dispersive

SOLUTION BRIEF · FINANCIAL SERVICES

Protect Financial Data Now, Before Quantum Turns Today's Collection into Tomorrow's Breach

Dispersive® Stealth Networking delivers post-quantum cryptography, crypto agility and Harvest Now, Decrypt Later (HNDL) mitigation on the communications it carries, built on a FIPS 140-3 validated cryptographic module.

Executive Summary

Financial institutions hold data that must stay confidential for decades, and U.S. authorities from Treasury to NIST have started the clock on post-quantum readiness. Two problems sit inside that pressure: adversaries are collecting encrypted traffic today against decryption that becomes possible later, and AI-accelerated cryptanalysis means a scheme's assumptions can be overturned faster than an estate can be re-engineered.

The timing is closer than most migration plans assume. Citi Institute's January 2026 quantum threat report cites about 39 percent odds of a useful quantum computer before 2030. The stakes are systemic: the Hudson Institute estimates a single-day quantum attack on one top-five U.S. bank's access to Fedwire would cost the U.S. economy $2.0 to $3.3 trillion in indirect impact. Collection of the data it would decrypt is happening now.

Dispersive® Stealth Networking answers both problems as a network-layer overlay, built on a FIPS 140-3 validated cryptographic module, the standard that replaced FIPS 140-2 when its certificates moved to historical status in September 2026. It installs on the network you already run, so protection starts the day it is deployed.

INDEPENDENT RESEARCH

Citi Institute's Recommendations, Delivered in One Deployment

CITI INSTITUTE RECOMMENDS	WHAT DISPERSIVE DELIVERS
Deploy network overlays now for immediate protection against harvest now, decrypt later.	A lightweight network-layer overlay, post-quantum protected from the day it is deployed.
Protect all inbound and outbound data flows without changing underlying applications.	No rip and replace. Applications, endpoints and providers stay as they are.
Use overlays as the rapid defense while longer-term cryptographic migration proceeds.	Protection now, with your migration program running on its own schedule.
Start piloting early rather than waiting for inventories and strategies to finish.	Highest-consequence paths protected while the estate is still being inventoried.
Build crypto agility to switch algorithms quickly as threats and standards change.	Algorithms change in one place, not inside every application.
Hold vendors to cryptographic foundations that keep pace with client timelines.	A vendor readiness response for your third-party risk management record.

Recommendations derived from Citi Institute, Quantum Threat: The Trillion-Dollar Security Race Is On (January 2026). Reference to third-party research does not imply endorsement.

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

The Clock Is Already Running

U.S. financial authorities have moved from awareness to action. Treasury's Financial Sector Quantum Readiness Task Force, launched in August 2026, is assessing technology vendors and third parties and promoting cryptographic agility. The Treasury-co-chaired G7 Cyber Expert Group roadmap points to 2030–2032 for the most critical financial systems, and NIST proposes deprecating RSA-2048 and ECC P-256 after 2030. As the chair of the Financial Services Sector Coordinating Council put it, post-quantum readiness is now "a present-day risk control." For data collected today, the deadline has already passed.

Data in motion	Why it is a target	How long it must stay confidential
Customer identity and account data	Account numbers, Social Security numbers, credentials and biometrics remain usable for fraud long after they are captured.	The life of the customer relationship, and beyond.
Payments and interbank messaging	Payment instructions, settlement and interbank messages expose counterparties, account data and the authentication that moves money.	As long as the accounts and relationships they expose remain active.
Mortgage and lending files	Income, asset and identity records sit inside loans that run for up to 30 years.	The life of the loan, plus record retention.
Trading, risk and M&A communications	Strategies, models and deal terms lose their value the moment someone else reads them.	Until the strategy is retired or the deal is public.
Insurance and reinsurance flows	Policyholder and claims records, underwriting models and reinsurance treaty terms move between carriers, brokers and reinsurers.	The life of the policy, plus claims and record retention.
Data moving to and from AI initiatives	Training data, inference calls and agent traffic carry the records above in bulk between data centers, clouds and partners.	As long as the most sensitive record it carries.

The Financial Services PQC Timeline

Regulators, standards bodies and the threat itself are setting the pace. Data harvested before these dates stays exposed after them.

Jan 2026
G7 PQC roadmap
Treasury-co-chaired roadmap for the financial sector published

Aug 2026
Treasury task force
Quantum Readiness Task Force launched; vendor readiness under review

Sep 2026
FIPS 140-2 historical
Validation claims now point to FIPS 140-3

Now
Harvesting underway
Data collected today stays exposed after migration

2030–2032
Critical systems
G7 window for the most critical systems; NIST proposes deprecating RSA-2048 and ECC P-256 after 2030

Risk marker: about 39% odds of a useful quantum computer before 2030

2034–2035
Full transition
G7 overall target; NIST proposes disallowing RSA and ECC

Risk marker: 19–34% probability of widespread public-key breaking by 2034

Sources: U.S. Department of the Treasury; NIST IR 8547 (initial public draft); risk markers from data cited by Citi Institute.

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

Three PQC Realities Are Network Problems

Each one shows up on the paths your data travels while systems are being migrated. Data in motion is vulnerable at the transport layer. Here is how Dispersive protects it.

01 · CITI INSTITUTE

The most acute quantum risk is not a future attack. It is the harvesting of encrypted data happening now.

They can't break what they can't capture.

Harvest depends on capturing whole conversations. Dispersive splits each session into independently encrypted segments across paths that keep moving, so a collector on any one link captures fragments, and reassembly requires collecting across several paths at once while preserving their timing. It addresses the half of quantum risk that algorithm replacement does not.

Multipath splitting · Automated Moving Target Defense · Costlier collection

02 · CITI INSTITUTE

Migration runs as a phased program over several years, paced by vendor readiness and regulatory guidance.

Keep data moving while crypto is replaced.

Migration happens in stages: HSMs and encryptors re-keyed, endpoints and branch systems refreshed, gateways re-platformed, each on its own schedule. Because Dispersive carries each session across several network paths at once, taking one offline for an upgrade simply shifts traffic to the others, so payments, trading and customer service keep running.

Multipath session splitting · Automatic path failover · Transport-agnostic

03 · CITI INSTITUTE

The challenge is not the lack of a solution. It is implementing one at scale, across thousands of applications.

Resilience without another system to migrate.

Dispersive is a lightweight overlay on transport already in place, replacing none of the endpoints, appliances or encryptors on your migration plan. Because it operates at the transport layer, algorithm change happens in one place rather than inside every application.

Lightweight overlay · Crypto agility in one place · No rip-and-replace

Findings derived from Citi Institute, Quantum Threat: The Trillion-Dollar Security Race Is On (January 2026). Reference to third-party research does not imply endorsement.

One Deployment Solves Three Requirements

Most PQC programs leave harvested data for last, and by then it is already gone. Dispersive delivers all three in one deployment, on the infrastructure you already run.

Requirement	What Dispersive delivers
Post-quantum cryptography	NIST-standardized ML-KEM and ML-DSA across the data plane and the control plane, on FIPS 140-3 validated cryptographic modules. Headers and payloads use separate AES-256 keys, so compromising one does not expose the other. AES-256 is the symmetric algorithm specified in CNSA 2.0, so together this covers all three parts of the CNSA 2.0 core: key establishment, signatures and data transport. Traffic carried over Dispersive is post-quantum protected from the day it is deployed.
Crypto agility	Algorithms change in one place rather than inside every application, appliance and endpoint. This is the requirement institutions find hardest to evidence, and the one that determines the cost of every transition after this one.
Harvest Now, Decrypt Later mitigation	Each session is split into independently encrypted segments across paths that keep changing, so a collector on any one link captures fragments rather than conversations. This is the half of quantum risk that algorithm migration does not reach.

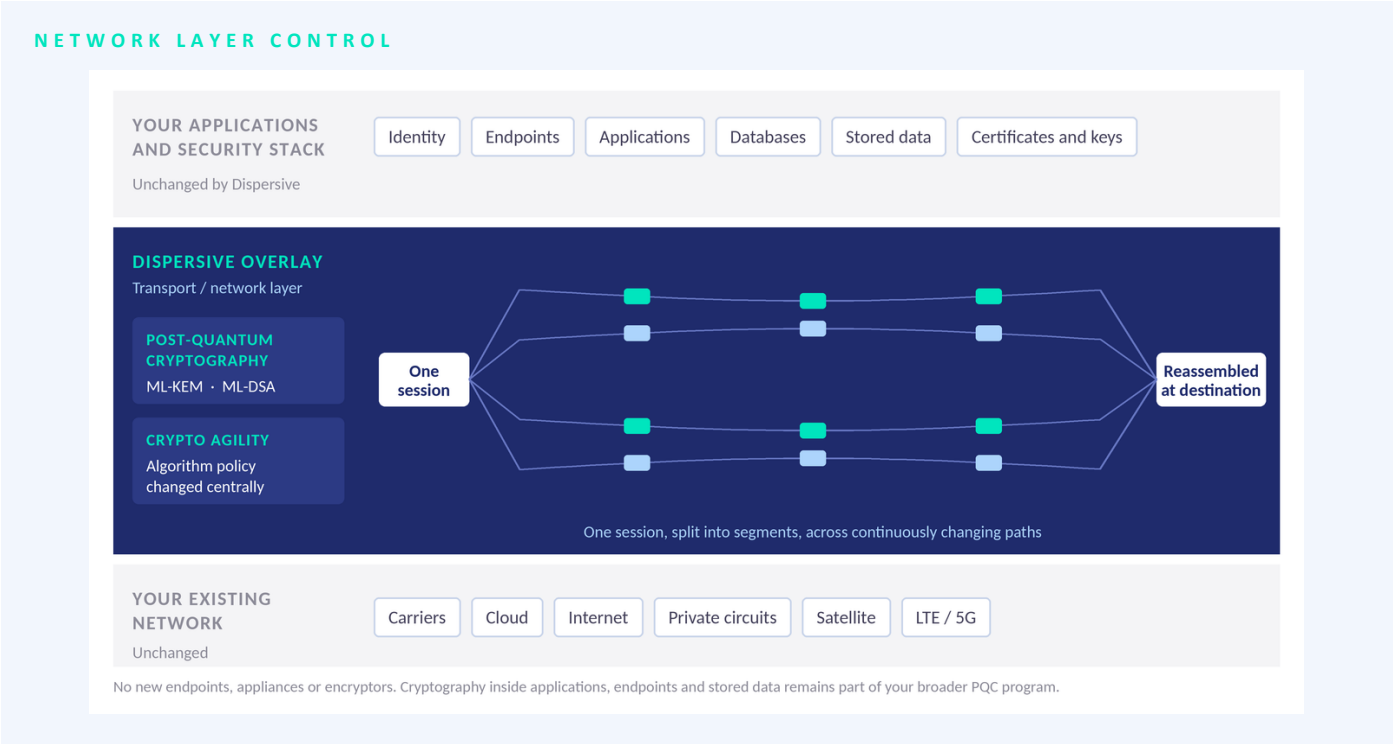
© 2026 Dispersive Holdings, Inc. | All Rights Reserved | dispersive.io

Dispersive Accelerates PQC Compliance

Dispersive installs as a lightweight overlay, as DispersiveCloud® managed service or DispersiveFabric™ on premises. That makes it a practical insertion point: no rip and replace, and none of the endpoints, appliances or encryptors on your migration plan touched. The communications it carries are post-quantum protected on NIST-standardized ML-KEM and ML-DSA from the day it is deployed. Keep the encryption you already run. Dispersive encapsulates existing traffic inside its post-quantum protected transport, so nothing in your environment changes. Add Dispersive, and the communications it carries gain post-quantum protection, crypto agility and HNDL mitigation the day it is deployed.

Your highest-consequence paths are protected while the rest of the estate is still being inventoried. Your crypto agility requirement has a working answer rather than a plan. And the vendor readiness response we supply goes straight into your third-party risk management record, the same vendor readiness Treasury's task force is now examining.

Dispersive provides a network-layer control that supports and accelerates compliance for the communications it carries. Multipath segmentation and moving paths make collection and reconstruction materially harder, particularly from a single observation point. Inventory, applications, endpoints, identities, signatures, stored data, governance, and third-party coordination remain part of the broader program.



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

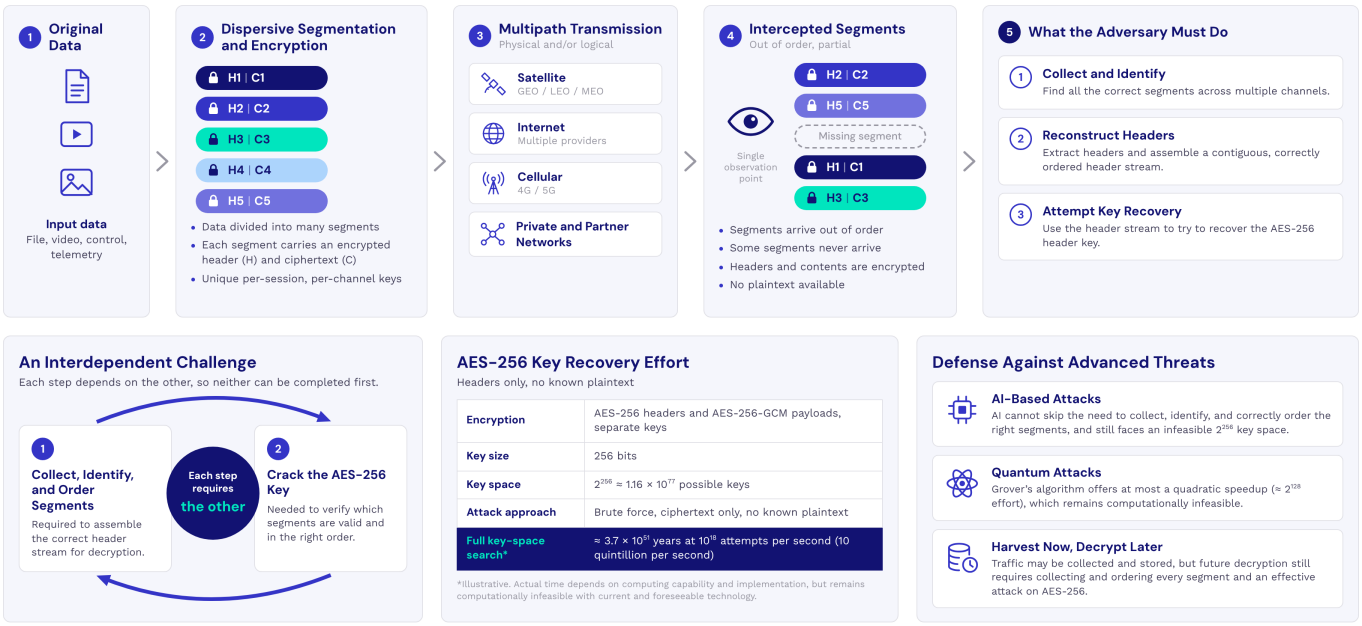
Harvest Now, Decrypt Later

The adversary is already on the network. Salt Typhoon reached inside the major U.S. telecommunications carriers that financial data travels over, and Volt Typhoon has been prepositioned in U.S. critical infrastructure. Financial data has a long tail, so harvest now, decrypt later is today's collection and tomorrow's breach. On a conventional encrypted tunnel, the full session travels one predictable path, and a single vantage point captures all of it. Citi Institute's January 2026 quantum threat report makes the cost of waiting explicit: post-quantum cryptography protects what is transmitted after migration, not what was collected before it.

Dispersive moves the problem from mathematics to collection. A quantum computer or a frontier AI model attacks the math. Neither puts a collector on every path at once. Headers are encrypted as well as payloads, so a collector cannot pick out the segments that belong to a given conversation. To attempt to break Dispersive, an adversary must collect every segment on every path, reconstruct the encrypted headers in the correct order, and only then attempt to recover the header key. Identifying the right segments and their order depends on that same key. This does not address endpoint compromise, key compromise, or data already at rest.

What an Adversary Must Do to Attempt to Crack Dispersive® Stealth Networking

An interdependent collection, identification, and decryption challenge



An Interdependent Challenge

Each step depends on the other, so neither can be completed first.

AES-256 Key Recovery Effort

Headers only, no known plaintext

Encryption	AES-256 headers and AES-256-GCM payloads, separate keys
Key size	256 bits
Key space	$2^{256} \approx 1.16 \times 10^{77}$ possible keys
Attack approach	Brute force, ciphertext only, no known plaintext
Full key-space search*	$\approx 3.7 \times 10^{51}$ years at 10^{18} attempts per second (10 quintillion per second)

*Illustrative. Actual time depends on computing capability and implementation, but remains computationally infeasible with current and foreseeable technology.

Defense Against Advanced Threats

AI-Based Attacks
AI cannot skip the need to collect, identify, and correctly order the right segments, and still faces an infeasible 2^{256} key space.

Quantum Attacks
Grover's algorithm offers at most a quadratic speedup ($\approx 2^{128}$ effort), which remains computationally infeasible.

Harvest Now, Decrypt Later
Traffic may be collected and stored, but future decryption still requires collecting and ordering every segment and an effective attack on AES-256.

Layered advantage Segmentation + Encrypted headers + Multipath diversity + Per-session keys

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

Crypto Agility Is an Immediate Requirement

AI is accelerating cryptanalysis, and it may reach some cryptography before quantum computers do. A Financial Times report (28 October 2026) found that AI advances could break some core encryption methods, including some newer quantum-resistant algorithms, before quantum computing becomes a comparable threat. The Wall Street Journal (6 November 2026) reported that cryptographers are now debating whether AI-driven mathematics will reach encryption first. In July 2026, Anthropic's Frontier Red Team reported that a researcher working with Claude Mythos Preview cut the effective key size of HAWK, a post-quantum signature candidate, in half in roughly sixty hours. HAWK has since been withdrawn.

The standards held. ML-KEM and ML-DSA were unaffected. But quantum threatens today's public-key math and AI may erode confidence in its replacements, so agility decides whether the next break is a configuration change or a re-engineering program.

Sources: Financial Times, "AI maths advances raise fears over security of global encryption," 28 October 2026; The Wall Street Journal, "Quantum Computers Are Poised to Crack Encryption. AI Could Beat Them to It," 6 November 2026. References do not imply endorsement.

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

Credentials

THE DISPERSIVE OVERLAY

- Lightweight software overlay: multipath session splitting and Automated Moving Target Defense (AMTD)
- Operates at the transport layer, so algorithm change happens in one place rather than inside every application
- DispersiveFabric™ on-premises, DispersiveCloud® as a managed option
- Deploys in minutes, with no disruption to existing VPN, ZTNA or SD-WAN investments

CRYPTOGRAPHY AND COMPLIANCE

- Post-quantum cryptography across the data plane and control plane, using NIST-standardized ML-KEM and ML-DSA
- Separate AES-256 keys for headers and payloads, so compromising one does not expose the other
- FIPS 140-3 Validated Cryptographic Module #5247; SOC 2 Type II and HIPAA certified
- DARPA-origin research heritage; 53 granted patents
- ECCN 5D002 under EAR, not ITAR

Validated FIPS 140-3 cryptography. FIPS 140-2 certificates moved to historical status in September 2026, so validation claims in vendor due diligence now need to point to FIPS 140-3. The cryptographic module powering Dispersive services is FIPS 140-3 validated under CMVP certificate #5247, which institutions can cite directly in third-party risk assessments.

Accelerate PQC Readiness with Dispersive

01
Identify the critical use cases, data flows and assets that require post-quantum protection or compliance.

02
Start a path-assessment pilot on one critical flow or business unit, such as payments, trading or a branch network.

03
Receive a migration blueprint built on the pilot results, extending protection across the estate without changing your network or providers.

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