3 Exigences essentielles pour une parfaite protection des données

En quête d'un meilleur CASB et d'une DLP plus forte? Vous devez commencer par jeter les bonnes bases.

Ceux qui travaillent dans le domaine de la sécurité informatique ou des réseaux peuvent confirmer — la protection des données était autrefois beaucoup plus facile lorsque toutes vos données se trouvaient dans le data center et que vos employés travaillaient tous au bureau. Mais les temps ont vraiment changé.

À présent, vos données ont quitté le data center et se retrouvent partout, disséminées à travers des centaines d'applications cloud. Et vos employés adoptent le télétravail — hors du réseau d'entreprise et loin de vos contrôles de sécurité. Comme si cela ne suffisait pas, la plupart du trafic Internet est crypté et difficile à inspecter, ce qui explique pourquoi les acteurs malveillants y dissimulent leurs menaces. Qui plus est, vos employés utilisent des réseaux non sécurisés ou des appareils non gérés, ce qui expose vos données à encore plus d'opportunités de fuites.

Dans ce nouveau monde téméraire, les entreprises ont besoin d'une plate-forme de protection des données conçue dès le départ pour le cloud et la mobilité, et celle-ci devrait inclure ces exigences essentielles.

Bon à savoir

La protection de vos données avec un CASB et un DLP n'a de valeur que si l'architecture sur laquelle il repose est bonne. Bien comprendre la recette du succès est primordial.

Première exigence essentielle

Insister sur une architecture SASE dédiée

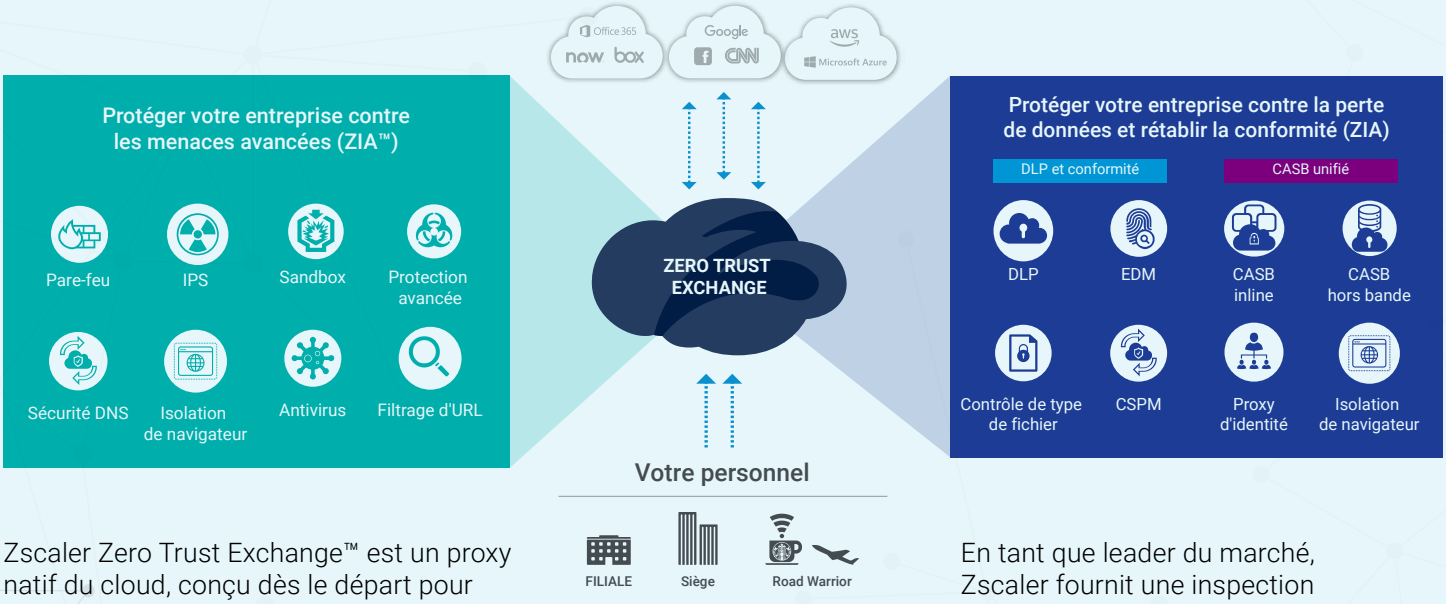
Avec le cloud et la mobilité, les appliances de sécurité ne peuvent pas être partout. Lorsque les utilisateurs quittent le réseau, vous perdez la visibilité, ce qui expose à la fois vos utilisateurs et vos données. De plus, pour offrir d'hermétiques capacités de CASB (Cloud Access Security Broker) et de protection contre les pertes de données (DLP), vous avez besoin d'une inspection SSL complète. Les appliances sont tout simplement incapables d'assumer cette tâche en raison de contraintes matérielles.

Une plate-forme cloud SASE spécialement conçue est la première exigence dont vous avez besoin pour fournir des connexions de haute performance, permanentes et sécurisées, quel que soit l'emplacement de l'utilisateur. SASE unifie tous les services CASB, DLP et de sécurité dans une plate-forme cloud distribuée à l'échelle mondiale de manière à vous faire bénéficier d'une complexité réduite, d'une meilleure protection des données et d'une expérience utilisateur rapide.

Bon à savoir

Il n'est pas facile de construire une architecture de protection des données inline de niveau entreprise qui s'adapte au SSL. Confiez votre trafic qu'à un fournisseur qui a le plus d'expérience, un bilan éprouvé, et qui dispose de SLA de niveau entreprise.

La stratégie de Zscaler™



Zscaler Zero Trust Exchange™ est un proxy natif du cloud, conçu dès le départ pour la protection des données et l'inspection SSL à grande échelle à travers 150 data centers. Chaque utilisateur bénéficie d'une connexion rapide et sécurisée. Et notre capacité SSL illimitée signifie que vous pouvez sécuriser toutes vos données à travers chaque connexion d'utilisateur, sur le réseau ou en dehors.

En tant que leader du marché, Zscaler fournit une inspection inline depuis plus d'une décennie. Mieux encore, comme le DLP, le CASB et tous les autres services de sécurité sont intégrés, vous bénéficiez d'une politique simplifiée et d'une approche unifiée de la protection des données et contre les menaces.

Deuxième exigence essentielle

Une meilleure protection des données nécessite le meilleur contexte

Pour classer correctement les données dont vous disposez, vous avez besoin de contexte, mais c'est la qualité du contexte qui vous aide à prendre les meilleures décisions, des décisions éclairées.

Auparavant, c'était facile — les utilisateurs accédaient aux e-mails à partir d'un serveur Exchange ou alors vous aviez juste quelques serveurs de fichiers. Tout ce dont vous aviez besoin pour prendre des décisions éclairées était entièrement là, à portée de main.

Aujourd'hui, vos données transitent à travers des centaines de canaux — des applications cloud aux cloud publics, aux plateformes de partage de fichiers. Et tout le contexte dont vous avez besoin dans ces canaux est dissimulé dans le chiffrement SSL.

Bon à savoir

Le contexte est l'élément vital de votre CASB et de votre DLP. Recherchez une plate-forme dotée du moteur de classification le plus puissant qui révèle le plus d'attributs dans chaque transaction cloud – sur le réseau ou en dehors, et même à l'intérieur du trafic SSL.

La stratégie de Zscaler

En ce qui concerne le contexte, Zscaler n'a pas d'égal.

Notre plateforme Zero Trust Exchange et notre application Client Connector vous aident à assurer une protection permanente des données pour chaque connexion, soit sur le réseau ou en dehors. Il offre également une visibilité sur TOUT votre trafic SSL, ce qui donne aux entreprises un trésor de contexte.

De plus, en exploitant les dictionnaires industriels et personnalisés de Zscaler et en utilisant des techniques avancées, telles que l'empreinte digitale Exact Data Match (EDM), vous pouvez rapidement classer les données dans les formats industriels courants (PCI, HIPAA) et les définitions personnalisées.

Contexte à partir d'un pare-feu ou d'un proxy	**172.16.1.12** source IP **64.81.2.24** IP de destination **TCP/443** port de destination **Protocole** SSL **Protocole** HTTPS	Les approches traditionnelles inline n'offrent pas assez de visibilité sur le contexte.
Ajout du contexte que vous obtenez avec le décryptage complet SSL	**JohnDoe** utilisateur **groupe** prodmgmt **Emplacement** du siège social **télécharger** fonction d'application **application** jumpshare **type de fichier** PowerPoint **partage de fichiers** Catégorie d'URL **contenu** « Confidentiel »	Lorsque vous êtes capables de tout décrypter du SSL sans limites, alors vous avez le contexte nécessaire pour prendre de meilleures décisions en terme de protection.

Troisième exigence essentielle

Exiger une plate-forme unifiée qui protège tous les canaux

Pour protéger vos données contre les fuites et les exfiltrations, la sécurité doit être présente partout où se trouvent vos données. Si vous n'êtes pas capables de contrôler chaque canal, alors vos données sont vulnérables et exposées à de potentielles menaces.

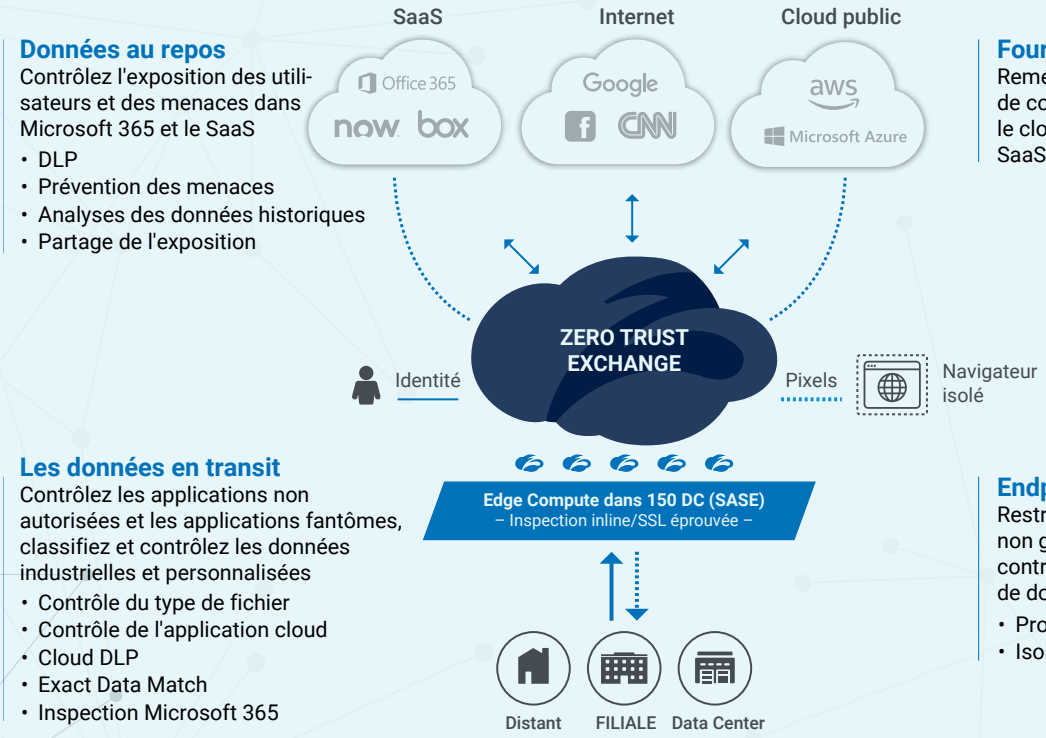
De plus, si vous ne pouvez pas unifier toutes les protections CASB et DLP en une seule plateforme, vous rendez les choses bien trop complexes. Sans une vue panoramique de la plate-forme, vous vous retrouvez avec une politique incohérente, des failles de sécurité et une plus grande propension à faire des erreurs de configuration coûteuses.

Bon à savoir

Pour tous les principaux canaux de données – en transit, au repos, endpoints et fournisseurs de services cloud – une plateforme unifiée améliorera considérablement la force de votre politique et simplifiera vos flux de travail.

La stratégie de Zscaler

Comme tous les services cloud de Zscaler sont intégrés dans une architecture cloud inline spécialement conçue, tous les services travaillent en harmonie pour unifier les politiques et rationaliser la protection de vos canaux de données cloud.



Données au repos
Contrôlez l'exposition des utilisateurs et des menaces dans Microsoft 365 et le SaaS
- DLP
- Prévention des menaces
- Analyses des données historiques
- Partage de l'exposition

Fournisseurs
Remédiez aux erreurs de configuration dans le cloud public et le SaaS (CSPM)

Les données en transit
Contrôlez les applications non autorisées et les applications fantômes, classifiez et contrôlez les données industrielles et personnalisées
- Contrôle du type de fichier
- Contrôle de l'application cloud
- Cloud DLP
- Exact Data Match
- Inspection Microsoft 365

Endpoints
Restreignez l'accès non géré/BYOD et contrôlez toute fuite de données
- Proxy d'identité
- Isolation du navigateur

Voici comment cela fonctionne:

Les données en transit: L'inspection inline de niveau entreprise est essentielle pour assurer une protection des données en temps réel. Grâce au cloud inline spécialement conçu de Zscaler, vous pouvez suivre tous les utilisateurs hors réseau et à l'intérieur du trafic SSL. Classifiez et bloquez rapidement les données essentielles, quelle que soit leur destination, et verrouillez les applications cloud non autorisées.

Données au repos: Lorsque vos utilisateurs adoptent leurs applications cloud, vous devez vérifier qu'ils prennent les bonnes décisions. Avec le CASB hors bande de Zscaler, vous pouvez facilement contrôler le partage inapproprié de fichiers dans les applications Microsoft 365, telles que SharePoint et OneDrive, tout en scannant les dépôts de fichiers pour détecter les problèmes de DLP et de programmes malveillants.

Les Endpoints: Ce canal vise à s'assurer que seules les bonnes personnes accèdent à vos données. Avec le contrôle des accès BYOD, vous pouvez effectuer une recherche rapide SAML/SSO et bloquer l'accès non autorisé aux ressources Microsoft 365. En outre, Zscaler Cloud Browser Isolation vous aide à prévenir les fuites sur les périphériques non gérés (BYOD) car il rend les données uniquement sous forme de pixels au niveau des endpoints. Cela signifie qu'un prestataire peut visualiser les données et interagir avec celles-ci, mais il ne sera pas en mesure de les enregistrer, de les télécharger ou d'en faire un copier-coller. Cela garantit que rien ne s'échappe de l'appareil après la session.

Fournisseurs: La mauvaise configuration accidentelle des applications cloud est l'une des causes les plus courantes de l'exposition des données, ce qui coûte aux entreprises du temps et de l'argent. Zscaler Cloud Security Posture Management (CSPM) identifie et corrige automatiquement les erreurs de configuration des applications SaaS, IaaS et PaaS, de manière à ce que vous réduisiez votre risque de perte de données et mainteniez la conformité.

Résumé

Le cloud et la mobilité ont modifié la façon dont les entreprises font des affaires et celle dont les employés travaillent. Les données sont désormais traitées de manière différente, et doivent par conséquent être protégées. Les appliances de sécurité n'offrent plus à vos données la protection adéquate à l'ère moderne. Vous avez besoin d'une plateforme de sécurité conçue pour le cloud — avec une base SASE — qui protège vos données où qu'elles se trouvent. Vous avez besoin de Zscaler.

Voir notre CASB/DLP inline en action
youtube.com/watch?v=R88TlNEMgGE

Voir notre CASB hors-bande en action
youtube.com/watch?v=1KtoW-IXgMs

Contactez-nous ou réservez une démo personnalisée
zscaler.com/company/contact

À propos de Zscaler
Zscaler accélère la transformation numérique grâce Zero Trust Exchange, une plate-forme basée sur SASE qui fournit des connexions rapides et sécurisées entre les utilisateurs, les appareils et les applications sur n'importe quel réseau.

Zscaler, Inc.
120 Holger Way
San José, Californie
+1 408 533 0288
www.zscaler.com