

SERVICE & DATA HANDLING

Security and enterprise hosting

A practical overview for your security and deployment review.

This is an informational overview of the standard hosted service and the proposed enterprise review process. It is not an audit report, certification, signed data-processing agreement or customer-specific hosting commitment.

Data flow

Your client collects protection scripts and browser/session context and supplies the intended request to Rayon. Rayon generates Shape telemetry; your client sends the subsequent target request. Rayon generation does not fetch target pages or perform that target request. Inputs can include scripts, profile/canvas, URLs, JavaScript-visible cookies and request bodies. Those inputs may contain personal information or secrets.

Safeguards

Public API and dashboard connections use HTTPS. API keys are associated with active accounts and approved domains, stored as secret hashes and revocable. Dashboard mutations use origin and CSRF protections. Customer JavaScript executes in restricted private workers; reviewed native paths handle approved material separately. Standard accounts use shared infrastructure with account-scoped access controls. Dedicated environments require a separately agreed deployment.

Retention and diagnostics

Material references have five minutes of logical validity; eviction may happen earlier and physical cleanup later. Separate encrypted learned definitions can retain profile/canvas and source/request/cookie constraints with 30-day logical retention and restart restoration. Source-reference expiry does not delete those derived copies. Relevant generation failures may automatically produce encrypted diagnostic captures, with detected credentials, session values and sensitive body fields excluded or redacted. Redaction cannot guarantee arbitrary material is secret-free. Captures expire after 72 hours, may be deleted sooner, are restricted to authorized engineers with a limited capture-action history, and are excluded from ordinary backups. They are not used to replay target requests or for marketing. Detailed usage history is retained for 30 days and hourly aggregates for 365 days. Account, billing, infrastructure and backup records have their own purposes and retention, described in the Privacy Policy.



DEPLOYMENT & ASSURANCE

Agree the boundaries before production.

Providers and locations

The standard service uses Hetzner for API infrastructure/storage and Vercel for web and proxy services, plus Discord, Stripe, Doppler and relevant email/infrastructure services. Provider roles and locations must be confirmed for a particular enterprise deployment. The standard service is not represented as US-only. The Privacy Policy describes UK, EEA, US and other provider processing locations.

Enterprise deployment

Rayon-managed dedicated deployments are reviewed individually, subject to provider availability, capacity and technical review. The schedule must define physical-server versus virtual-instance isolation, any shared dependencies and the agreed country or region. A mandatory country requirement cannot be replaced with a nearby country without explicit customer agreement. The review covers processing and ingress, caches, diagnostics, logs, backups, remote support access and relevant provider access. Location commitments are verified before activation. Customer-hosted installations require separate review and are not advertised as a standard installation package.

Sensitive-data onboarding

Use test accounts and minimized evidence during evaluation. Passwords and payment-card data are prohibited. Before sending other sensitive production data, agree the purpose, permitted inputs, data-processing agreement, provider/location schedule, diagnostic and retention requirements, security responsibilities and incident contacts. Do not email full session captures, credentials or customer records with the initial inquiry. Customer target authorization, end-user authority, MFA and downstream account operations remain the customer's responsibility.

Assurance

Rayon API does not currently claim SOC 2 attestation or ISO 27001 certification. Provider certifications do not certify the service. Availability, recovery, incident-notification and other customer-specific commitments must be agreed separately. This overview does not promise absolute security or universal encryption of every storage layer.

Current public information

Security and data handling: rayonapi.com/security

Enterprise hosting: rayonapi.com/enterprise

[Privacy Policy](#) / [Terms of Service](#) / [API reference](#)