Zscaler et AWS

Déployer une sécurité Zero Trust pour les utilisateurs, les données et les instances

Available in AWS Marketplace

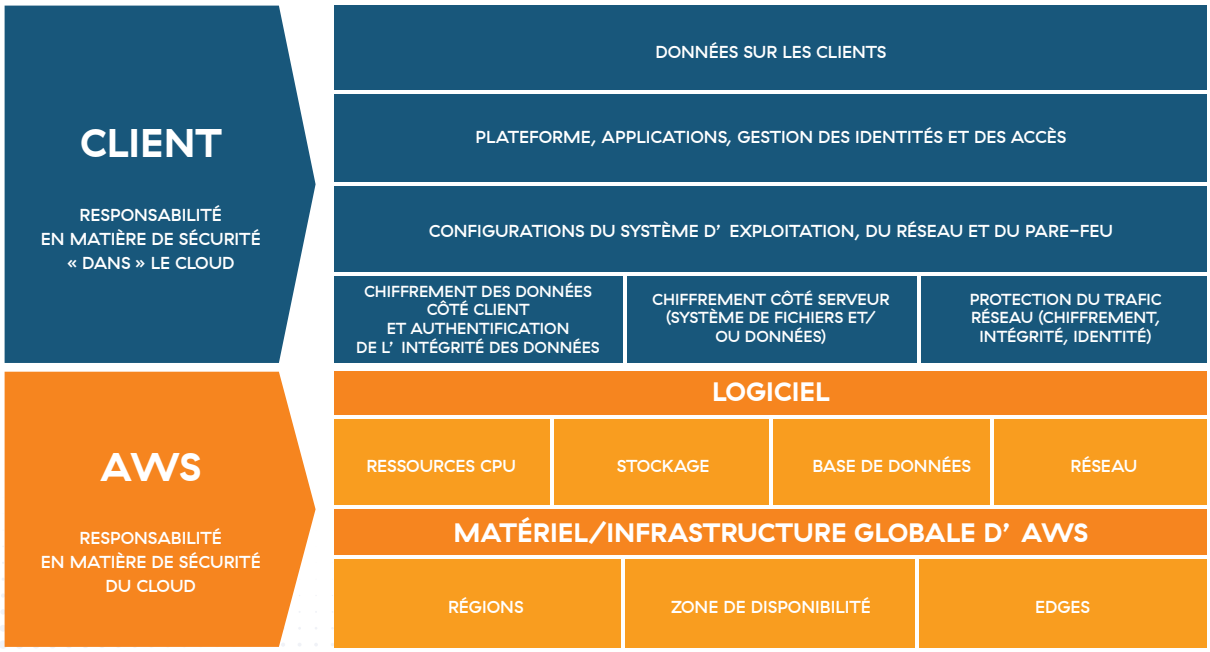
Introduction

La migration des instances vers Amazon Web Services (AWS) est désormais une réalité pour de nombreuses entreprises et administrations. La récente pandémie mondiale a incité les organisations à accélérer leur transformation digitale et à identifier des stratégies de migration des applications critiques vers AWS, pour assurer la continuité et la résilience des activités, réduire les dépenses et gagner en efficacité. Les environnements informatiques modernes ont évolué, passant de serveurs physiques sur site à une infrastructure virtualisée qui prend en charge les applications et les instances sur plusieurs régions AWS : les utilisateurs accèdent à ces applications et instances, d'où ils le souhaitent, quand ils le souhaitent.

Le modèle de sécurité périmétrique ne répond pas aux besoins des entreprises modernes

Le modèle de sécurité qui prévaut dans le cloud est fondé sur le partage des responsabilités, AWS étant responsable de la sécurité de l'infrastructure cloud, tandis que les entreprises clientes assument la responsabilité de sécuriser leurs instances et applications dans le cloud.

Modèle de responsabilité partagée d'AWS



Source : https://aws.amazon.com/compliance/shared-responsibility-model/

Au cours des 30 dernières années, les entreprises ont créé et optimisé des réseaux complexes, étendus et en étoile, connectant les utilisateurs et les sites distants au data center via un réseau privé. Ces réseaux en étoile étaient sécurisés par un panel d'appliances de sécurité, pour le VPN et le pare-feu notamment, pour définir un modèle de sécurité réseau cloisonnée (castle-and-moat security). Cette approche était efficace lorsque la majorité des collaborateurs travaillait dans les bureaux de leur entreprise et que leurs données et applications étaient hébergées dans le data center.

Aujourd'hui, les utilisateurs travaillent d'où ils le souhaitent et accèdent fréquemment à des applications et à des données hébergées dans le cloud. Pour une collaboration rapide et productive, les utilisateurs ont besoin d'un accès direct aux applications, d'où qu'ils se trouvent et à tout moment. Il n'est plus judicieux d'acheminer le trafic des utilisateurs vers le data center pour assurer l'accès aux applications hébergées sur AWS et en garantir la sécurité.

À mesure que les cyberattaques gagnent en sophistication et que les utilisateurs sont disséminés, la sécurité périmétrique qui mise sur un VPN et un pare-feu se révèle incomplète et incohérente. L'expérience utilisateur qui en résulte est médiocre pour les raisons suivantes :

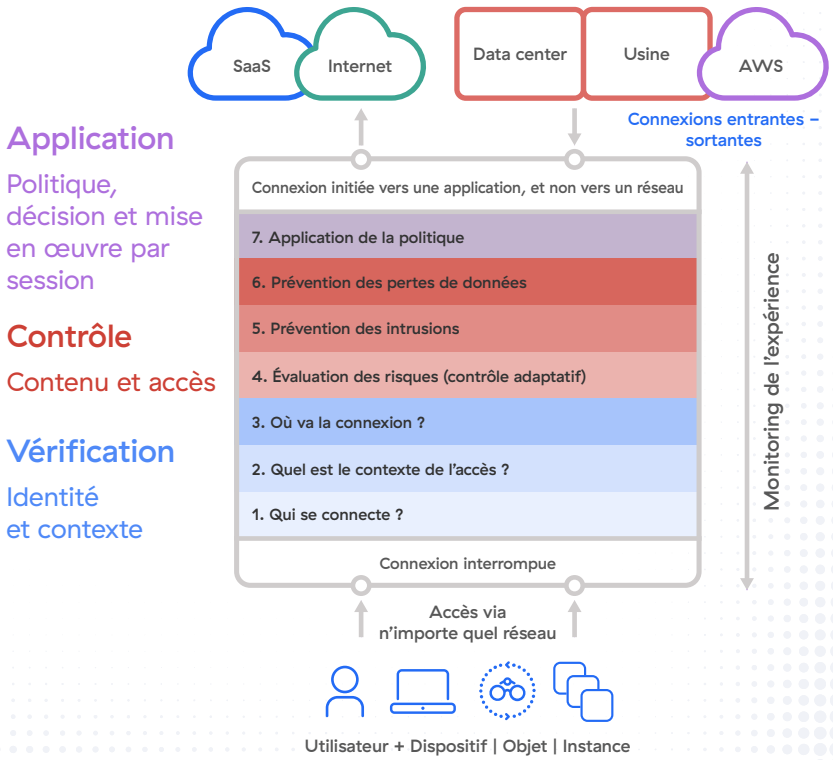
- Les VPN et les pare-feux étendent le réseau de l'entreprise, élargissant la surface d'attaque et permettant aux menaces de se déplacer en interne de manière rapide, ce qui entraîne des failles de sécurité.
- Un mix de produits de sécurité autonomes et cloisonnés renchérit les coûts et la complexité, si bien que certaines attaques peuvent ne pas être détectées.
- Le backhauling du trafic des utilisateurs distants vers le data center à des fins de gestion des accès et de sécurité (trafic de type « hairpinning ») génère de la latence, freine les performances et pèse lourdement sur l'expérience utilisateur.
- Les produits issus de plusieurs fournisseurs technologiques procurent une sécurité incohérente entre les utilisateurs, les appareils et les sites. Cette hétérogénéité ne facilite en rien la hiérarchisation des menaces (plusieurs tableaux de bord).
- Les assaillants contournent les défenses traditionnelles et diffusent des menaces de plus en plus sophistiquées et à grande échelle.
- Alors que les entreprises procèdent à la transformation de leurs applications (migration des applications vers AWS ou adoption d'applications SaaS), elles doivent abandonner la sécurité cloisonnée basée sur des pare-feux et des VPN au profit d'une architecture moderne qui permet un accès rapide, direct et sécurisé aux applications, de n'importe où et à n'importe quel moment.

Elles ont ainsi tout intérêt à adopter une architecture Zero Trust.

Zscaler Zero Trust Exchange

Partenaire Advanced Tier Software d'AWS, Zscaler est un leader de la sécurité Zero Trust depuis une décennie et a aidé des milliers d'entreprises à sécuriser leur transformation digitale avec Zscaler Zero Trust Exchange.

L'architecture Zero Trust de Zscaler définit une plateforme intégrée qui agit comme un commutateur intelligent pour négocier dans AWS les connexions entre les utilisateurs, les appareils et les applications. Chaque requête est vérifiée à l'aide d'éléments d'identité et de contexte : appareil, site, application et contenu. Une fois l'identité et le contexte vérifiés, l'architecture Zero Trust évalue le risque associé à la demande de connexion, et inspecte le trafic à la recherche de cybermenaces et de données sensibles. Enfin, les politiques sont appliquées avant



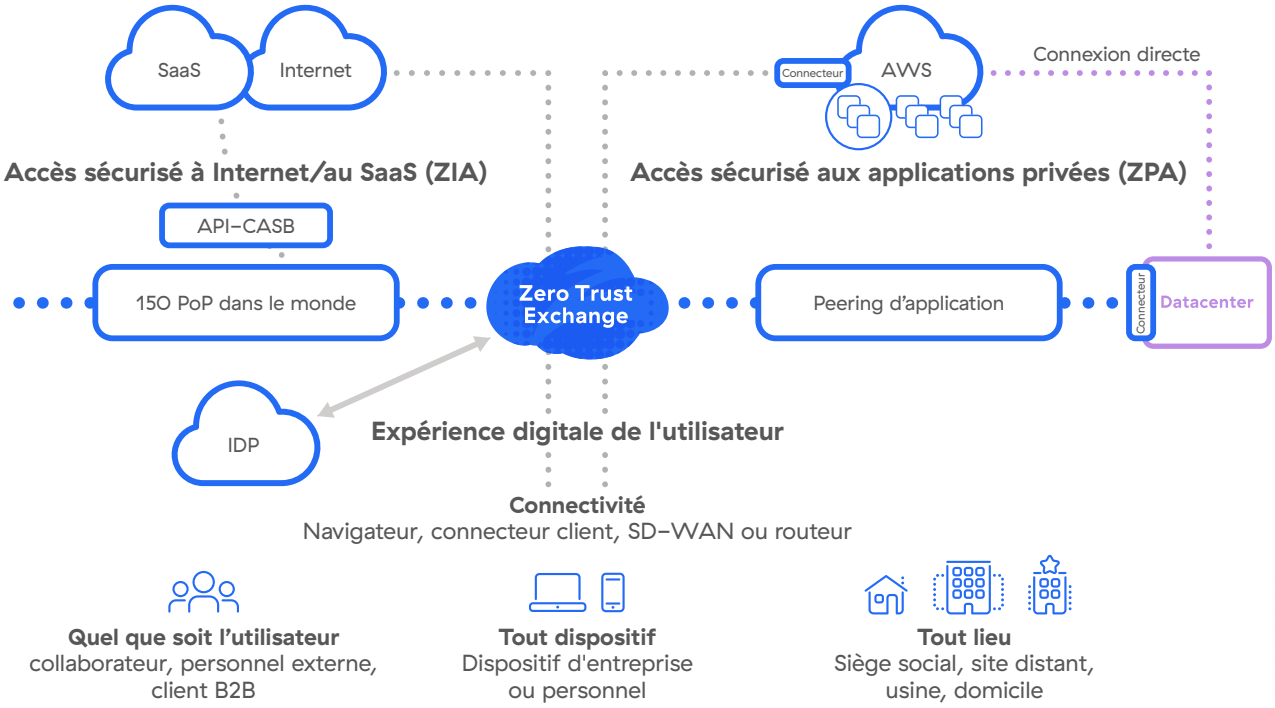
d'établir une connexion aux applications AWS. Cette approche moderne élimine les difficultés liées à la sécurité, au réseau et au/aux backhauling/performances : les entreprises accélèrent ainsi la migration de leurs applications et de leurs instances vers AWS, tout en offrant une sécurité supérieure et une expérience utilisateur satisfaisante.

Zero Trust Exchange constitue le plus grand cloud de sécurité au monde avec plus de 150 points de présence (PoP) dans le monde, présents dans la plupart des régions AWS. L'architecture multisite avec des hubs de performance garantit l'envoi direct et sécurisé de toute communication à AWS.

Comment Zscaler et AWS contribuent à une transformation digitale sécurisée

1. Protéger les utilisateurs

La gestion sécurisée de collaborateurs hybrides, axée sur l'utilisateur, exige une flexibilité à même d'accompagner les collaborateurs et les tiers dans n'importe quel lieu et sur n'importe quel dispositif. Elle implique une expérience utilisateur basée sur un accès rapide, sécurisé et fiable aux données, aux applications et aux instances au sein d'AWS. Elle exige une solution capable d'évoluer avec l'entreprise et qui la protège contre les menaces connues et inconnues.



Zscaler protège les utilisateurs d'AWS :

- En connectant les utilisateurs directement à des instances AWS spécifiques et jamais au réseau. Les menaces ne peuvent ainsi pas se propager en interne pour infecter d'autres utilisateurs, dispositifs et applications.
- En plaçant les utilisateurs et les applications en aval de Zero Trust Exchange afin de les rendre invisibles depuis Internet.
  Les acteurs malveillants ne peuvent pas s'en prendre ce qu'ils ne peuvent pas voir. Par conséquent, les utilisateurs ne sont pas affectés par les malwares ou autres cybermenaces tels que le ransomware et le phishing.

Les entreprises peuvent ainsi réduire considérablement leurs risques, améliorer leur productivité et garantir une expérience utilisateur optimale.

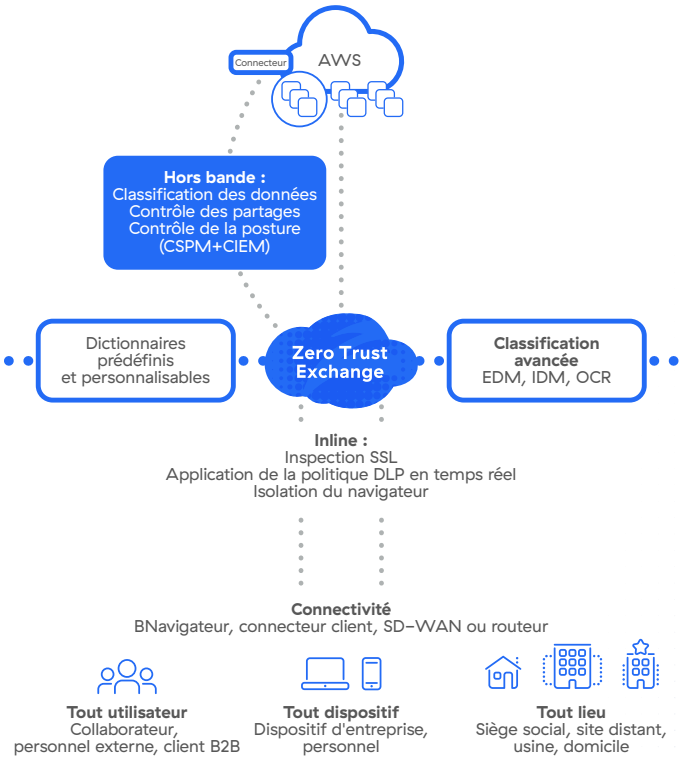
Zscaler est une solution cloud, multifonctions et intégrée. Elle se substitue aux produits autonomes et ponctuels et permet de concrétiser un Security Service Edge (SSE). Pour cela, elle fédère plusieurs technologies de base pour prendre en charge les instances AWS. Ces technologies sont les suivantes :

- Zscaler Internet Access (ZIA) qui offre une passerelle de sécurité web, un CASB (Cloud Access Security Broker), une fonction de prévention des pertes de données (DLP) dans le cloud, et davantage
- Zscaler Private Access (ZPA) pour un accès réseau Zero Trust (ZTNA) de nouvelle génération
- Zscaler Digital Experience (ZDX) pour surveiller l'expérience digitale (DEM)

2. Protéger les données

Les utilisateurs travaillent à distance à l'aide de différents dispositifs. Ils chargent des données dans des environnements AWS de type S3 et y accèdent. Par conséquent, les appliances de sécurité périmétrique ne peuvent pas protéger ces données, et le recours à un produit spécifique pour chaque nouveau cas d'utilisation génère des coûts et accentue la complexité.

Zscaler Data Protection applique les principes du Zero Trust à toutes les données, où qu'elles se trouvent. Les données sont analysées en mode inline pour garantir leur classification et une application des politiques en temps réel. La fonction d'isolation du navigateur restitue les données sous forme de pixels sur les appareils non gérés pour empêcher leur exfiltration. Les données au repos dans AWS sont analysées pour déceler les informations sensibles et prévenir automatiquement tout partage à risque de ces données. Posture Control restaure les erreurs de configuration et de permissions, susceptibles d'exposer les données sensibles via, par exemple, des compartiments S3 rendus publics de manière fortuite.



Zscaler Data Protection se distingue par les caractéristiques suivantes :

- Fait partie de la plateforme de sécurité la plus unifiée qui répond aux besoins du SSE et au-delà.
- Utilise un moteur unifié de politiques qui protège les données de manière cohérente, quelle que soit leur destination.
- Effectue une inspection SSL complète à partir du cloud de sécurité le plus vaste et le plus performant au monde.
- S'intègre à une plateforme éprouvée et déployée à grande échelle, par les plus grandes entreprises du monde.

3. Protection des instances

À mesure que les instances migrent vers le cloud, les entreprises éprouvent un besoin urgent et impérieux de moderniser leurs réseaux et leur sécurité pour gagner en compétitivité. Les réseaux basés sur un périmètre, qui ont été conçus pour des environnements statiques, ne peuvent tout simplement pas répondre aux besoins de connectivité du cloud. Ils engendrent des problèmes de taille pour les entreprises, tels qu'une plus grande surface d'attaque, un risque de propagation des menaces en interne, une dégradation de la productivité et de la collaboration, ainsi que des coûts plus élevés et une gestion complexe des architectures de sécurité réseau pour sécuriser un personnel hybride et des applications basées sur le cloud.

Zscaler relève ces défis pour les entreprises qui utilisent AWS avec la solution complète Zscaler for Workloads qui sécurise les applications de leur conception à leur mise en production. Conçue sur une architecture Zero Trust innovante, Zscaler for Workloads associe les modules Posture Control (CNAPP) et Workload Communications. Elle unifie la sécurité des applications cloud natives et celle des applications hébergées sur des VM d'AWS, en remplaçant les produits de sécurité autonomes traditionnels par une solution complète conçue pour le Zero Trust. Cette approche consolidée élimine non seulement la nécessité d'acquérir et de gérer des outils distincts (ce qui creuse les coûts et les charges d'exploitation), mais elle renforce également la collaboration pluridisciplinaire entre les équipes et accélère la transformation digitale.

Solution de sécurité cloud pour AWS

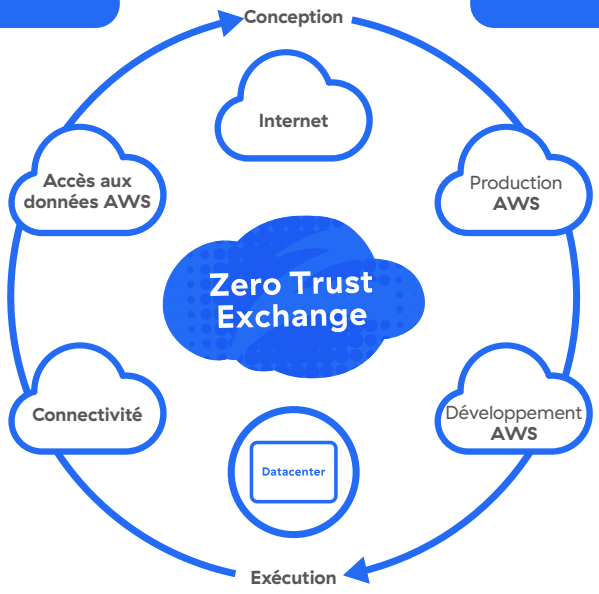
Posture Control (CNAPP)

Analyse de l'exposition aux risques (sans agent)

- Identification des ressources à risque et les vulnérabilités (surface d'attaque)
- Identification des données sensibles

Analyse de la configuration

- Identifier et hiérarchiser les erreurs de configuration
- Identifier les autorisations excessives pour les utilisateurs et les instances



Workload Communications

Instance vers Internet

- Réduction de la surface d'attaque
- Prévention des compromissions et des pertes de données sans pare-feu/proxy virtuels

Instance à Instance

- Comptes AWS
- AWS vers le data center

Segmentation

- Segmentation utilisateur à application, application à application sans segmentation du réseau
- Micro-segmentation basée sur l'identité de l'instance AWS

1. Posture Control (CNAPP)

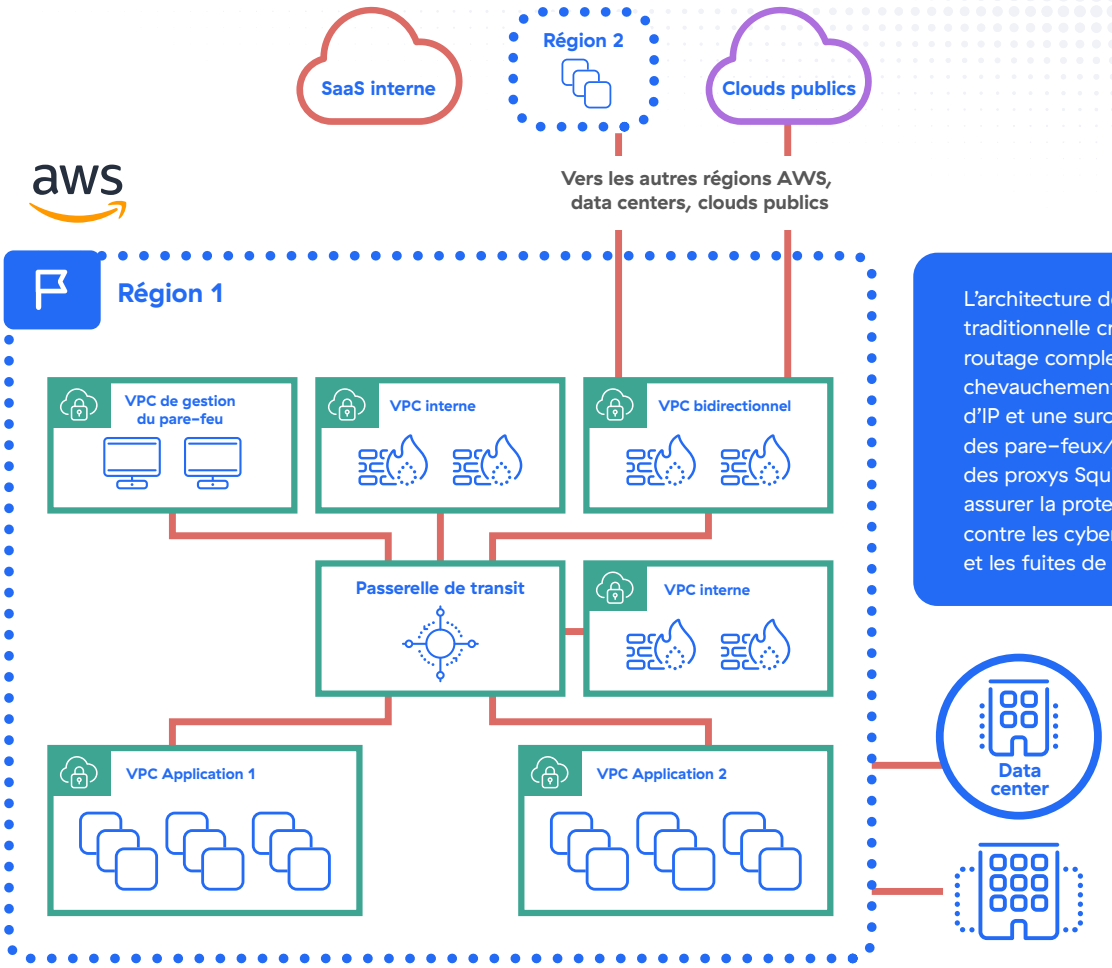
Posture Control, plateforme de protection des applications cloud natives (CNAPP), réinvente la sécurité des applications cloud natives sous la forme d'une solution sans agent qui fait appel au Machine Learning (apprentissage automatique) pour identifier les risques furtifs induits par les erreurs de configuration, les menaces et les vulnérabilités dans les environnements AWS. Cette solution permet aux équipes de sécurité, de développement et DevOps de hiérarchiser et de remédier efficacement aux risques liés aux applications cloud et déployées sur des machines virtuelles, le plus tôt possible dans leur cycle de développement.

Principaux avantages :

- Réduit la complexité et les coûts liés à la gestion de plusieurs solutions autonomes pour sécuriser les environnements cloud et assurer la conformité.
- Applique des politiques de sécurité cohérentes pour tous les services cloud grâce à un moteur de politiques unifié.
- Prévient les erreurs de configuration et les problèmes de sécurité imputables à des ressources et compétences limitées.
- Intègre la sécurité dans le workflow des développeurs, ce qui permet de hiérarchiser les risques critiques et d'y remédier tout en évitant la multiplication des alertes.
- Tire parti de fonctions robustes de visualisation et de reporting pour mettre en évidence les failles de sécurité, les erreurs de configuration, les autorisations et les données à risques.

2. Workload Communications

Avec Workload Communications, Zscaler a complètement réinventé la connectivité cloud en assurant un modèle Zero Trust pour les instances cloud, pour un accès simple et sécurisé des instances à Internet et aux applications privées. Contrairement aux solutions réseau traditionnelles, Workload Communications fournit une architecture d'accès direct vers AWS qui tire parti de la plateforme éprouvée Zero Trust Exchange de Zscaler pour établir le niveau de confiance sur la base de l'identité et du contexte. Cette confiance, lorsque validée, permet des communications sécurisées entre les instances et Internet, entre instances sur plusieurs régions et zones de disponibilité AWS et entre instances au sein de l'environnement AWS.



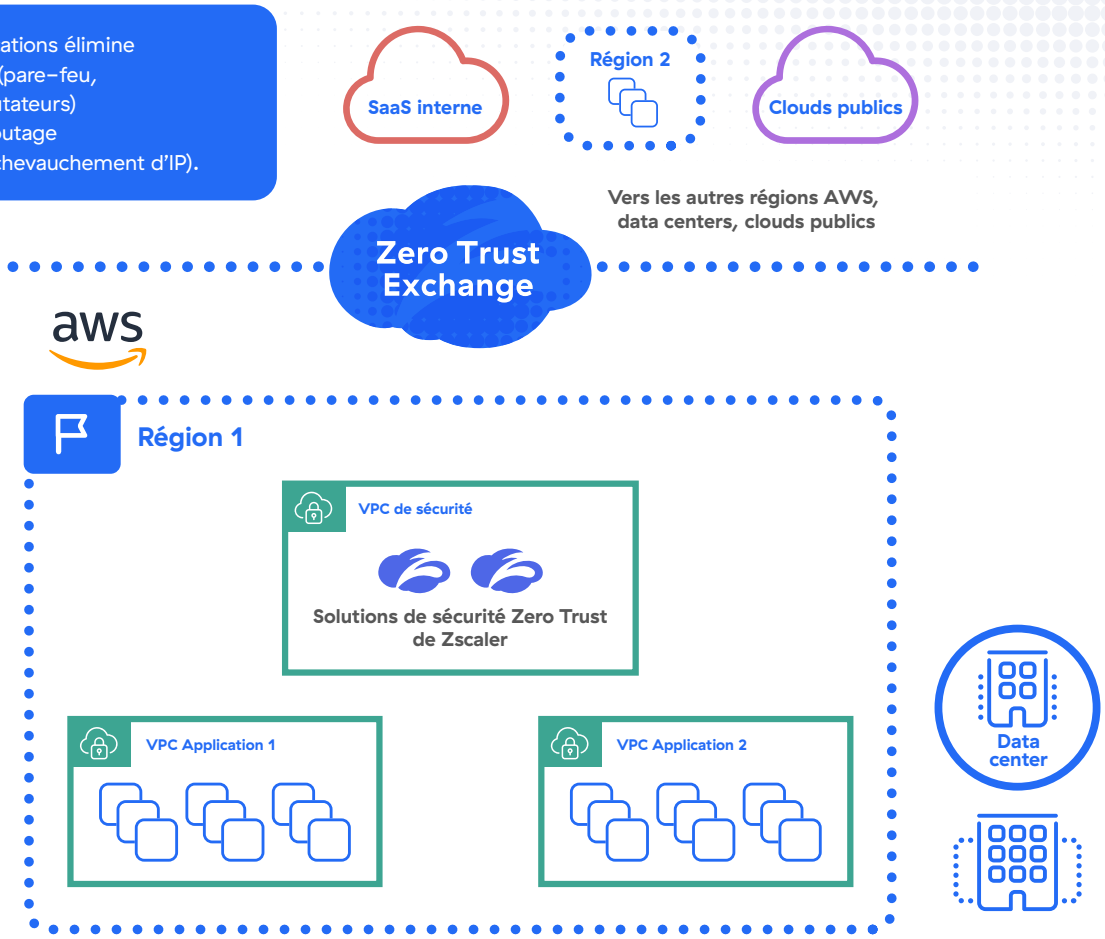
L'architecture de sécurité traditionnelle crée un routage complexe, un chevauchement/conflit d'IP et une surcharge des pare-feux/VM et des proxys Squid pour assurer la protection contre les cybermenaces et les fuites de données.

Principaux avantages :

Workload Communications élimine la surface d'attaque du réseau en connectant directement les instances à Internet et aux applications privées via un proxy. Cette architecture simplifie considérablement la connectivité en éliminant le routage, les VPN, les passerelles de transit, les hubs de transit et les pare-feux. Elle permet un routage flexible et facilite la gestion des politiques grâce au framework éprouvé des politiques de ZIA et de ZPA. Cette approche unique offre trois avantages majeurs aux utilisateurs d'AWS :

- Suppression de la surface d'attaque : grâce à une connexion directe vers le cloud qui évite au trafic de transiter via le réseau d'entreprise, les applications dans les environnements AWS sont invisibles aux cybermenaces, réduisant ainsi le risque de perte de données.
- Connectivité cloud simplifiée : l'architecture Zero Trust permet d'éviter les pertes de performances, en supprimant les problématiques de chevauchement d'IP et de planification du routage. Les instances se connectent directement à d'autres applications.
- Meilleures performances des applications à grande échelle : Zscaler repose sur une architecture distribuée où chaque communication qui atteint le Service Edge est traitée instantanément en fonction d'éléments d'identité et de contexte. La relation de peering avec AWS dans la plupart des régions du monde garantit le chemin le plus court entre les applications, quel que soit l'endroit où elles sont hébergées, réduisant ainsi la latence et améliorant les performances des applications.

Workload Communications élimine la surcharge des VM (pare-feu, proxys Squid, commutateurs) et la complexité du routage (aucun problème de chevauchement d'IP).



Synthèse

Ensemble, Zscaler et AWS aident les entreprises à mener leur transformation digitale sécurisée, en proposant les avantages suivants :

- Routage efficace qui réduit la latence et accélère la migration des instances vers AWS
- Simplification de l'architecture réseau et de sécurité via l'élimination des pare-feux et des VPN
- Accès permanent qui améliore l'expérience de l'utilisateur final
- Posture de sécurité plus solide et complète pour éliminer les menaces pesant sur les applications cloud
- Plus grande agilité pour assurer un avantage concurrentiel
- Réduction des coûts pour libérer des fonds qui seront mieux utilisés pour d'autres projets d'entreprise

Les solutions de sécurité Zero Trust de Zscaler sont disponibles à l'achat sur AWS Marketplace. Nous proposons tout ce dont vous avez besoin pour protéger vos utilisateurs, vos données et vos instances.

En savoir plus sur Zscaler pour AWS

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. Adossé à plus de 150 data centers dans le monde, Zero Trust Exchange est la plus grande plateforme cloud de sécurité SSE proposée en mode inline. Pour en savoir plus, rendez-vous sur **zscaler.fr** ou suivez-nous sur Twitter **@zscaler**.

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