TAMUNIO
POWERED BY COMFORTE

TAMUNIO - Data Security for AI

Make sensitive data safe to use in AI

- Data-centric protection for secure AI, analytics, and cloud adoption
- Trusted by global enterprises and financial institutions
- 64% of global card transactions secured

Organizations are rapidly adopting AI to accelerate analytics, automate operations, and engage customers. But AI introduces a critical tradeoff: sensitive enterprise data flowing into AI systems creates exposure, regulatory risk, and compliance failures — forcing many initiatives to stall before they deliver value.

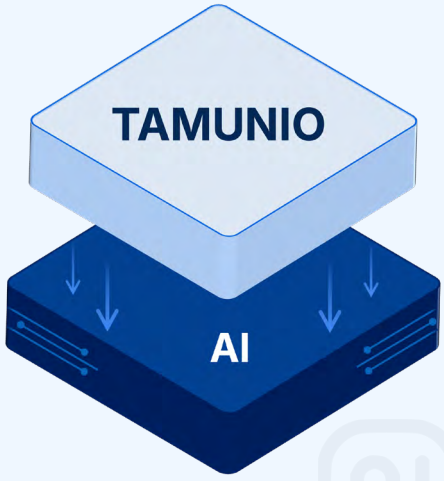
To deliver real enterprise AI value and ROI, organizations need governed but open access to high-value data sets — enabling AI, analytics, and innovation without exposing sensitive data or compromising compliance.

TAMUNIO helps organizations protect sensitive data at ingest, so teams can safely use high-value enterprise data in AI workflows sooner, instead of delaying AI initiatives while data protection controls are designed and implemented separately.

The risk landscape

AI systems consume data across the enterprise — names, payment records, health data, account identifiers — and move it through public LLMs, RAG architectures, third-party copilots, cloud analytics platforms, external AI ecosystems, and MCP-enabled connections to databases, applications, and other enterprise information sources. Without data-level protection, organizations face a stark choice: **limit AI to low-sensitivity use cases or accept high-risk exposure.**

- Regulatory violations – including GDPR and PCI DSS
- Leakage into third-party AI models and workflows
- Sensitive data exposure through MCP-connected databases and enterprise sources
- Loss of data sovereignty
- Delays in AI deployment and longer time-to-value
- Insider threats and breach exposure
- Lack of governance & audit trail



Fast AI innovation vs. strong data protection — TAMUNIO eliminates that tradeoff

TAMUNIO helps reduce these risks by protecting the data itself, not just the systems around it.

With data-centric protection, sensitive information can be discovered, classified, protected, monitored, and governed before it enters AI workflows, as it moves through AI systems, and whenever authorized workloads require access to original plaintext data. TAMUNIO uses vaultless tokenization and format-preserving encryption (FPE) to secure sensitive data while preserving its usability for analytics, AI, and business applications — enabling organizations to innovate without exposing regulated information.

By protecting data at ingest, TAMUNIO reduces the time and effort required to make enterprise data safe for AI. Instead of forcing teams to pause AI adoption until every data source, AI workflow, or MCP-connected integration has been separately secured, organizations can apply consistent data-centric protection earlier in the data lifecycle and accelerate time-to-value.

Three Layers of AI Data Protection

01 / Before AI

De-identify before AI touches your data
Protect data before it reaches any AI system

Sensitive fields — names, payment cards, health records, account IDs — are tokenized before being sent to public LLMs, AI copilots, third-party analytics, RAG pipelines, or MCP-connected AI workflows that access databases and enterprise information sources.

- ✓ Prevent leakage into AI model training
- ✓ Enable safe use of external AI services
- ✓ Protect sensitive data accessed through MCP-connected databases and enterprise sources
- ✓ Simplify GDPR and PCI DSS compliance
- ✓ Reduce breach exposure at the source
- ✓ Accelerate AI time-to-value by protecting data at ingest

Tokenization · Format-preserving encryption · Ingest-time protection

02 / During AI

Secure AI interactions in real time
Protect data flows during AI operations

TAMUNIO detects and de-identifies sensitive data elements on the fly — across AI prompts, text-based outputs, MCP-connected data exchanges, and third-party model interactions — with continuous monitoring and full audit trails.

This applies to structured and semi-structured sensitive data in text, such as names, payment data, account identifiers, health data, customer records, and transactional fields.

- ✓ Prevent accidental leakage in GenAI prompts
- ✓ Reduce risk from human error
- ✓ Secure MCP-enabled access to databases and enterprise data sources
- ✓ Enable safer employee use of AI copilots
- ✓ Real-time audit log for every interaction

PII detection · On-the-fly de-identification · MCP-aware data protection · Audit

03 / Sensitive Processing

Run AI on original data in isolated zones
Confidential compute for mission-critical workloads

When AI must access plaintext data, Data Sovereignty Zones provide hardware-level isolation, runtime security policies, and customer-controlled keys for secure model training and inference.

- ✓ Train and run AI on sensitive original data
- ✓ Full isolation at the hardware level
- ✓ Keys always under customer control
- ✓ Safe cloud adoption for regulated industries

Confidential computing · Quantum-safe encryption

Business Outcomes

- ▶ Accelerate AI adoption without new risk vectors
- ▶ Improve time-to-value by protecting sensitive data at ingest, before it enters AI, analytics, RAG, or MCP-enabled workflows
- ▶ Unlock higher-value AI use cases involving customer, payment, account, health, employee, and transaction data
- ▶ Protect structured and semi-structured sensitive text data used in prompts, outputs, and MCP-connected data flows
- ▶ Reduce breach exposure and insider threat risk
- ▶ Strengthen compliance with GDPR, PCI DSS, and emerging AI governance
- ▶ Future-proof with post-quantum-safe encryption

TAMUNIO — Transform data security from innovation barrier into competitive advantage. Learn more