



AI for Enterprise Financial Services

Secure AI infrastructure for banks, hedge funds, and private equity.

Built for institutions that expect the highest standard of data security, regulatory compliance, and client confidentiality.

The Problem

Financial institutions handle the most sensitive data imaginable: trading strategies, M&A deal flow, client portfolios, material non-public information. Your clients and regulators expect the highest standard of protection.

When your teams use public AI tools, you may not have clear control over retention, access, and downstream handling, creating exposure in discovery or regulatory examination.

The Solution

TPAI Enterprise provides AI infrastructure designed so that TPAI cannot access your content by default. You connect through private links, and the environment has no public internet egress. Your information stays within controlled boundaries.

Deployment is measured in weeks, not years. A POC with 20-30 users can be operational in 1-2 weeks. Full enterprise deployment in under 30 days. Compare that to a typical 18-36 month, \$1.5M+ in-house build.

If you save 5 hours/week/user, and each employee’s time is worth \$100/hour, a one month delay in adopting AI costs you \$200,000, just for 100 users.

Use Cases

Task	How AI Helps
Investment Research	Summarize 10-K/10-Q filings, earnings transcripts, and market data into investment memos.
Deal Analysis	M&A due diligence, CIM review, valuation modeling, document extraction.
Client Communications	Draft quarterly letters, LP updates, and portfolio reports with client-specific context.
Compliance & Risk	Draft supervisory procedures, policy mapping, exam prep packs, audit documentation.
Internal Knowledge	Search policies, procedures, and historical decisions without external exposure.

Why It Matters

- **Regulatory expectations are increasing.** AI governance, vendor risk, and data protection are under growing scrutiny.
- **Internet-connected AI increases risk.** Public AI tools expand the attack surface and create data exposure vectors.
- **Competitors are adopting AI.** Standing still means falling behind. You need to adopt safely, not avoid adoption.
- **Client trust is non-negotiable.** Your clients expect their information to be protected. Full stop.

Security Architecture

Network Isolation	No public internet egress. Access via private connectivity only (VPN/private links) with strict allowlisting.
Encryption	Customer-managed keys available. In customer-managed deployments (including your AWS account), TPAI does not control decryption.
Access Control	TPAI cannot access customer content by default. Any support access requires explicit approval and is logged.
Data Sovereignty	Deploy in your cloud or region of choice. US available now; EU region planned Q2 2026.
Model Training	Customer content is not used to train models. Your data stays yours.
Compliance	Designed to support common control frameworks (NIST 800-53, SOC 2, GDPR). Evidence pack available.

Engagement Model

Proof of Concept: Start with a focused pilot. 20-30 users, 6 weeks, real workflows. Prove value before broader commitment.

Enterprise Deployment: Full deployment with 100-250+ seats. Includes onboarding, training, and ongoing maintenance (upgrades, security patching, support).

Timelines depend on security review and procurement, but technical deployment is typically within 4-6 weeks. Contact us for a proposal tailored to your requirements.

Next Steps

Schedule a security and value demo. 30 minutes to see the architecture, understand the deployment model, and discuss your specific requirements.

- Book a call: calendly.com/rcastillo-totally-private
- Email directly: rcastillo@totallyprivate.ai

Your Data. Your AI. Totally Private.