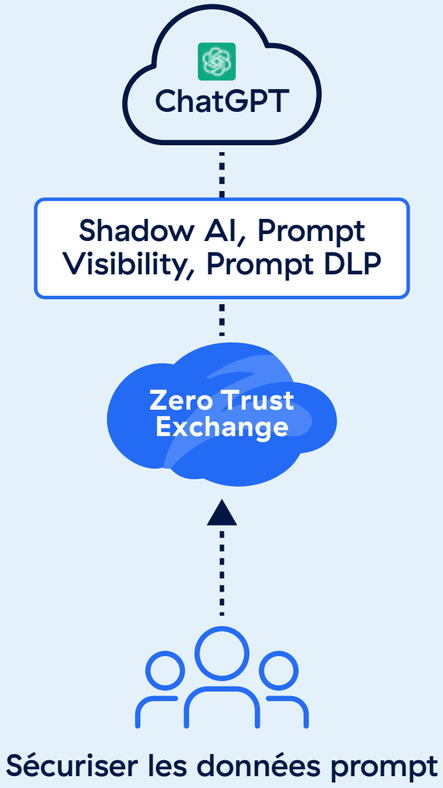


© 2025 Zscaler, Inc. Tous droits réservés.

Sécurité de l’IA générative

Les données alimentent la puissance des outils d’IA, mais sans protections appropriées, elles peuvent exposer les entreprises à des risques non négligeables, notamment la perte de données et des accès non autorisés.

Zscaler GenAI Security fournit une solution proactive pour identifier les occurrences d’IA fantôme (Shadow AI) et déployer des garde-fous robustes pour des interactions de données sécurisées. Son tableau de bord interactif offre une visibilité claire sur l’exposition des applications d’IA fantôme parmi les utilisateurs et les données, révélant les modèles d’utilisation avec des informations au niveau des invites, une catégorisation des invites et des contrôles DLP inline. Ces fonctionnalités fonctionnent ensemble pour prévenir la perte de données sensibles et améliorer la sécurité des opérations pilotées par l’IA.

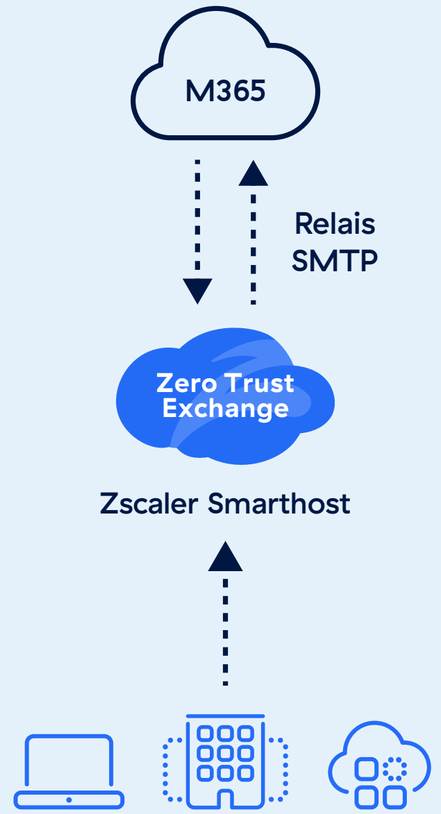


Sécuriser les données prompt

E-mail DLP via Smarthost

Les e-mails représentent l’un des vecteurs de perte de données les plus courants. Les utilisateurs peuvent facilement transférer des données sensibles en dehors de l’entreprise ou vers des messageries personnelles.

Avec la DLP pour les e-mails de Zscaler, les administrateurs de sécurité disposent d’un moyen extrêmement simple d’insérer une inspection DLP dans leur architecture de messagerie. Mis en œuvre en tant que Smarthost, Zscaler peut être ajouté comme prochain saut après votre service de messagerie via le relais SMTP. Appliquez l’inspection DLP et des actions telles que le blocage, le chiffrement et la mise en quarantaine, le tout avec des modifications minimes de vos paramètres de messagerie ou MTA.



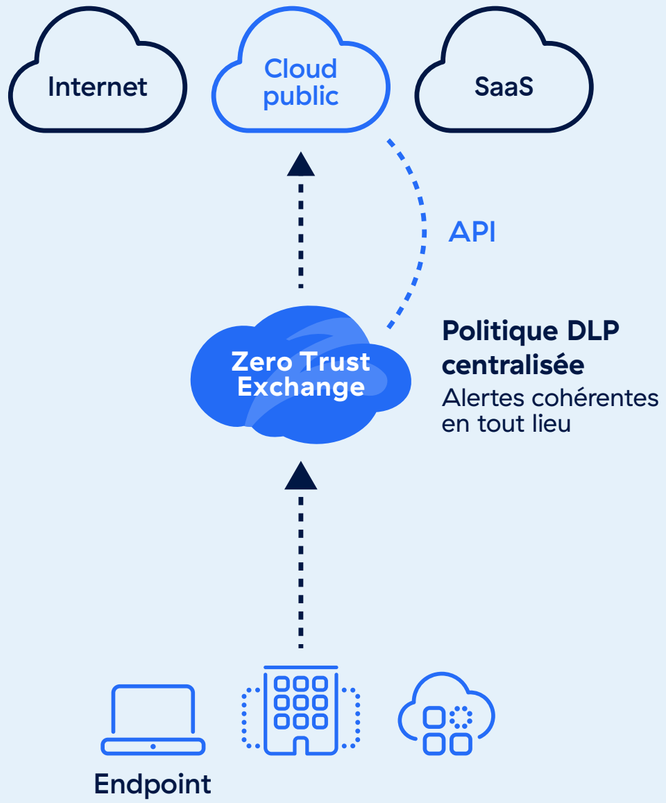
Zscaler Smarthost

© 2025 Zscaler, Inc. Tous droits réservés.

Gestion de la posture de sécurité des données (DSPM)

Les données sensibles stockées dans les clouds publics tels qu'AWS et Azure peuvent être dynamiques. Qu'il s'agisse de privilèges excessifs, de vulnérabilités ou de données fantômes, les équipes informatiques doivent pouvoir mieux identifier, cataloguer et sécuriser les données du cloud public.

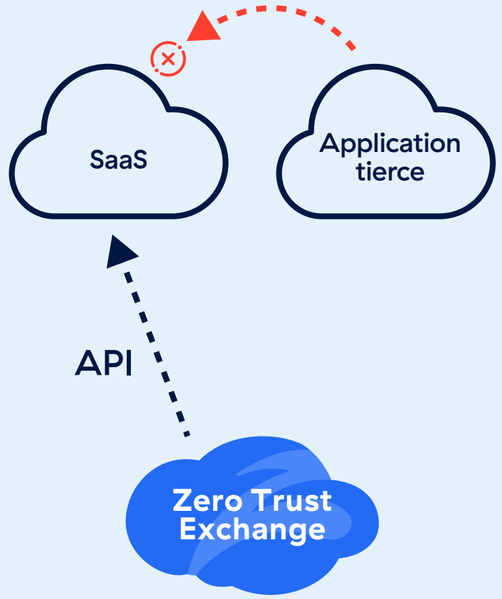
La DSPM de Zscaler découvre rapidement les données sensibles, comprend les risques et contrôle l'accès et la posture. Mieux encore, la DSPM intégrée de Zscaler exploite le même moteur DLP qui protège tous les autres canaux de fuite potentielle de données (terminaux, réseaux, SaaS) : vos alertes gagnent ainsi en cohérence, quelle que soit la destination des données en transit.



Sécurité SaaS unifiée (SSPM, chaîne d'approvisionnement du SaaS, CASB)

De nombreuses violations du cloud sont imputables à des erreurs de configuration dangereuses, des accès ou des applications tierces connectées à des plateformes SaaS. Comprendre et piloter votre posture SaaS est un levier clé pour sécuriser de vastes volumes de données sensibles dans ces clouds.

Avec la sécurité SaaS unifiée de Zscaler, les entreprises bénéficient d'une approche unifiée pour analyser et sécuriser les plateformes SaaS telles que Microsoft 365 ou Google. Bénéficiez d'une visibilité précise sur les erreurs de configuration et les intégrations d'applications à risque grâce à un processus automatique de restauration, des recommandations et la possibilité de révoquer toute connexion à risque d'une application.



© 2025 Zscaler, Inc. Tous droits réservés.

COMPOSANTS DE ZSCALER DATA SECURITY		PLATEFORME ZSCALER ESSENTIALS	PLATEFORME ZSCALER
Norme de sécurité des données	Arrêter la perte de données avec les fonctions de contrôle des applications cloud, de découverte de l'informatique fantôme, de restriction d'entité, de DLP Web inline (en mode de surveillance uniquement) et de CASB pour 1 application	Inclus	Inclus
DLP Web inline — Toutes les applications	Prévenir la perte de données grâce à une DLP Web inline sur le Web, l'IA générative et les applications privées	Module complémentaire	Inclus
DLP pour les e-mails	Sécuriser vos e-mails et pièces jointes avec DLP sur Exchange Online, Exchange On-Prem ou Gmail	Module complémentaire	Module complémentaire
DLP pour les terminaux	Sécuriser les données des terminaux via USB, les partages réseau et l'impression tout en réduisant le nombre d'agents sur les terminaux	Module complémentaire	Module complémentaire
Sécurité SaaS unifiée (CASB, SSPM et Chaîne d'approvisionnement)	Gouverner et contrôler les données et la posture SaaS via une plateforme unifiée	Module complémentaire	Module complémentaire
Classification des données et chiffrement avancé	Utilisez la classification LLM pour retrouver du contenu en fonction de l'intention. Exploitez l'EDM, l'IDM et l'OCR pour les empreintes de données personnalisées, formulaires et images (captures d'écran). Expurger, chiffrer et filigraner les données.	Module complémentaire	Module complémentaire
Isolation avancée du BYOD	Prévenir le BYOD et les appareils non gérés lors de l'accès aux applications SaaS (portail utilisateur 2.0)	Module complémentaire	Module complémentaire
Gestion de la posture de sécurité des données (DSPM)	Découvrir, classer et protéger rapidement les données sensibles dans les clouds publics	Module complémentaire	Module complémentaire
Sécurité de l'IA générative	Contrôler les applications de l'IA générative avec un tableau de bord interactif, une visibilité et une classification au niveau des invites et des contrôles DLP au niveau des invites.	Module complémentaire	Module complémentaire

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 160 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 **www.zscaler.com/fr** ou suivez-nous sur X (ex-Twitter) **@zscaler**.

© 2025 Zscaler, Inc. Tous droits réservés. Zscaler™ 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**

zscaler™

Zero Trust Everywhere