AWS et Zscaler : Une solution unifiée pour une sécurité cloud solide et évolutive

aws

zscaler™

Table des matières

Le défi du cloud : se développer rapidement, mais en toute sécurité 3

La solution moderne, complète et cloud-first de Zscaler 4

ZPA : une solution d'accès Zero Trust transparente et cloud-first pour les applications privées 5

ZIA : une pile de sécurité en tant que service fiable pour le cloud 6

ZDX : des expériences rapides et transparentes pour les utilisateurs finaux 7

Une solution commune facile à déployer et rapidement opérationnelle 8

Prêt à transformer votre sécurité cloud ? 9

Le défi du cloud : se développer rapidement, mais en toute sécurité

Les VPN et autres pratiques de sécurité basées sur le périmètre ne peuvent pas répondre aux défis du cloud moderne. Quelles sont donc les solutions ?

En 2020, plus de la moitié des entreprises ont migré leurs charges de travail vers le cloud, et 76 % d'entre elles ont choisi Amazon Web Services (AWS). Les avantages de l'adoption du cloud sont indéniables, des économies de coûts à une évolutivité agile. Les entreprises qui opèrent dans le cloud sont confrontées à deux nouveaux défis : la gestion de l'accès et des opérations dans le contexte du recours croissant aux structures de travail à distance et hybrides, et la menace de plus en plus sophistiquée que représentent les logiciels malveillants et les ransomwares.

Historiquement, la mise en œuvre d'un environnement sécurisé exigeait un VPN centré sur le réseau, qui sacrifiait la vitesse, la facilité d'utilisation et la flexibilité au profit du contrôle. Aujourd'hui, alors que les entreprises migrent vers le cloud et que l'ampleur des opérations informatiques augmente, les inconvénients de l'utilisation d'un VPN l'emportent sur les avantages.

À la base, le VPN n'est pas conçu pour fournir un accès Internet fondamentalement sécurisé et impose au personnel la charge de disposer d'une connexion internet solide, ainsi que des mesures de sécurité à jour. Les sociétés qui se tournent vers le cloud emploient des utilisateurs qui travaillent depuis n'importe où ; les connexions entrantes se sont donc développées, multipliant les possibilités d'attaques par DDoS. Cela ajoute à la complexité de la segmentation de l'accès dans un contexte de moindre visibilité sur qui fait quoi sur le réseau. En fin de compte, ces obstacles limitent l'évolutivité, augmentent les coûts, affectent la productivité et nuisent à l'expérience utilisateur des employés. Dans certains cas, ils ont également un impact sur l'utilisateur final ultime : le client.

Ces obstacles expliquent pourquoi Zscaler, l'une des principales plateformes Zero Trust Exchange qui révolutionne le secteur des réseaux et de la sécurité, collabore si efficacement avec AWS. En tant que partenaire technologique avancé d'AWS, Zscaler fournit un service de sécurité basé sur un modèle Zero Trust permettant aux entreprises de réaliser une véritable transformation cloud, en toute sécurité et en toute simplicité, aujourd'hui et demain.

La solution moderne, complète et cloud-first de Zscaler

Une suite de produits configurables destinés à simplifier l'accès et à renforcer la sécurité, conçus pour la complexité du multicloud.

Qu'une entreprise cherche à transférer des charges de travail vers le cloud ou à s'affranchir tout simplement du VPN, le verdict est tombé : l'association de Zscaler et d'AWS procure une sécurité de premier ordre et une formidable expérience utilisateur grâce à une technologie de pointe et à un modèle Zero Trust.

Les services de sécurité centrés sur les applications de Zscaler sont construits dans le cloud dès le départ, remplaçant les traditionnelles passerelles entrantes/sortantes pour une approche plus moderne (idéale pour les sociétés fonctionnant sur AWS). Trois services de base aident les clients d'AWS à tirer le meilleur parti de leurs opérations dans le cloud :

Zscaler Private Access (ZPA) rend le VPN obsolète en connectant les utilisateurs aux applications, et non aux réseaux, en séparant les applications d'Internet pour un environnement plus sécurisé et une complexité back-end réduite (gestion plus fluide des outils et opérations en arrière-plan avec lesquels les utilisateurs n'interagissent pas).

Zscaler Internet Access (ZIA) est une pile de sécurité complète fournie dans le cloud qui atténue le coût et la complexité des approches traditionnelles de passerelle Web sécurisée.

Zscaler Digital Experience Monitoring (ZDX) est une plateforme de surveillance multi-entité, basée sur le cloud, qui analyse, évalue et mesure les expériences digitales de chaque utilisateur au sein d'une entreprise.

Ensemble, Zscaler et AWS aident les entreprises à préparer leur futur avec :

- Un accès permanent qui améliore les expériences de l'utilisateur final
- Un routage plus efficace qui réduit la latence et accélère le délai de production
- Une posture de sécurité plus forte et plus complète pour éliminer les menaces
- Une migration plus rapide des applications pour réduire au minimum les temps d'arrêt
- Une plus grande agilité commerciale pour un avantage concurrentiel
- Une réduction des coûts pour libérer des fonds qui seront mieux utilisés dans d'autres secteurs de l'entreprise

Si ces outils permettent à toute entreprise d'être pérenne, ils se révèlent particulièrement utiles dans les cas d'utilisation à fort impact. Par exemple, Zscaler élimine une grande partie des soucis techniques auxquels les équipes informatiques sont confrontées au cours des fusions et des acquisitions. En proposant un processus d'intégration beaucoup moins complexe tout en appliquant les bonnes pratiques en matière de sécurité, Zscaler a aidé les entreprises à réduire le délai de configuration technique de plusieurs mois à quelques semaines. Les sociétés fusionnées peuvent connecter les employés directement aux applications sans avoir à subir les inconvénients ou les retards liés à la création ou au déplacement de réseaux.

Zscaler en chiffres

Chaque jour, Zscaler :

Bloque

7 milliards

de menaces

Traite

plus de 200 milliards

de demandes

Fournit

plus de 200 000

mises à jour de sécurité uniques

ZPA : une solution d'accès Zero Trust transparente et cloud-first pour les applications privées

Remplacer les VPN peu pratiques par un accès transparent qui maintient les applications privées à l'écart d'Internet et les rend invisibles aux menaces extérieures

Autrefois considérés comme la meilleure option pour l'accès privé, les VPN sont devenus encombrants et vulnérables dans un monde basé sur le cloud, car ils acheminent essentiellement un utilisateur vers un réseau pour le renvoyer ensuite vers l'extérieur. En traversant le globe pour passer par différents points de contact, du pare-feu aux équilibreurs de charge, les connexions d'applications pour les travailleurs distants ajoutent encore davantage d'étapes. En outre, le VPN oblige les utilisateurs à comprendre quel profil ils doivent utiliser et quelles ressources leur permettront de se connecter au réseau, ce qui n'est pas la meilleure expérience utilisateur, en particulier pour les employés moins au fait de la technologie.

Maintenir vos bureaux satellites en orbite

ZPA fournit un accès distant sécurisé aux applications sans passer par un VPN, totalement hors réseau, et sans jamais dépendre d'appliances physiques ou virtuelles centrées sur l'IP. Il gère l'accès des utilisateurs autorisés avant, pendant et après la migration des applications vers AWS en utilisant une voie beaucoup plus efficace et sécurisée : une solution Zero Trust, au périmètre défini par logiciel (SDP), qui exploite une connexion interne établie à partir d'un connecteur d'applications AWS dans le cloud sécurisé mondial de Zscaler. (Il complète également les groupes de sécurité natifs d'AWS, ainsi que d'AWS Direct Connect). Quel que soit l'endroit d'où un utilisateur tente de se connecter aux applications internes, ZPA accélère la migration des applications, diminue les coûts et réduit la cible des menaces (même pour les entreprises qui dépendent encore d'un data center privé), ce qui est idéal pour associer évolutivité et agilité.

ZPA Northstar : comment GROWMARK maintient la production alimentaire en activité

GROWMARK, une société agricole nord-américaine qui fournit divers matériaux et services destinés à soutenir la croissance des cultures, emploie du personnel dans plus de 500 sites ruraux. L'entreprise connaît donc bien les défis posés par un Internet peu fiable. Lorsque la pandémie de COVID-19 est survenue et que la chaîne d'approvisionnement a été touchée, il était plus important que jamais d'assurer le bon déroulement des opérations. Dans le cadre de ses projets de modernisation, GROWMARK a déplacé des centaines d'applications vers AWS, mais en a également hébergé certaines sur site. Il lui fallait par conséquent une solution à même de fonctionner avec sa structure hybride. Après avoir choisi ZPA, GROWMARK a pu procurer à ses employés une connexion plus fiable tout en supprimant les interfaces publiques de son environnement privé, réduisant ainsi sa surface d'attaque. Au plus fort de la pandémie, 98 % du personnel de GROWMARK se connectait à ZPA sans pratiquement aucun problème.

ZIA : une pile de sécurité en tant que service fiable pour le cloud

Réduire les risques et les coûts de réseau en abandonnant le périmètre de sécurité obsolète au profit d'une protection Zero Trust dans le cloud

Les entreprises fonctionnant sur des data centers et des modèles de sécurité basés sur le périmètre découvrent que l'adoption du cloud entraîne une transition vers des approches de passerelle Web plus sécurisées.

Le passage d'un data center au cloud place les applications dans un nouveau contexte ; les passerelles centralisées qui autrefois simplifiaient l'accès et réduisaient les coûts ne sont plus adaptées aux nouvelles vulnérabilités résultant d'un trafic utilisateur dirigé directement vers le cloud. Le cadre du périmètre de sécurité existant devient alors un handicap. Si l'on ajoute à cela la prolifération de nouvelles appliances de sécurité qui alourdissent une passerelle déjà surchargée, il devient difficile au service informatique de réagir.

Dans l'espace, il n'y a aucune place pour l'erreur

Zscaler et AWS fonctionnent sur le principe de Zero Trust, de sorte que vous n'êtes jamais en situation de faiblesse en territoire inconnu. Cela donne déjà une longueur d'avance aux entreprises, Zero Trust devenant rapidement l'architecture de sécurité de prédilection, selon Forrester.

Avec ZIA, les entreprises peuvent établir une connexion plus sûre aux solutions SaaS (Software as a Service), en apportant une visibilité sur l'ensemble de l'activité Internet des utilisateurs au sein de la société, tout en maintenant un accès à distance simple et sécurisé aux applications internes sur AWS.

Grâce à la structure et aux services de Zscaler, les utilisateurs constatent une réduction des surfaces d'attaque, un meilleur contrôle d'accès et une protection renforcée des données, ce qui permet d'appliquer des politiques granulaires à grande échelle.

ZIA Northstar : comment MAN Energy Systems a adopté ZIA

La société allemande MAN Energy Systems, spécialisée dans la fabrication et les services de transport, fournit des produits et des services à fort impact qui contribuent à faire fonctionner le monde, tels que des moteurs diesel et des turbomachines. Pour rester compétitive, la société a migré ses charges de travail vers AWS, mais les équipes de MAN, en pleine croissance et disséminées dans le monde entier, ont de plus en plus besoin d'un accès mobile aux applications et à des outils professionnels personnalisés. Cela posait un risque de sécurité élevé et mécontentait les employés en raison du processus d'authentification et d'accès long et compliqué requis au niveau individuel pour un grand nombre d'applications. Parallèlement à l'abandon du VPN, les dirigeants ont adopté ZIA afin que seuls les utilisateurs fiables puissent accéder à des applications fiables, connectant ainsi en toute sécurité leurs travailleurs mobiles aux applications SaaS de MAN, à tout moment et depuis n'importe quel emplacement.

ZDX : des expériences rapides et transparentes pour les utilisateurs finaux

Obtenir des informations détaillées et exploitables sur votre expérience utilisateur grâce à une vue unifiée des mesures de performance des applications, des points d'accès et de CloudPath

En tant que consommateurs, nous nous sommes habitués à une expérience utilisateur de premier ordre, au point qu'une panne temporaire des réseaux sociaux fait la une des journaux. Alors que les entreprises commençaient à maîtriser l'expérience utilisateur au bureau avec la technologie adaptée, les congestions sont devenus monnaie courante, car les équipes distantes et hybrides sont en butte à des obstacles, tels qu'une mauvaise connexion Internet et une panoplie d'appareils mobiles personnels (parfois obsolètes). Lorsque cela se produit sous la forme de temps morts et de constantes reconnexions, les tickets d'assistance s'accumulent et certaines tâches ne sont plus effectuées, ce qui met le service informatique sous pression pour trouver la cause de problèmes uniques et les résoudre.

Apporter une expérience fluide à chaque utilisateur final

ZDX est une plateforme de surveillance multi-entité, basée sur le cloud, qui analyse, évalue et mesure les expériences digitales de chaque utilisateur au sein d'une entreprise, où qu'il se trouve. ZDX détermine en temps réel la cause du problème (par exemple, la connexion Internet ou le fournisseur d'accès), puis déploie ses fonctionnalités de dépannage à distance. La fonction d'analyse mesure les performances dans le temps par emplacement, utilisateur et service afin de déterminer les tendances et d'apporter des améliorations. Le résultat ? Une véritable architecture SASE (Secure Access Server Edge) qui se concrétise par une expérience utilisateur supérieure (et beaucoup moins de tickets d'assistance informatique).

ZDX Northstar : comment Liberty Mutual a amélioré l'expérience de ses employés

Liberty Mutual Insurance pouvait garantir ses data centers et la bande passante de son FAI, mais ne pouvait pas garantir la qualité du service Internet pour les employés en télétravail, une situation que tout le monde a connue en masse en 2020. En commençant par 100 utilisateurs pour valider le concept, l'équipe de sécurité de Liberty a commencé à déployer ZDX pour les utilisateurs confrontés à des problèmes persistants dans un premier temps. Cela a permis de transférer les problèmes à l'équipe du service d'assistance de niveau 2 qui a pu facilement résoudre les problèmes des utilisateurs concernant les réseaux domestiques. Liberty Mutual a à présent intégré ZDX dans toute l'entreprise, identifiant et éliminant les problèmes de latence des fournisseurs de services, les problèmes de routeurs sans fil, les lacunes de mémoire sur les ordinateurs de bureau, ainsi que les problèmes de FAI concernant le temps de récupération des pages, entre autres choses.

Une solution commune facile à déployer et rapidement opérationnelle

Grâce à un processus de déploiement conçu pour la rapidité et à Zscaler Client Connector qui gère l'accès, vos équipes peuvent être opérationnelles en quelques minutes.

La migration vers une nouvelle plateforme et une nouvelle infrastructure informatique peut se révéler complexe et de longue haleine. C'est pourquoi Zscaler a articulé le processus d'adoption autour de la rapidité et de la simplicité, en facilitant les opérations sécurisées dans le cloud et les transitions en douceur pour les personnes appropriées, à tout moment, avec Zscaler et AWS.

Bien que ZPA, ZIA et ZDX puissent être utilisés seuls, ils sont particulièrement efficaces lorsqu'ils sont utilisés ensemble dans un cadre bien architecturé. Au cœur de leurs processus figure Zscaler Client Connector (ZCC).

ZPA utilise Client Connector pour connecter les utilisateurs à des applications privées selon une approche Zero Trust, mais l'accès par navigateur est également disponible pour les applications privées purement Web.

ZIA utilise Client Connector pour protéger les utilisateurs en dehors du réseau de l'entreprise, en faisant transiter le trafic Internet par le service de Zscaler pour garantir une politique de sécurité granulaire.

ZDX utilise Client Connector pour effectuer une analyse synthétique vers une application SaaS (Software-as-a-Service) ou un service Internet souhaité (par exemple, Salesforce, Zoom, etc.).

Dites adieu aux VPN

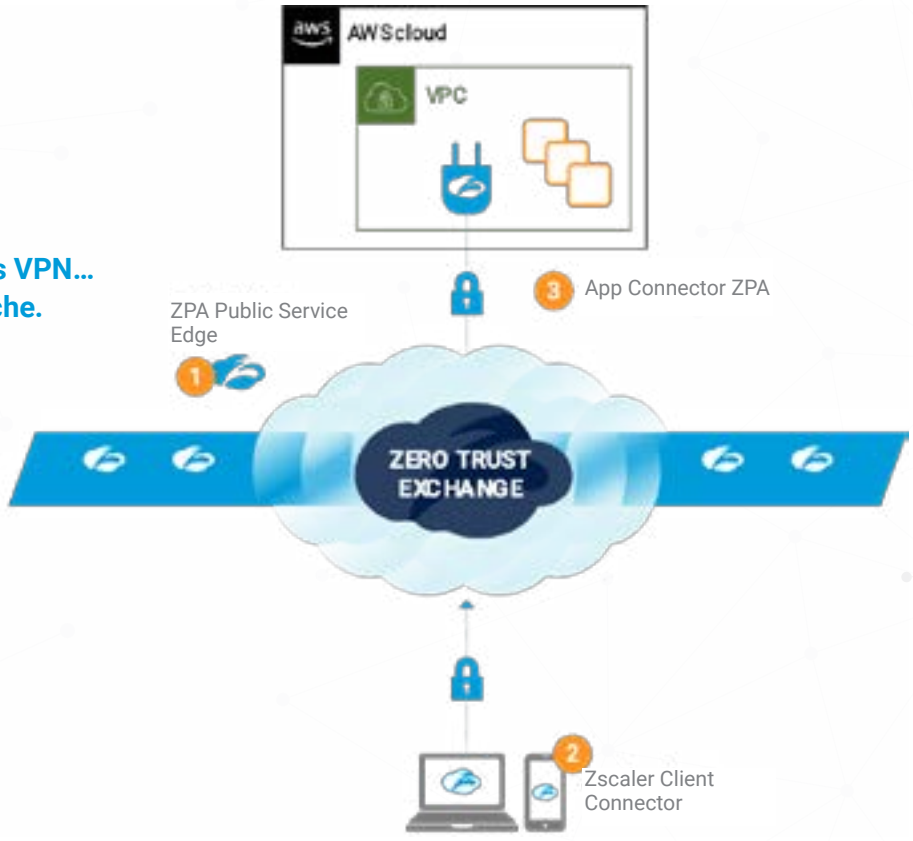
Nos clients abandonnent définitivement les VPN et profitent de l'installation rapide et conviviale de Zscaler.

1. Le service informatique installe les connecteurs d'applications dans AWS, où résident les applications, afin que Zscaler puisse atteindre les applications auxquelles les utilisateurs devront accéder.
2. Dans le portail ZPA, vous définissez les applications et les connecteurs et les affectez à des groupes de serveurs.
3. Une fois installé, Client Connector peut servir à plusieurs fins : décider où les demandes sont liées, où elles devraient aboutir, et où connecter les utilisateurs.

En savoir plus sur le paramétrage de Client Connector.

Les clients de Zscaler abandonnent rapidement et en toute sécurité leurs VPN… pour de bon. Voici comment ça marche.

1. **ZPA Public Service Edge** héberge le moteur de politique et les connexions de négociation.
2. **Zscaler Client Connector** transmet le trafic au cloud Zscaler via son agent endpoint.
3. **ZPA App Connector** connecte aux applications privées et découvre de nouvelles applications.



Prêt à transformer votre sécurité cloud ?

Zscaler et AWS ont ouvert la voie à une approche ultime de l'accès utilisateur, et elle comprend de très nombreuses possibilités. Découvrez les solutions Zscaler sur AWS Marketplace.

Essayez une démonstration hébergée gratuite de 7 jours.

En quelques clics, Zscaler préparera un rapport d'évaluation approfondie de votre posture de sécurité cloud, qui vous indiquera où se situent vos vulnérabilités sur Internet. Commencez sans plus attendre votre analyse de la vulnérabilité aux attaques Internet.