AYI NEDJIMI Consultants

Comparatif ZTNA 2026 : Cloudflare vs Tailsc Pangolin

29 April 2026 • Mis à jour le 29 April 2026 • 60 min de lecture •

Comparatif détaillé des solutions ZTNA : Cloudflare One, Tailscale, Headsc ans, sécurité, matrice de décision par profil.

Le paysage de la cybersecurite d'entreprise a connu une mutation profonde ces d Zero Trust s'est impose comme le nouveau standard de reference pour securiser informatiques. Face a la multiplication des solutions ZTNA (Zero Trust Network Ac responsables IT et RSSI se trouvent confrontes a un dilemme complexe : quelle so Tailscale, Headscale, Pangolin, Teleport et leurs nombreuses alternatives ? Ce co profondeur six solutions majeures selon plus de quinze criteres techniques, econo examinerons les architectures sous-jacentes, les modeles de deploiement (SaaS v chiffrement, l'integration aux fournisseurs d'identite, la gestion des postures de se fonctionnalites d'audit et d'enregistrement de sessions, ainsi que le cout total de p differentes tailles d'organisation. Que vous soyez une startup cherchant une soluti souhaitant reprendre le controle de ses donnees avec une solution auto-hebergee

une conformite stricte aux normes ISO 27001 et SOC 2, ce guide vous fournira tou
decision eclairee et migrer sereinement depuis votre VPN traditionnel vers une arc

Pourquoi le VPN traditionnel ne suffit plus : le contexte Zero Trust

Pendant plus de deux decennies, le VPN (Virtual Private Network) a constitue la p
ressources d'entreprise. Le modele etait simple : un tunnel chiffre relie le poste de
l'entreprise, lui accordant de facto un acces large, souvent non segmente, a l'ense
paradigme, herite de l'ere du perimetre reseau, repose sur une hypothese fondam
authentifie et connecte au VPN, l'utilisateur est considere comme « de confiance »
pratiquement illimite.

Les limites de ce modele sont devenues criantes avec l'evolution des menaces et
mouvement lateral, ou un attaquant compromet un compte VPN puis se deplace li
representent aujourd'hui l'un des vecteurs d'intrusion les plus devastateurs. L'affa
attaques contre Colonial Pipeline en 2021, et plus recemment les compromissions
Ivanti et Fortinet en 2024-2025 ont demontre que le VPN constitue non seulement
(SPOF), mais aussi une surface d'attaque considerable. Chaque concentrateur VP
potentielle pour les acteurs malveillants qui exploitent des vulnerabilites zero-day

C'est dans ce contexte que le NIST (National Institute of Standards and Technolog
SP 800-207 — Zero Trust Architecture, qui formalise les principes du Zero Trust.

> **Never trust, always verify** — Aucune confiance implicite n'est accordee, que l'
> l'exterieur du reseau.
>
> **Least privilege access** — Chaque utilisateur, appareil et service ne recoit que l
> necessaires a l'execution de sa tache.