Sept éléments d'une architecture Zero Trust extrêmement efficace

Guide de l'architecte pour Zero Trust Exchange de Zscaler

Les architectures de sécurité traditionnelles exposent les entreprises à des risques

Les approches de sécurité standard, qui font appel aux pare-feu et aux VPN, connectent les utilisateurs au réseau, ce qui permet aux hackers de compromettre les utilisateurs, les appareils et les charges de travail, et de se déplacer latéralement pour atteindre des ressources de grande valeur et extraire des données sensibles.

L'environnement de travail hybride moderne exige une approche de la sécurité basée sur le principe de Zero Trust

Pour protéger leurs entreprises, les dirigeants innovants se tournent vers Zero Trust, une solution de sécurité globale qui repose sur l'accès sur la base du moindre privilège et l'idée qu'aucun utilisateur ou application ne devrait être intrinsèquement considéré comme fiable.

Comment une architecture Zero Trust est-elle mise en œuvre ?

La véritable solution Zero Trust est fournie par **Zscaler Zero Trust Exchange**, une plateforme intégrée cloud native qui connecte en toute sécurité les utilisateurs, les appareils (IoT/OT) et les charges de travail aux applications sans se connecter au réseau.

Sept éléments forment la base d'une véritable architecture Zero Trust

Grâce à cette approche unique, Zscaler élimine la surface d'attaque, empêche le déplacement latéral des menaces et protège votre entreprise contre la compromission et la perte de données.

1. Qui se connecte ?

Met fin à la connexion demandée, puis vérifie l'identité de l'utilisateur, de l'appareil IoT/OT ou de la charge de travail.

2. Quel est le contexte de l'accès ?

Valide le contexte du demandeur de connexion en examinant des attributs tels que le rôle, la responsabilité, le moment et les circonstances de la demande.

3. Où va la connexion ?

Confirme que la destination est connue, comprise et catégorisée contextuellement pour l'accès. Si la destination est inconnue, sollicite une analyse plus approfondie.

4. Évaluer le risque

Fait appel à l'IA pour calculer dynamiquement un score de risque associé à la connexion en fonction de facteurs tels que la posture de l'appareil, les menaces, la destination, le comportement et la politique.

5. Prévenir toute compromission

Inspecte le trafic et le contenu inline afin d'identifier et de bloquer les contenus malveillants.

6. Empêcher la perte de données

Inspecte le trafic sortant afin d'identifier les données sensibles et d'empêcher leur exfiltration.

7. Appliquer la politique

Applique la politique par session et détermine l'action conditionnelle à prendre concernant la connexion demandée. Une fois qu'une décision « d'autorisation » est prise, une connexion sécurisée à Internet, à une application SaaS ou à une application interne est établie.

Êtes-vous prêt à découvrir comment appliquer les sept éléments fondamentaux d'une conception Zero Trust à votre entreprise afin **d'éliminer votre surface d'attaque, d'empêcher le déplacement latéral des menaces** et **de protéger votre entreprise contre la compromission et la perte de données ?**

Consultez l'e-Book

Experience your world, secured.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408 533 0288
www.zscaler.fr