E-BOOK

La protection de vos données à l'ère du télétravail

Protégez vos informations critiques avec Zscaler Data Protection

Sommaire

La protection de vos données est plus que jamais un défi

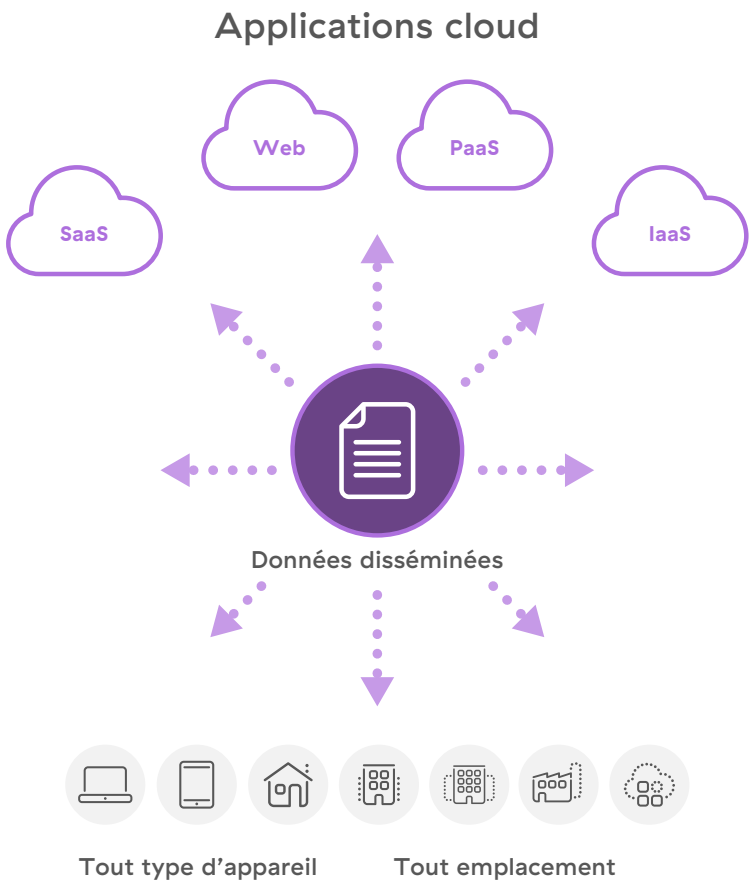
Avec les applications cloud, vos données sont désormais disséminées à grande échelle tandis que vos collaborateurs se connectent aux ressources de votre entreprise à partir de lieux géographiques différents. Les approches traditionnelles de protection des données vous privent d'un contrôle pertinent sur vos données. Et ce, pour plusieurs raisons :

Pas de tracking des utilisateurs
Vous ne pouvez assurer une protection optimale des données, car vos applications cloud sont accessibles via Internet. Elles sont hors de votre réseau et de vos fonctionnalités de protection.

Statut de conformité inconnu
Il est difficile d'évaluer le statut de votre conformité dans la mesure où vos applications cloud sont disséminées sur plusieurs sites et groupes.

Inspection TLS/SSL limitée
Le trafic est majoritairement chiffré. Cependant, les approches traditionnelles de protection des données ne peuvent pas inspecter le trafic TLS/SSL à grande échelle : vous ne disposez donc pas de visibilité sur tous les risques potentiels.

Absence de vue d'ensemble
Les produits de sécurité cloisonnés et le déploiement de nouvelles couches de sécurité vis-à-vis de l'existant alimentent la complexité et vous privent de cette visibilité consolidée pourtant nécessaire pour comprendre votre exposition aux risques.



Solution Zscaler

Reprendre la main sur vos données avec Zscaler

Zscaler Data Protection optimise la protection de vos données grâce ces principes fondamentaux :

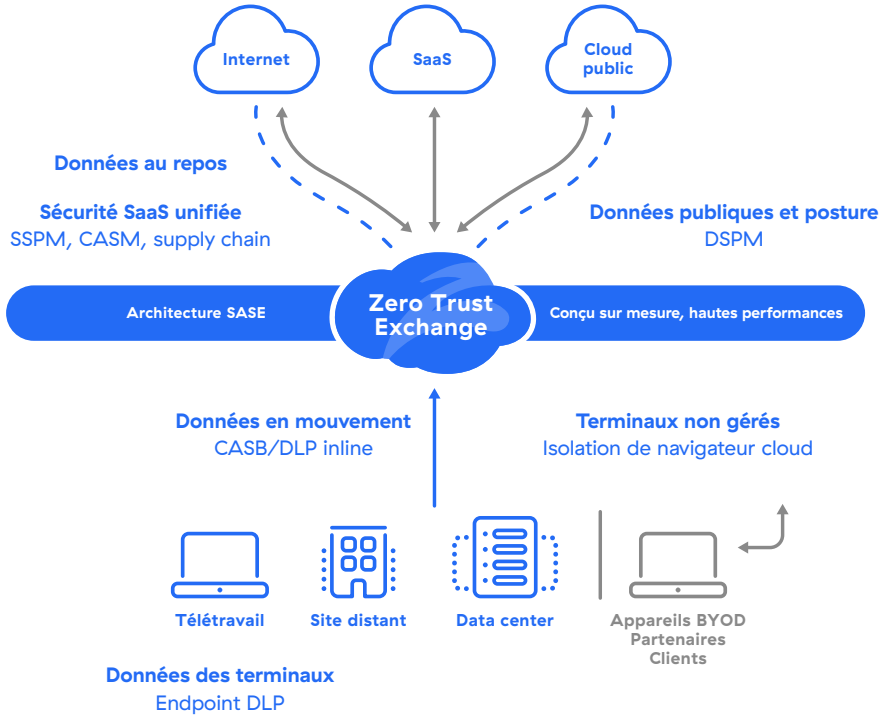
Architecture SASE dédiée
Protégez en temps réel tous vos utilisateurs à partir d'un cloud inline haute performance et adossé à 150 data centers dans le monde.

Inspection SSL à grande échelle
Inspectez l'ensemble du trafic SSL pour évaluer le niveau d'exposition de toutes vos données aux risques.

Visibilité sur la conformité
Assurez votre conformité sur le long terme en analysant vos applications SaaS, Microsoft 365, ainsi que les clouds publics à la recherche d'intrusions ou d'erreurs de configuration.

Une seule plateforme, une seule politique, une visibilité intégrale
Sécurisez tous vos canaux de données (données en transit, au repos et présentes sur les terminaux et clouds) grâce à une plateforme simple et unifiée.

Zscaler Data Protection : présentation de la solution



CASB hors bande (out of band)

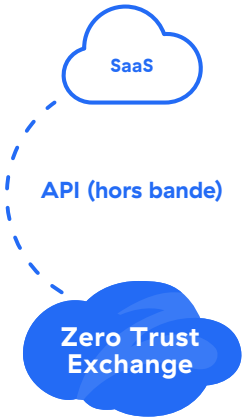
Gérer en toute sécurité les applications autorisées avec un CASB hors bande

Vos applications cloud favorisent la collaboration, en particulier avec les télétravailleurs, mais elles peuvent également mettre vos données en péril. Les collaborateurs peuvent involontairement faire des erreurs dans l'utilisation de leurs applications, ce qui peut favoriser les activités malveillantes.

Comment sécuriser vos applications et vos données dans le cloud avec le CASB hors bande de Zscaler :

- **Sécuriser les données au repos qui sont à risque**
  Identifiez les données critiques dans les applications cloud, la messagerie électronique et les espaces de partage de fichiers. Appliquez les politiques DLP pour contrôler l'accès à ces données et leur exposition.

- **Prévenir le partage inapproprié de données**
  Appliquez une politique granulaire aux données sensibles au repos pour éviter qu'elles soient partagées hors de l'entreprise.



- **Neutraliser les menaces**
  Analysez les données présentes dans les services d'hébergement de fichiers tels que OneDrive ou Box, afin de détecter et mettre en quarantaine rapidement tout contenu malveillant.

- **Simplifier la protection des données**
  Évitez les produits autonomes complexes, grâce à une plateforme unifiée qui fournit une politique unique en matière de données et de menaces pour toutes les données en transit et au repos.

CASB inline

Une visibilité et un contrôle en temps réel grâce à un CASB inline

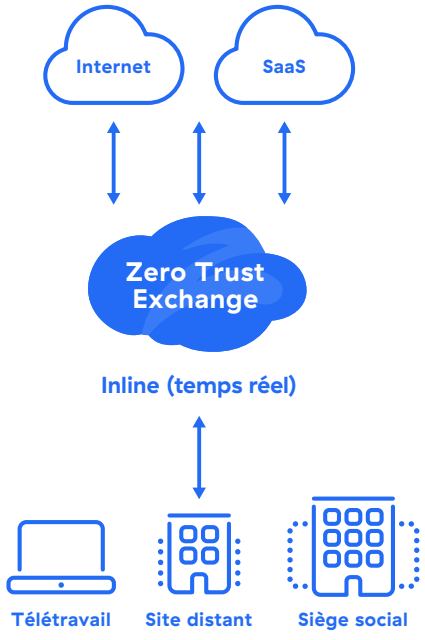
Si le CASB hors bande permet de sécuriser les données au repos, vous devez néanmoins pouvoir contrôler en temps réel vos applications cloud. Comment un CASB inline sécurise-t-il votre adoption du cloud ?

- **Maîtrise les risques liés au Shadow IT**
  Déterminez rapidement quelles sont les applications cloud, sécurisées ou non, qui sont utilisées au sein de l'entreprise.

Exemple : bloquer les tâches des applications à risque qui accèdent à vos données, comme les outils en ligne de conversion PDF ou les sites de partage de fichiers.

- **Impose les applications officiellement validées**
  Limitez l'activité des utilisateurs aux applications cloud validées en interne.

Exemple : améliorer le partage de fichiers et la productivité dans Microsoft 365 en autorisant uniquement OneDrive et en bloquant Box.



Mode de travail hybride

- **Prévient les pertes de données grâce à un contrôle sur les types de fichiers**
  Limitez le transfert de données par type de fichier grâce à un blocage conditionnel et à des alertes.

Exemple : empêcher le téléversement ou le téléchargement de fichiers Word, Excel ou PowerPoint, par utilisateur ou groupe d'utilisateurs.

- **Applique des restrictions aux instances**
  Contrôlez les flux de données en n'autorisant que des instances spécifiques d'applications cloud.

Exemple : éviter les fuites de données via des instances personnelles de Microsoft 365 en n'autorisant l'accès qu'à Microsoft 365 Business.

DLP pour les terminaux

Simplifier le contrôle des données sur les terminaux avec une DLP dédiée

Une protection efficace des données doit prendre en compte les terminaux. Avec une DLP dédiée aux terminaux, vous bénéficiez d'une protection totale et simple des dispositifs d'utilisateurs.

- **Politique et visibilité unifiées**
  Avec un moteur DLP centralisé, vous bénéficiez d'alertes cohérentes sur les terminaux et le cloud.
- **Agent unique et léger**
  Intégré à l'agent Zscaler, cette DLP améliore l'expérience utilisateur et réduit le nombre d'agents présents sur les terminaux.
- **Déploiement rapide**
  Tirez parti de vos politiques Zscaler DLP existantes pour être opérationnel rapidement.
- **Gestion accélérée des incidents**
  Réagissez plus rapidement aux incidents grâce à une automatisation des workflows, des tableaux de bord détaillés et des analyses approfondies.

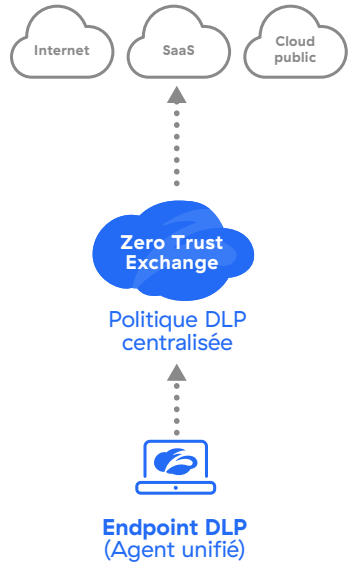
Principaux cas d'utilisation de la DLP pour Endpoint

Protéger davantage de données
Assurez-vous que les données de valeur sont suivies correctement et protégées partout, en permanence.

Sécuriser les données suite au départ de collaborateurs
Assurez-vous que celles et ceux qui quittent votre entreprise ne copient aucune donnée présente sur leur dispositif.

Supprimer la DLP endpoint traditionnelle
Éliminez les produits autonomes et privilégiez une solution unifiée.

Améliorer la conformité
Restez en conformité réglementaire sur l'ensemble des fichiers et des endpoints.



Canaux protégés

Support amovible	Synchronisation avec un stockage cloud personnel
Partages réseau	Impression

DLP pour l'email

Une DLP unifiée pour les emails, active en temps réel

L'email constitue un vecteur majeur de perte de données. Grâce au module de Zscaler Email DLP, les entreprises peuvent déployer une couche de contrôle DLP intégrale pour les données de messagerie.

Les approches traditionnelles de sécurisation des données de messagerie peuvent être lourdes et fastidieuses. Avec l'adoption du SSE, les équipes informatiques veulent privilégier des approches unifiées et simples pour sécuriser les données échangées par email.

Grâce au module de Zscaler Email DLP qui s'appuie sur Smarthost, la protection en temps réel des données peut être facilement étendue à la messagerie électronique. En utilisant le relais SMTP, Zscaler permet une intégration fluide dans les architectures de messagerie existantes, avec un contrôle complet sur les données de messagerie et les pièces jointes.

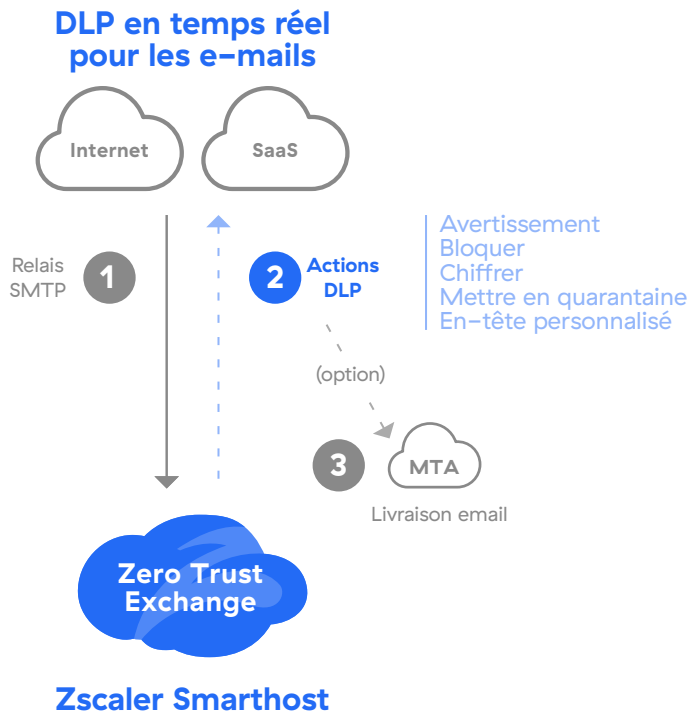
Avantages du module de Zscaler Email DLP :

Interopérable avec différents protocoles
Fonctionne sur les dispositifs gérés, non gérés, et notamment les dispositifs mobiles.

Déploiement simplifié
Aucune modification de l'enregistrement MX n'est requise.

Politique flexible
Des définitions modulables de politique et des évaluations granulaires de politique sont utilisées.

Centralisé et unifié
Une interface utilisateur unique et des moteurs DLP sont disponibles sur tous les canaux.

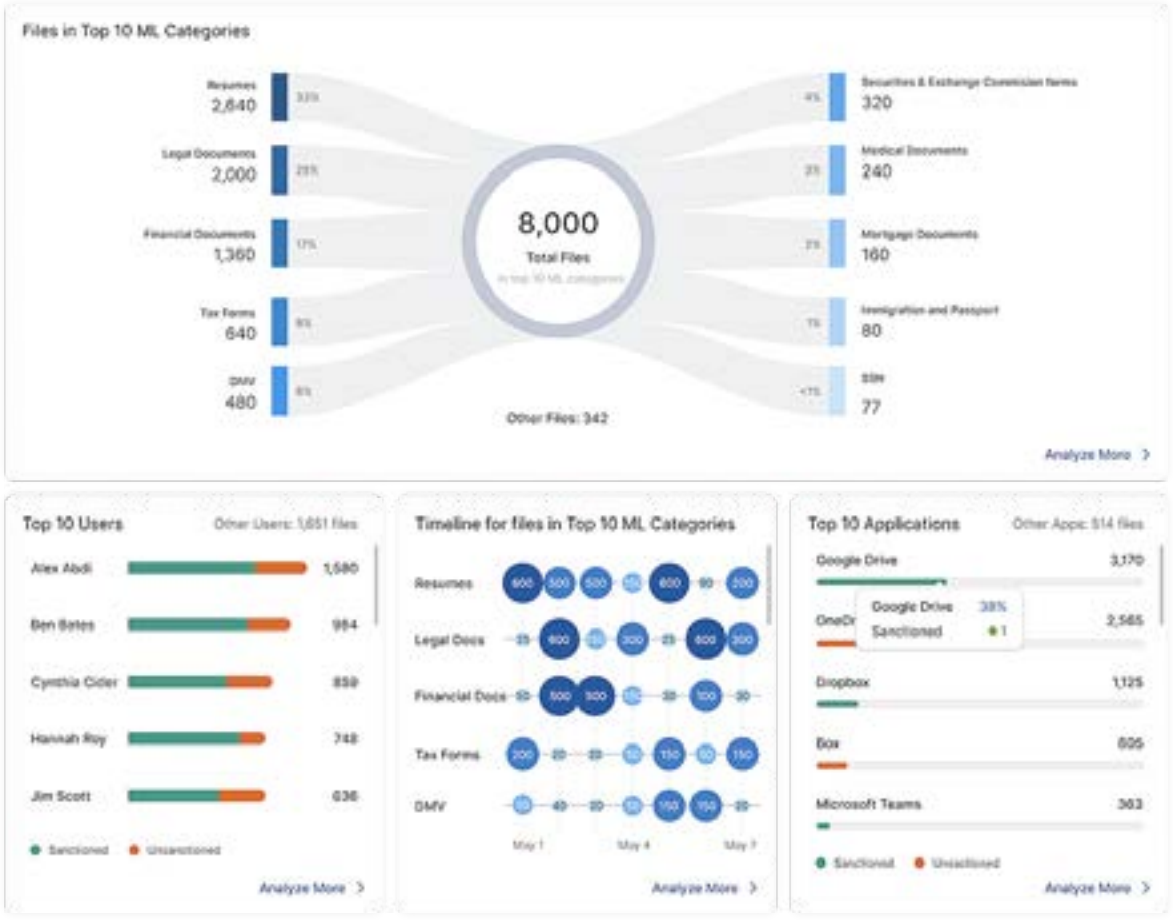


Détecter et protéger les données via une identification optimisée par IA

Le déploiement et la mise en œuvre d'un programme de protection des données sont souvent chronophages. Grâce à la solution innovante d'identification des données de Zscaler, vous pouvez comprendre rapidement les risques et les comportements associés à vos données.

Avantages d'une identification de données optimisée par IA :

- Identifier les données sur les terminaux, dans les environnements en ligne et dans les clouds publics
- Comprendre rapidement les risques de perte liés aux utilisateurs et aux applications
- Créer une politique en quelques clics



Classifier et protéger les données, formulaires et images contre le risque de perte

La classification des données est au cœur de tout programme efficace de DLP. Grâce à une classification avancée, vous pouvez prévenir toute perte de profils particuliers de données sensibles.

Exact Data Match (EDM)

Fingerprinting et sécurisation des données d'entreprise. Exemple : activez des alertes qui sont déclenchées par rapport aux informations de carte de paiement des clients, mais pas sur toutes les cartes de paiement (comme lors d'un achat sur Amazon).

Indexed Document Match (IDM)

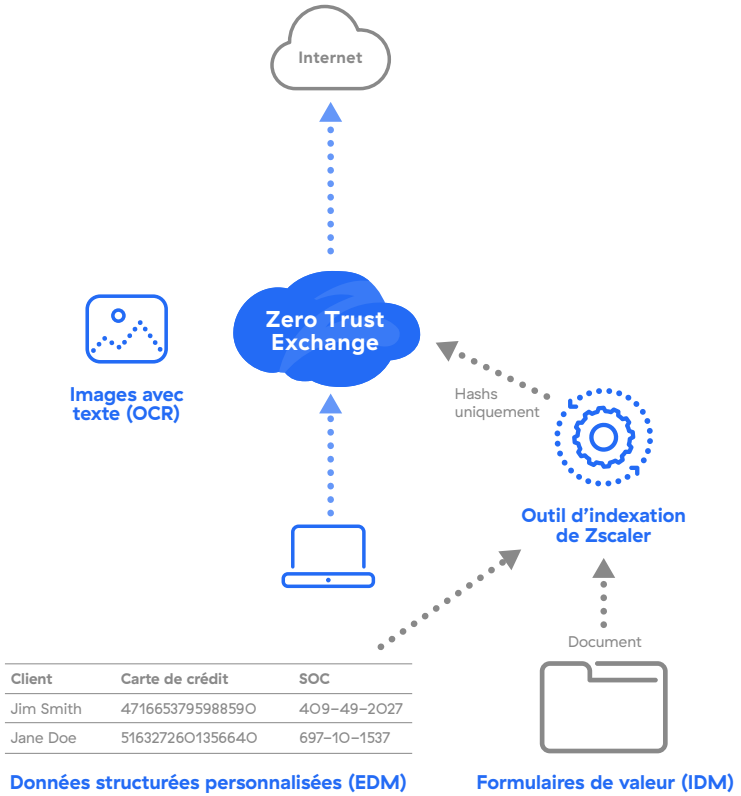
Fingerprinting et sécurisation des documents et des formulaires personnalisés. Exemple : prenez l'empreinte d'un formulaire fiscal ou bancaire vierge et empêchez de remplir tout autre exemplaire.

Reconnaissance optique de caractères (OCR)

Identifier et prévenir la perte de données en identifiant le texte dans les images. Exemple : surveillez les captures d'écran affichant un contenu sensible.

Outil d'indexation Zscaler

Complémentaire à l'outil de fingerprinting pour l'EDM et l'IDM. Cet outil crée des hashs pour les données et charges EDM et IDM dans Zscaler Cloud à des fins de création de politiques.



Optimiser la visibilité et le contrôle sur les applications d'IA générative

Le contrôle de la perte de données sensibles via les applications d'IA générative garantit que ces applications vont contribuer sans risques à la productivité de leurs utilisateurs. La nouvelle approche de Zscaler centralise la protection et la visibilité en un seul endroit.

Les applications d'IA générative (ou GenIA) ont le potentiel d'améliorer la productivité de vos activités sur l'ensemble de votre périmètre organisationnel. Cependant, vous devez disposer d'une visibilité et d'un contrôle complets sur ces applications, pour neutraliser pertinemment celles présentant un risque de sécurité.

Zscaler propose une sécurité innovante de l'IA générative. Les équipes informatiques identifient toutes les applications GenIA dans entreprise, avec une visibilité précise sur les requêtes saisies et la possibilité de les bloquer ou pas.

Avantages

- Une visibilité contextuelle et complète sur les requêtes des utilisateurs envoyées aux applications IA
- Des contrôles de politique flexibles pour assurer l'inspection DLP et le contrôle des applications cloud
- Un accès cloisonné pour protéger les données avec Zscaler Cloud Browser

Visibilité sur l'IA générative

Détection de l'IA fantôme
Catalogue de toutes les applications IA populaires

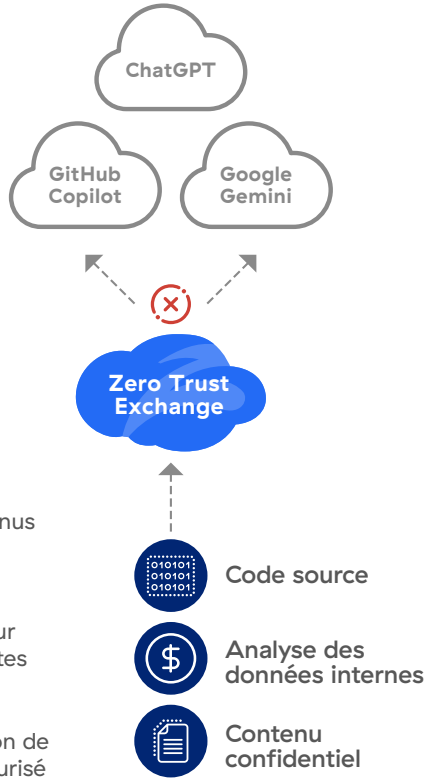
Visibilité sur les requêtes saisies
Voir les requêtes saisies que les utilisateurs envoient aux applications IA

Contrôles des applications d'IA générative

Inspection DLP
Bloquer la fuite de données et de contenus sensibles vers les applications d'IA

Contrôle des applications cloud
Contrôle d'accès aux applications IA pour tous les utilisateurs, départements et sites

Isolation du navigateur
Cloisonnement des données et utilisation de l'application via un navigateur cloud sécurisé

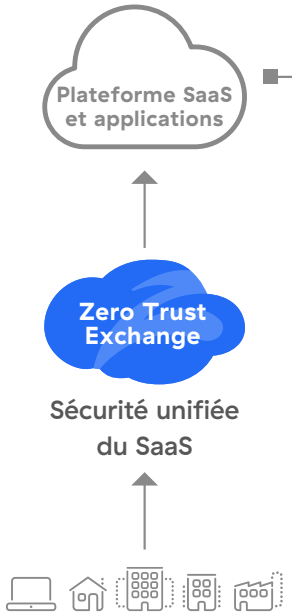


Une approche intégrée pour protéger votre plateforme SaaS

La sécurisation des clouds et des données SaaS requiert de trop nombreux outils. En unifiant les approches de gestion de la sécurité du SaaS, il est possible de simplifier la façon dont les équipes informatiques protègent les données SaaS.

De nombreux incidents de sécurité dans le cloud résultent d'erreurs de configuration ou d'applications tierces connectées aux plateformes SaaS. Comprendre et piloter votre posture SaaS est un levier clé pour sécuriser des volumes importants de données sensibles dans ces clouds.

Grâce à la solution SaaS Security Posture Management (SSPM) de Zscaler, vous bénéficiez 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.



Sécurité SaaS unifiée
Tout pour sécuriser le SaaS en un seul endroit

Gestion de la posture de sécurité SaaS (SSPM)
Corriger les erreurs de configuration

Sécurité de la chaîne collaborative du SaaS
Sécuriser les intégrations tierces à risque

API CASB
Prévenir le partage à risque de données sensibles

Activité de l'utilisateur
Surveiller les accès et les collaborateurs à risque

Éléments de contexte, corrélation et maîtrise des risques

Gestion de la posture de sécurité des données (DSPM)

Sécuriser les données et les clouds publics via une approche intégrée de protection des données

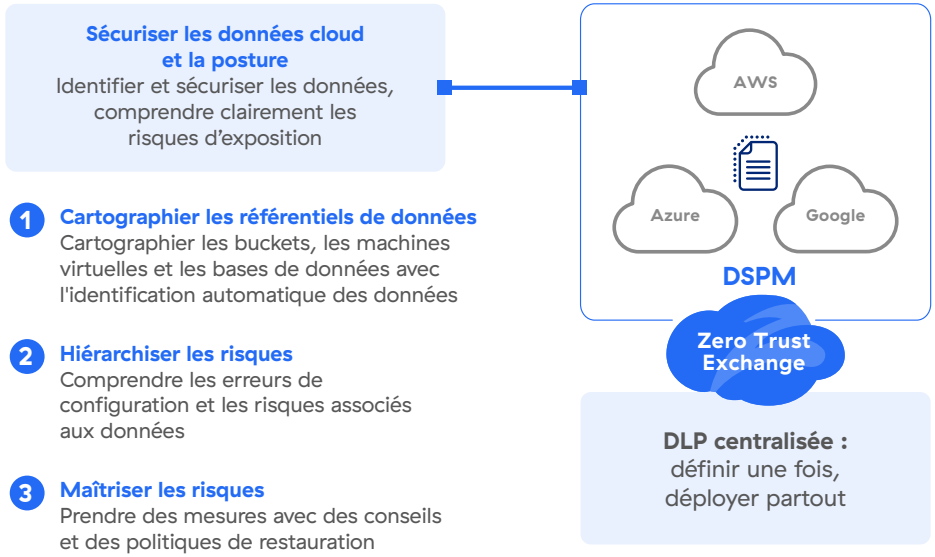
Les équipes chargées de la protection des données ont besoin d'une approche unifiée pour sécuriser les données présentes dans le cloud public. Zscaler DSPM s'intègre de manière transparente aux programmes déjà en place de protection des données.

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, classifier et sécuriser les données du cloud public.

Zscaler DSPM identifie rapidement les données sensibles, comprend les risques, et contrôle les 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.

Avantages

- Détecter rapidement des données sensibles grâce à une identification automatisée et optimisée par IA
- Corréler les erreurs de configuration, les niveaux d'exposition et les vulnérabilités pour mieux comprendre les risques liés aux données dans le cloud
- Appliquer les dictionnaires DLP existants aux données du cloud public pour gagner en visibilité, sur les éléments de contexte
- Neutraliser rapidement les risques grâce à un accompagnement sur les mesures correctives



Isolation du navigateur

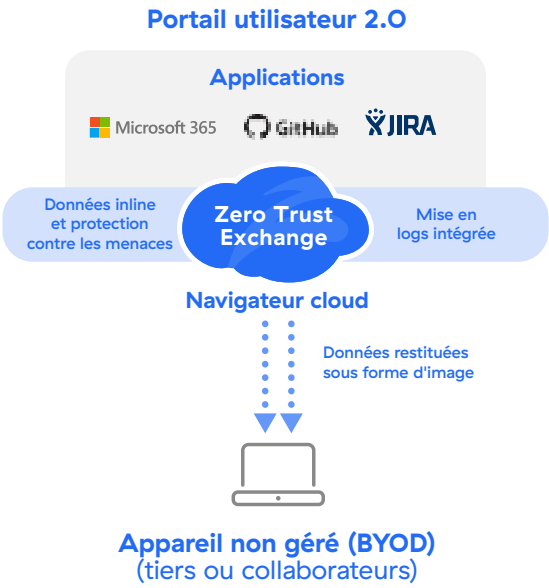
Sécuriser les données des applications Web et les accès pour les dispositifs personnels (BYOD)

Les partenaires, fournisseurs ou collaborateurs doivent parfois pouvoir accéder à vos données à partir de leurs dispositifs personnels. Comment garder le contrôle sur ces données alors que ces dispositifs ne sont pas gérés ?

Grâce au portail utilisateur 2.0 et au navigateur cloud de Zscaler, les entreprises prennent en charge en toute sécurité les dispositifs non gérés. Voici comment.

Comment le portail utilisateur 2.0 sécurise les accès et les données :

- Les utilisateurs s'authentifient sur le portail et accèdent à un tableau de bord des applications Web autorisées (SaaS ou privées). Aucun agent logiciel n'est à installer sur le terminal.
- Les utilisateurs accèdent à l'application via un navigateur cloisonné/isolé. Les données sont ensuite transmises en toute sécurité vers le terminal sous forme d'images.
- Les applications sont totalement interactives, mais certaines actions (couper, coller, télécharger et imprimer) sont désactivées. Les captures d'écran sont marquées d'un filigrane.



Avantages du BYOD :

Protection des données et contre les menaces
L'inspection de l'ensemble du trafic est effectuée en mode inline, garantissant le même niveau de sécurité dont bénéficie les dispositifs gérés pour le BYOD.

Cloisonnement des données et des fichiers
Affichez les documents ou partagez des fichiers (entre applications), sans ni fonctionnalité de téléchargement et de presse-papiers sur le terminal.

Politiques DLP intégrées
Tirez parti des politiques d'entreprise pour garantir une protection et des alertes cohérentes pour les données sensibles.

Zscaler Workflow Automation

Mieux gérer les incidents de perte de données avec Workflow Automation

Pour un coup d'accélérateur à votre programme de protection des données, il vous faut un outil de gestion des incidents puissant qui simplifie les opérations et guide les utilisateurs.

De nombreux programmes de protection rencontrent des difficultés en raison d'incidents multiples ou de l'utilisation d'outils disparates. De plus, les utilisateurs ne sont jamais alertés de leurs comportements à risque en cas de manipulation incorrecte des données.

Zscaler Workflow Automation fournit un outil dédié aux administrateurs DLP pour améliorer la gestion des incidents.

Grâce à la centralisation des analyses, les administrateurs comprennent rapidement les comportements à risque, attribuent les incidents aux utilisateurs pour qu'ils puissent se justifier, et prennent des mesures pour résoudre les incidents.

Comment Workflow Automation contribue à votre programme de protection des données

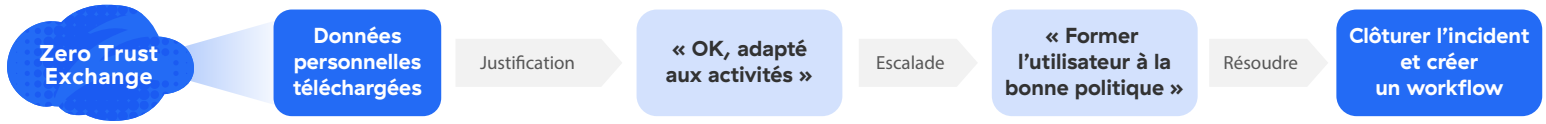
Gestion accélérée des incidents
Gagnez du temps grâce à une plateforme spécialement conçue pour la gestion des incidents de perte de données.

Routines automatisées
Simplifiez les opérations quotidiennes à l'aide de workflows qui automatisent les tâches répétitives et les escalades.

Accompagnement des utilisateurs
Expliquez les incidents auprès des utilisateurs via Slack, Teams ou par e-mail, tout en les sensibilisant aux bonnes pratiques de protection des données.

Intégration étroite
Évitez les carences courantes des programmes de protection en fournissant un système complet de gestion des incidents.

Flux de travail robustes
Gérer les incidents, former les utilisateurs et automatiser les workflows



Synthèse

Protection maximale, effort minimal

La protection des données de Zscaler suit vos utilisateurs et les applications auxquelles ils accèdent pour protéger vos données dans un contexte orienté cloud et mobilité. Zscaler Zero Trust Exchange™ offre la protection et la visibilité dont vous avez besoin pour simplifier la mise en conformité et assurer la protection des données.

La plateforme Zero Trust Exchange multiple les avantages :

- **Un même niveau de protection pour tous** afin que vous puissiez fournir une politique de protection des données cohérente à tous les utilisateurs, quel que soit leur connexion ou leur emplacement.
- **Une inspection de la totalité du trafic TLS/SSL** afin d'éliminer les zones d'ombre, tout en bénéficiant d'accords de niveau de service (SLA) particulièrement performants.
- **Une mise en conformité simplifiée** pour identifier et contrôler les données PCI et personnelles, tout en améliorant la mise en conformité réglementaire.
- **Des opérations simplifiées** grâce à une plate-forme unifiée qui permet de sécuriser tous vos canaux de données dans le cloud : données en transit, au repos, et sur les terminaux et les clouds.

Bénéficiez d'une protection des données dans un contexte de mobilité et cloud

Vos données ne se limitent plus à votre data center. Elles sont disséminées et accessibles aux télétravailleurs. Vos approches traditionnelles de sécurité ne peuvent plus protéger les données dans un monde axé sur la mobilité et le cloud. Grâce aux services de Zscaler Data Protection, vous protégez à l'identique toutes vos données critiques, quel que soit le lieu de connexion des utilisateurs ou la localisation des applications. **Laissez-nous vous montrer comment.**

Consulter les témoignages de clients sur Zscaler Data Protection >

Obtenir l'e-book

En savoir plus sur la plateforme Zscaler Data Protection >

Consulter

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 les pertes des données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Adossée à plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur un 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 Twitter **@zscaler**.

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