FOR DEFENSE CONTRACTORS · GOVERNMENT SUPPLIERS · ISSOS · CMMC ASSESSMENT PREP

Move CUI directly — evidence for assessors, not marketing adjectives

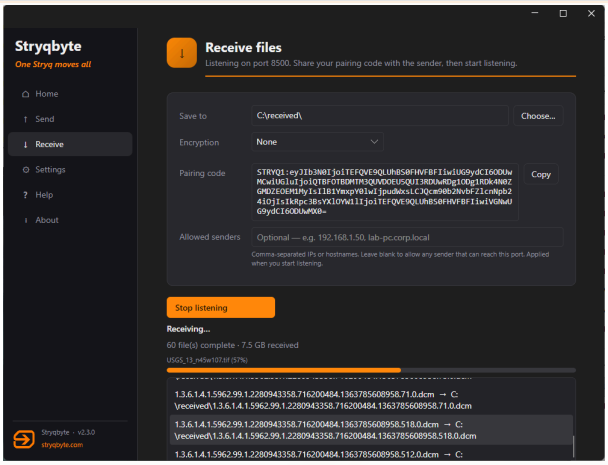
Stryq helps teams transfer Controlled Unclassified Information between authorized Windows endpoints with technical controls and NIST SP 800-171 mapping your System Security Plan can reference — without routing payloads through a vendor cloud file service.

No cloud custody	TLS 1.3	CMMC-on mode	Offline seats
Payloads peer-to-peer between machines you authorize — not a Stryqbyte blob store	Every session · optional AES-256-GCM payload encryption · SHA-256 integrity	Stronger in-app policy when deploy-as-documented compliance workflows are required	Machine-bound licensing validated on device — no live license checks during transfers

Fully encrypted, CMMC-oriented direct transfer. Certificate pinning, optional mutual TLS, audit logging of security and transfer events, enterprise deployment templates, and full control-mapping documentation for SSP and assessor review.

WHAT DEFENSE TEAMS NEED FROM FILE TRANSFER

- **No third-party cloud custody** of CUI payloads during normal operation
- **Session authenticity** — certificate pinning; optional mTLS between endpoints
- **Integrity proof** — SHA-256 verification; corrupted segments automatically re-sent
- **Audit trail** — timestamped security and transfer events exportable for SIEM / SSP evidence
- **Documented mapping** to NIST SP 800-171 controls — not a substitute for organizational certification
- **IT-managed deployment** — offline seat tokens, Group Policy–friendly templates, optional self-hosted rendezvous (metadata-only; off by default)



Operator-visible progress and integrity confirmation — June 2026 throughput study on large structured datasets

CONTROL EXAMPLES (FULL MAPPING IN PRODUCT DOCS)

Requirement area	Stryq technical capability
Protect CUI in transit	TLS 1.3; optional AES-256-GCM payload encryption
Cryptography	NIST-approved algorithms via OS / .NET stack
Session authenticity	Certificate pinning; pairing codes; optional mTLS
Audit & accountability	Configurable security and transfer event logging

WHY NOT CONSUMER TOOLS OR CLOUD SYNC FOR CUI?

vs cloud sync / portals
Upload-notify-download puts CUI in a third-party blob path. Stryq stays direct between authorized endpoints.

vs ad-hoc FTP
No integrity proof, no pinning, no SSP-ready audit trail — and operators hate the scripts.

vs consumer LAN utilities
No seat licensing, no control mapping, no CMMC-on mode for regulated environments.

Throughput still matters
Large imagery and test sets: up to **11×** vs FTP on XL structured volumes in our June 2026 benchmark.

Important: CMMC certifies an organization's information system and practices — not a software product. Stryq provides technical controls that help satisfy specific requirements when configured and operated as documented. Physical security, personnel, policy, and surrounding infrastructure remain customer responsibilities.

Built for Big Data in Motion · contact@stryqbyte.com · www.stryqbyte.com

Request a demo →