SOLUTION BRIEF

Dispersive® Stealth Networking

for Telecom Operators

A transport-agnostic stealth overlay for dense 5G, edge, and multi-transport networks.

THE CHALLENGE

Telecom Networks Are Easy to Find and Easy to Break

Telecom networks are no longer centralized or predictable. 5G densification, edge computing, private networks, and heterogeneous transport have sharply increased operational complexity and attack surface, and adversaries increasingly target telecom infrastructure as a strategic control layer. In 2025, telecom operators faced 444 cyber incidents, including 90 ransomware attacks, alongside stealthy intrusions linked to espionage and long-term surveillance (Cyble Research & Intelligence Labs, Telecommunications Sector Threat Landscape Report 2025).

Many telecom networks are already compromised, whether or not it has been discovered.

Traditional models assume compromise will be detected early, affected systems can be isolated or rebuilt, traffic paths and tunnels can be trusted, and investigation can happen before operations resume. In telecom, those assumptions do not hold. Operations must continue while part of the network is degraded, monitored, or under attack. AI raises the stakes: automated reconnaissance moves faster than detection, and operators are adding GPU and AI workloads at the edge.

5G AND THE EDGE

Built for 5G Densification and Edge AI

As architectures shift from centralized cores to distributed edge deployments, the same connectivity that enables performance also expands attack surface and blast radius. Static tunnels, single-path routing, and perimeter controls were never built for multi-transport, always-on 5G networks. Dispersive replaces static tunnel models with dynamic, per-session isolation, preserving session continuity across fluctuating links and limiting blast radius at the flow level, without infrastructure replacement.

Edge sites now host GPU and AI workloads, and the agents running on them. Dispersive protects agent traffic in transit. Gateways are authenticated by the controller before they join the fabric, and AI workloads are reached on private IPs, with no public IP, DNS name, or inbound port for scanners to find. Agent, inference, and GPU traffic is split across multiple paths, so there is no single stream to profile or intercept. URL filtering gives operators granular control over which destinations agents, users, and applications can reach, limiting where a compromised agent can send data.

American Tower and Vertical Data — Edge AI Pilot
In a multi-month pilot with American Tower and Vertical Data, Dispersive secured a GPU AI workload at an edge data center: 5% to 30% higher throughput than OpenVPN by protocol, sub-second failover across up to 9 active paths, and a workload invisible without an authenticated client.

© 2026 Dispersive Holdings, Inc. | All Rights Reserved | dispersive.io

THE DISPERSIVE APPROACH

Operate Securely, Even When Compromised

Most overlays wrap traffic in a tunnel and protect the tunnel. Dispersive changes how the traffic itself moves. Most security tools determine access. Dispersive® Stealth Networking changes how traffic moves after access is granted. It is a lightweight overlay that aggregates fiber, 5G, satellite, microwave, and cloud into one continuously connected fabric. It does not rely on network trust, inspection, or cleanup, and it can be deployed after compromise to secure command, control, telemetry, and coordination while existing security, monitoring, and incident response continue in parallel.

PER-FLOW ISOLATION	Every session, device, and workload operates independently at the traffic-flow level. Compromise of one radio, site, or edge workload does not propagate laterally.
SESSION CONTINUITY	Multipath transport and automatic path failover keep sessions running as the underlay fluctuates, with no renegotiation storms or static tunnel resets.
NO STATIC TARGETS	Each session is split into independently encrypted streams across paths that keep shifting, with keys rotating per channel. No shared tunnels, static identifiers, or predictable routes for attackers to observe, and endpoints are not directly exposed.
TRANSPORT-AGNOSTIC	Fiber, 5G, satellite, microwave, and cloud combine into one fabric, with bandwidth aggregated across every available link.

Post-quantum cryptography in Dispersive extends throughout the data plane and control plane, incorporates FIPS 140-3 validated cryptographic modules, and supports NIST-standardized PQC algorithms, including ML-KEM and ML-DSA. Crypto agility lets algorithms change as standards evolve, without re-architecting the network. TLS fingerprint mitigation helps traffic blend into ordinary web communications, reducing the metadata adversaries can observe.

DEPLOYMENT OPTIONS

Rapid Deployment With No Changes to Existing Infrastructure

Dispersive overlays existing fiber, 5G, satellite, and core infrastructure, and rollout can begin with a single site, region, or service. It complements DDoS mitigation, radio security, and perimeter controls rather than replacing them. Where static VPN tunnels or SD-WAN are the source of fragility or exposure, Dispersive replaces them.

DispersiveCloud ®

Fully managed SaaS. The fastest path to operational capability, with no infrastructure to deploy. SOC 2 Type II certified.

DispersiveFabric™

Self-managed on premises, in private cloud, or air-gapped. Your team hosts and controls every component, with no external cloud dependency. Software or hardware gateways.

Dispersive Client

Endpoint agent for Windows, macOS, Linux, iOS, and Android. Operates beneath existing applications.

© 2026 Dispersive Holdings, Inc. | All Rights Reserved | dispersive.io

CREDENTIALS & PARTNERSHIPS

Defense-Grade Roots. Carrier-Scale Reach.

Dispersive is named in three Gartner Emerging Tech Impact Radar categories: Zero-Trust Stealth Networking, Automated Moving Target Defense, and Advanced Obfuscation. Dispersive integrates with CrowdStrike Falcon, so a customer's detection policies can trigger enforcement at the Dispersive gateway.

DARPA-Incubated	Dispersive's core architecture originated in U.S. Department of Defense programs, engineered for environments where detection means compromise. The platform is protected by 53 granted patents.
Performance	Up to 10x throughput in degraded or variable network conditions versus static IPsec, up to 20% lower latency, and up to 90% less jitter, per Dispersive testing. Results vary with bearers and conditions.
Marketplaces	Dispersive is an AWS ISV-A partner, available on the AWS Commercial Marketplace and the AWS IC Marketplace, and a Google Cloud Partner Advantage partner.



FIPS 140-3 Validated
Cryptographic Module #5247

Validated Cryptography

The cryptographic module powering Dispersive services is FIPS 140-3 validated (CMVP Certificate #5247). Post-quantum cryptography extends across the data plane and control plane with NIST-standardized ML-KEM and ML-DSA. Dispersive and DispersiveCloud® are SOC 2 Type II certified.

GETTING STARTED

Getting Started with Dispersive

Step 1: Network Assessment

We review your transport mix, edge footprint, and exposure, and identify the site, region, or service to start with.

Step 2: Technical Proof of Value

Dispersive runs on your live transport, validating session continuity, isolation, and performance before you decide.

Step 3: Deploy and Scale

Scale across sites, regions, and services with no changes to existing infrastructure, and ongoing support.

To begin, contact Dispersive at dispersive.io/company/contact-us.

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

dispersive

© 2026 Dispersive Holdings, Inc. | All Rights Reserved | dispersive.io