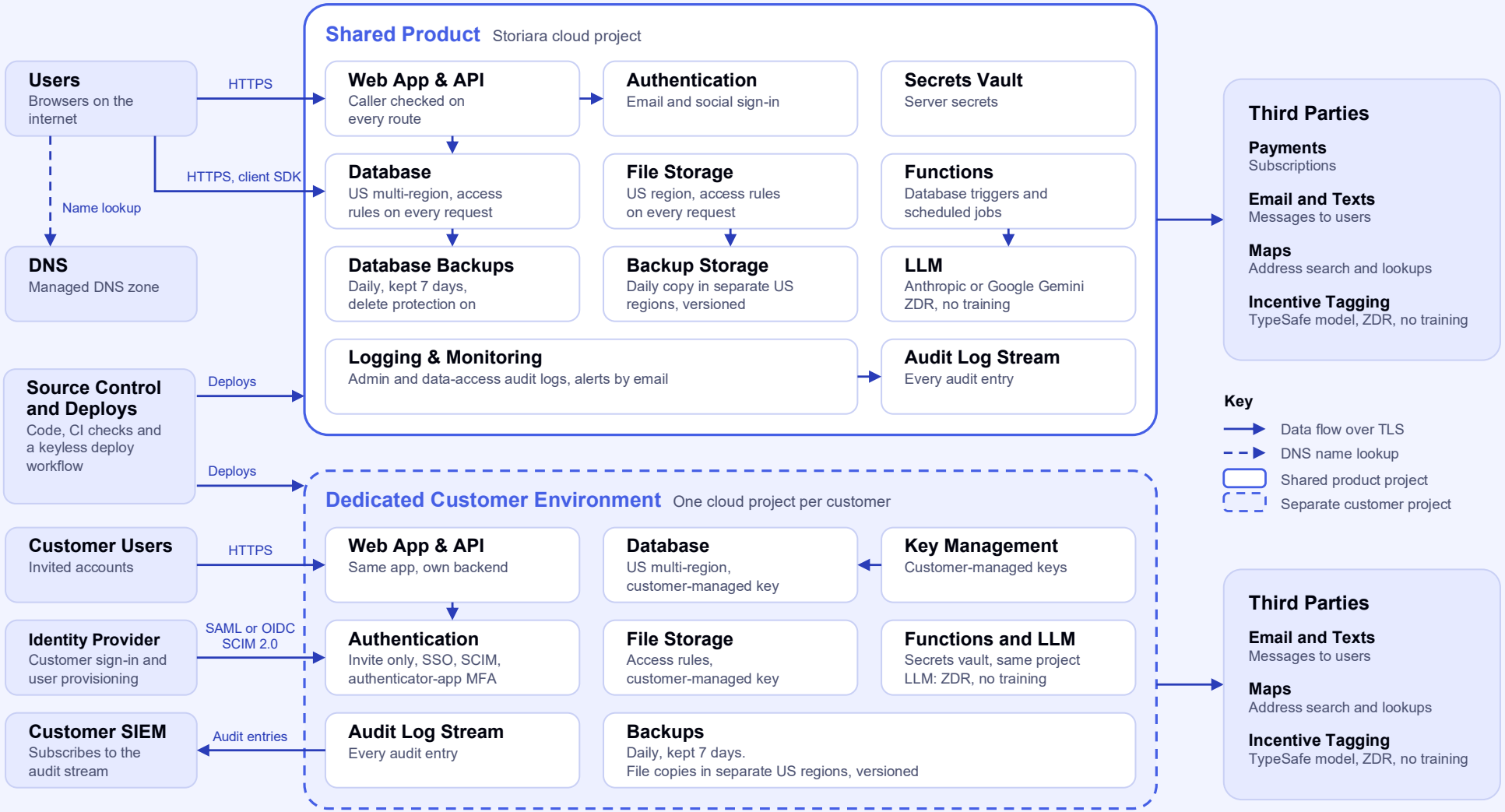
Network Diagram

How traffic reaches Storiara, where data is stored, and where the boundary sits between the shared product and a dedicated customer environment.

Contact security@storiara.com



STORIARA

Zones and Data Flows

Storiara runs on managed cloud services. The cloud provider operates the datacenters, the network and the operating systems. Each zone is entered only through the control named in the last column.

Zone	What Is in It	What Controls Entry
Internet	Browsers of signed-in members, and recipients of shared call sheet and availability links.	Nothing here is trusted. Every request is checked where it enters.
DNS	The storiara.com zone, managed with a DNS provider.	DNS account sign-in.
Shared product	Web app and API, authentication, database, file storage, functions, secrets vault, LLM, backups, logging and monitoring.	HTTPS only, with HSTS. API routes verify the caller's identity and project membership. Access rules on the database and files decide each read and write, and deny by default. Services act under their own least-privilege identities.
Dedicated customer environment	The same services in a separate cloud project for one customer: its own database, files, users, functions, secrets, LLM calls and backups. Database and files use customer-managed encryption keys.	The same controls as the shared product. Invitation-only accounts, no self sign-up. Company SSO (SAML or OIDC), SCIM 2.0 provisioning and authenticator-app MFA are supported.
Source control and deploys	Source code, CI checks, the deploy workflow and dependency security alerts.	Account sign-in. Deploys authenticate without stored cloud keys, and each cloud project trusts only Storiara's own workflows.
Third parties	Payments (shared product only), email and texts, maps, and incentive tagging (TypeSafe model, ZDR, no training).	Outbound HTTPS only. Server-side keys are kept in the secrets vault.

From and To	What Travels	Control on the Flow
Browser to web app	Pages and API calls: AI features, exports, sharing, account deletion.	TLS with HSTS. Identity and membership checks on signed-in routes. Rate limits.
Browser to authentication, database and file storage	Sign-in, project reads and writes, file uploads and downloads.	TLS and the user's identity token. Access rules check project membership and role.
Web app to database, files and authentication	Token checks and server-side reads and writes.	The server's own identity. Each route checks the caller first.
Web app and functions to LLM	Script text and pages, breakdown lists, character descriptions and budget facts. Anthropic or Gemini models, with zero data retention (ZDR) and no training.	The server's own identity, inside the same project.
Database and files to backups	A daily database backup and a daily copy of all files.	Kept 7 days. Delete protection on the database. Backup copies in separate US regions, with versioning.
Audit logs to audit stream	Every admin and data-access audit entry.	A log sink writes to the stream. A customer's SIEM can subscribe.
Source control to cloud	Function code, database and file access rules, and app rebuilds.	A keyless deploy identity limited to deploy roles.
Web app and browser to third parties	Payment sessions, messages, addresses and coordinates for maps, and budget line descriptions to the TypeSafe model for incentive tagging (ZDR, no training).	HTTPS. Server keys in the secrets vault.