Résumé exécutif

Le mythe de la cybersécurité :

Pourquoi les solutions correctives progressives sont insuffisantes – et comment EzIP offre une approche plus simple et plus sécurisée.

Internet est le moteur de la société moderne, mais il reste vulnérable. Les récentes pannes mondiales chez Cloudflare (novembre 2025) et les fréquentes interruptions des services d'Amazon Web Services (AWS) soulignent cette fragilité persistante, même chez les principaux fournisseurs censés garantir la sécurité et la fiabilité. Les initiatives fédérales (avis de proposition de réglementation de la FCC, 2024) et la feuille de route de la Maison Blanche pour le renforcement de la sécurité du routage Internet (2024) visent à améliorer la surveillance et la validation du protocole BGP (Border Gateway Protocol). Ces mesures sont utiles, mais elles ne s'attaquent qu'aux symptômes d'un problème plus profond : la pénurie initiale d'adresses IPv4. Pour faire face à cette limitation d'adresses :

• L'attribution dynamique (DHCP) a rendu les adresses IP temporaires.
• Le système DNS a assuré le suivi des modifications.
• Les réseaux se sont fragmentés en milliers de domaines (systèmes autonomes), s'appuyant sur le protocole BGP pour les interconnecter.
• Les réseaux de diffusion de contenu (CDN) ont centralisé le trafic afin de gérer cette complexité.

Cette architecture crée de la confusion, des points de défaillance uniques et des avantages pour les attaquants : les adresses usurpées sont faciles à utiliser et difficiles à tracer, tandis que les utilisateurs légitimes laissent des traces claires. Les réseaux de diffusion de contenu (CDN) centralisés deviennent des cibles privilégiées, et les correctifs ajoutent des couches supplémentaires sans résoudre la cause profonde du problème. EzIP (Easy IPv4) résout ce problème en réutilisant le bloc d'adresses IPv4 240/4, longtemps réservé, pour fournir des adresses publiques statiques et uniques à des millions de sites – suffisamment pour desservir des régions entières sans réattribution dynamique ni dépendance excessive à des protocoles problématiques. Principaux avantages :

• Sécurité intrinsèque renforcée : les adresses statiques permettent de détecter les usurpations d'identité, améliorent la traçabilité et réduisent les surfaces d'attaque.
• Fiabilité accrue : la complexité réduite diminue les risques de pannes ; la géolocalisation précise facilite la gestion et l'intervention.
• Perturbation minimale : le système se superpose à l'Internet existant, se déploie progressivement via des routeurs régionaux améliorés, sans nécessiter de mises à jour massives des appareils.
• Avantages plus larges : réduction des risques liés à la centralisation, amélioration de l'architecture Internet et facilitation de l'identification des responsables par les forces de l'ordre.

EzIP complète IPv6 et les outils existants en s'attaquant à la pénurie fondamentale qui rendait Internet vulnérable. Ce protocole s'inscrit dans la droite ligne des objectifs visant à construire une infrastructure numérique plus résiliente et plus équitable. Pour une analyse complète, veuillez consulter le site web suivant :

https://avinta.com/gallery/CyberSecurityMyth-FR.pdf

Préparé par: Abraham Y. Chen / Avinta Communications, Inc.
Contact: AYChen@Avinta.com / +1(650)248-1829
Janvier 2026