LangSmith security overview

Where your data lives, and who can reach it

For each deployment model (Cloud, BYOC, self-hosted): where your data is stored, which paths cross a trust boundary, how each path is protected, what LangChain personnel can access, and which subprocessors are involved. Read alongside the SOC 2 Type II report, ISO/IEC 27001 and 42001 certificates and policies on this Trust Center.

Holds for every deployment option

Encrypted at rest (AES-256) in every option. LangSmith Cloud and the standard BYOC ingress on AWS, Google Cloud and Azure enforce TLS 1.2 or higher in transit; in self-hosted, or with a custom ingress, you set the TLS policy at your own terminator.

Each customer's data is logically isolated by application-level controls.

AI-powered features are controlled at the organization level; an organization admin decides whether they run.

SDK masking removes sensitive fields before data leaves your application. There is no server-side redaction: what you send is what is stored.

Deployment options

Three deployment models

The difference is where your trace data sits and who operates the software that holds it.

	LangSmith Cloud (SaaS)	Bring your own cloud (BYOC)	Self-hosted
Where data lives	LangChain's cloud, in the region you select at sign-up	Your AWS account, Google Cloud project or Azure subscription, in the region you choose	Your own Kubernetes environment
Who operates it	LangChain	LangChain, through scoped access you grant and can revoke	You. LangChain has no standing access
What leaves your region (non-US regions)	Billing and payment records, usage and operational metadata (US). Content for AI-powered features, only if your admin turns them on	Control plane only (US): sign-in, users and roles, organization and workspace settings, API keys, billing and usage metadata	License checks and usage counts, unless you run offline mode. Telemetry is optional
Who can view your data	Limited engineering staff, for support cases only, logged and reviewed (page 4)	Nobody in normal operation. Break-glass access needs your approval (pages 3 and 4)	Nobody
Plans	All plans	Enterprise	Enterprise add-on
Documentation	`docs.langchain.com/langsmith/cloud`	`docs.langchain.com/langsmith/byoc`	`docs.langchain.com/langsmith/self-hosted`

Independent assurance

SOC 2 Type II, audit period July 1, 2025 to June 30, 2026. Unqualified opinion, no exceptions.

ISO/IEC 27001:2022, certificate `ISMS-LA-063026`.

ISO/IEC 42001:2023, certificate `AIMS-LC-101926`, covering the AI features where LangChain manages the model.

Annual third-party penetration test; executive summary on this Trust Center.

Legal frameworks

GDPR: Standard Contractual Clauses (Module 2) incorporated in our Data Processing Addendum, self-serve on this Trust Center.

HIPAA: Business Associate Agreements on Enterprise for approved PHI use cases; not offered by default.

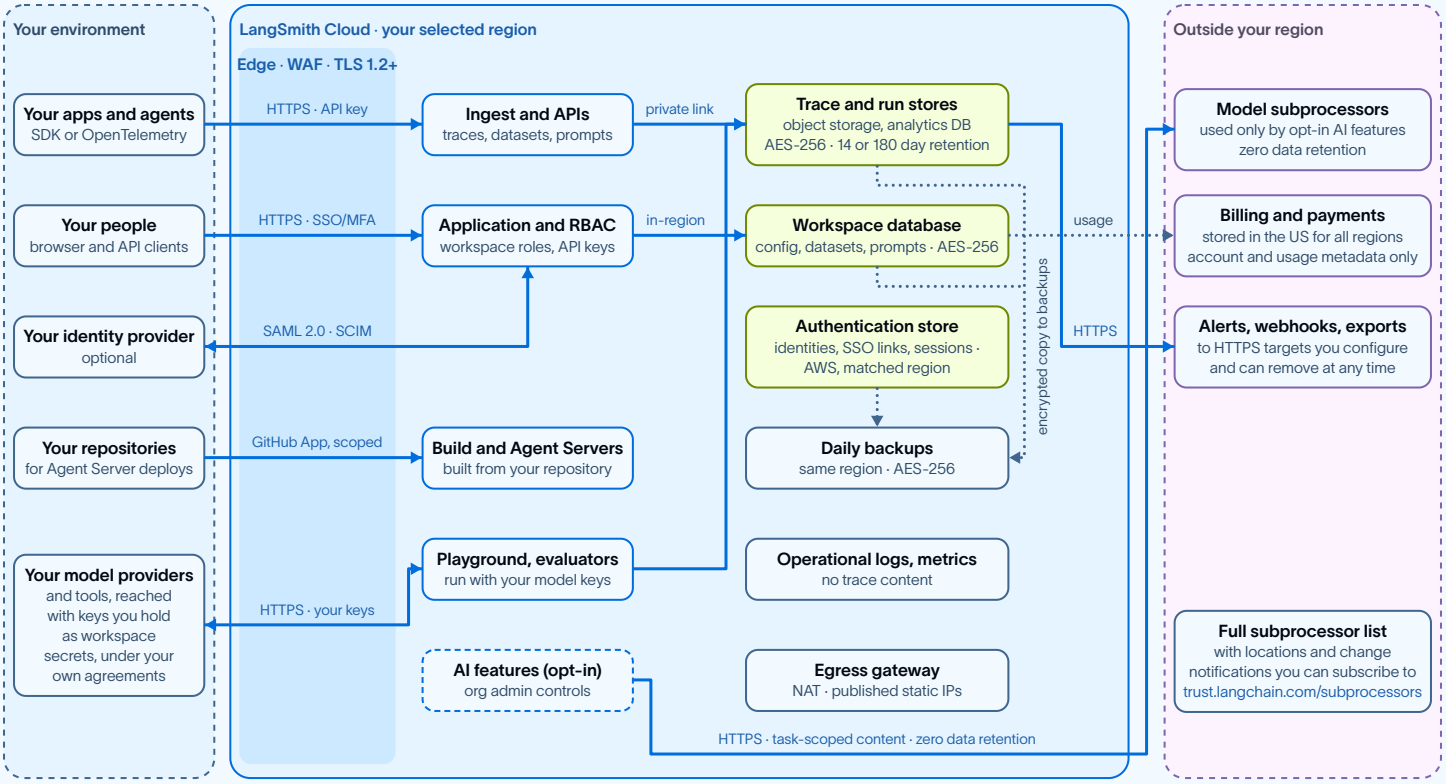
EU transfer impact assessment, pre-filled, on this Trust Center.

Subprocessor list with locations and change notifications: `trust.langchain.com/subprocessors`.

LangSmith Cloud

How your data moves, how each path is protected, and where it stops

One managed LangSmith instance per region. Content enters through the edge, is processed and stored inside your region, and leaves only on paths you configure. Each arrow is labeled with its protocol and control.



Protocols and controls on each path

Path	Protocol	Control
Apps and agents to Ingest	HTTPS, TLS 1.2+ (SDK or OpenTelemetry)	Workspace-scoped API key; SDK masking before send; Enterprise can use AWS PrivateLink or GCP Private Service Connect
People to LangSmith	HTTPS, TLS 1.2+	SAML 2.0 SSO and SCIM from your IdP, MFA, workspace RBAC, API keys with expiry
Repositories to Build	GitHub App	Authorized once by your org; reads only repositories you select; revoke by uninstalling
Services to trace stores	Private endpoint (GCP), AWS PrivateLink (AWS)	Never crosses the public internet; stays in region; AES-256 at rest
Playground to your providers	HTTPS	Your keys held as workspace secrets; egress from published static IPs you can allow-list
AI features to subprocessors	HTTPS	Only when an org admin has turned them on; task-scoped content; zero data retention

Bring your own cloud

What LangChain can and cannot reach in your account

BYOC runs on AWS, Google Cloud and Azure. All three use the same split. The control plane runs in LangChain's cloud, in the US, and holds no sensitive application data. The data plane runs in your cloud account and holds everything sensitive.

Same on every cloud

Control plane holds authentication, organization and workspace configuration, billing and usage metadata, LangSmith API keys and static frontend assets.

Data plane holds traces, prompts, datasets, evaluators, experiments, annotation queues, agent deployments, workspace secrets and all other application data.

Your browser loads the UI code from the control plane, then sends every request for application data to your data plane. SDKs point at your data plane directly.

The data plane calls the control plane over a private connection for sign-in, API key checks, health and usage. It does not use the internet.

LangChain's access

You grant the access with a Terraform module LangChain publishes, and you can remove it at any time.

It is scoped to building and running the data plane. It carries no role to read your stored data.

LangChain administers the Kubernetes cluster that runs LangSmith, to install, upgrade and repair it.

No standing data access. If an incident needs it, you either run the queries yourself or approve break-glass access, which ends with a written summary.

Provisioning actions are recorded in your cloud provider's audit log.

By cloud

	AWS	Google Cloud	Azure
Control plane	LangChain's AWS, `us-east-2`, at `aws.smith.langchain.com`	LangChain's Google Cloud, `us-central1`, at `smith.langchain.com`	LangChain's Azure, `centralus`, at `azure.smith.langchain.com`
Data plane	Your AWS account: dedicated VPC, private EKS cluster, RDS, ElastiCache, S3	Your GCP project: VPC, private GKE cluster, Cloud SQL, Memorystore, Cloud Storage	One resource group in your subscription: VNet, private AKS cluster, Azure PostgreSQL, Managed Redis, Blob Storage
Data plane to control plane	AWS PrivateLink	Private Service Connect	Azure Private Link
How LangChain gets access	One cross-account IAM role you create	One provisioner service account you create, which one LangChain identity can impersonate	One LangChain application added to your tenant, with roles on the data plane resource group only
How LangChain reaches the cluster	PrivateLink to the EKS API, which has no public endpoint	The GKE DNS endpoint, which requires a Google IAM token; nodes are private	Private Link to the AKS API, which has no public endpoint
What that access cannot read	No `s3:GetObject` on the trace bucket, no `rds-db:connect`, no `elasticache:Connect`	No `storage.objects.get`, no secret values, no database login	No data role on Blob Storage, PostgreSQL or Redis; no role to read Key Vault secrets
Reducing access further	Bring your own VPC and bring your own IAM remove network and IAM management from the role	`byo_iam`: you create the service accounts, and the provisioner can no longer change project IAM	`reduced_access`, set once the data plane is active: LangChain can upgrade, scale and repair, but not delete or assign roles

Read before you choose

Use an account, project or resource group that holds only LangSmith. On Google Cloud the limits come from the roles granted, not from deny policies.

On Azure, until you set `reduced_access`, the access includes the ability to assign roles in the resource group, which could include a data role. Your Activity Log records every role assignment.

On Google Cloud and Azure you choose a public or internal load balancer for the data plane. The standard ingress enforces TLS 1.2 or higher on all three clouds.

Data at rest uses keys managed by the cloud provider on all three. Customer-managed keys are planned; ask your account team if you need them.

Full detail per cloud: `docs.langchain.com/langsmith/byoc-architecture-aws`, `-gcp` and `-azure`. Who is responsible for what: `docs.langchain.com/langsmith/byoc-shared-responsibility`.

Self-hosted

Everything runs in your Kubernetes environment, behind an ingress and TLS configuration you control. LangChain has no standing access; support works through tickets and what you choose to share.

The only outbound call is to `beacon.langchain.com` for license checks and usage counts, which carry no content. Offline mode makes no connection at all. Operational telemetry is optional.

You pull published images and Helm charts into your own registry, scan them, and deploy under your own change process.

Documentation: `docs.langchain.com/langsmith/self-hosted`.

Network requirements for LangSmith Cloud

Your side needs outbound HTTPS (port 443) only, no inbound rules. Air-gapped agents cannot reach LangSmith Cloud; use self-hosted.

LangSmith's outbound traffic leaves from published static IPs per region, listed at `docs.langchain.com/langsmith/cloud`, so you can allow-list it.

Enterprise customers can connect privately over AWS PrivateLink or GCP Private Service Connect: `docs.langchain.com/langsmith/cloud`, Private connectivity.

Your content leaves LangSmith on three paths only: your model providers and tools, with keys you hold; LangChain's inference subprocessors, for AI-powered features your admin has turned on; and webhook or export targets you configure. Billing and usage metadata goes to the US separately, with no content.

Regional storage (LangSmith Cloud)

Region	Sign-up URL	Platform and trace stores	Authentication store
GCP US	`smith.langchain.com`	GCP `us-central1` (Iowa)	AWS `us-east-1` (N. Virginia)
GCP EU	`eu.smith.langchain.com`	GCP `europe-west4` (Netherlands)	AWS `eu-central-1` (Germany)
GCP APAC	`apac.smith.langchain.com`	GCP `australia-southeast1` (Sydney)	AWS `ap-southeast-2` (Sydney)
AWS US	`aws.smith.langchain.com`	AWS `us-east-2` (Ohio)	AWS `us-east-2` (Ohio)

The authentication store holds user identities (name, email, SSO identifiers) and session tokens, no trace content. Organizations cannot span regions and are not migrated between regions; a customer needing more than one region runs one organization per region. Tracing can be turned off per workspace. Billing, payment and usage records are stored in the US for every region.

Who can view your data

Deployment	LangChain personnel access	Controls on that access
LangSmith Cloud	A limited set of engineering staff may access customer data to debug and support the service. Scoped to the case at hand; no bulk search across customers.	Least-privilege roles behind SSO with MFA and managed-device trust, granted just in time. Every access logged and retained at least 12 months. Access rights reviewed quarterly.
BYOC	Operations run through scoped access you grant, with no role to read your stored data. LangChain does not need your data in normal operation.	Break-glass only with your approval, kept narrow and short, followed by a written summary. Provisioning actions are recorded in your cloud provider's audit log.
Self-hosted	None. No standing access to your environment.	You decide what to share through support tickets.

What a trace contains

The inputs and outputs of each step of your application, plus metadata, tags, token counts, latency and errors.

It is visible only inside LangSmith, to users your RBAC allows.

What LangChain's systems see

Operational logs and metrics carry request metadata: tenant identifiers, request paths, status codes and timings.

Trace content is not written to operational logs in normal operation.

Audit logs

Enterprise. Tamper-resistant record of administrative and configuration actions across settings, membership, credentials, workspaces, datasets, projects and prompts.

Timestamp, actor, operation, resources, outcome. Retained up to 400 days.

UI for org admins, and an API in OCSF format for your SIEM. Primarily write operations today.

Keys and roles

Personal keys are workspace-scoped and expire. Service keys carry org- or workspace-level roles.

LangSmith stores only a masked prefix; the full key shows once. You store and rotate it.

Default and custom roles. SAML 2.0 SSO with just-in-time provisioning; SCIM for lifecycle.
Self-hosted: OAuth2/OIDC.

Sensitive data

Mask or drop sensitive fields in the SDK before send. Nothing is redacted server-side.

Use online evaluators to catch PII that slips through; keep sensitive projects in their own workspace and restrict who can open traces.

The SDK's optional failed-trace directory writes rejected batches to local disk as unencrypted JSON, owner-only permissions, never replayed automatically. Off by default.

AI-powered features

An organization admin decides whether they run. They read content you already sent; no new data source.

Where LangChain manages the model, only task-scoped content goes to a subprocessor, under zero data retention.

Outputs are proposals a person approves. Repository access uses a GitHub App with one-hour tokens, scoped to repos you select.

Lifecycle

LangSmith Cloud trace retention per project: 14 days or 180 days. On BYOC, retention tiers are set per data plane. Expired traces are deleted and cannot be restored; use bulk export if you need them later.

Delete a whole project in the UI or API, or specific traces by ID or metadata via the delete API (batch job, not instant). Dataset examples support hard delete. Everything is exportable via API and UI.

LangSmith Cloud backups are daily, encrypted and stay in the same region.

Deleting a BYOC data plane removes the cluster, databases and network LangChain created. On Google Cloud and Azure the trace storage is kept in your account for you to delete, and on Google Cloud the database backups too. You end LangChain's access by removing the grant.

Protecting the service

WAF, CDN and enforced rate limits in every LangSmith Cloud region. Hardened minimal base images.

Continuous scanning of code, dependencies and containers; annual independent penetration test. Open-source framework advisories published on GitHub.

Remediation from confirmation: Critical and High 15 days, Medium 30, Low 90. Actively exploited issues handled immediately.

24/7 managed detection and response; incident response aligned to NIST SP 800-61. Confirmed incidents affecting you are notified without undue delay to your admins and security contacts.

What you control

The region that holds your data, and the deployment model.

What enters LangSmith: SDK masking strips sensitive fields before they leave your application.

Who can view it: SSO, SCIM, MFA and workspace-level RBAC.

Which providers and tools LangSmith reaches with your keys, and whether any AI-powered feature is on at all.

On BYOC, the access LangChain holds in your account, and when it ends.

The SOC 2 Type II report, ISO/IEC 27001 and 42001 certificates, penetration test summary, pre-filled CAIQ and EU transfer impact assessment are on this Trust Center.