Security practices

Quantalyze is a data-analytics platform, not a custodian. We read your trade history from your exchange via a read-only API key and compute verified performance metrics. We never hold funds, never place trades, and never move tokens.

Key handling

CIPHER	AES-256-GCM envelope encryption
PER-ROW DEK	Generated at encrypt time, wrapped by a platform KEK
KEK STORAGE	Supabase Vault (KMS-backed)
DECRYPTION PATH	Python analytics service under service-role client only; web tier cannot decrypt. Encrypted columns revoked from anon and `authenticated` roles.
SCOPE ENFORCEMENT	Validated against the exchange at submission; trading or withdrawal permissions rejected before ciphertext is written.

READ	TRADE	WITHDRAW
Accepted	Rejected	Rejected

Data handling

RAW FILLS RETENTION	30 days; hard-deleted by daily job
AGGREGATE ANALYTICS	Retained indefinitely (Sharpe, Sortino, drawdown, daily returns)
TENANT ISOLATION	Postgres RLS + SECURITY DEFINER trigger refusing cross-tenant `api_key_id` linkage on `strategies`
DELETION	Key revoke + listing removal in a single transaction; decryption path lost immediately
SUPPORTED EXCHANGES	Binance, OKX, Bybit (read-only scope on each)

Compliance posture

Preparing for SOC 2 Type 1; internal controls — access reviews, change management, vendor management, incident response — are documented and followed today, with the formal attestation to follow. Allocators under diligence: engage the security contact below for a current posture letter under NDA.

Coordinated vulnerability disclosure follows RFC 9116 via `/.well-known/security.txt`.