Un bref historique de Zero Trust, d'une page blanche à la Maison Blanche

Les entreprises se tournent vers le modèle Zero Trust pour répondre aux exigences du marché moderne. Pour comprendre à quel point l'architecture Zero Trust est révolutionnaire, les entreprises doivent se pencher sur l'évolution de Zero Trust et sur la façon dont elle bouleverse radicalement les idées reçues vieilles de plusieurs décennies sur les réseaux et la sécurité des entreprises.

1987

Construction des murs du périmètre réseau

Des ingénieurs de la Digital Equipment Corporation (DEC) publient le premier article sur la technologie des pare-feu, inaugurant ainsi des décennies de réflexion sur la sécurité cloisonnée des réseaux.

1990

Séparation de base par la segmentation du réseau

Les premières tentatives de segmentation du réseau à l'aide de VLAN ou de sous-réseaux font leur apparition : une approche extrêmement limitée, sans authentification, avec des restrictions minimales et peu de fonctionnalités de sécurité interne. Toutes les restrictions mises en place sont aisément contournées.

2001

Le contrôle d'accès au réseau est ajouté

L'IEEE Standards Association publie le protocole 802.1X pour le contrôle d'accès au réseau (NAC). Stimulé par l'adoption des VLAN, il permet d'authentifier les connexions réseau et donne un accès au niveau du réseau (LAN/VLAN), mais il se révèle complexe et difficile à déployer à grande échelle.

2004

La graine du Zero Trust est plantée

Le forum Jericho est créé. Il prend acte du fait que les utilisateurs et les applications quittent le réseau de l'entreprise et introduit les premiers concepts de Zero Trust via le principe de « déprimétrisation ».

2010

Zero Trust est né

L'analyste John Kindervag présente le « modèle Zero Trust » dans un article pour Forrester Research. Il déplace l'authentification et la sécurité inline, et suggère la segmentation des sessions. Toujours axé sur l'accès au réseau, il déplace le périmètre à l'intérieur de celui-ci.

2014

Google définit son propre modèle

L'initiative BeyondCorp de Google réinvente l'architecture de sécurité à la suite de l'attaque Operation Aurora, menant à un déploiement de Zero Trust à l'échelle de l'entreprise.

2016

Zscaler transfère Zero Trust au cloud

Zscaler présente la première solution Zero Trust fournie par le cloud, permettant aux entreprises d'éliminer la surface d'attaque externe et de minimiser le potentiel de déplacement latéral, simplifiant ainsi fondamentalement la mise en œuvre de Zero Trust.

2019

Gartner entre dans la danse

Gartner introduit le concept de SASE (Secure Access Service Edge) et dynamise le concept de Zero Trust, en le redéfinissant en tant que Zero Trust Network Access (ZTNA).

2020

Le NIST définit un cadre standard de Zero Trust

Le NIST publie la norme SP 800-207 en tant que cadre unifié pour l'établissement d'une architecture Zero Trust (ZTA) et introduit le premier véritable changement par rapport à la définition de Zero Trust dans le contexte du réseau.

2021

Gartner définit un chemin sécurisé

Gartner définit les composants de sécurité du SASE comme une nouvelle catégorie de marché, appelée Security Service Edge (SSE).

2022

Le gouvernement américain impose le Zero Trust

L'Office of Management and Budget impose l'adoption des principes de Zero Trust pour toutes les agences d'ici 2024.

Découvrez plus en détail l'historique de Zero Trust et son devenir.

Lire le livre blanc

Experience your world, secured.

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