Chunkr Security Architecture

Chunkr's security architecture follows the highest security standards, with all services operating within a private VPC/VNET to maintain network isolation. Our system uses Kubernetes for orchestration with robust authentication via Keycloak, ensuring all access is properly validated and audited. Processed data is stored in an S3 bucket or filesystem and a postgres SQL database, both of which are encrypted at rest. This data can be deleted via the `expires_in` field in the API requests or manually using our API's `delete /api/v1/task` route. As the data is never stored outside of the VPC, on a managed instance or on a self-hosted instance, the data will not leave your security perimeter.

When utilizing external providers (OpenAI, Google AI Studio, Azure Document AI, etc.), data is transmitted via encrypted channels and all external providers are optional. Any external provider used by Chunkr is audited and is low risk. All client connections are secured through Cloudflare's TCP protection layer, providing DDoS mitigation and traffic inspection.