zscaler™

LA CONFIANCE SE CONSTRUIT DE ZÉRO

Trois stratégies pour accélérer la transformation de votre entreprise

Réinventer le succès à l'ère du digital.

Il n'a jamais été aussi impératif d'accélérer la transformation digitale de votre entreprise pour...

- Construire un avantage concurrentiel à long terme
- Rendre l'entreprise plus agile
- Offrir une expérience utilisateur optimale

Que vous soyez DSI, RSSI, responsable des réseaux, responsable de la sécurité ou leader de l'infrastructure informatique, aider l'entreprise à accélérer sa transformation avec sérénité et en toute sécurité est une priorité absolue. L'ancienne infrastructure de réseau et de sécurité était efficace par le passé, mais elle fait désormais obstacle à la transformation.

Au fur et à mesure que votre entreprise se transforme, elle évolue vers un monde axé sur le cloud où votre écosystème de clients, de partenaires, d'employés, d'applications et de données convergent en utilisant Internet comme tissu d'interconnexion. Dans ce monde, la sécurité doit être assurée via le cloud, à proximité de votre écosystème d'entreprise, en utilisant les principes de Zero Trust pour rendre le cloud sûr.

C'est pourquoi la transformation commence de zéro.
Découvrez comment. →

SIEMENS

TÉMOIGNAGES DE CLIENTS

« Le cloud sera notre nouveau data center et Internet notre nouveau réseau. Nous avons réduit les coûts de mise en réseau de 70 %. »

— Frederik Janssen, VP de la stratégie informatique, Siemens

VISUALISATION

Scruter l'avenir du travail.

Internet est la **nouvelle couche de connectivité** :

4,6x

croissance (2016–2021)[1]

Le cloud est le **nouvel eldorado** :

220x

croissance (2016–2021)[1]

Les affaires se déroulent partout, **sur n'importe quel appareil** :

1,4B

d'appareils 5G d'ici 2023[2]

Croissance exponentielle de serveurs, IoT et **du trafic OT** :

50 %

de tous les appareils connectés d'ici 2023[2]

Sources : 1. Principales prévisions Cisco VNI (2016-2021). 2. Rapport annuel sur Internet de Cisco (2018-2023).

Surmonter les obstacles à la transformation.

La transformation et la connectivité cloud bouleversent 30 années de pratiques en matière de mise en réseaux et de sécurité informatiques. L'infrastructure ancienne était centrée sur la construction de réseaux privés pour connecter les filiales et les utilisateurs aux applications dans le data center. Tout le trafic s'acheminait vers le data center et les affaires se déroulaient sur un réseau privé fiable. Ce modèle-là n'existe plus.

Tenter d'adapter des architectures de réseau et de sécurité obsolètes aux exigences d'une entreprise moderne, axée sur le cloud, constitue un obstacle à la transformation.

OBSTACLES À LA TRANSFORMATION		STRATÉGIES POUR LES SURMONTER
Coût opérationnel exorbitant Les réseaux d'entreprise traditionnels utilisent un modèle en étoile, et les bureaux et filiales sont souvent connectés aux emplacements centraux comme le data center à l'aide de liaisons WAN MPLS coûteuses. Les utilisateurs en dehors du bureau utilisent généralement le VPN pour accéder au réseau. Cette méthode est onéreuse, lente et ajoute une complexité opérationnelle.	→	**Faites d'Internet votre nouveau réseau** en allant directement vers le cloud page 6
Risque Le transfert des activités vers Internet élargit considérablement la surface d'attaque et rend archaïque la sécurité traditionnelle des réseaux. Les anciennes infrastructures de sécurité telles que les VPN de site à site perpétuent un mouvement latéral des menaces, créant ainsi un énorme risque d'infection.	→	**Adoptez Zero Trust** pour sécuriser le cloud page 7
Expérience médiocre Les architectures actuelles de réseau et de sécurité reposent sur des backhauling vers le data center, ce qui introduit des problèmes de latence qui ont un impact sur la productivité et offrent une mauvaise expérience des applications cloud. Il est également difficile de surveiller l'expérience utilisateur ou de résoudre les problèmes de performance dans des architectures réseau complexes.	→	**Mettez la mobilité au service de votre entreprise,** grâce à un accès plus rapide et à une meilleure expérience utilisateur page 9

STRATÉGIE

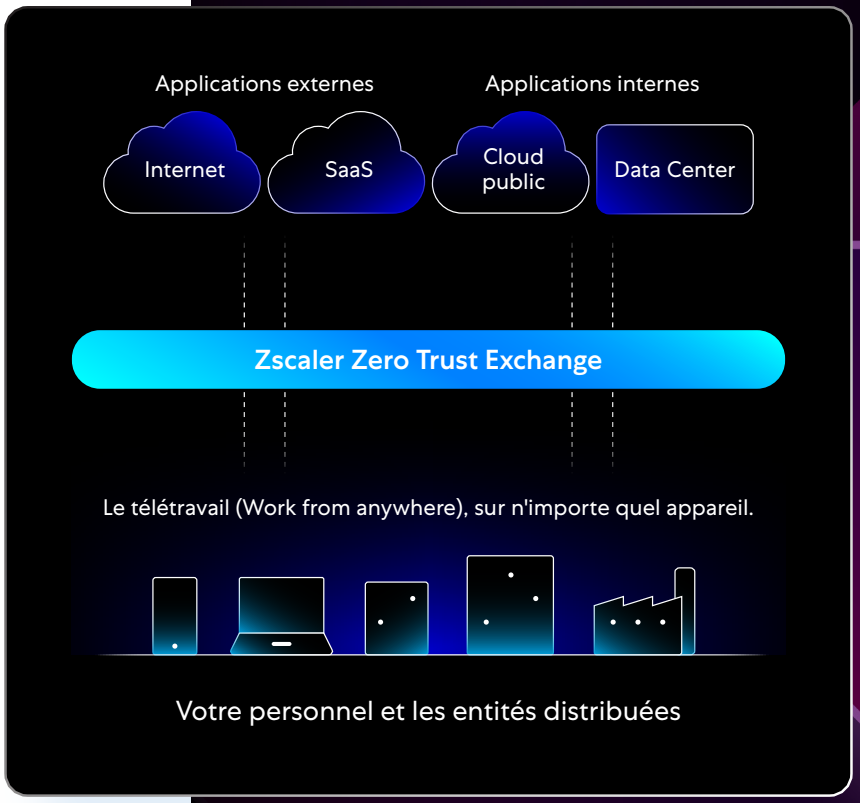
Faites d'Internet votre nouveau réseau.

Au fur et à mesure que les applications migrent du data center vers le cloud, vous devez commencer à transformer votre réseau, du modèle en étoile vers un modèle Direct-to-cloud. Grâce à une approche sécurisée et Direct-to-cloud, vous pouvez considérablement réduire les coûts et la complexité tout en améliorant l'agilité et la réactivité informatiques de l'entreprise. Finies les frictions. Plus question d'attendre les connexions réseau pour accéder aux applications cloud.

Zscaler rend cela possible. Avec **Zscaler Zero Trust Exchange**, vous pouvez :

- ✓ Réduire les coûts et la complexité en déplaçant la sécurité vers le cloud, éliminant ainsi le besoin d'un périmètre traditionnel de sécurité
- ✓ Offrir une bien meilleure expérience utilisateur en vous connectant directement aux applications cloud
- ✓ Éliminer la surface d'attaque d'Internet avec des applications qui se trouvent derrière la plate-forme Zero Trust Exchange, empêchant ainsi la découverte et les attaques ciblées
- ✓ Empêcher le mouvement latéral des menaces en connectant les utilisateurs directement aux applications, sans accès au réseau

Vous pouvez accomplir cette opération en plusieurs étapes, au fil du temps, en réduisant les coûts MPLS et en éliminant des infrastructures telles que les pare-feux dans les filiales lorsque vous transformez votre réseau.



En savoir plus sur la façon de moderniser votre réseau

STRATÉGIE

Adoptez Zero Trust.

Pour accélérer la transformation en toute sérénité, vous devez également transformer votre approche de la sécurité en commençant de zéro. Au lieu de la sécurité réseau traditionnelle aujourd'hui passée de mode, l'approche Zero Trust — qu'intègre merveilleusement **Zscaler Zero Trust Exchange** — connecte en toute sécurité les applications et les utilisateurs sur Internet en fonction des politiques de l'entreprise, pour :

- ✓ Éliminer la surface d'attaque d'Internet
- ✓ Réduire les mouvements latéraux sur le réseau
- ✓ Juguler les menaces cachées et la perte de données
- ✓ Empêcher les infections de type patient zéro

Zscaler Zero Trust Exchange s'appuie sur trois principes pour connecter en toute sécurité les utilisateurs, les appareils et les applications à l'aide de politiques d'entreprise, et ce sur n'importe quel réseau :

1. **Accès aux applications sans accès au réseau :** sur la base de l'identité, connecter les utilisateurs et les applications aux ressources, et non au réseau d'entreprise.
2. **Surface d'attaque réduite à zéro :** rendre les applications invisibles sur Internet afin d'éliminer la surface d'attaque et d'obtenir l'isolation des applications sans qu'une segmentation de réseau ne soit nécessaire.
3. **Architecture proxy :** utiliser une architecture proxy, et non un pare-feu de type « passthrough », pour toutes les connexions aux applications, afin d'améliorer la protection des données et se prémunir contre la cybermenace.

PRINCIPAUX CONCEPTS DU ZERO TRUST

Le modèle Zero Trust repose sur les principes d'accès basé sur le moindre privilège et sur le fait qu'**aucune entité (utilisateur ou application) ne devrait de but en blanc être tenue pour fiable.**

Plutôt que d'autoriser l'accès à un réseau, une stratégie Zero Trust utilise l'identité d'une entité et la politique commerciale pour accorder l'accès à des ressources spécifiques. Les politiques comprennent **quatre éléments clés (utilisateur, appareil, application et contenu)** et sont appliquées par la plate-forme Zero Trust Exchange.

En savoir plus sur Zscaler Zero Trust Exchange

VISUALISATION

Accroître l'adoption de Zero Trust.

Les contrôles **ZTNA (Zero trust network access)** et **CASB (Cloud Access Security Broker)** seront les deux principales technologies Zero Trust dans lesquelles les entreprises prévoient d'investir au cours des 12 à 18 prochains mois.

72 %

Entreprises dotées d'une stratégie Zero Trust

76 %

Entreprises ayant un nouveau budget alloué à Zero Trust

82 %

Entreprises qui augmenteront leurs dépenses en matière de technologies au cours des 12 à 18 prochains mois

Source : "The State of Zero-trust Security Strategies", John Grady, Enterprise Strategy Group, février 2021

STRATÉGIE

Stimuler la mobilité de l'entreprise.

En plus de faire du cloud un espace sécurisé pour les affaires, vous devez le rendre **agréable et productif** pour les utilisateurs. Offrir un accès sécurisé et direct au cloud élimine la latence inhérente aux architectures backhaul, VPN et VDI, améliorant ainsi l'expérience utilisateur et optimisant la productivité. La fourniture de services et de peering à la périphérie, près des utilisateurs, offre les performances les plus rapides possibles.

Pourtant, il ne suffit pas d'offrir une expérience utilisateur de qualité : vous avez également besoin d'une bonne visibilité sur les performances ainsi que d'un moyen d'identifier et de résoudre rapidement les problèmes qui pourraient avoir un impact sur l'expérience. Zscaler vous offre une **visibilité totale** du terminal à l'application pour tous vos utilisateurs à travers le monde. Avec Zscaler, vous pouvez **identifier et résoudre les problèmes plus rapidement**, ce qui signifie beaucoup moins de demandes d'assistance informatique auxquelles votre équipe doit répondre.

Explorez d'autres ressources sur le télétravail

DES RÉSULTATS PROBANTS

La sécurité à la vitesse du cloud.

500

entreprises du Forbes Global 2000 font confiance à Zscaler

150 Md

demandes traitées quotidiennement dans le monde

plus de 10

années d'exploitation du plus grand cloud de sécurité inline

175k

mises à jour de sécurité uniques effectuées au quotidien

plus de 150

data centers sur 6 continents, avec peering dans les échanges Internet, rapprochant la sécurité de l'utilisateur pour une expérience rapide

7 Md

de menaces bloquées/ politiques appliquées au quotidien

POURQUOI ZSCALER ?

Choisir le partenaire idéal pour votre transition.

Peu importe où vous en êtes dans votre parcours de transformation, Zscaler peut vous aider à l'accélérer en toute sérénité. Zscaler offre les éléments, l'infrastructure et les outils pour protéger l'entreprise moderne tout en préservant la productivité des utilisateurs.

- **Architecture Zero Trust native du Cloud,** fonctionnant à la périphérie à travers 150 data centers dans le monde entier
- **L'IA et des analyses des données robustes** fournissent contrôle et visibilité via Cloud Sandbox, sécurité DNS, antivirus, protection avancée contre les menaces, IPS et isolation du navigateur
- **Utilisateurs directement connectés aux ressources dont ils ont besoin** via une politique dynamique : aucune segmentation complexe n'est requise, ni la moindre exposition inutile, et aucun mouvement sans restriction n'est nécessaire dans quelque direction que ce soit pour contrer les attaques
- **L'inspection SSL inline complète à grande échelle,** associée à la pile de sécurité complète de Zscaler, offrent une protection améliorée, dénuée des limitations d'inspections des appliances
- **Première équipe mondiale de recherche sur les menaces dans le cloud :** notre équipe de chercheurs s'attache à identifier de nouvelles vulnérabilités et à apporter des améliorations constantes à tous les clients
- **Une expérience utilisateur continue, stable et sans tracas** avec une vitesse/performance améliorée des applications, peu importe l'emplacement de vos utilisateurs
- **Tableaux de bord et rapports robustes,** et flux de journaux cloud à cloud qui s'intègrent à d'autres outils et flux de travail SecOps

LA CONFIANCE SE CONSTRUIT DE ZÉRO

Accélérez votre migration vers le cloud avec Zscaler Zero Trust Exchange.

En savoir plus

Zscaler (NASDAQ : ZS) accélère la transformation numérique pour permettre aux entreprises d'améliorer leur agilité, leur efficacité, leur résilience et leur sécurité. Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte de données en connectant en toute sécurité les utilisateurs et les applications, n'importe où et sur n'importe quel appareil. Répartie sur plus de 150 datacenters à travers le globe, Zero Trust Exchange, qui repose sur le modèle SASE, est la plus grande plate-forme de sécurité en mode cloud au monde.

zscaler™