



L'essentiel sur Zscaler™ SSE

Avantages de Zscaler Security Service Edge (SSE)

Maîtrise des coûts et de la complexité informatiques

Cette solution est simple à déployer et à gérer en tant que service automatisé, évolutif et fourni depuis le cloud.

Accès Zero Trust

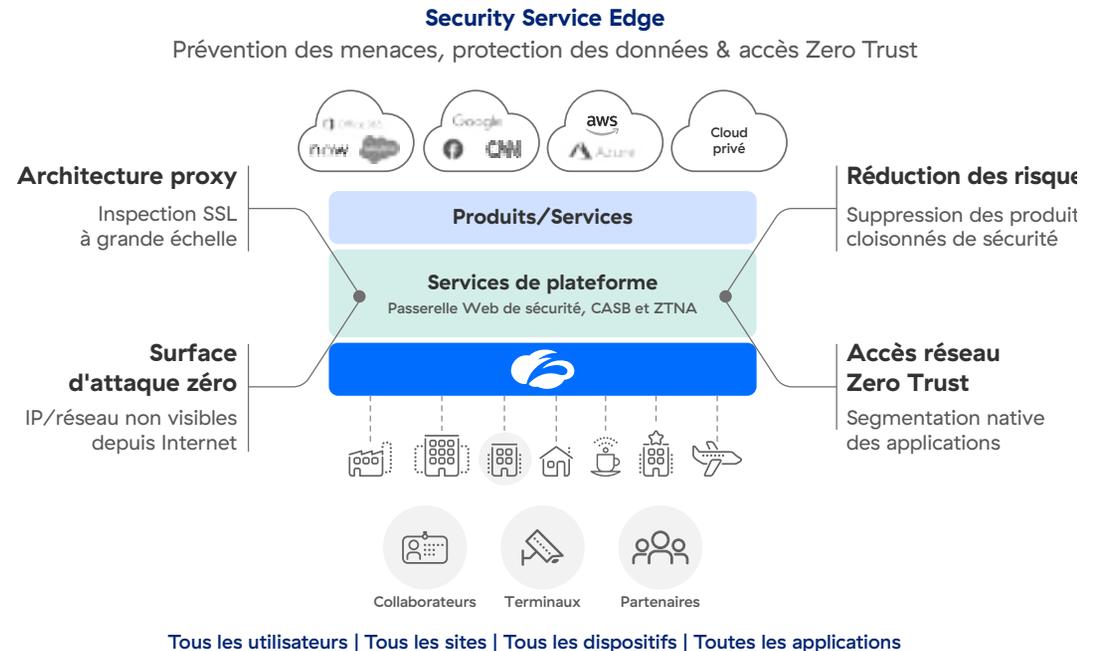
L'accès sur la base du moindre privilège permet un accès à distance plus sécurisé, sans positionner l'utilisateur sur le réseau.

Maîtrise des risques

La protection contre les menaces et la protection des données sont consolidées au sein d'un service de sécurité cloud qui inspecte le trafic chiffré de tous les utilisateurs et sites.

Pour juguler les risques liés aux incidents de cybersécurité et aux ransomwares, les entreprises recherchent de nouveaux et meilleurs moyens de sécuriser leurs opérations, en allant au-delà de la sécurité réseau traditionnelle.

Les pare-feu et les VPN ont été conçus en intégrant l'idée du périmètre réseau. Or ce périmètre est de moins en moins pertinent dans la réalité actuelle de la mobilité et du cloud.



Les données sont aujourd'hui disséminées en dehors du data center, dans des applications cloud. De leur côté, les utilisateurs sont souvent à l'extérieur du réseau d'entreprise et accèdent à des contenus qui sont également hors de ce réseau. Gartner a élaboré un framework qui définit les services de sécurité nécessaires dans le contexte actuel : le Security Service Edge (SSE). Le SSE revisite les fondamentaux de la sécurité en supprimant la confiance implicite accordée aux utilisateurs qui accèdent à Internet, aux services SaaS et aux applications privées.

Zero Trust Exchange de Zscaler est une plateforme SSE conçue pour maîtriser les risques, améliorer les performances et renforcer l'évolutivité. En tant que plateforme multisite, disponible à l'échelle mondiale, Zscaler veille à déployer une sécurité auprès de tous les utilisateurs et tous les sites, avec une expérience utilisateur optimale. Zscaler SSE va au-delà de la sécurisation des utilisateurs en protégeant également les instances, les dispositifs et les tiers qui accèdent aux ressources. En tirant parti d'un service qui consolide différentes fonctionnalités (Secure Web Gateway – SWG, Cloud Access Security Broker – CASB et Zero Trust Network Access – ZTNA), les entreprises maîtrisent leurs coûts et la complexité tout en renforçant leur posture de cybersécurité.

Fonctionnalités clés



Architecture cloud-first

La plateforme cloud SSE de Zscaler accélère et sécurise la transformation numérique grâce à une approche transparente qui consolide les services de sécurité et les fournit de manière simple depuis le cloud. Zscaler propose une plateforme unifiée qui capitalise sur l'IA pour réduire les risques, en sécurisant les utilisateurs, les instances, les dispositifs IoT/OT et les tiers.



Inspection SSL en mode inline, à grande échelle

La majorité du trafic sur Internet étant désormais chiffrée, vous avez besoin d'une architecture basée sur un proxy pour inspecter le trafic SSL à grande échelle, vous protéger efficacement contre les menaces et prévenir les pertes de données.



Une sécurité rapide et cohérente

Les services de sécurité sont positionnés à proximité des utilisateurs, dans un cloud multisite et mondial qui propose plus de 150 points de présence. Toutes les connexions utilisateur-application sont gérées par une seule politique. Elles sont protégées contre les menaces et contre la perte des données, sans impact sur l'expérience utilisateur.



Accès réseau Zero Trust

Zscaler propose un accès aux applications centré sur l'utilisateur et l'application. En tant que service entièrement fourni depuis le cloud, Zscaler assure une segmentation native des applications en appliquant des politiques d'entreprise qui connectent un utilisateur authentifié à une application autorisée, sans que cet utilisateur ne dispose d'un accès illimité au réseau.



Suppression de la surface d'attaque

Les hackers ne peuvent cibler ce qu'ils ne peuvent pas voir. C'est la raison pour laquelle Zscaler Zero Trust Exchange évite de rendre les applications privées visibles depuis Internet. Cette approche élimine cette surface d'attaque généralement générée par les outils réseau traditionnels qui exposent les entreprises à des risques d'incident.

« Le SSE prend en charge les collaborateurs hybrides, où qu'ils se trouvent et à tout moment, en privilégiant une approche orientée cloud pour appliquer la politique de sécurité. »

– Gartner

 | **Experience your world, secured.™**

Zscaler (NASDAQ : ZS) accélère la transformation digitale et permet à ses clients de gagner en agilité, productivité, 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 dispositifs et les applications, quel que soit leur emplacement. Adossé à plus de 150 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.fr ou suivez-nous sur Twitter @zscaler.

©2024 Zscaler, Inc. Tous droits réservés. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIAT™, Zscaler Private Access™, ZPA™ et les autres marques commerciales répertoriées sur zscaler.fr/legal/trademarks sont soit 1) des marques déposées ou marques de service, soit 2) des marques commerciales ou marques de service de Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques appartiennent à leurs propriétaires respectifs.