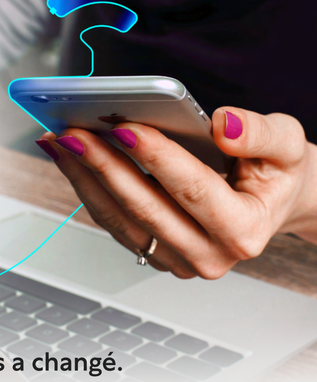
INFOGRAPHIE

Les pare-feu et les VPN ne sont pas conçus pour le modèle Zero Trust

Donner les moyens à vos effectifs à distance et les protéger exige une nouvelle approche de la sécurité.



La façon dont nous travaillons a changé.

Vos utilisateurs, vos données et vos applications sont partout.

300 %
augmentation du pourcentage de l'ensemble des employés qui sont des utilisateurs distants.[1]

50 %
de toutes les données d'entreprise sont stockées dans le cloud.[2]

70 %
des applications professionnelles utilisées aujourd'hui par les sociétés sont basées sur le SaaS.[3]

La sécurité ne devrait-elle pas également changer ?

Protéger le périmètre et faire confiance à ce qui se trouve à l'intérieur du réseau fonctionnait bien lorsque tout se trouvait sur site. Mais aujourd'hui, le périmètre a disparu et les anciennes méthodes de sécurisation du réseau ne fonctionnent plus.

des entreprises estiment qu'elles doivent améliorer leur sécurité pour mieux protéger les équipes sur site et à distance.[4]

des sociétés privilégient l'adoption d'un modèle Zero Trust.[5]

La solution : Zero Trust.

Pour que les entreprises puissent accueillir la main-d'œuvre moderne et demeurer agiles et compétitives, les architectures de sécurité doivent évoluer. Il est temps de passer à une solution qui autorise les connexions en fonction du contexte et des politiques pour chaque session, de chaque utilisateur à chaque application, partout.

Mais les pare-feu et les VPN ne peuvent pas assurer la confiance zéro ou le Zero Trust. Pourquoi ?

Les menaces peuvent accéder au réseau et s'y déplacer facilement, car les pare-feu nécessitent toujours que les utilisateurs et les appareils soient connectés au réseau pour accéder aux applications.

Les applications sont publiées sur Internet, ce qui augmente votre surface d'attaque.

Les architectures de pare-feu passthrough ne laissent qu'une capacité limitée pour inspecter le trafic et protéger les données.

des entreprises ne sont pas convaincues que leurs technologies existantes peuvent les aider à instaurer le modèle Zero Trust.[5]

des entreprises feront confiance à tort à leurs technologies existantes et placeront des utilisateurs sur le réseau de l'entreprise.[5]

Le modèle Zero Trust requiert une approche fondamentalement différente.

Contrairement aux approches traditionnelles qui font confiance à tout ce qui se trouve à l'intérieur du périmètre du réseau, le modèle Zero Trust est fondé sur le principe de l'accès sur la base du moindre privilège et sur le concept qu'aucun utilisateur ou application n'est intrinsèquement fiable. Une véritable solution Zero Trust connecte en toute sécurité les applications et les utilisateurs sur Internet sur la base de politiques d'entreprise afin de :

Éradiquer le mouvement latéral
Connecter directement les utilisateurs et les appareils aux applications, jamais au réseau.

Minimiser la surface d'attaque
Rendre les utilisateurs et les applications invisibles sur Internet. S'ils ne peuvent pas être découverts, il n'existe pas de surface d'attaque à exploiter.

Stopper les menaces et les pertes de données
Fournit une inspection complète, y compris du trafic chiffré, pour une protection efficace contre les cybermenaces et la perte de données.

Zscaler : le leader du Zero Trust.

Bâti sur le plus grand cloud sécurisé de la planète, Zscaler Zero Trust Exchange aide les équipes informatiques à adopter le modèle Zero Trust pour réduire les risques, accroître l'agilité de l'entreprise et proposer une expérience utilisateur exceptionnelle.

Chaque jour, Zscaler Zero Trust Exchange :

SÉCURISE PLUS DE 200 MILLIARDS
de transactions

PRÉVIENT PLUS DE 7 MILLIARDS
d'incidents de sécurité et de violations de politiques

TRAITE PLUS DE 200 000
mises à jour de sécurité uniques

Commencez votre parcours Zero Trust avec Zscaler.

Zscaler a aidé plus de 5 000 sociétés à se transformer en toute sécurité grâce à Zero Trust.

Nous pouvons également vous aider.

Découvrir comment

1. *Grady, John. (2021). L'état des stratégies de sécurité Zero Trust. Enterprise Strategy Group. https://info.zscaler.com/resources-industry-report-the-state-of-zero-trust-security-strategies*
2. *Statista. Pourcentage de données et de données sensibles stockées dans le cloud à l'échelle mondiale. https://www.statista.com/statistics/1202541/sensitive-data-cloud-location*
3. *Better Cloud. (2021). L'état des SaaSOps 2021. https://stateofsaasops.bettercloud.com/?_ga=2.154979740.241347013.1636678142-1969514686.1636678142*
4. *IDG Marketpulse Survey. (2020). Approches de la sécurité des réseaux et la valeur de Zero Trust. https://info.zscaler.com/industry-report-leading-ciso-and-it-leaders-see-it-future-in-zero-trust*
5. *Cybersecurity Insiders. (2021). Rapport sur les risques liés aux VPN. https://info.zscaler.com/resources-industry-reports-vpn-risk-report-cybersecurity-insiders*

©2021 Zscaler, Inc. Tous droits réservés. Zscaler™, Zscaler Zero Trust Exchange™, Zscaler Internet Access™, Zscaler Private Access™, ZIA™, ZPA™ et Zscaler B2B™ sont soit (1) des marques déposées ou des marques de service, soit (2) des marques déposées ou des marques de service de Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales sont la propriété de leurs détenteurs respectifs.

Zscaler, Inc.
120 Holger Way
San José, Californie
+1 408 533 0288
www.zscaler.fr