SOLUTION BRIEF

Dispersive® Stealth Networking

for Critical Infrastructure

Keep operations running on networks adversaries are already mapping.

THE CHALLENGE

Operational Networks Are Easy to Find and Easy to Break

Energy, water, transportation, and industrial operations depend on controllers, sensors, and remote sites connected across aging, semi-trusted, and third-party networks. Those connections were built for availability, not concealment: static paths and exposed endpoints can be mapped long before an attack. Advanced persistent threats live off the land and wait until activated, and AI-driven reconnaissance now moves faster than detection and response.

When the network carries physical operations, a compromise is not just a data problem, it is an outage.

Operational environments are exposed in four ways:

Exposed OT and IoT	Controllers, sensors, and connected devices that cannot be patched or run agents become pivot points into operational systems.
Remote and Vendor Access	Vendors and field technicians reach operational systems over VPNs and gateways that attackers can find and target.
Single-Path Fragility	A cut fiber, a failed cellular link, or a targeted disruption can stop telemetry and control at a remote site.
Long Asset Lives	Equipment stays in service for decades, so systems deployed now must stay protected well into the post-quantum era.

OPERATIONS THAT KEEP RUNNING ON NETWORKS THAT ADVERSARIES CANNOT MAP.

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

THE DISPERSIVE APPROACH

Continuity and Concealment by Design

Most security tools determine access. Dispersive® Stealth Networking changes how traffic moves after access is granted. Operational traffic is split into independently encrypted streams and spread across multiple paths at once, so there is no fixed route to find, intercept, or cut. A compromised device, site, or vendor credential does not have to mean compromised operations.

INVISIBLE	Operational systems have no exposed IPs or open ports and stay unreachable without an authenticated client. There is no single stream to intercept.
RESILIENT	Multipath transport runs across fiber, cellular, satellite, and microwave at once. Automatic path failover shifts traffic in under a second when a link fails, so telemetry and control keep flowing.
CONTAINED	Micro-segmentation limits each session to the specific system or workflow it needs, so a compromise at one site or device does not spread to another.
SOVEREIGN	The operator controls how its data moves. With DispersiveFabric™, every component can run on premises or air-gapped, with no external cloud dependency.

Critical infrastructure operators face no dated federal post-quantum mandate. The practical driver is asset life measured in decades against a migration horizon measured in years. 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.

AI IN OPERATIONS

Securing AI Before It Reaches the Control System

Operators are adding AI for monitoring, maintenance, and operations, with agents and models reaching into operational data and edge compute. 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.

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

USE CASES

Where Dispersive Protects Critical Operations

OT and IoT Protection	Isolate data moving to and from controllers, sensors, and devices behind invisible segments, without installing agents on devices that cannot be modified.
Remote and Vendor Access	Replace broad VPN access with segmented, policy-controlled connectivity to only the systems a vendor or technician needs.
Remote Site Connectivity	Keep remote and field sites connected across every available link, with continuity through outages and disruption.
Control Center Continuity	Keep telemetry and control flowing between field assets and operations centers when individual links degrade or fail.
Edge AI Workloads	Protect GPU and AI workloads running at the edge, and the data moving between them and the core.

PROVEN IN THE FIELD

Validated in Demanding Infrastructure Environments

American Tower and Vertical Data — Edge Infrastructure
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.

Performance Under Degraded Conditions
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.

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

DEPLOYMENT OPTIONS

Works With What You Have

Dispersive deploys as a lightweight overlay on existing networks. Firewalls, identity platforms, OT monitoring, and control systems stay in place, and rollout can begin with a single site, vendor connection, or workflow. Where legacy VPN tunnels or SD-WAN between sites 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.

CREDENTIALS & PARTNERSHIPS

Defense-Grade Roots. Infrastructure-Ready 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.
Coalition-Ready	Dispersive is classified ECCN 5D002 under the EAR, not ITAR, giving allied and coalition partners a more direct licensing path.
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.

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

GETTING STARTED

Getting Started with Dispersive

1. Operational Assessment	We review your OT, remote site, and vendor connectivity, and identify the site, vendor connection, or workflow to start with.
2. Technical Proof of Value	Dispersive runs on your operational networks, validating continuity, concealment, and performance before you decide.
3. Deploy and Scale	Extend across sites and assets on DispersiveCloud, DispersiveFabric, or a hybrid model, 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