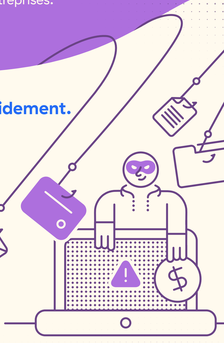
Zero Trust :
La base d'un environnement professionnel sécurisé

Les analystes d'IDC se sont récemment penchés sur l'avenir du modèle Zero Trust et ont partagé leurs réflexions sur l'impact qu'il aura sur la sécurité des entreprises.

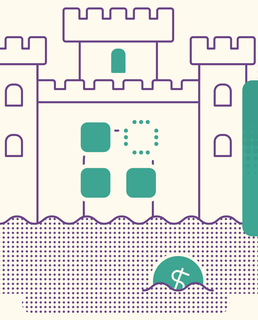


Le paysage des menaces s'accélère rapidement.

80 % d'augmentation des attaques par ransomware au cours de l'année écoulée[1]

314 % d'augmentation des attaques sur des canaux chiffrés[2]

436 % d'augmentation des attaques par hameçonnage dans les secteurs du commerce de détail et de la vente en gros[3]

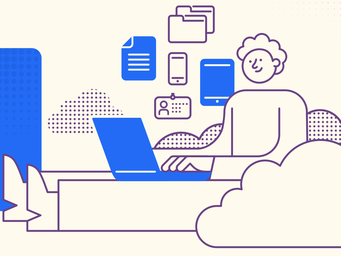


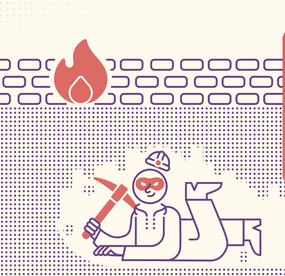
Les architectures de sécurité basé sur le périmètre ont été conçues pour le passé.

La sécurité basée sur le périmètre a été conçue pour une époque où les employés travaillaient principalement au bureau d'où ils accédaient aux applications et aux ressources dans le data center.[4]

L'espace de travail hybride moderne est beaucoup plus complexe.

Les utilisateurs travaillent partout, utilisent plusieurs appareils et accèdent à des données et des applications réparties dans des SaaS, des data centers et des clouds publics.





Les défenses d'hier sont insuffisantes.

Les pare-feu, les pare-feu virtuels, les VPN et autres défenses axées sur le périmètre sont incapables d'arrêter les menaces dynamiques et persistantes.[4]

Les entreprises modernes ont besoin d'une approche nouvelle.

Les entreprises se tournent vers le modèle Zero Trust pour relever ces défis. Contrairement aux approches de sécurité basées sur le périmètre, Zero Trust repose sur le principe de l'accès sur la base du moindre privilège et sur l'idée qu'aucun utilisateur ou application ne devrait être intrinsèquement considéré comme fiable.

Éléments fondamentaux de Zero Trust

Zero Trust n'est pas une simple technologie ; il s'agit d'une stratégie qui constitue le cœur de votre écosystème de sécurité. Selon IDC, Zero Trust se compose de six éléments clés[4] :

- **Autorisation granulaire**
- **Identité et authentification robustes**
- **Politiques basées sur le contexte**
- **Application universelle de Zero Trust**
- **Détection/protection permanente des menaces**
- **Accès basé sur le « besoin de savoir » uniquement**

Avantages de l'adoption du Zero Trust

Une architecture Zero Trust permet aux entreprises d'atténuer les risques commerciaux tout en **réduisant les coûts, en simplifiant l'informatique et en améliorant l'expérience utilisateur.**

Construire les bases de votre réussite

Découvrez comment une architecture Zero Trust établit une base sécurisée pour la transformation digitale.

Lire le dossier d'analyste d'IDC

[1] Zscaler, « Rapport 2022 de ThreatLabz sur l'état des ransomwares. »
[2] Zscaler, « Rapport 2021 de ThreatLabz sur l'état des attaques chiffrées. »
[3] Zscaler, « Rapport 2022 de ThreatLabz sur l'état de l'hameçonnage. »
[4] Dossier d'analyste IDC, sponsorisé par Zscaler, « Implémenter Zero Trust comme base de la sécurisation des entreprises. » Document #US49043922, avril 2022

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