Le RSI du Zero Trust

5 aspects de la réduction de votre surface d'attaque à l'aide d'une stratégie de sécurité Zero Trust qui permettent à votre entreprise d'économiser du temps et de l'argent

CLOUDFLARE

01 Réduction de la surface d'attaque

D'après les hypothèses formulées par Gartner, les entreprises qui isolent la navigation à haut risque des systèmes des utilisateurs finaux et séparent l'accès aux applications des réseaux constateront une réduction de 91 % du nombre d'attaques susceptibles d'atteindre leur environnement.[1]

02 Réduction des coûts de violation

Une surface d'attaque réduite garantit une protection plus efficace contre les agressions destructrices, comme les violations de données. D'après le rapport d'IBM Cost of a Data Breach (Coût d'une violation de données), les entreprises matures en termes de niveau d'adoption du modèle Zero Trust dépensent moins pour récupérer de telles violations, avec 3,28 millions de dollars contre 5,04 millions pour les entreprises sans stratégie Zero Trust.[2]

03 Accélération de l'intégration

Lorsque l'adoption du modèle Zero Trust va de pair avec le remplacement des approches traditionnelles en matière d'accès à distance, comme le VPN et les contrôles basés sur IP, les clients Cloudflare du type d'eTeacher Group signalent qu'ils passent moins de temps à intégrer les nouveaux utilisateurs, avec une réduction de l'ordre de 60 % du temps nécessaire à la configuration d'un accès pour un nouvel utilisateur.

04 Réduction des tickets informatiques

Lorsque les utilisateurs n'ont pas besoin de gérer un VPN sur leur appareil, les entreprises constatent une diminution significative du temps passé à répondre aux tickets informatiques liés aux problèmes d'accès. Certaines signalent ainsi une réduction pouvant atteindre 80 %.

05 Réduction de la latence

L'adoption du modèle Zero Trust pour la navigation Internet et l'accès aux applications a une incidence considérable sur la vitesse de connexion de votre entreprise. Elle évite le « hairpinning » du trafic vers un datacenter éloigné des utilisateurs ou des ressources. De plus, lorsque les utilisateurs se connectent à ces dernières via le réseau Cloudflare plutôt que par les chemins Internet par défaut, les applications web publiques et privées se chargent 30 % plus vite et profitent d'un temps TCP aller-retour 17 % plus rapide.

Démarrez en moins de 30 minutes

Déployez sans effort

Terminez avec un des meilleurs RSI par rapport au temps investi

Réduction de la surface d'attaque

Réduction des coûts de violation

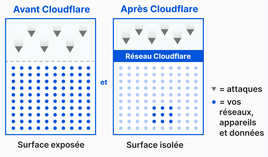
Accélération de l'intégration

Réduction des tickets informatiques

Réduction de la latence

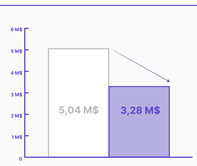
Implique des couches de protection intégrées contre les menaces suivantes :

- mouvements latéraux des logiciels malveillants
- rançongiciels
- phishing
- vulnérabilités du VPN
- attaques sur la chaîne d'approvisionnement ou par contournement de la MFA

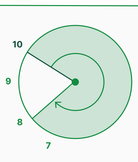


91 %
Minimise le taux d'attaques réussies de jusqu'à 91 %

30 %
Rend la connexion aux applications et aux services 30 % plus rapide



35 %
Réduit le coût moyen d'une violation de données de 35 %, de 5,04 M$ à 3,28 M$



Avant : 10 h/semaine
Après : 2 h/semaine
8 heures économisées pour 800 utilisateurs

80 %
Diminue jusqu'à 80 % le temps passé à répondre aux tickets liés à l'accès à distance

60 %
Accélère le temps d'intégration d'un nouveau collaborateur de jusqu'à 60 %

01 | 02 | 03

Démarrez en moins de 30 minutes

La plate-forme de sécurité Zero Trust de Cloudflare améliore la visibilité, élimine la complexité et réduit les risques liés à la connexion aux applications et à Internet par vos collaborateurs.
30 minutes de configuration suffisent pour vous lancer.

Déployez sans effort

Diffusez rapidement vos politiques de sécurité Zero Trust à de nouveaux utilisateurs à travers le monde, car les services Zero Trust de Cloudflare se déploient de manière cohérente dans chacune des 250 villes composant notre réseau mondial.

Terminez avec un des meilleurs RSI par rapport au temps investi

Soutenez votre vaste gamme de types d'applications et de protocoles grâce à un processus d'intégration facile et rapide. Vous n'aurez jamais besoin de gérer la bande passante manuellement ou de payer plus suite à l'augmentation du nombre de vos requêtes.

Prêts à vous lancer ?

Cliquez ici

[1]Réunit les hypothèses de deux publications Gartner : « Innovation Insight for Remote Browser Isolation », 8 mars 2018, et « It's Time to Isolate Your Services From the Internet Cesspool », 17 novembre 2017
[2]IBM, rapport Cost of a Data Breach, 2021

+33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/