EXECUTIVE OVERVIEW

Dispersive® Stealth Networking for OSINT Operations

Invisible by Design. Safe by Architecture.

The IC OSINT Strategy 2024–2026 designates open source intelligence the "INT of First Resort" — the foundation upon which all other intelligence functions increasingly depend. Federal programs have invested heavily in protecting the analyst: hardened browsers, managed attribution platforms, isolated workstations. Yet the network transport between analyst and target remains almost entirely exposed. The wire itself is the largest unaddressed vulnerability in the modern OSINT enterprise. Dispersive® Stealth Networking closes that gap.

The Problem

THE BROWSER IS HIDDEN. THE WIRE IS NOT.

Every managed attribution platform in use today controls the analyst's browser fingerprint: language, time zone, OS, user agent. None dissolve the network-layer signature. Every session still egresses through one tunnel, from one point of presence, with one source IP. That is precisely the artifact adversaries fingerprint, correlate, and burn. Once a vendor's IP pool is identified, every analyst on it inherits the burn — past and future.

The internet is not a passive environment. Sophisticated forum operators, hostile state actors, and foreign intelligence services watch the wire, not just the browser. Collecting against a target that watches back requires an architecture where the wire itself reveals nothing.

The Solution

DISPERSIVE COMPLETES THE ATTRIBUTION STACK

Dispersive® Stealth Networking is the network-layer foundation that sits underneath existing managed attribution platforms, closing the gap those platforms were never designed to address. Browser-layer MA controls the digital persona. Dispersive controls how data moves through the network. Together they address the full attribution surface. Either layer alone leaves the analyst partially exposed. Dispersive integrates transparently beneath leading Secure Enterprise Browsers including Seraphic (CrowdStrike), Kasm, and Tehama and does not require reconfiguration or workflow changes.

Dispersive's patented active-active multipath transport fragments each session into independently encrypted streams that traverse dynamically selected paths through a distributed deflect cloud. No single source IP address touches the target, no tunnel exists to fingerprint, and no single observer or interception point in transit ever sees a complete flow.

Managed attribution controls the browser-layer identity.
Dispersive provides the invisible transport layer those platforms cannot.

	Browser-isolation MA alone	With Dispersive underneath
Source IP	Single egress IP per session, drawn from a finite vendor pool	No single source IP. Fragments arrive from many independent paths.
Tunnel	Recognizable VPN/proxy fingerprint. Machine Learning (ML) classifiers flag commercial managed attribution (MA) pools.	Tunnel-free transport. Nothing for Machine Learning (ML) detectors to fingerprint.
Correlation	Predictable single-path flow enables timing and volume correlation.	Split-session multipath defeats correlation. No observer sees a full flow.
Resilience	Single tunnel fails as one unit. Session is lost.	Paths reroute mid-session. Sessions persist through degradation.
Routing	Choose Point-of-Presence (POP) region. Intermediate hops are arbitrary.	Path selection actively avoids high-risk jurisdictions.

Mission Scenarios

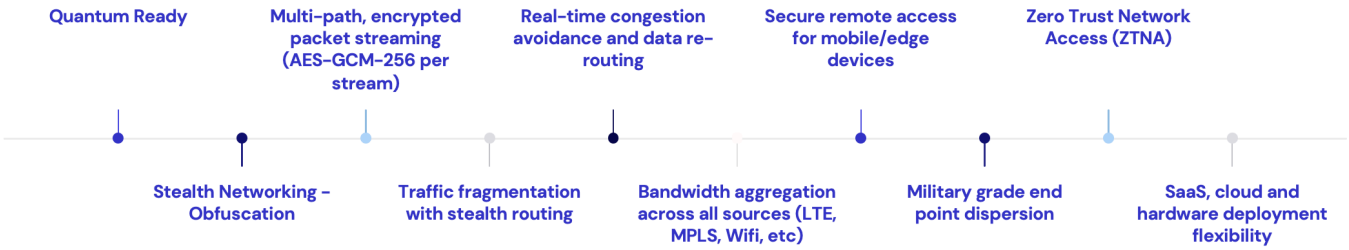
WHERE THE NETWORK LAYER DECIDES THE OUTCOME

- **Persistent collection against a denied-area forum.** The operator maintains block lists of commercial MA egress ranges and feeds deception to identified collectors. With Dispersive, traffic arrives as fragments from multiple unrelated paths. No pool to identify. No analyst to burn. Persistent collection continues because the network layer never presents a stable surface to analyze.
- **When using tunnels, in-region collection where the tunnel itself is the signal.** The MA platform provides an in-region browser fingerprint, but the connection to the POP still presents as a recognizable VPN tunnel, detectable by in-country surveillance apparatus. Dispersive dissolves the tunnel signature itself. No monolithic flow. No classification possible.
- **Tactical edge collection in a contested environment.** Single egress paths are targetable, jammable, or surveilled. Dispersive's multi-path routing traverses commercial internet, satellite, and cellular with paths reconfigured in motion as conditions change. The session survives degradation that drops a conventional tunnel.

How Dispersive Works

ARCHITECTURE

Origin: Data is fragmented into independent encrypted streams before leaving the device. No single stream is contiguous when it leaves the origin.
Dispersal: Each segment stream takes a different dynamic path through ephemeral deflect nodes across AWS, Azure, Oracle, and GCP.
Encryption: Every fragment is protected with independent AES-GCM-256 encryption, with keys rotating continuously and upon any detected anomaly.
Transport: All paths run simultaneously. If one is disrupted, the others continue. No session loss.
Reassembly: Streams recombine at the destination. No single interception point had access to the complete data.



Aligned to the IC OSINT Strategy 2024-2026

STRATEGIC ALIGNMENT

"OSINT is the INT of First Resort." The IC OSINT Strategy 2024–2026, released jointly by ODNI and CIA in March 2024, is not aspirational guidance. It is a directive with budgetary implications and implementation timelines. Dispersive aligns with three of its four strategic focus areas.

- **Next-Generation Workforce and Tradecraft.** Network-layer stealth is the next evolution of managed attribution tradecraft. Browser-layer obfuscation was the first generation. Transport-layer invisibility is the second. Adopting Dispersive advances the tradecraft baseline.
- **Drive OSINT Innovation to Deliver New Capabilities.** Dispersive operates at the unclassified level, integrating with commercial internet infrastructure and existing analyst workstations. No classified network access, special facilities, or dedicated infrastructure required.
- **External Partnerships.** Dispersive is a U.S.company with DoD program lineage and SOC 2 Type II certification, as well as hyperscaler partnerships with AWS and Azure. Sits alongside existing MA platforms inside existing cloud accreditation boundaries.

Deployment

FLEXIBLE DEPLOYMENT | MINIMAL FRICTION

Dispersive is workspace-agnostic by design, operating beneath any Secure Enterprise Browser (SEB) as the invisible transport layer beneath existing environments.

DispersiveCloud™	DispersiveFabric™	Dispersive Client
Managed SaaS · SOC 2 Type II	Self-Managed · On-Premises / Air-Gapped	Endpoint · Any Platform
Fully managed. Any region, operational in minutes. AWS and Azure accredited. No infrastructure ownership required.	Full infrastructure sovereignty. Deployable on any infrastructure, on-premises or air-gapped.	Windows, macOS, Linux, Android, iOS, Docker. Deploys as sidecar. No inbound ports. Outbound-only.

Getting Started

FROM ASSESSMENT TO OPERATIONAL SCALE

Step 1: Mission and Attribution Assessment. A focused assessment of your OSINT collection architecture, managed attribution stack, and operational security requirements.

Step 2: Technical Proof of Value. Demonstrates stealth transport capability against your actual operational environment and threat profile. This phase typically takes four to six weeks.

Step 3: Deploy and Scale. Dispersive deploys the selected architecture, integrates with existing MA platforms, and scales to operational coverage.

To initiate the process, contact Dispersive at https://dispersive.io/company/contact-us

dispersive