Livre blanc

La plateforme One True Zero Trust

Zscaler Zero Trust Exchange : le catalyseur d'une transformation numérique sécurisée.

Introduction

La transformation numérique n'est pas un phénomène nouveau, mais pour de nombreuses entreprises, la pandémie a été un catalyseur de l'adoption de technologies digitales et processus associés, au service des clients, mais aussi pour équiper les collaborateurs et leur permettre de travailler d'où ils le souhaitent. La migration des applications des data centers vers le cloud améliore l'efficacité et l'agilité des entreprises, ce qui leur confère un avantage concurrentiel certain. Les entreprises peuvent favoriser la productivité de leurs télétravailleurs, simplifier leurs processus opérationnels et révolutionner les expériences digitales des clients.

Cependant, *une transformation numérique sécurisée* exige de repenser l'architecture et la sécurité des connexions pour les utilisateurs, les applications et les données. Au cours des trois dernières décennies, les entreprises ont développé des réseaux complexes, étendus et en étoile destinés à connecter les utilisateurs travaillant au bureau aux applications hébergées dans le data center. Ces réseaux s'adossaient à un panel d'appliances de sécurité et de pare-feu pour empêcher toute intrusion externe, mais accordaient des privilèges quiconque se trouvait au sein du réseau.

Ce modèle, connu sous le nom de sécurité cloisonnée, fonctionnait relativement bien lorsque la plupart des applications étaient hébergées dans un data center et que la majorité des utilisateurs travaillaient depuis leur bureau en entreprise. Cependant, l'évolutivité n'était pas au rendez-vous et ce modèle s'est avéré de plus en plus obsolète à mesure que les applications ont migré vers le cloud et que le télétravail s'est généralisé. Les politiques de sécurité ne pouvaient s'appliquer aux utilisateurs et applications hors du réseau qu'en routant leur trafic vers un data center central (backhauling) à des fins d'inspection. Par conséquent, plus il y avait d'utilisateurs distants, plus il était difficile de garantir une expérience utilisateur de qualité.

Les écosystèmes cloud-first actuels, géographiquement disséminés, et au sein desquels les utilisateurs se connectent de n'importe où et accéder aux ressources de l'entreprise où qu'elles se trouvent, exigent une sécurité différente. Ces dernières années, le Zero Trust a connu une adoption massive en devenant la norme de facto qui permet aux entreprises et organisations (y compris les administrations et collectivités) de sécuriser leurs utilisateurs, leurs applications, leurs objets connectés (IoT) et leurs instances, quels que soient les réseaux ou les ressources cloud auxquels ils se connectent, ainsi que leur lieu ou mode de connexion.

Le Zero Trust s'affranchit des contraintes inhérentes aux architectures de sécurité cloisonnée, qui élargissent inévitablement la surface d'attaque à mesure que les environnements IT gagnent en complexité. Dans l'ancien modèle, chaque ressource visible depuis Internet (applications cloud, appareils des utilisateurs finaux, réseaux privés virtuels (VPN), pare-feu, etc.) pouvait potentiellement être identifiée et exploitée. Suite à un exploit initial, les assaillants pouvaient facilement se déplacer, en interne, d'une cible de valeur à une autre, au sein d'un réseau d'entreprise où tout le trafic est considéré comme fiable. Et une fois immiscés au sein du réseau, les assaillants pouvaient profiter de cette confiance pour exfiltrer des données à partir d'applications et de référentiels de données, que ce soit dans le data center, les applications SaaS ou le cloud public.

Évolution du Zero Trust

Bien que l'idée de « décloisonner » les réseaux soit évoquée depuis près de deux décennies, le terme « Zero Trust » a été inventé en 2010 dans un article publié par John Kindervag, analyste chez Forrester. Ce document affirmait que la présence d'un utilisateur ou d'un appareil sur un réseau ne constituait pas, à elle seule, un critère suffisant pour lui faire confiance. En tant que concept clé de ce nouveau mode de pensée, le Zero Trust est rapidement devenu un mot à la mode.

Peu de temps après la publication de l'article de John Kindervag, Gartner a présenté le concept d'une évaluation adaptative et continue des risques et des niveaux de confiance (CARTA pour « Continuous Adaptive Risk and Trust Assessment ») : l'idée est d'accorder un accès sur la base d'une évaluation permanente de l'environnement, d'informations contextuelles et des rôles/responsabilités de chaque utilisateur. Au fil des ans, CARTA a évolué pour donner lieu au Secure Access Service Edge (SASE), un framework architectural qui fédère des technologies de sécurité cloud-native (y compris le ZTNA) et des fonctions de réseau étendu (WAN) pour interconnecter en toute sécurité les utilisateurs, les systèmes et les terminaux (endpoints) aux applications et aux services. Jusqu'en 2021, Gartner a dissocié le marché du SASE

en deux segments : le WAN et le Security Service Edge (SSE). Ce SSE faisait référence à un ensemble convergent de services de sécurité fournis à partir d'une plateforme cloud unifiée. Le SSE permettait à une entreprise d'appliquer des politiques de Zero Trust de manière uniforme, même aux utilisateurs hors du réseau, afin de répondre aux besoins d'accès sécurisé en temps réel des entreprises digitales modernes.

Le Zero Trust est devenu une norme nationale aux États-Unis avec la sortie en 2020 de la Publication Spéciale 800-207 du National Institute of Standards and Technologies (NIST). Ce document définit explicitement le Zero Trust en tant que modèle d'architecture dont le principe est « qu'aucune confiance implicite [ne doit être] accordée aux ressources ou aux comptes d'utilisateurs sur la seule base de leur emplacement physique ou du réseau utilisé (c'est-à-dire les réseaux locaux par rapport à Internet), ou sur la base de la propriété des ressources/dispositifs (corporate ou personnel) ». En d'autres termes, la confiance n'est jamais accordée avant vérification. Enfin, en 2022, une nouvelle exigence réglementaire du gouvernement américain portant sur la conception d'architectures de sécurité basées sur les principes du NIST a fait du Zero Trust le paradigme de sécurité par défaut pour la protection des applications, du trafic, des utilisateurs, des instances et des dispositifs au sein des environnements informatiques modernes.

Cependant, la confusion persiste sur le marché concernant ce qu'est — et n'est pas — une véritable solution Zero Trust. Cette confusion a été entretenue par les fournisseurs d'outils de sécurité en périphérie de réseau qui risquent de perdre des parts de marché lorsque les clients se rendront compte que leurs solutions n'incluent pas les composants de base nécessaires à la conception d'une architecture Zero Trust, et ne peuvent pas remplir les fonctions requises de sécurité. Il est important de noter qu'une architecture Zero Trust est fondamentalement à l'opposé d'une architecture basée sur la sécurité du réseau. Il est impossible d'appliquer le Zero Trust sur un réseau de routage en utilisant des pare-feu et des VPN. Le Zero Trust exige une vérification d'identité et du contexte avant d'autoriser l'accès aux ressources, sans se connecter via un réseau.

Nous avons élaboré ce guide pour couper court aux malentendus et aider les équipes de sécurité et IT à comprendre comment concevoir des architectures de sécurité qui répondent aux besoins des entreprises modernes. Il détaille les principes architecturaux du Zero Trust et explique comment une solution comme Zscaler Zero Trust Exchange™ permet de les mettre en œuvre facilement.

Qu'est-ce qu'une architecture Zero Trust ?

Le Zero Trust part du principe que tout ce qui se trouve sur le réseau est malveillant ou compromis, et que l'accès à une application n'est accordé qu'après vérification de l'identité de l'utilisateur, de la posture de l'appareil utilisé et du contexte opérationnel, et après application des règles et politiques en vigueur. Dans ce modèle, l'ensemble du trafic doit être journalisé et inspecté, ce qui exige un degré de visibilité que n'offrent pas les fonctions traditionnelles de sécurité.

Une architecture Zero Trust est expressément conçue pour minimiser la surface d'attaque, empêcher les menaces de se mouvoir en interne et juguler les risques de piratage. Elle est déployée avec une architecture basée sur un proxy qui connecte les utilisateurs directement aux applications plutôt qu'au réseau, et qui applique des contrôles supplémentaires avant que les connexions ne soient autorisées ou bloquées.

Une véritable architecture Zero Trust diffère de l'architecture traditionnelle à trois égards :

1. **Elle met fin à chaque connexion.** Ceci diffère de l'approche pass-through des technologies de type pare-feu qui inspectent les fichiers au fur et à mesure qu'ils sont transmis. Si un fichier malveillant est détecté, il est souvent trop tard lorsque l'alerte est donnée. En revanche, interrompre chaque connexion permet une inspection inline de tout le trafic. Ainsi, les ransomwares, les malwares et le trafic malveillant sont neutralisés en amont de leur destination.

2. **Elle protège les données à l'aide de politiques granulaires et contextuelles.** Une architecture Zero Trust vérifie l'identité et les éléments de contexte (identité de l'utilisateur, identité de l'appareil, emplacement de l'appareil, type de contenu et application pour lequel l'accès est demandé) avant d'accorder un accès. Ces politiques doivent être flexibles afin que les privilèges d'accès puissent être réévalués en permanence en fonction de l'évolution des conditions ou des comportements des utilisateurs.

3. **Elle élimine la surface d'attaque.** Dans un réseau traditionnel, toute personne connectée à un réseau traditionnel voit l'ensemble des autres nœuds de ce réseau. En revanche, dans une architecture Zero Trust, les utilisateurs ne voient et ne peuvent se connecter qu'aux ressources auxquelles ils sont autorisés à accéder. Rien de plus. Les connexions directes d'utilisateur à application et d'application à application éliminent tout risque de déplacement en interne d'une menace et empêchent les appareils compromis de servir de vecteur d'une infection susceptible de se propager à d'autres ressources.

Modèle One True Zero : comment Zero Trust Exchange fournit les éléments clés d'une architecture Zero Trust

Zscaler est un leader de la sécurité Zero Trust depuis plus de dix ans. Pour aider les entreprises à sécuriser leur transformation numérique, Zscaler a créé Zero Trust Exchange, une plateforme intégrée de cybersécurité cloud-native, basée sur deux principes essentiels : un accès à moindre privilège et l'idée qu'aucun utilisateur, instance ou appareil n'est intrinsèquement digne de confiance. La plateforme accorde l'accès en fonction de l'identité et d'informations contextuelles (type d'appareil, emplacement, application et contenu), en négociant une connexion directe sécurisée entre une application et un utilisateur, une instance ou un appareil, quel que soit le réseau, quelle que soit la localisation.

Zero Trust Exchange est une plateforme intégrée de services qui agit comme un standard téléphonique intelligent. Son architecture proxy unique garantit l'application de politiques Zero Trust, indépendamment de la localisation. Cette approche considère toutes les communications comme potentiellement malveillantes, les bloquant toutes jusqu'à ce qu'elles puissent être validées selon des politiques basées sur l'identité. Chaque communication qui passe par Zero Trust Exchange est soumise à une série de contrôles avant qu'une connexion ne soit établie.

L'architecture Zero Trust comporte sept éléments essentiels.[1] Ces éléments peuvent être regroupés en trois catégories :

1. **Vérifier l'identité et le contexte**
   Chaque fois qu'un utilisateur, un appareil ou une instance demande une connexion, indépendamment du réseau sous-jacent, Zero Trust Exchange met d'abord fin à la connexion, puis vérifie l'identité et le contexte selon les critères de « qui, quoi et où » de la demande d'accès.

2. **Maîtriser les risques**
   Une fois l'identité et le contexte de l'initiateur de la demande vérifiés, et les règles de segmentation appliquées, Zero Trust Exchange évalue le risque associé à la demande de connexion. La solution inspecte également le trafic à la recherche de cybermenaces ou de données sensibles.

3. **Appliquer la politique**
   Enfin, la plateforme utilise ces résultats pour appliquer la politique de sécurité à chaque session. Elle détermine en dernier ressort s'il convient d'autoriser la connexion ou de la bloquer sous conditions. Si l'entité est autorisée à se connecter, la plateforme garantit que sa connexion à la ressource Internet, à l'application SaaS ou à l'environnement IaaS/PaaS est sécurisée.

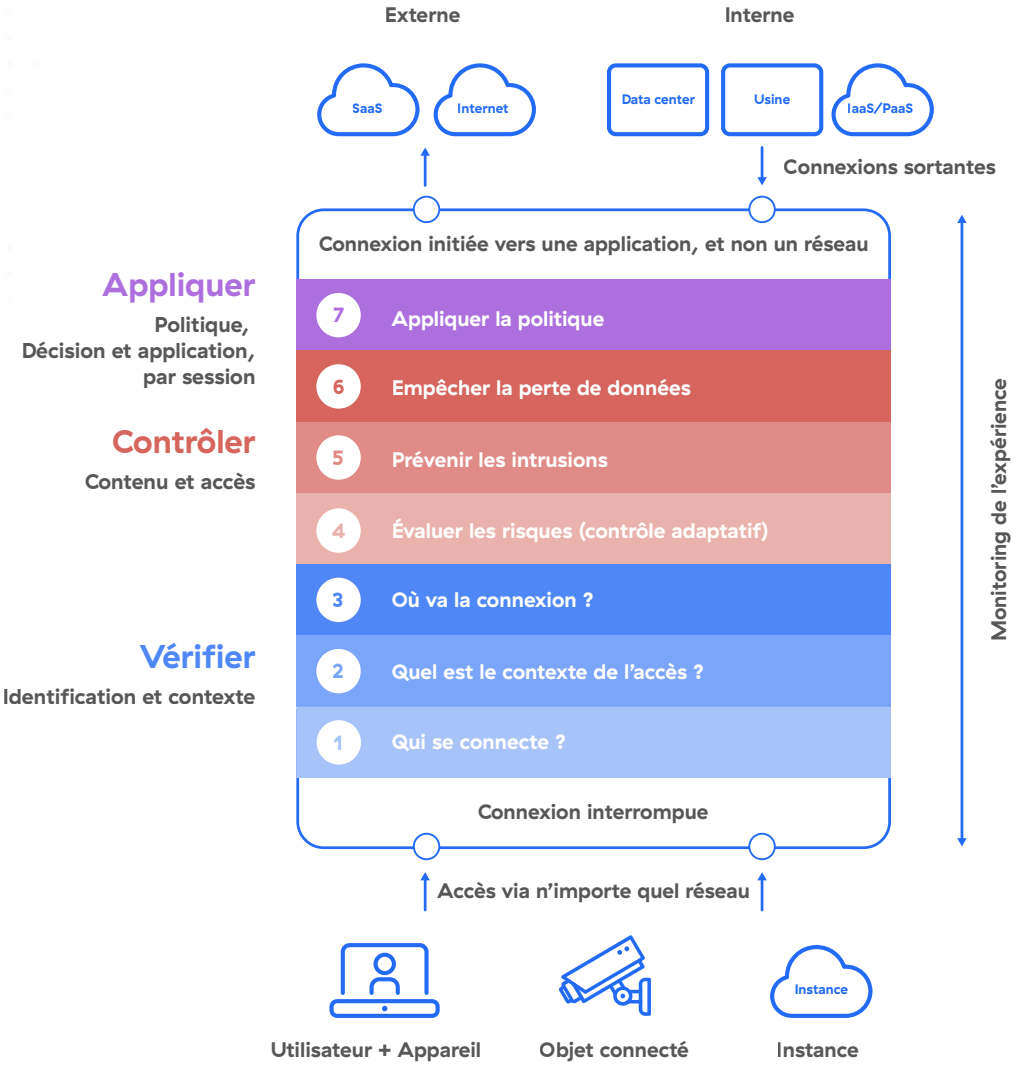

Illustration 1 : Les sept éléments de l'architecture Zero Trust.

Chacun des sept éléments des trois catégories principales alimente les autres, créant un arbre de décision dynamique qui permet de vérifier chaque connexion, à chaque fois. Avec Zero Trust Exchange, les décisions et l'application des politiques sont effectuées sans impacter l'expérience utilisateur : la plateforme surveille les performances et diagnostique toute problématique, garantissant ainsi une sécurité qui ne pèse pas sur les utilisateurs.

Examinons de plus près chacun de ces sept éléments.

Vérifier

À ce stade du processus de connexion, Zero Trust Exchange vérifie :

- Qui se connecte
- Quel est le contexte de l'accès
- Où va la connexion

1. **Qui se connecte :** Zero Trust Exchange établit généralement l'identité de l'entité se connectant grâce à des intégrations avec des fournisseurs d'identité (IdP). Le service IdP valide l'identité

de l'entité qui se connecte par le biais d'une authentification (idéalement MFA ou plus forte), tandis que Zero Trust Exchange exploite ensuite les valeurs d'identité, les certificats et les détails partagés fournis par le service IdP. Pour identifier les appareils qui ne peuvent pas être authentifiés par un IdP, tels que les objets connectés (IoT) ou certains dispositifs industriels (OT), Zero Trust Exchange exploite les informations de localisation sur le réseau. Chaque instance peut également être identifiée sur la base de ses caractéristiques, de fonctions de processus ou d'autres facteurs.

2. **Définition du contexte d'accès :** lorsque Zero Trust Exchange analyse le contexte de l'accès, il évalue précisément tous les éléments de contexte associés à la connexion. La validation du contexte de l'accès est basée sur les informations d'identité et de profil. Au lieu de simplement indiquer qu'une personne est un collaborateur, ces informations révèlent davantage l'intention et les autorisations de cette personne, ce qui permet une décision d'accès plus nuancée.

   D'autres attributs du contexte d'accès peuvent être pris en compte :

   - Localisation de l'appareil
   - Heure de la demande
   - Mission, fonctions et responsabilités de l'utilisateur
   - Manière dont la demande d'accès est effectuée (par exemple, peut-elle être considérée comme normale ?)
   - Identité de l'appareil (personnel ou corporate, géré ou non géré)

3. **Destination de la connexion :** une fois que Zero Trust Exchange a examiné l'identité du demandeur de la connexion et qu'il a pris connaissance du contexte de la requête, la solution recherche alors la destination de la connexion. Zero Trust Exchange identifie l'application souhaitant être accédée, en examinant sa fonction, sa localisation, les risques et problèmes connus, ainsi que la relation avec l'identité de celui qui demande l'accès. L'application est-elle connue ou inconnue ? Est-elle disponible sur l'Internet public ?

   Zero Trust Exchange fonctionne au sein d'une architecture basée sur un proxy et peut, à ce titre, se concentrer sur le contexte de l'application de destination plutôt que sur sa seule adresse IP. Il devient possible de réaliser une segmentation précise de type utilisateur-application, sur la base des politiques tenant compte de l'identité. Chaque application peut être évaluée individuellement : un ERP sera traité différemment de YouTube.

   Zero Trust Exchange fournit ainsi un accès fondé sur le principe du moindre privilège, en appliquant des politiques spécifiques pour chaque application, y compris pour les instances critiques. La solution peut également apprendre au fur et à mesure, en déduisant des informations à partir des flux de trafic utilisateur-instance, et en faisant évoluer les politiques si nécessaire. Elle est en outre suffisamment intelligente pour évaluer les niveaux de risque associés aux applications inconnues disponibles sur Internet.

Contrôler

En général, les décisions et les mesures d'application qui entrent dans cette catégorie ont trait à la compréhension du risque et à l'inspection du contenu. Ce degré de contrôle est difficile à atteindre dans les architectures conventionnelles basées sur des pare-feu, où l'inspection de l'intégralité du contenu impose de déployer des services supplémentaires.

À ce stade du processus de connexion, Zero Trust Exchange va :

- Évaluer le risque en appliquant des contrôles adaptatifs
- Empêcher les intrusions
- Prévenir les pertes de données

4. **Évaluer le risque (avec des contrôles adaptatifs) :** Zero Trust Exchange évalue les risques de manière continue. Des signaux actualisés sont exploités pour garantir la fiabilité des scores de risque. Ces scores de risque alimentent ensuite un moteur de décision qui détermine si l'accès doit être accordé, ou doit continuer à l'être. Il est ainsi possible d'appliquer des décisions d'accès basées sur les risques pendant toute la durée de vie d'une connexion. Un changement de posture ou de comportement de l'utilisateur ou de l'appareil déclenche une mise à jour en temps réel de la décision d'accès.

   Les scores de risque prennent en compte des facteurs tels que le comportement (un client SQL doit communiquer avec un serveur SQL, et non avec un serveur non reconnu et localisé dans un emplacement géographique inconnu), ainsi que des informations provenant d'outils tiers de type EDR, SIEM et SOAR.

   Les scores de risque peuvent également prendre en compte des éléments tels que les risques liés au secteur d'activité, la répartition des risques au sein d'une entreprise (le service informatique est-il plus exposé que le service commercial ?), ainsi que les risques liés aux localisations. L'algorithme propriétaire de Zero Trust Exchange calcule un score de risque sur la base de tous ces facteurs. Son objectif est de permettre un meilleur contrôle et une plus grande visibilité au moment d'appliquer les politiques. Il peut également corréler les informations provenant de moteurs de sécurité cloud-native pour mettre en lumière les risques méconnus résultant d'erreurs de configuration, de menaces ou de vulnérabilités des environnements cloud. Les scores peuvent également être ajustés en fonction des dernières découvertes de ThreatLabZ, l'équipe de recherche de Zscaler composée d'experts en sécurité et d'ingénieurs réseau qui analysent les menaces sur l'ensemble du cloud de sécurité de Zscaler, ainsi que le panorama mondial des menaces.

5. **Déjouer les piratages :** Zero Trust Exchange inspecte les contenus en mode inline pour prévenir les piratages et compromissions. La majorité du trafic Internet (y compris le trafic lié aux attaques) étant désormais chiffré par SLS/TLS, l'inspection de ce protocole sécurisé est donc impérative. C'est le seul moyen de se protéger contre les nouvelles attaques ou d'arrêter l'exfiltration de données chiffrées. Cette inspection est effectuée en fonction du risque métier et du type d'application, afin de protéger le droit à la confidentialité des utilisateurs.

   L'architecture de Zero Trust Exchange est conçue dans une optique de performances et d'évolutivité. Sa solution Zero Trust fournie en périphérie analyse tout le contenu en un seul passage, sans copier les paquets ni ajouter de latence. De plus, le forward proxy basé dans le cloud permet l'utilisation de technologies telles que le sandboxing et l'isolation du navigateur, qui permettent la mise en quarantaine des menaces et la diffusion d'images pixelisées vers l'utilisateur au lieu d'une page Web réelle. Elle peut aussi appliquer de manière intelligente le contrôle adéquat à une application donnée (il n'est, par exemple, pas nécessaire d'inspecter le contenu du flux vidéo de Zoom ou Teams).

6. **Prévenir la perte de données :** Zero Trust Exchange offre des fonctionnalités contre la perte de données. En surveillant le trafic véhiculé sur l'Internet ouvert (SaaS ou applications internes hébergées dans des clouds publics), la solution peut neutraliser l'exfiltration de données sensibles ou d'éléments de propriété intellectuelle. Ces fonctions assurent également une protection contre la perte accidentelle et le partage excessif de données, ainsi que contre les erreurs de configuration (des espaces de stockage cloud notamment).

Zero Trust Exchange est particulièrement efficace en matière de prévention des pertes de données. Son moteur d'inspection optimisé par IA peut appliquer des règles basées sur des dictionnaires ou moteurs prédéfinis à des fins de conformité. Les utilisateurs peuvent également créer des dictionnaires personnalisés avec des mots-clés et des modèles spécifiques à leur entreprise. La solution est également capable de procéder à une classification avancée des données. Zero Trust Exchange applique les politiques de protection des données au niveau de l'edge réseau, c'est-à-dire à proximité de l'utilisateur, et non de manière centralisée, ce qui introduirait une certaine latence. L'application des politiques est permanente et uniforme. Zero Trust Exchange peut également analyser les API des fournisseurs SaaS pour protéger les données stockées au sein d'applications SaaS . Les données en transit peuvent également être analysées et donc protégées. Des contrôles out-of-band sont également proposés, sur la base des définitions des applications cloud, des contrôles des types de fichiers et des attributs de risque. Il est donc possible de définir des types de fichiers acceptables, de déterminer les applications cloud autorisées (et celles qui ne le sont pas), voire de bloquer les données sensibles présentes dans des images, des captures d'écran ou des documents.

Appliquer

Au cours des deux étapes précédentes, Zero Trust Exchange aura effectué une évaluation des risques basée sur l'identité et le contexte. Il ne s'agit pas d'une opération statique effectuée une fois pour toutes, mais d'un processus continu et dynamique.

7. **Appliquer la politique :** au stade de l'application, le moteur de politique prend en compte les résultats de l'évaluation des risques pour chaque session, afin de déterminer s'il convient de décider d'une « autorisation conditionnelle » ou d'une « interdiction conditionnelle ». À noter que les décisions de refus peuvent être prises avant ce stade.

   « L'autorisation conditionnelle » accorde l'accès à l'application, mais la plateforme peut encore proposer des contrôles supplémentaires, tels que l'isolation du navigateur, l'inspection du contenu et des mises en garde. Plusieurs types de contrôles relevant de cette catégorie peuvent être appliqués. Parmi lesquels :

   - **Avertir et autoriser :** l'accès est accordé, mais l'utilisateur est informé que le risque lié à la destination n'est pas clair.
   - **Prioriser :** cette fonction de contrôle de la bande passante permet d'établir des liens réseau dédiés afin de préserver l'accès aux applications critiques pour l'entreprise, en reléguant au second plan le trafic des réseaux sociaux ou de streaming par exemple.
   - **Isoler :** ce contrôle restitue le contenu demandé sous forme d'un flux de pixels au lieu d'une page Web complète, éliminant ainsi le risque de fuite de données ou de menaces actives.
   - **Orienter :** cette fonction envoie le trafic vers une destination non standard.
   - **Mettre en quarantaine et autoriser :** cette fonction utilise une sandbox cloud pour exécuter le contenu potentiellement dangereux. L'accès n'est autorisé que si le contenu s'avère inoffensif.

   Le « blocage conditionnel » intervient si une demande d'accès ne remplit pas les conditions pour lesquelles elle a été évaluée lors des étapes précédentes. Les fonctions de neutralisation portent sur la neutralisation simple, le déploiement de leurres pour détecter les menaces actives, et la neutralisation assortie d'une mise en quarantaine. La capacité de Zero Trust Exchange à appliquer des politiques à plusieurs niveaux favorise des fonctions puissantes et granulaires, ainsi qu'une prise de décision précise et nuancée. Les entreprises peuvent établir différents niveaux d'application des politiques en fonction des résultats des six éléments précédents. Plusieurs politiques peuvent être appliquées au cours d'une même session. Il est ainsi possible de générer les résultats métiers souhaités, d'atténuer les risques et d'appliquer une posture de sécurité robuste.

Zero Trust Exchange : la plateforme Zero Trust par excellence

La plateforme Zscaler Zero Trust Exchange offre un panel complet de fonctionnalités de protection contre les cybermenaces et de sécurité de la connectivité, à partir d'une solution unique. Elle supprime la surface d'attaque et prévient les pertes de données, grâce à une architecture qui applique des politiques Zero Trust à tous les utilisateurs, instances et dispositifs présents dans un environnement d'entreprise.

La plateforme Zero Trust Exchange multiple les avantages :

- Elle simplifie et automatise la connectivité des instances, depuis tout lieu et vers toute destination, que ce soit dans le cloud public ou dans un data center privé. Contrairement aux VPN qui multiplient les risques en connectant les instances aux réseaux, Zero Trust Exchange étend la connectivité uniquement aux instances qui en ont besoin, conformément aux politiques de l'entreprise. Cette approche rend presque impossible la propagation des malwares ou le déplacement d'assaillants en interne sur un réseau.
- Elle inspecte tout le contenu, y compris le contenu chiffré par SSL, en appliquant des contrôles robustes qui défendent contre les cybermenaces et protègent les données.
- Elle rend les applications invisibles depuis Internet grâce à son architecture unique basée sur un proxy, ce qui élimine la surface d'attaque externe. Elle vérifie l'identité d'une entité et détermine le contexte de la demande d'accès avant d'accorder (ou d'interdire sous conditions) l'accès.
- Elle s'intègre avec les solutions de fournisseurs de sécurité et d'applications informatiques, ce qui permet d'assurer des déploiements à l'échelle mondiale. Il s'agit notamment de solutions de gestion des identités, de détection et de réponse aux menaces sur les endpoints, ainsi que des outils de sécurité et d'opérations informatiques, des applications SaaS, des plateformes de SD-WAN, etc.

Cette architecture est spécialement conçue pour offrir des expériences utilisateur optimales à grande échelle. Contrairement aux architectures traditionnelles où l'ensemble du trafic est routé vers un data center pour y être inspecté, Zero Trust Exchange procure une connectivité directe vers n'importe quel cloud ou URL Internet. Le trafic est intelligemment acheminé vers le site Zscaler le plus proche (parmi 150 data centers répartis dans le monde entier qui disposent de relations de peering avec les principaux fournisseurs de cloud tels qu'AWS et Microsoft Azure), garantissant ainsi le chemin de communication le plus court, quel que soit l'endroit où les applications sont hébergées. Tout le contenu est analysé en un seul passage ; il n'est donc pas nécessaire de copier les paquets, ce qui ajouterait de la latence.

La plateforme élimine également les inefficacités opérationnelles qui résultent de la complexité. Toutes les applications SaaS, Internet et privées peuvent être sécurisées au sein d'une seule plateforme, ce qui dispense de conserver plusieurs appareils de sécurité matériels ou virtuels. Une plateforme Zero Trust unifiée et cloud native se configure rapidement, se gère facilement et est beaucoup plus évolutive que les solutions de sécurité périmétrique. L'application inline des politiques simplifie également grandement le processus de transposition des règles métiers en politiques de réseau.

Cette approche réduit les coûts associés à la transformation numérique. Les équipes de sécurité n'ont plus besoin de budgétiser ni planifier l'acquisition de pare-feu, de solutions VPN ou de réseaux MPLS coûteux assortis de besoins complexes en matière de routage, de commutation et de segmentation du réseau. Zero Trust Exchange réduit également les délais de déploiement de plusieurs mois à quelques jours, tout en accélérant la capacité de l'entreprise à détecter et à prévenir les violations de données qui pourraient s'avérer particulièrement onéreuses.

Zero Trust Exchange est une plateforme complète offrant une large gamme de fonctionnalités, ce qui permet d'éviter le déploiement de plusieurs produits de sécurité distincts :

- **Protection contre les cybermenaces :** les utilisateurs, les instances et les appareils se trouvent en aval de la plateforme, ce qui les rend invisibles depuis l'Internet public. Ne pouvant être identifiés, ils ne présentent aucune surface d'attaque exploitable. De plus, la plateforme inspecte tout le trafic, en utilisant une protection contre les menaces avancées, grâce au Machine Learning, pour empêcher toute compromission.
- **Protection des données :** Zero Trust Exchange sécurise les données sur les environnements IaaS/PaaS, le SaaS, la messagerie électronique et les endpoints. La prévention des pertes de données est assurée par une classification avancée de celles-ci et à une inspection inline du trafic sortant.
- **Connectivité Zero Trust :** les réseaux traditionnels sont ouverts, ce qui signifie qu'une fois que vous y avez accès, vous pouvez vous déplacer sur la totalité de leur périmètre. Zero Trust Exchange modifie fondamentalement la nature de la connectivité réseau en connectant les utilisateurs aux applications plutôt qu'aux réseaux, ce qui rend les déplacements internes tout simplement impossibles.
- **Gestion de l'expérience digitale :** Zero Trust Exchange surveille l'expérience utilisateur de bout en bout, des endpoints aux applications. Son moteur IA inline peut identifier l'origine des problèmes, ce qui permet aux équipes informatiques de les résoudre de manière proactive.

Conclusion

Zero Trust Exchange favorise une architecture Zero Trust transparente, sécurisée *et* économique, sans avoir à faire de compromis. Cette solution se différencie de par son architecture qui permet aux entreprises de :

- Supprimer la surface d'attaque. Les applications étant invisibles depuis l'Internet public, elles n'offrent aucune surface d'attaque externe.
- Fournir une expérience utilisateur optimale à grande échelle. Avec 150 data centers répartis dans le monde entier et des relations de peering avec les principaux fournisseurs de clouds, Zero Trust Exchange gère et optimise intelligemment les connexions directes vers n'importe quel cloud ou destination Internet, sans backhauling du trafic. Ceci garantit une latence minimale et des performances de premier ordre.
- Supprimer les inefficacités opérationnelles liées à la complexité, grâce à une approche de plateforme unifiée et multifonction.
- Réduire le coût de la transformation numérique.
- Supprimer la prolifération d'appliances et de produits de sécurité distincts.

Zero Trust Exchange est conforme aux exigences architecturales des normes de Zero Trust connues, notamment le NIST 800-207 et les frameworks SASE et SSE de Gartner. Éprouvé à l'échelle mondiale, Zero Trust Exchange est le plus grand cloud de sécurité au monde, traitant plus de 250 milliards de transactions par jour. Ainsi, les moteurs de machine learning peuvent être entraînés sur davantage de données (par rapport à d'autres plateformes), rendant ainsi la détection des menaces plus précise. Il est possible de neutraliser les menaces les plus sophistiquées, de manière transparente vis-à-vis des utilisateurs, sans impact sur leur productivité. En tant que plateforme cloud complète, Zero Trust Exchange permet aux entreprises de toutes tailles de concevoir une architecture Zero Trust rapide, fiable et facile à gérer, tout en réduisant le coût et la complexité associés à l'utilisation de produits de sécurité distincts.

Source : 1. Nathan Howe, Sanjit Ganguli et Gerard Festa, Seven Elements of Highly Successful Zero Trust Architectures, Second Edition, deuxième édition, août 2022.

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