## Sumário executivo

## O mito da cibersegurança:

Porque é que as soluções incrementais são insuficientes — e como o EzIP oferece um caminho mais simples e seguro.

A internet impulsiona a sociedade moderna, mas continua vulnerável. As recentes interrupções globais na Cloudflare (novembro de 2025) e as frequentes falhas nos serviços da Amazon Web Services realçam a fragilidade persistente, mesmo entre os principais fornecedores concebidos para aumentar a segurança e a fiabilidade. Os esforços federais (FCC NPRM, 2024) e o Roteiro da Casa Branca para a Melhoria da Segurança do Encaminhamento da Internet (2024) visam o Protocolo de Gateway de Borda (BGP) para uma monitorização e validação mais rigorosas. Estas medidas são úteis, mas abordam os sintomas de um problema mais profundo: a escassez original de endereços IPv4. Para lidar com a limitação de endereços:

• A atribuição dinâmica (DHCP) tornou os endereços IP temporários.
• O DNS acompanhava as alterações.
• As redes foram fragmentadas em milhares de domínios (Sistemas Autónomos), que dependiam do BGP para se ligarem.
• As Redes de Distribuição de Conteúdo (CDNs) centralizaram o tráfego para gerir a complexidade.

Esta arquitetura gera confusão, pontos únicos de falha e vantagens para os atacantes: os endereços falsificados são fáceis de utilizar e difíceis de rastrear, enquanto os utilizadores legítimos deixam registos claros. As CDN centralizadas tornam-se alvos principais, e as correções acrescentam mais camadas sem resolver a causa raiz do problema. O EzIP (Easy IPv4) resolve isto, recuperando o bloco IPv4 240/4, há muito reservado, para fornecer endereços públicos estáticos e únicos para milhões de locais — o suficiente para servir regiões inteiras sem reatribuição dinâmica ou dependência excessiva de protocolos problemáticos. Principais benefícios:

• Segurança inerente mais robusta — Os endereços estáticos tornam a falsificação detetável, melhoram a rastreabilidade e reduzem as superfícies de ataque por natureza.
• Maior fiabilidade — A complexidade reduzida diminui os riscos de interrupções; a geolocalização precisa auxilia na gestão e na resposta a incidentes.
• Interrupção mínima — Funciona sobre a Internet existente, é implementado gradualmente através de routers regionais melhorados, sem necessidade de atualizações em massa de dispositivos.
• Vantagens mais amplas — Reduz os riscos de centralização, melhora a arquitetura da Internet e facilita a atribuição de responsabilidade nas investigações policiais.

O EzIP complementa o IPv6 e as ferramentas existentes, abordando a escassez fundamental que tornou a internet vulnerável. Está alinhado com os objetivos de uma infraestrutura digital mais resiliente e equitativa. Para uma análise completa, visite:

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

Preparado pela: Abraham Y. Chen / Avinta Communications, Inc.
Contacto: AYChen@Avinta.com / +1(650)248-1829
janeiro de 2026