SOLUTION BRIEF

Dispersive® Stealth Networking

for Secure and Resilient Communications

Resilient, hard-to-find connectivity for the AI era, on the network you already run.

THE PROBLEM

Operations Depend On Networks That Are Easy to Find and Easy to Break

Data moves across carriers, cloud providers, and third-party infrastructure the enterprise does not own or control, along static, predictable paths that can be found, mapped, intercepted, and disrupted. AI raises the stakes on both sides: agents and AI workloads add traffic and new paths, and AI-driven attackers find and exploit them faster than detection and response can keep up. **Most security tools determine access, then assume those networks are safe. They are not.**

Organizations feel the consequences in four familiar ways:

Risk	Sensitive data in motion remains visible and discoverable. Even when encrypted, traffic patterns, metadata, and routing behavior can be observed and targeted.
Downtime	Single-path connectivity creates operational fragility. A disruption, outage, or targeted event breaks continuity. Systems may be secure, but communications are not resilient by design.
Cost	Organizations compensate for transport-layer exposure with layers of tools — VPNs, ZTNA, SD-WAN, managed services — each adding cost without addressing the architectural weakness underneath.
Complexity	Security stacks have grown around the assumption of a stable, trustworthy network. As environments expand — cloud, remote work, third-party access, AI infrastructure — that assumption becomes harder to sustain and more expensive to maintain.

DISPERSIVE® STEALTH NETWORKING ADDRESSES THE PROBLEM AT ITS SOURCE. INSTEAD OF ADDING ANOTHER CONTROL ON TOP OF A VULNERABLE MODEL, DISPERSIVE CHANGES HOW DATA BEHAVES IN TRANSIT.

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

AI COMMUNICATIONS

Securing the AI Communication Layer

AI is turning enterprise networks into autonomous decision fabrics, built on agents, inference calls, and machine-to-machine communications. **If that fabric can be observed, it can be studied, targeted, and exploited.**

LLMs, multi-agent systems, and GPU clusters create AI traffic flows that carry not only sensitive data, but instructions, context, and autonomous decisions. A compromised exchange between agents is not just a data breach. It can become a compromised decision-making chain.

Dispersive protects every one of those paths 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.

Dispersive extends that protection further. Post-quantum cryptography 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. TLS fingerprint mitigation randomizes fingerprints or mirrors common browser profiles, helping sensitive AI traffic blend into ordinary web communications. URL filtering gives operators granular control over which destinations AI agents, users, and applications can reach, reducing agent attack surfaces and limiting data exfiltration paths.

THE DISPERSIVE SOLUTION

Invisible, Resilient, and Sovereign.

Most security tools determine access. Dispersive® Stealth Networking changes how traffic moves after access is granted. Instead of relying on a single, observable path, Dispersive creates a communications fabric that is invisible, resilient by design, and under your control.

INVISIBLE	Data in motion is fragmented and sent across multiple dynamic paths simultaneously. No single stream exists to intercept. No predictable route exists to target. The transport layer becomes unobservable, taking away the target that traditional tools leave exposed.
RESILIENT	Communications run across all available paths simultaneously. If one path is disrupted, degraded, or attacked, the others carry the load without interruption. There is no failover, no reconnection, and no downtime window. This ensures continuity for operations, revenue, and mission-critical services.
SOVEREIGN	Your organization regains control over how its data moves — independent of carriers, cloud providers, or third-party infrastructure. The transport layer becomes something you control, not something you inherit. This reduces dependency risk and strengthens operational autonomy.

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

WHERE DISPERSIVE FITS

Augment What You Run. Replace What Falls Short.

Most secure networking tools were designed for a world where the network could be assumed stable, visible, and trustworthy. That assumption no longer holds. These tools strengthen access and policy, **but none of them secures how data moves across the network.**

In most environments, Dispersive deploys as a lightweight overlay alongside the tools already in place. It operates after authentication, so identity platforms stay where they are. Where a VPN or SD-WAN is the source of outages, exposure, or cost, Dispersive replaces it.

Solution	What It Does	With Dispersive
VPN	Encrypts a tunnel between two endpoints	Replace it where it is the problem. Dispersive does what the VPN does, across multiple paths at once, with no fixed tunnel to find.
ZTNA	Controls who can access what, based on identity	Stays in place. Dispersive works alongside it, protecting how authenticated traffic moves after access is granted.
SD-WAN	Aggregates multiple links for performance and basic redundancy	Works alongside it, or replaces it where predictable paths, outages, or circuit costs are the problem.
Dispersive®	**Changes how traffic moves across every path, after access is granted**	**Augments existing infrastructure or replaces elements of the stack, in DispersiveCloud® or DispersiveFabric™.**

OTHERS ASSUME THE NETWORK CAN BE TRUSTED.
DISPERSIVE® STEALTH NETWORKING OPERATES WHEN IT'S NOT.

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

CORE BUSINESS OUTCOMES

What Changes with Dispersive in Place

Dispersive® Stealth Networking delivers value where executives feel the impact most directly: risk, continuity, and cost. Organizations experience improved performance, resilience, and operational efficiency across diverse, mixed, and semi-trusted network environments.

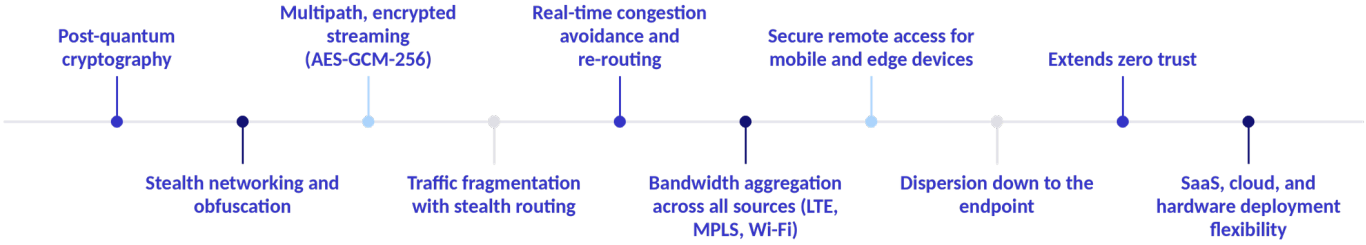
RESILIENCE	Communications run across multiple simultaneous paths. If one path degrades, is disrupted, or is actively targeted, traffic continues across the others without interruption. There is no failover event, no reconnection, and no downtime window. Communications remain stable under degraded conditions, with fewer outages and fewer escalations to network teams. **Executive Value: Stronger operational continuity and reduced business disruption. This protects revenue, service-level agreements, and mission-critical operations.**
SECURITY	Data in motion is fragmented across dynamic, non-deterministic paths. No single stream exists to intercept. No predictable route exists to target. The transport layer, historically the most exposed part of the enterprise, becomes invisible and uncorrelatable. TLS fingerprint mitigation reduces observable metadata signals. Post-quantum cryptography across the data and control plane addresses harvest-now-decrypt-later threats. **Executive Value: A foundational reduction in risk that access controls, encryption alone, and perimeter tools cannot provide.**
PERFORMANCE	Organizations operating across high-latency, high-loss, or globally distributed networks see meaningful throughput and responsiveness gains. Up to 10× throughput in degraded or variable network conditions versus static IPsec. More consistent application behavior across regions and carriers. Reduced sensitivity to jitter, packet loss, and congestion. **Executive Value: Improved user experience and operational efficiency without infrastructure changes.**
COST EFFICIENCY	Dispersive works alongside the infrastructure already in place, with no migration and no architectural overhaul. Where VPN tunnels or SD-WAN create cost or fragility, Dispersive can replace them. By securing the transport layer itself, organizations reduce the need to stack additional tools to compensate for its weaknesses. Lower reliance on MPLS or high-cost dedicated circuits. Reduced operational overhead from troubleshooting and failover. More predictable performance across commodity networks. **Executive Value: Lower total cost of ownership with improved performance and resilience. Complexity and operational overhead decrease and long-term cost curves flatten.**

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

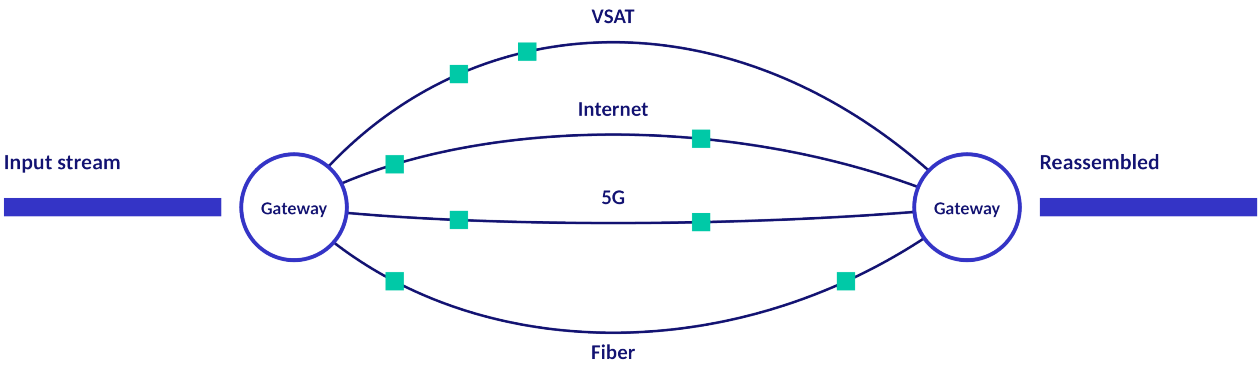
TECHNICAL OVERVIEW

How Dispersive Stealth Networking Protects Data in Motion

Traditional networking sends data along a single, observable path from point A to point B. That path can be discovered, intercepted, disrupted, or degraded — even when encrypted. Dispersive® Stealth Networking changes how data moves so that the transport layer becomes invisible and resilient by design.



01 Origin	Data is divided into multiple independent streams before it ever enters the network. No single stream contains enough information to be useful to an attacker.
02 Dispersal	Each stream travels across a different, dynamic path. Paths shift continuously, eliminating predictable routes. Each stream is independently encrypted with AES-GCM-256 across diverse channels.
03 Transport	All paths operate simultaneously. If one path is disrupted or targeted, the others continue carrying traffic without interruption. Continuity is preserved by design, not through failover. Dispersive delivers up to 10x throughput in degraded or variable network conditions versus static IPsec.
04 Reassembly	At the destination, the independent streams recombine into the full, intact payload. At no point in transit does any single interception point have access to the complete data.



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

REAL-WORLD OUTCOMES

Validated in Demanding, High-Consequence Environments

Dispersive® Stealth Networking is deployed in environments where downtime, interception, or instability carry operational and financial impact.

American Tower and Vertical Data — Edge AI Infrastructure
In a multi-month pilot with American Tower and Vertical Data, Dispersive demonstrated measurable performance and security gains for high-throughput workloads at the network edge: up to 30% throughput improvement, sub-second autonomous failover, and enhanced traffic segmentation. The project validated transport-layer resilience and invisibility at edge scale without replacing underlying infrastructure.

New American Funding — AI Traffic and Security Response
Agentic AI traffic overwhelmed New American Funding's enterprise network. Dispersive came in as a lightweight overlay carrying branch and endpoint traffic, with no network redesign. The customer sets policy and risk thresholds in CrowdStrike Falcon, and Dispersive adjusts access accordingly, cutting detection to enforcement from hours or days to seconds.

U.S. Government and Defense Programs
Select federal programs, including the U.S. Department of Defense, use Dispersive to protect mission-critical communications in contested, remote, or degraded environments. Dispersive provides non-deterministic, resilient transport that maintains continuity even when traditional links are disrupted.

CREDENTIALS & PARTNERSHIPS

Defense-Grade Roots. Enterprise-Ready Reach.

Dispersive® Stealth Networking is a DARPA-incubated, dual-use, commercial-first platform with 53 patents granted. It has been validated in mission-critical national security environments and is designed from first principles for environments where the network cannot be trusted. Gartner names Dispersive in three 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 traffic detection results in mission compromise and where resilience must be maintained under active attack. That lineage is the foundation of every commercial deployment.
53 Patents Granted	Dispersive holds 53 granted patents covering multipath fragmentation, dynamic path selection, independent per-channel encryption, and stealth transport. The platform's architecture is proprietary and purpose-built, not assembled from commodity components.
AWS Defense Accelerator	In 2022, Dispersive was one of only two U.S. companies selected for the AWS Defense Accelerator. Dispersive is an AWS ISV-A partner, available on the AWS Commercial Marketplace and the AWS IC Marketplace, making it accessible to enterprise and public sector buyers through existing procurement channels.

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



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.

DEPLOYMENT OPTIONS

Works With What You Have. Scales to What You Need.

Dispersive® Stealth Networking deploys as an overlay in either model below. Firewalls, identity platforms, endpoint tools, and routing systems remain in place, and rollout can begin with a single use case, site, or segment. Where a VPN or SD-WAN is the source of outages, exposure, or cost, Dispersive replaces it.

DispersiveCloud ®	DispersiveFabric™	Dispersive Client
Fully managed SaaS. Fastest path to operational capability. No infrastructure deployment required. SOC 2 Type II certified, managed via REST API.	Self-managed deployment on-premises, in private cloud, or in air-gapped environments. Full control of the transport plane. No external cloud dependency.	Endpoint agent for per-device stealth transport. Cross-platform: Windows, macOS, Linux, iOS, and Android. Operates transparently beneath existing applications.

GETTING STARTED

Getting Started with Dispersive

1. Environment Assessment	We map your current architecture and identify the workload, site, or path where Dispersive will make the greatest difference.
2. Technical Proof of Value	Dispersive runs in your environment, against your use cases, so you see invisibility, resilience, and performance before you decide.
3. Deploy and Scale	Roll out on DispersiveCloud, DispersiveFabric, or a hybrid model, then expand coverage at your pace, with 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