ONE-PAGER

Securing AI Workloads & Infrastructure

Dispersive® Stealth Networking

Executive Summary

EXECUTIVE SUMMARY

The network your AI trusts should be invisible to everyone else.

AI workloads and infrastructure are the new perimeter. Organizations deploying LLMs, multi-agent systems, and GPU clusters are creating communication paths that carry not only consequential and sensitive data, they also carry instructions, context, and autonomous decisions. The security architectures built to protect human access were never designed for this. The attack surface compounds with every command, and tools available to address it are insufficient.

THE PROBLEM

Every AI model deployment creates new API surfaces, agents can spin up more agents, and every LLM API call and GPU-to-GPU data transfer creates a communication path that traditional security architectures were never built to protect. As agents communicate, models call external APIs, and inference traffic moves between nodes, those paths are observable, interceptable, and targetable. The attack surface compounds exponentially with the infrastructure itself.

> Legacy tools like VPNs and SASE have two fundamental flaws: they are built primarily to verify access, and they assume the network they operate on is secure. With the explosion of AI, organizations are no longer only securing humans accessing systems, they are securing the workloads and infrastructure those systems communicate across and within autonomously, continuously, and at scale.

A compromised communication path between agents is not a data breach, it is a compromised decision-making chain. The instructions an agent receives, the context it acts on, and the outputs it produces can all be manipulated at the transport layer before any application-level security has a chance to intervene. The blast radius is categorically different from anything legacy architectures were designed to contain.

THE SOLUTION

Dispersive® Stealth Networking is a lightweight overlay that drops into your existing infrastructure without replacing it. Every path an AI agent traverses, every model inference call, every east-west data transfer between nodes moves across dynamic, non-deterministic paths that cannot be correlated, intercepted, or targeted. Operations continue under disruption, degradation, or active attack, and your AI infrastructure remains invisible, resilient, and sovereign by design.

INVISIBLE	RESILIENT	SOVEREIGN
Communications fragmented across dynamic, non-deterministic paths. Traffic cannot be correlated, intercepted, or targeted.	Operations continue under disruption, degradation, or active attack.	You control the transport plane. No external control-plane dependencies. No reliance on infrastructure you don't own.

Trusted in High-Consequence Environments

Validated at military scale and in enterprise edge deployments. Dispersive® Stealth Networking protects human operators and autonomous systems alike, in environments where failure is not an option.

Quantum-Resilient Architecture

- No single path to intercept, observe, or correlate
- No tunnel signature – traffic fragments across dynamic, non-deterministic routes
- No disruption to existing VPN, ZTNA, or SD-WAN investments
- Post-quantum architecture aligned with NIST PQC and DHS guidance
- Lightweight overlay that deploys in minutes with no rip-and-replace

Complementary to Your Existing Security Stack

Legacy tools were built for a world where humans initiated the traffic. AI changed that. Dispersive® Stealth Networking is a lightweight overlay that fills the gaps these tools were never designed to cover.

Tool	What It Does	What It Misses	Dispersive® Stealth Networking
VPN	Encrypts the tunnel	Exposes metadata; single path; blind to agent-to-agent traffic	**Fragments across dynamic paths; agent-to-agent traffic invisible by design**
ZTNA	Controls who accesses what	Assumes network is benign post-auth; not built for autonomous API calls	**Protects how data moves post-auth, including autonomous API calls and agent communications**
SD-WAN	Multi-path performance routing	Paths are deterministic and observable; no protection for east-west GPU traffic	**Paths are dynamic, non-deterministic; east-west GPU and inference traffic moves invisibly**
SIEM / EDR	Detects threats on endpoints and logs	Cannot protect data in transit; no visibility into inference-layer communications	**Eliminates the interception surface at the transport layer before there is anything to detect**

Others assume the network can be trusted.

Dispersive® Stealth Networking operates when it's not.

Dispersive Holdings, Inc.
300 Colonial Center Pkwy Suite 100 | Roswell, GA 30076 USA
dispersive.io | 1.844.403.5850

dispersive