E-BOOK

Comment garantir une sécurité cohérente des instances dans le multicloud

Sommaire

Introduction

Les entreprises migrent rapidement leurs applications et leurs instances vers le cloud public à un rythme, et elles ont raison de le faire.

La transformation cloud multiplie les avantages, de la réduction des coûts à l'amélioration de la productivité opérationnelle, et davantage. L'adoption du cloud est un élément clé de la transformation numérique des entreprises qui veulent gagner en agilité, répondre aux besoins des clients, partenaires et partenaires tiers, et doper l'expérience du client.

Alors qu'un nombre croissant d'entreprises, tous secteurs confondus, adoptent des stratégies cloud pour renforcer leurs avantages concurrentiels, le cloud public est devenu le nouveau data center d'entreprise. Parallèlement, les environnements hybrides et multicloud sont devenus la norme. IDC Research a récemment prédit que d'icila fin 2025, une majorité d'entreprises feront appel au cloud public pour déployer des plateformes d'IA générative (GenIA), des outils de développement et leur infrastructure : le cloud devrait ainsi supplanter les environnements sur site.[1]

Les trois principaux fournisseurs de cloud détiennent 67 % des parts de marché.

Gartner prédit que 51 % des dépenses informatiques consacrées aux applications logicielles, à l'infrastructure et aux services de processus d'entreprise auront basculé vers le cloud public d'ici 2025, supplantant ainsi les dépenses consacrées à l'informatique traditionnelle.[4]

La migration vers le cloud est dynamique et les revenus cumulés des fournisseurs de cloud public devant dépasser 800 milliards de dollars d'ici la fin 2024[2]. Le marché reste néanmoins dominé par seulement trois acteurs :[3]

- Amazon Web Services (AWS), avec 31 % de parts de marché
- Microsoft Azure, avec 25 % de parts de marché
- Google Cloud, avec 11 % de parts de marché

Ces fournisseurs de cloud public permettent à leurs clients de gagner en rapidité, en agilité et en élasticité dans leur utilisation de ressources informatiques. Leurs offres cloud permettent aux développeurs de créer de nouveaux environnements en quelques secondes seulement. Et ce sont des centaines de services différents qui sont proposés, gérés en self-service ou par le fournisseur cloud.

Néanmoins, ce contexte contribue également à l'émergence de nouveaux risques de sécurité, en particulier pour les entreprises qui continuent de s'adosser à des architectures de sécurité traditionnelles pour sécuriser leurs environnements cloud modernes. L'inadéquation entre la sécurisation traditionnelle des instances sur site et l'approche qui serait nécessaire pour les environnements cloud modernes aboutit souvent à protection des instances cloud coûteuse et complexe.

1. IDC Research, IDC FutureScape: Worldwide Cloud 2024 Predictions, 2023.
2. IDC Research, Worldwide Semiannual Public Cloud Services Tracker.
3. Statista, Cloud Infrastructure Market, 2024.
4. Gartner, Gartner affirme que plus de la moitié des dépenses informatiques des entreprises dans les principaux segments du marché sera affectée au cloud d'ici 2025.

Défis liés à la sécurité des instances cloud

Les entreprises qui migrent leurs instances vers le cloud sans pour autant moderniser leur approche à la sécurité rencontrent de nombreuses problématiques.

L'application aléatoire ou inefficace des politiques expose les instances à des cybermenaces et attaques.

Le choix d'une approche traditionnelle pour sécuriser et interconnecter les instances cloud est inévitablement complexe et coûteux. Les architectures de cybersécurité basées sur des pare-feu et des réseaux privés virtuels (VPN) n'ont tout simplement pas été conçues pour le cloud computing actuel.

Les instances exposées peuvent facilement être compromises. Les cybercriminels peuvent prendre les entreprises en otage via des attaques de ransomware dévastatrices, tandis que la restauration suite à un tel incident peut se révéler coûteuse et chronophage.

Les instances cloud requièrent un réseau étendu de communications avec d'autres instances et Internet. Les approches de sécurité traditionnelles ne sont pas adaptées à cette connectivité permanente.

44 %

des entreprises ont subi un piratage de données dans le cloud en 2024.[5]

49 %

rapportent que la complexité du cloud constitue un défi majeur pour la conformité et la sécurité.[6]

69 %

ont connu des dépassements budgétaires dans leurs dépenses cloud en 2023.[7]

5. Thales Group, 2024 Cloud Security Study.
6. Ibid.
7. Gartner, 2024 Cloud Spending: IT Balances Costs with GenAI Innovation.

Avec l'évolution constante des applications modernes, la stratégie Zero Trust devrait suivre

Avec la généralisation du télétravail et du travail hybride, les entreprises, tous secteurs d'activité confondus, adoptent le Zero Trust pour sécuriser leurs utilisateurs. Dans le cadre d'une approche Zero Trust, la confiance n'est jamais implicite. Au contraire, chaque demande d'accès est supposée potentiellement malveillante, si bien que l'accès à une application n'est accordé que si les conditions suivantes sont réunies :

- L'identité du requérant et le contexte de sa demande (qui veut accéder à quoi et où) peuvent être vérifiés.
- Les risques associés à cette demande peuvent être évalués en profondeur.
- Les politiques peuvent être appliquées pour chaque session.

Face à des applications et instances toujours plus nombreuses à migrer vers le cloud, il est essentiel que les entreprises appliquent, à l'ensemble de leurs ressources et services cloud, le même degré de protection dont bénéficient les accès aux applications sur site. Ceci impose d'étendre la sécurité du Zero Trust à chacune de vos instances dans le cloud.

Lorsque les entreprises migrent leurs applications monolithiques traditionnelles vers le cloud, elles choisissent souvent de les restructurer en utilisant les microservices. L'objectif est de tirer parti de fonctionnalités propres au cloud, qu'il s'agisse de bases de données cloud spécialisées, de fonctionnalités serverless ou d'une architecture orientée évènements. Cette approche renforce la productivité, permet de réduire les coûts et instaure un environnement dynamique et automatisé. Au sein de cet environnement, les instances communiquent constamment entre elles.

Les instances cloud doivent fréquemment :

- Se connecter à Internet
- Communiquer avec d'autres instances

Le volume de communications entre les instances est bien plus élevé dans le cloud que dans un data center traditionnel.

Qu'est-ce qu'une instance ?

Une instance (ou workload) est un élément constitutif d'une application cloud moderne. Dans les environnements sur site traditionnels, la plupart des instances étaient des composants d'applications monolithiques. Ceci n'est pas le cas dans les environnements cloud natifs modernes, où les applications sont généralement constituées de nombreux composants modulaires ou de microservices. Chaque service exécute une tâche spécifique et communique avec d'autres services pour exécuter une tâche logique.

Voici quelques exemples d'instances :

- Conteneurs
- Machines virtuelles (VM)
- Postes de travail virtuels (VDI)
- Fonctionnalités serverless

La sécurité réseau traditionnelle peine à protéger l'entreprise cloud native

Beaucoup d'entreprises ont entrepris leur transformation cloud sans repenser leur stratégie de sécurité. Or, les architectures de sécurité réseau traditionnelles ont été conçues pour le data center sur site, et non pour le cloud. Lorsque ces entreprises tentent de les migrer vers le cloud, l'architecture qui en résulte se révèle complexe et inefficace.

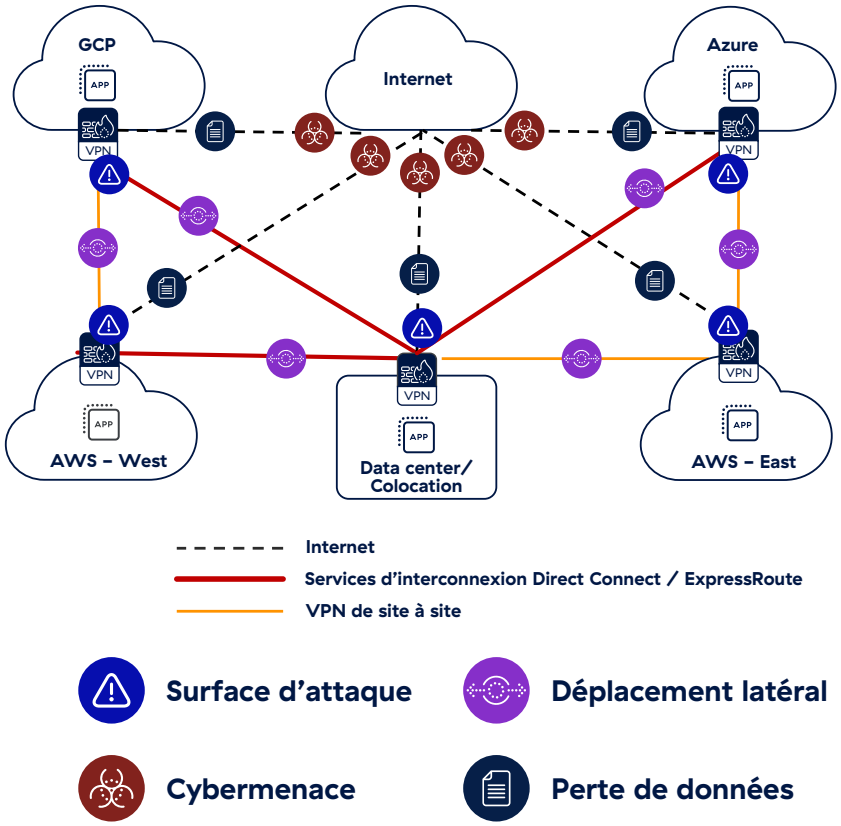
Les instances cloud doivent communiquer en toute sécurité entre elles et avec Internet. Pour ce faire, l'approche traditionnelle consiste à bâtir des réseaux routés entre les infrastructures cloud au moyen de pare-feu et de VPN, ce qui revient à étendre le WAN de l'entreprise vers le cloud.

Dans ce modèle, les entreprises doivent déployer des pare-feu virtuels de nouvelle génération (vNGFW) pour tous les environnements hébergeant leurs instances. Dans un monde où les environnements hybrides et multicloud sont omniprésents, cette approche donne lieu à des réseaux mesh, au sein desquels chaque nœud se connecte directement à tous les autres. Cette architecture est extrêmement complexe à gérer.

Si les entreprises souhaitent déployer des fonctionnalités de sécurité supplémentaires, à l'image d'une protection contre les pertes de données (DLP) ou une inspection TLS/SSL, elles devront ajouter des appliances de sécurité virtuelles supplémentaires, accentuant ainsi la complexité.

Même au sein d'un environnement proposé par un seul fournisseur de services, les entreprises devront configurer et gérer plusieurs vNGFW supplémentaires pour sécuriser le trafic externe et interne des instances cloud.

Les communications des instances multiplient les défis de complexité et de sécurité.



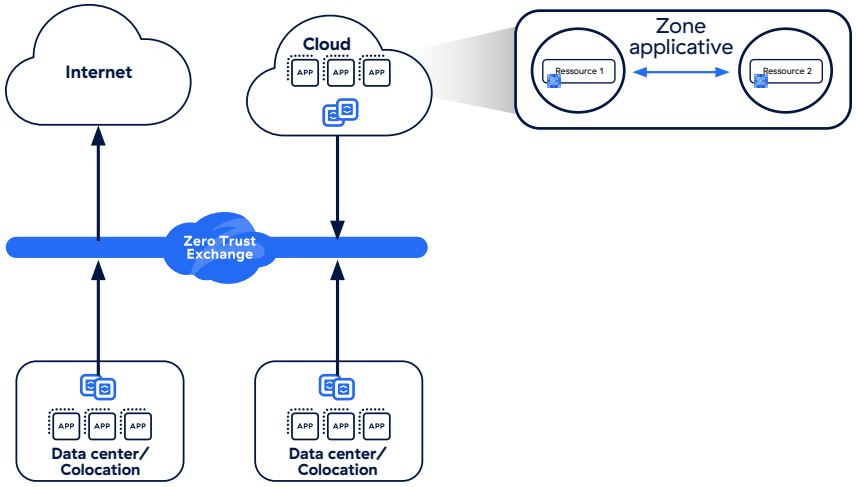
Une cyber-défense peu adaptée aux écosystèmes informatiques actuels

Faire appel aux approches traditionnelles pour sécuriser et connecter les instances cloud génère des risques :

- **Expansion de la surface d'attaque.** Chaque vNGFW possède un emplacement réseau visible que les hackers peuvent identifier. Plus le nombre de pare-feu déployés est important, plus la surface d'attaque est vaste.
- **Compromission des instances.** Tout assaillant qui s'introduit dans l'environnement via une passerelle d'entrée est susceptible de compromettre les instances.
- **Déplacement latéral des menaces.** Toutes les instances sont connectées via un réseau mesh : une seule instance compromise permet aux assaillants de se déplacer latéralement sur le réseau pour en cibler d'autres.
- **Aucune protection des données sensibles.** Au fil de leur déplacement sur le réseau, les hackers peuvent identifier et exfiltrer des données sensibles telles que des informations financières et stratégiques de clients.

Une nouvelle approche s'impose pour sécuriser les instances cloud

Les écosystèmes informatiques actuels sont dépendants de leurs environnements infrastructure as a service (IaaS), platform as a service (PaaS) et software as a service (SaaS) fournis par différents fournisseurs de services cloud. Leur sécurité exige une approche différente qui fait des politiques de sécurité d'entreprise la clé de voûte de la conception des réseaux. Il s'agit de permettre un accès sécurisé sur la base du moindre privilège à la connectivité directe entre les instances, et entre les instances et Internet. Une telle approche simplifie la création et l'activation d'une architecture Zero Trust qui s'applique à toutes vos instances cloud.



Avec cette nouvelle approche :

- **La surface d'attaque est éliminée.** Contrairement aux solutions traditionnelles, les instances sont invisibles aux yeux des acteurs malveillants, ce qui élimine pratiquement toute la surface d'attaque.
- **Les instances sont sécurisées.** L'inspection complète du contenu, ainsi que les fonctionnalités DLP, offrent une sécurité robuste des données et des instances.
- **Le déplacement latéral des menaces est impossible.** Une connexion directe, sans passer par un réseau, empêche ce déplacement latéral.
- **Les données sont protégées.** Une inspection TLS/SSL à grande échelle et la DLP assurent une protection complète et évolutive des données.
- **La complexité et les coûts sont maîtrisés.** La gestion centralisée de la configuration et de la sécurité des environnements cloud, et la mis en place d'une connectivité directe, favorisent la simplicité et la maîtrise des coûts.

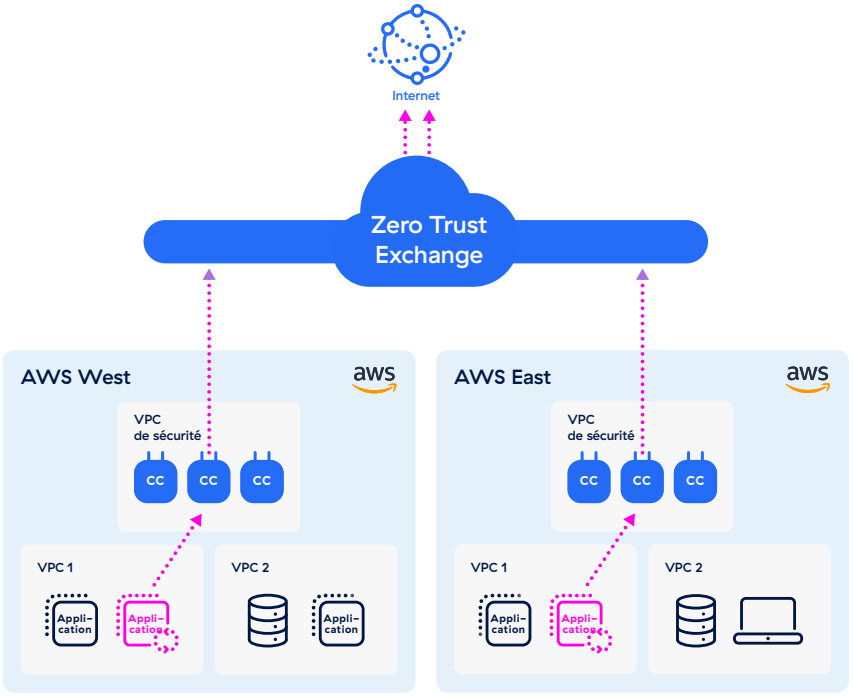
Simplifiez et sécurisez les communications entre les instances et Internet

Étant donné que chaque instance cloud s'adosse à une communication quasi constante vers l'Internet public, une solution Zero Trust pour les instances cloud doit être en mesure de sécuriser toutes les connexions sortantes. Dans le cadre d'une architecture directe vers le cloud, la solution doit fournir un accès Internet sécurisé à tous les instances, que celles-ci soient hébergées dans un cloud public ou dans le data center d'entreprise.

Voici les principales fonctionnalités nécessaires pour sécuriser les communications des instances vers Internet :

- Inspection TLS/SSL complète basée sur un proxy
- Élimination de la surface d'attaque
- Accès autorisé uniquement aux sites approuvés
- Protection contre les malwares avancés pour déjouer les menaces « zero day »

Imaginons par exemple que votre entreprise dispose d'applications dans AWS West et AWS East qui doivent être mises à jour. La demande devra être transmise à une plateforme centrale où les politiques sont appliquées et gérées. Une solution idéale sera en mesure d'appliquer des politiques Zero Trust et de connecter en toute sécurité les sources et les destinations.



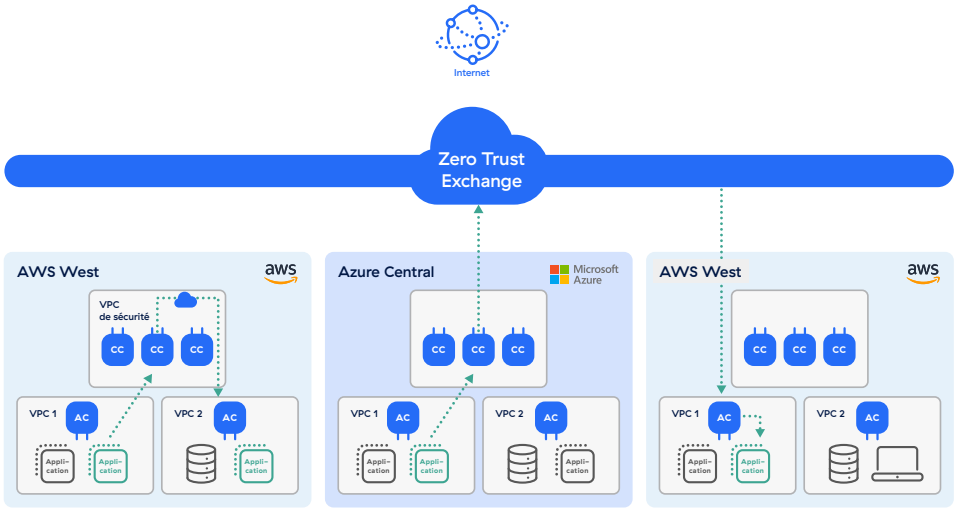
Simplifiez et sécurisez les communications entre les instances

L'application du principe Zero Trust aux instances cloud requiert également une connectivité sécurisée entre les instances. Il est essentiel que les instances puissent communiquer, à la fois sur plusieurs clouds et au sein d'un seul cloud privé virtuel (VPC – virtual private cloud). Ces communications doivent passer par la plateforme centrale Zero Trust, où sont appliquées les politiques de sécurité, et où l'identité et le contexte sont utilisés pour vérifier la fiabilité avant d'autoriser la connexion.

Il faudrait notamment disposer d'un mécanisme qui facilite les communications au sein des instances. Pour la connectivité de VPC à VPC, le trafic peut être acheminé d'un VPC vers un Service Edge privé, à partir duquel une connexion est ensuite négociée vers l'application de destination, située dans un autre VPC. Pour la connectivité de cloud à cloud, le trafic est acheminé vers une plateforme centrale Zero Trust, où une connexion est négociée vers une application de destination située dans un autre cloud.

Voici les principales fonctionnalités nécessaires pour sécuriser les communications des instances :

- Sécuriser la connectivité multi-cloud et multi-régions
- Sécuriser la connectivité inter-VPC/inter-VNET
- Éliminer la surface d'attaque du réseau grâce à un accès réseau Zero Trust (ZTNA)
- Prévenir le déplacement latéral des menaces



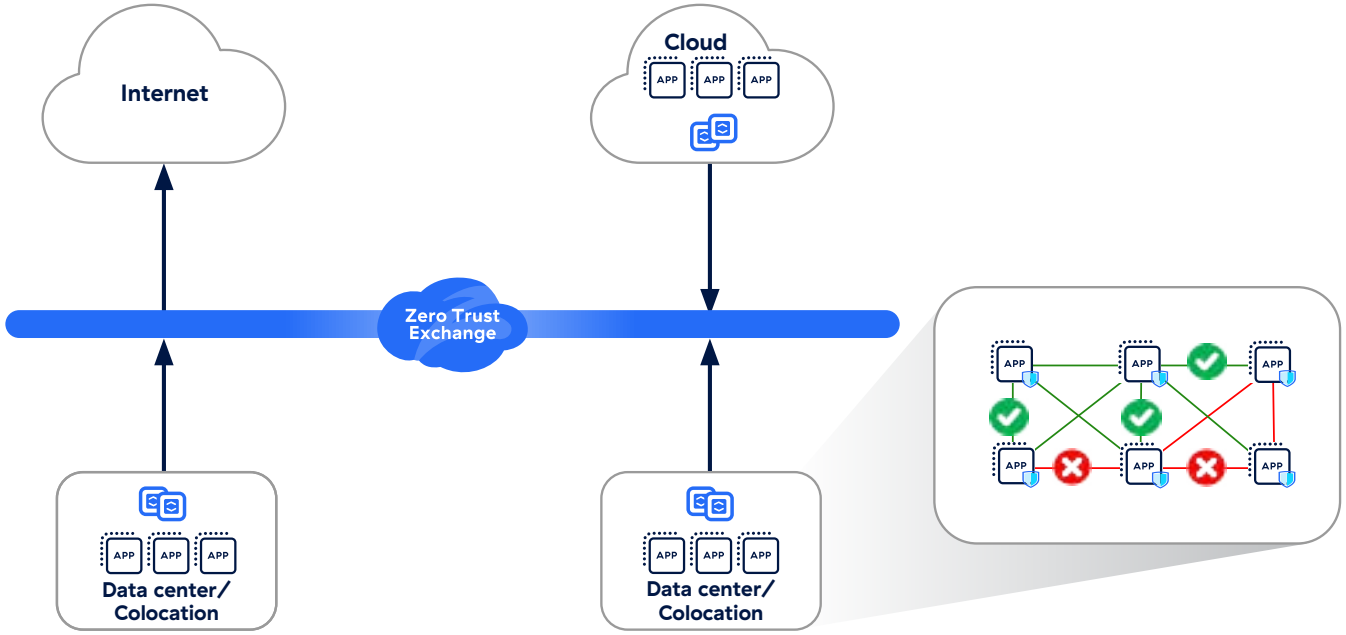
Mettre en œuvre une microsegmentation granulaire de manière simple

Composante essentielle de la sécurité Zero Trust, la microsegmentation prévient le déplacement latéral des menaces en dissociant des groupes d'applications ou d'instances en petits segments, en fonction des exigences de communication de chaque application. Les instances sont autorisées à communiquer sur le périmètre de leurs propres segments, mais ne sont pas autorisées à communiquer avec des instances externes.

La microsegmentation permet d'appliquer des politiques Zero Trust à un niveau granulaire sur l'ensemble du réseau interne de l'entreprise, et pas uniquement en périphérie, en étendant de manière cohérente les fonctionnalités de protection aux instances sur site et dans le cloud.

Voici les principales fonctionnalités nécessaires à la microsegmentation des instances :

- Identification en temps réel des ressources, optimisée par IA
- Segmentation basée ou non sur l'hôte
- Capacité à segmenter les instances au sein des VPC/VNET



Fonctionnalités clés qu'une solution Zero Trust pour les instances cloud doit proposer :

1. Capacité à inspecter le flux TLS/SSL à grande échelle

La plupart des menaces actuelles les plus dangereuses se dissimulent dans le trafic chiffré. Pour les détecter, vous devez disposer d'une plateforme capable d'effectuer une inspection TLS/SSL complète et à grande échelle, sans les contraintes de performances imposées par les applications traditionnelles.

Privilégiez une solution avec les caractéristiques suivantes :

- **Capacité illimitée** pour inspecter l'ensemble du trafic TLS/SSL de vos utilisateurs, avec le niveau de performances requis
- **Évolutivité** en fonction des demandes de trafic
- **Gestion simplifiée des certificats**
- **Contrôle granulaire des politiques** pour simplifier la mise en conformité, en excluant le trafic utilisateur chiffré pour certaines catégories de sites Web (soins de santé ou services bancaires par exemple)

2. Capacités robustes de protection des données

Une protection en profondeur des données impose d'appliquer à grande échelle des politiques de protection contre la perte de données (DLP), sans impact sur les performances, pour ainsi bénéficier d'une couche de protection supplémentaire. Si une instance cloud est compromise, un mécanisme en place applique les politiques et d'empêcher l'exfiltration des données.

Privilégiez une solution avec les caractéristiques suivantes :

- **Tableau de bord simplifié** pour configurer et gérer les politiques DLP
- **Techniques avancées de gestion des données** telles que la correspondance exacte de données (EDM – Exact Data Match) et la reconnaissance optique de caractères (OCR)
- **Inspection inline fiable du contenu à grande échelle**

3. Capacités de protection contre les menaces avancées

Pour bloquer les menaces actuelles les plus dangereuses et sophistiquées, une plateforme de sécurité des instances cloud Zero Trust doit pouvoir garantir que chaque paquet provenant de chaque instance peut être intégralement inspecté. Ceci fait appel à des capacités d'inspection TLS/SSL intégrées et permanentes, ainsi qu'à l'application de politiques précises pour l'ensemble du trafic.

Les principales capacités à privilégier sont les suivantes :

- **Technologies de leurre intégrées** utilisant des appâts et des honeypots pour protéger vos ressources de valeur, de manière fiable et avec un faible taux de faux positifs
- **Sandboxing cloud** pour mettre en quarantaine et inspecter les menaces potentielles plutôt que de les laisser entrer sur le réseau
- **Protection contre les malwares** qui peut bloquer les ransomwares, les spywares et les malwares connus, ainsi que les nouvelles menaces

4. Segmentation complète basée sur l'hôte

La microsegmentation prévient le déplacement latéral des menaces afin de minimiser le rayon d'action et les dommages d'un cyber-incident. La microsegmentation basée sur l'hôte s'appuie sur des agents installés sur les terminaux pour fournir un contrôle et une visibilité beaucoup plus granulaires, ce qui simplifie la gestion de la segmentation basée sur l'identité. L'utilisation d'un agent permet une segmentation basée sur des politiques dynamiques et compréhensibles par l'humain plutôt que des règles statiques au niveau du réseau.

Privilégiez notamment une solution qui vous apporte les fonctionnalités suivantes :

- **Identification de ressources en temps réel** en tirant parti de l'IA pour permettre une visibilité granulaire sur tous les dispositifs, services et ressources au sein de l'écosystème de votre entreprise
- **Recommandations de politique Zero Trust** sur la base d'une analyse du trafic
- **Intégration avec une plateforme Zero Trust** pour centraliser la protection et la segmentation de votre environnement, sans avoir à déployer plusieurs produits autonomes

Principaux cas d'utilisation pour sécuriser la connectivité des instances

Une solution Zero Trust pour la connectivité des instances aide les entreprises à résoudre plusieurs défis clés. En voici quatre parmi les plus courants :

Sécurisation du trafic vers Internet

Lorsque les applications communiquent avec Internet ou des applications SaaS, le trafic sortant doit être inspecté pour détecter d'éventuelles cyberattaques et fuites de données. Zscaler exploite la plus grande plateforme intégrée de sécurité cloud au monde, qui offre une protection contre les menaces avancées, sans impact sur les performances ni dégradation de service.

Segmentation des instances

Avec une solution pertinente pour gérer les communications des instances, il est possible d'adopter une approche granulaire et méthodique à la segmentation des instances. Il devient plus simple de contrôler la connectivité des instances sur les VPC, les régions et les clouds publics et privés.

Migration vers le cloud

Ce processus est souvent long et ardu pour les entreprises qui doivent prendre en compte de nombreux facteurs, notamment la stratégie de migration à suivre. Est-il judicieux de procéder à une simple migration, ou faut-il restructurer ou reconstruire les applications ? Une solution pertinente de communication des instances peut simplifier l'interconnexion des applications cloud nouvellement migrées.

Fusions et acquisitions

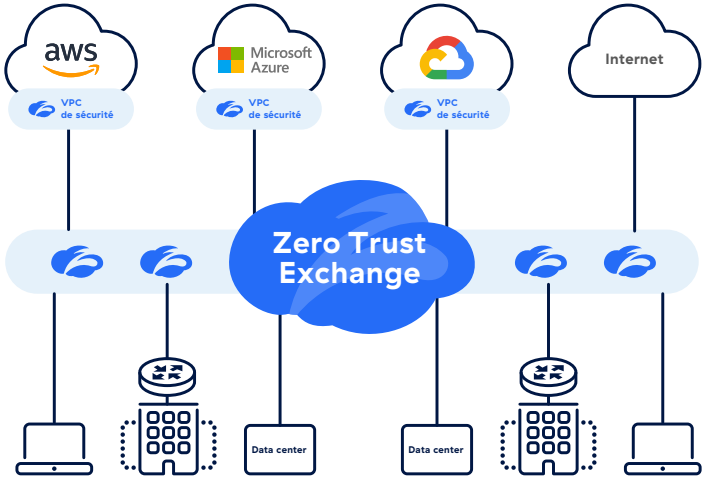
Une solution de communication des instances cloud native, moderne et basée sur le Zero Trust fournit un accès sécurisé aux applications présentes sur différents réseaux, sans qu'il soit nécessaire de repenser les réseaux pour les interconnecter.

Zscaler Workload Communications : un choix pertinent

Vous recherchez une solution qui vous apporte l'ensemble de ces avantages et bien plus ? Zscaler Zero Trust Exchange™ a permis de repenser complètement les communications des instances au sein d'une architecture direct-to-cloud simple et éprouvée.

Associant Zscaler Internet Access™ (ZIA) pour les communications des instances vers Internet, Zscaler Private Access™ (ZPA) pour les communications d'instances à instances et la microsegmentation Zero Trust, Zscaler Workload Communications propose une approche complète pour sécuriser la connectivité des instances dans le cloud et sur site. Par ailleurs, la solution est capable de proposer des performances pérennes qui garantissent à vos utilisateurs des expériences optimales. Elle se dimensionne au rythme de l'expansion de votre empreinte cloud et de vos opérations.

Zscaler Workload Communications fournit une sécurité cloud performante basée sur le Zero Trust qui évolue en fonction de vos besoins. L'auto-scaling de la solution assure une parfaite prise en charge des pics de trafic. En s'adossant à plus de 150 data centers disséminés dans le monde, Zero Trust Exchange opère à très grande échelle. Zscaler gère automatiquement toutes les mises à jour en votre nom. L'infrastructure est intégrée en natif avec les services de sécurité des fournisseurs de cloud public et tire pleinement parti de fonctionnalités comme les passerelles de transit et les équilibreurs de charge.



Qui plus est, Zscaler Workload Communications simplifie et centralise la gestion des politiques. Toutes les politiques peuvent être créées et mises à jour à partir une console unique, centralisée et conviviale. Elles sont appliquées au sein de Zero Trust Exchange, où les politiques ZIA ou ZPA peuvent être utilisées pour une inspection complète des contenus ainsi qu'un contrôle des communications des instances basé sur l'identité. Les communications peuvent ensuite être acheminées vers n'importe quelle destination, qu'il s'agisse d'Internet ou d'autres applications privées au sein d'environnements cloud. Les politiques peuvent facilement être appliquées à toute nouvelle instance déployée dans le cloud.

Si vous souhaitez en savoir plus sur les avantages de Zscaler Workload Communications, contactez-nous dès aujourd'hui. Plus d'informations également sur la page Web de Zscaler Zero Trust Cloud Connectivity.

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. Distribué dans plus de data centers dans le monde, Zero Trust Exchange, basé sur le SASE, constitue la plus grande 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