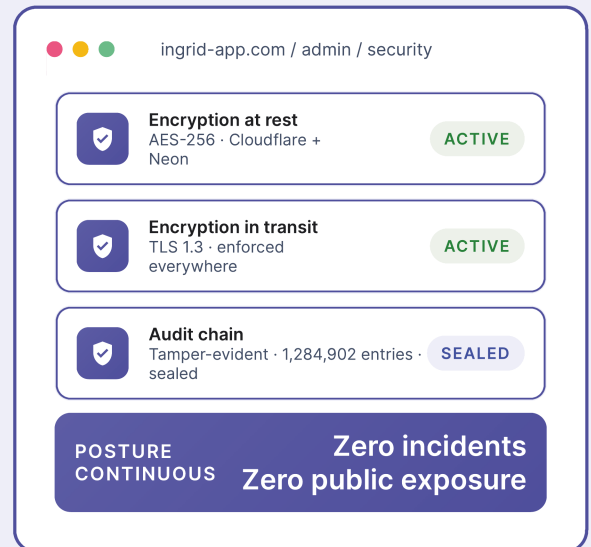


INGRID SECURITY

Built like a bank. Simple like conversation.

Ingrid is engineered with enterprise-grade security across every application and your data. Built on SOC 2 Type II-certified infrastructure, end-to-end encryption, private AI processing, and a **cryptographically chained, append-only audit log** — all working in the background so your team moves fast without worrying about what could leak, slip, or break.


AES-256

Encrypted at rest
Cloudflare + Neon enterprise infrastructure

TLS 1.3

Encrypted in transit
Modern encryption enforced everywhere

SOC 2

Type II infra
Built on Cloudflare's certified platform

Zero

Public exposure
Never appears in Google or public AI

Three pillars on the front. One on the back.

FOUR PILLARS

1
Private AI Processing

Your data is never used to train AI models. All processing happens in isolated, dedicated instances — fully separated from the public internet.

Trains public AI	Never
Dedicated instance	Yes
Public exposure	Zero
Export / delete	One click

2
Bank-Level Encryption

All data and transactions are encrypted and protected at rest and in transit, on infrastructure built, monitored and audited to enterprise standards.

At rest	AES-256
In transit	TLS 1.3
Infrastructure	SOC 2 Type II
Cloudflare	Enterprise platform

3
Role-Based Access

Fine-grained permissions configured in plain English — so everyone sees only what they should, and changes take effect instantly.

Plain-English rule	"Don't let Brenda view..."
Granular RBAC	Down to the field
Instant changes	No restart
Every change	Logged

WHY IT MATTERS

Every action, cryptographically sealed.

Every document upload, data export, permission change, and login is logged with cryptographic chaining — append-only and tamper-evident. We extend our secure logging to include transactions and changes in Spire too. One unified source of truth across every Ingrid module, ready for SOX, GDPR, and industry audits.

Why you can sleep at night

- ✓ **Spire transaction logging**
We capture transactions and changes users perform in Spire and log them for audit. See who changed what, when, across Spire and Ingrid.
- ✓ **AI anomaly detection**
Unusual access patterns and policy violations are flagged automatically — before they become incidents.
- ✓ **Source document controls**
Every transaction can be tied to a source document. Missing-doc alerts and one-click audit packages.
- ✓ **No public exposure**
Your financial data will never appear in Google, public AI training datasets, or any external repository. Ever.
- ✓ **Regular vulnerability scanning**
Continuous scanning on Cloudflare-hosted infrastructure plus periodic application-level review and a responsible-disclosure inbox.
- ✓ **Complete transparency**
See exactly what data Ingrid accesses and processes. Export or delete your data with one click. You stay in control.

Want a deeper look?

We'll walk your team through Ingrid's encryption, audit chain, access controls, and compliance posture.

EMAIL
info@ingrid-app.com

PHONE
416-642-2710

WEB
ingrid-app.com