



RISKQUILT

Security & Architecture Trust Pack

Hosting, data protection and secure engineering — for security and technology leaders.

Prepared for CISO evaluation · configuration at launch

AT A GLANCE

What a security reviewer needs first

Your data never touches our AI

You connect the AI you already approve; nothing is processed by a RiskQuilt model, and your data trains none.

No public database endpoint

The database sits on a private network with no internet-facing address — it cannot be reached directly.

No operator impersonation

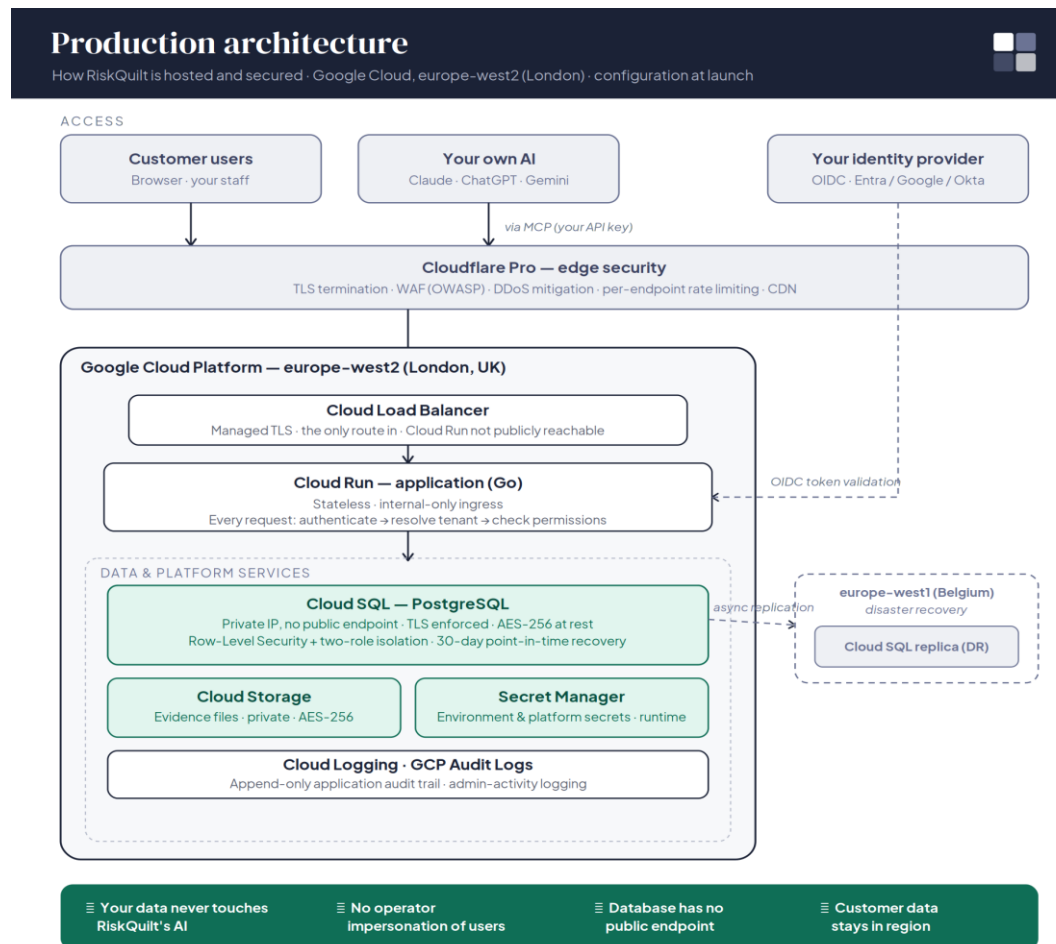
RiskQuilt staff cannot sign in as your users or read your risk data. The code paths do not exist.

Your data stays in region

Hosted in the UK (London), with encrypted backups and EU disaster recovery.

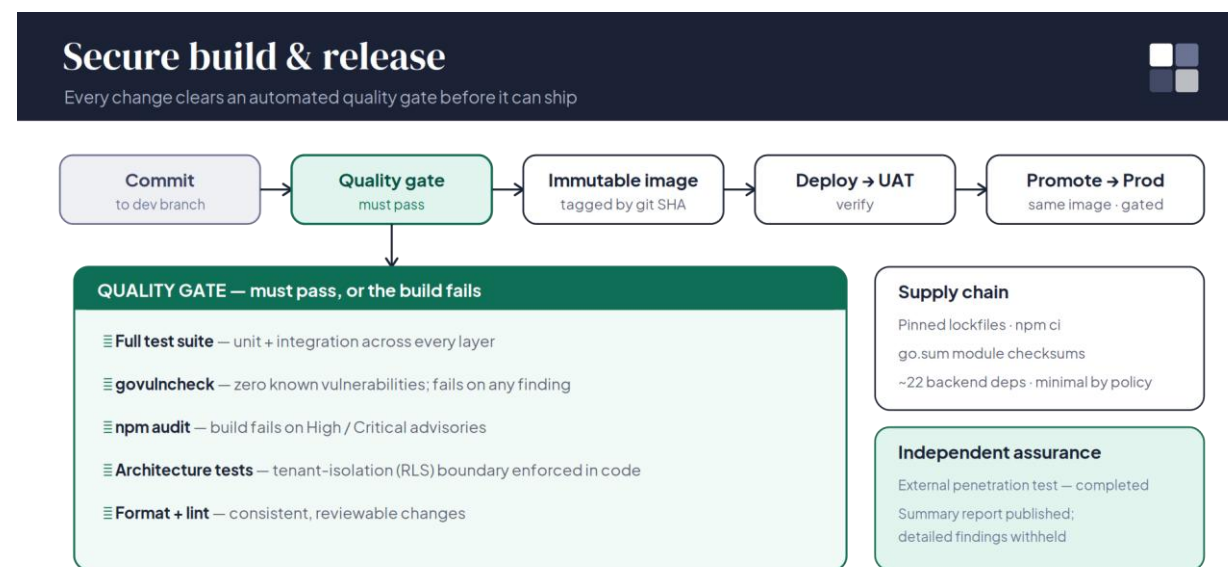
Where it runs, and how it is protected

- **Hosted in the UK.** Google Cloud, europe-west2 (London) — database, evidence files and backups all held in-region.
- **One controlled path.** Cloudflare edge (TLS, WAF, DDoS) → managed load balancer → application; the database is private, with no public endpoint.
- **Encrypted throughout.** TLS 1.2+ in transit end-to-end; AES-256 at rest, with customer-managed keys available.
- **Built to recover.** 30-day point-in-time recovery, regional high-availability, and an EU disaster-recovery replica.
- **Your identity, your secrets.** Authentication delegated to your own IdP; platform secrets held in Secret Manager, never in the database.



Security proven on every change

- **Security by default.** Encryption, least-privilege access and externalised authentication are a baseline every feature inherits.
- **An automated quality gate.** No change ships unless it passes the full test suite, govulncheck (zero-vulnerability policy), npm audit, and architecture tests that enforce tenant isolation.
- **Controlled promotion.** One immutable image, verified in UAT and promoted unchanged behind a gate; database migrations are run manually.
- **Independently tested.** An external penetration test of the application and infrastructure is complete; a summary report is published.



Risk Quilt Ltd · Company number 17049484 · riskquilt.com

Your AI, your data

- **Bring your own AI.** Connect Claude, ChatGPT, Gemini or any MCP-compatible client to your live risk data through the open MCP standard.
- **Never through our AI.** There is no RiskQuilt-hosted model; your data is never used to train one, and there is no new AI vendor to assess.
- **Same permissions as the screen.** Access is scoped to the individual user by exactly the role-based permissions that govern the interface.
- **Fully auditable.** Every AI-initiated change is attributed and written to the same append-only audit trail as manual changes.

*“You use the AI you
already trust — over the
whole risk picture.”*

Data flows directly between your AI and
your tenant — scoped, permissioned,
logged.

SUB-PROCESSORS

A deliberately small third-party footprint

Provider	Purpose	Data it handles	Assurance / location
Google Cloud	Hosting, database, file storage, backups	All customer data, at rest	UK (London); EU DR replica. ISO 27001, SOC 2.
Cloudflare	Edge security (TLS, WAF, DDoS), DNS, bot protection	Traffic in transit (inspected at the edge)	ISO 27001, SOC 2, GDPR. Regional Services available.
Twilio SendGrid	Transactional email (sign-in links, notifications)	Recipient email + message metadata	ISO 27001, SOC 2.
Stripe	Subscription billing	Billing & payment details	PCI DSS Level 1. Card data never touches RiskQuilt.

Your risk and control content is processed only within Google Cloud. The other providers handle transit, email or billing metadata only — never risk data.

UK GDPR posture

- **Controller and processor.** You remain the data controller; RiskQuilt acts as your processor under a Data Processing Agreement.
- **UK residency.** Personal and risk data is processed in the UK; the disaster-recovery replica is held in the EU.
- **Minimal by design.** No passwords are stored (authentication is externalised); the personal data held is essentially the identities your provider asserts.
- **72-hour breach notice.** Confirmed personal-data breaches are notified within 72 hours, in line with UK GDPR Article 33.
- **Deletion on exit.** On offboarding, tenant data is deleted from primary stores on request; backups age out on the retention cycle.

***You control the data.
We process it —
visibly and in the UK.***

Operator access is bounded: our staff cannot read your risk content.



See it working

Explore the live sandbox — sample data, no signup, resets every couple of hours: riskquilt.com/demo

Published pricing & one-month free trial — riskquilt.com/pricing