UNBREAKABLE SECURITY FOR EVERYTHING REMOTE

BEYOND ZERO TRUST – INVISIBILITY MAKES YOUR REMOTE NETWORK UNHACKABLE, FASTER, SIMPLER AND DRASTICALLY LOWERS COST.

NVIS enables organizations to quickly deploy a modern zero trust network that is more secure and maintainable than VPNs. Delivered as a cloud-based service, NVIS allows IT teams to easily configure a software defined perimeter using existing infrastructure, and centrally manage remote access, whether on-prem or in the cloud.

WHY NOW?

No VPN is truly secure. With remote work and site-to-site communication becoming the norm, traditional VPN solutions carry outdated hardware or complex software solutions that aren't scaling with today's increased demand for secure, remote access. These solutions also fail to limit many attacks by exposing VPN gateways that are a popular target for hackers to exploit. The NVIS zero trust framework is a a pressing security imperative for every organization.

Hackers Can't Hack What They Can't See. Be Invisible. Replace Corporate VPNs with NVIS

ASK FOR A DEMO
SALES@NVIS-INC.COM
HTTPS://NVIS-INC.COM
TEL +1 408-400-3256

NVIS

“VPN HACKS ARE A SLOW-MOTION DISASTER” – WIRED MAGAZINE

The way the world works has changed. Everyone must now work from anywhere, not just from an office. Applications are based in the cloud, not just on-premise. And today’s company network perimeter is spread across the internet. Using a traditional, network-centric VPN for remote access is not only outdated and difficult to maintain, but exposes businesses to security breaches and well publicized hacks.

EXPOSED PUBLIC GATEWAYS

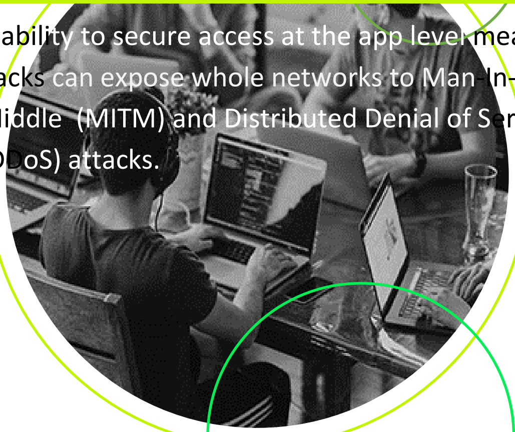
VPN gateways are visible on the internet, making them magnets for attacks. VPN passwords have been cracked and can still be seen because they operate on visible TCP/IP.

DIFFICULT TO MAINTAIN

VPN infrastructure is costly and time consuming to procure, deploy, and maintain. The IPsec and SSL protocols require more than average understanding to properly configure and still have protocol weaknesses and incompatiibilities.

LATERAL ATTACK VULNERABILITY

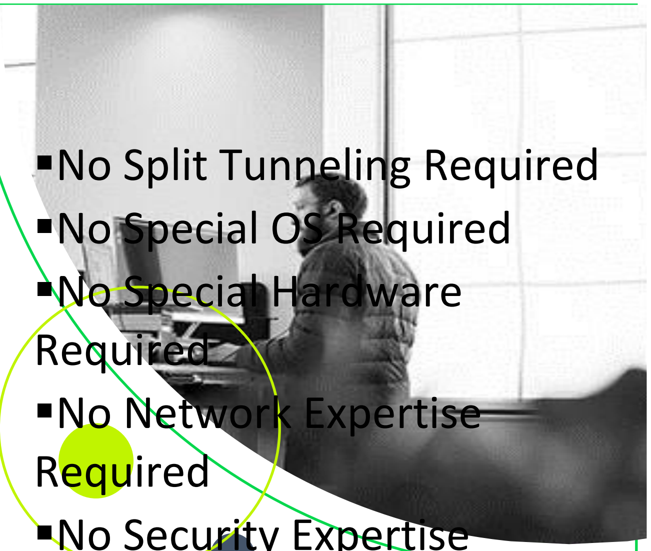
Inability to secure access at the app level means hacks can expose whole networks to Man-In-the-Middle (MITM) and Distributed Denial of Service (DDoS) attacks.



NVIS Advantages

- Zero Trust Network
- Software Defined Perimeter
- Invisible to **any** outside attack
- Layer 2 Network
- End-to-End Encryption
- Peer-to-Peer Architecture
- High Performance & Scalable

- Configure & Deploy in Seconds
- Private Static IPs over Internet
- Untraceable & Unblockable
- Multiplatform Support
- Enterprise Grade/SMB Priced
- No Tracking or Data Selling



- No Split Tunneling Required
- No Special OS Required
- No Special Hardware Required
- No Network Expertise Required
- No Security Expertise Required