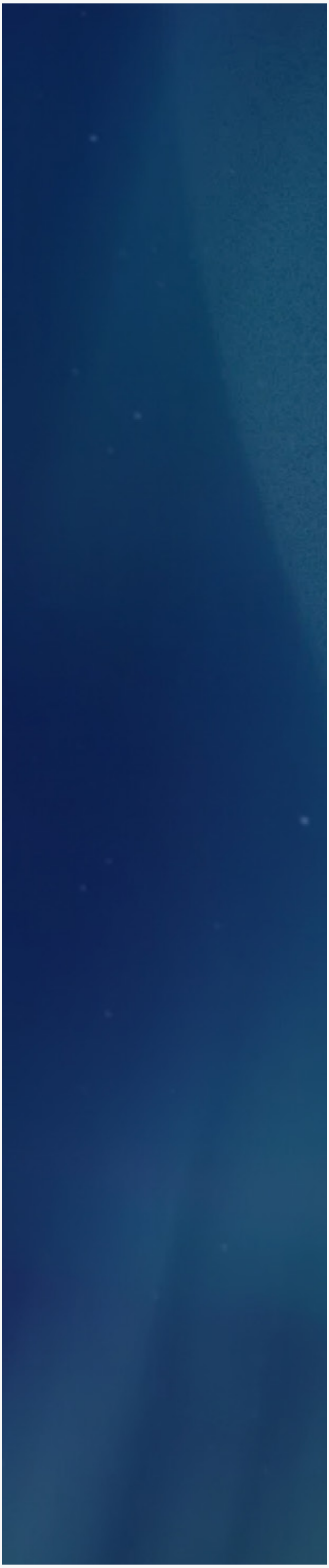
Conclude Security Whitepaper



conclude

Table of Contents

Navigating this White Paper

Click on titles or page numbers to navigate to each section.

Executive Summary

Conclude enables secure, real-time collaboration across Slack and Microsoft Teams. Security, privacy, and compliance are built into our platform, processes, and culture. This document provides a clear, practical view of how we protect customer data, how we operate, and which proofs and standards we meet.

At a glance

- Encryption in transit (TLS 1.2+) and at rest (AES-256)
- Robust GCP-based serverless architecture with least-privilege access
- SOC 2 Type II (Security) attested period: **Sept 1, 2024** - **Aug 31, 2025**, report issued **Oct 2025**
- HIPAA-aligned safeguards; GDPR-compliant data rights & processes
- Clear data deletion path; standard deletion within 30 days (or sooner upon request)

Platform Overview

Who we are. Conclude is a European software company building no-code apps and collaboration tools that connect Microsoft Teams and Slack. We are headquartered in **Oslo, Norway,** with a hub in **Barcelona, Spain**, and presence in **Palo Alto, USA.**

What we provide.

- **Conclude Connect** – real-time interoperability between Slack and Microsoft Teams with channel/chat mirroring and file reference passthrough for unified collaboration.
- **Conclude Apps** – customizable, no-code workflow apps (incidents, issues, support, bug tracking, and more) that run inside Slack and Microsoft Teams. Apps can be enhanced with **Jira** and **Zendesk** integrations.

How we run. We operate on **Google Cloud Platform (GCP)** with a serverless architecture (Cloud Run) behind a global load balancer and WAF, using managed data services (Cloud SQL/PostgreSQL, Memorystore/Redis, Cloud Storage) and least-privilege IAM. Our frontend is **React/TypeScript;** backend services are **Go (Golang).**

Reference Architecture

High-level

- Cloud Load Balancer + Cloud Armor WAF - Cloud Run Service
- Identity/Secrets: Service Accounts (IAM) & Secret Manager
- Private egress via Serverless VPC Connector
- Data services: Cloud SQL (PostgreSQL), Memorystore (Redis), Cloud Storage (GCS)
- Observability: Cloud Logging & Monitoring with alerting; logs protected from tampering and restricted by IAM

Regionality

- Primary production region: **GCP us-central1 (Iowa).** Regional scoping is revisited with customers as needed.

Diagrams

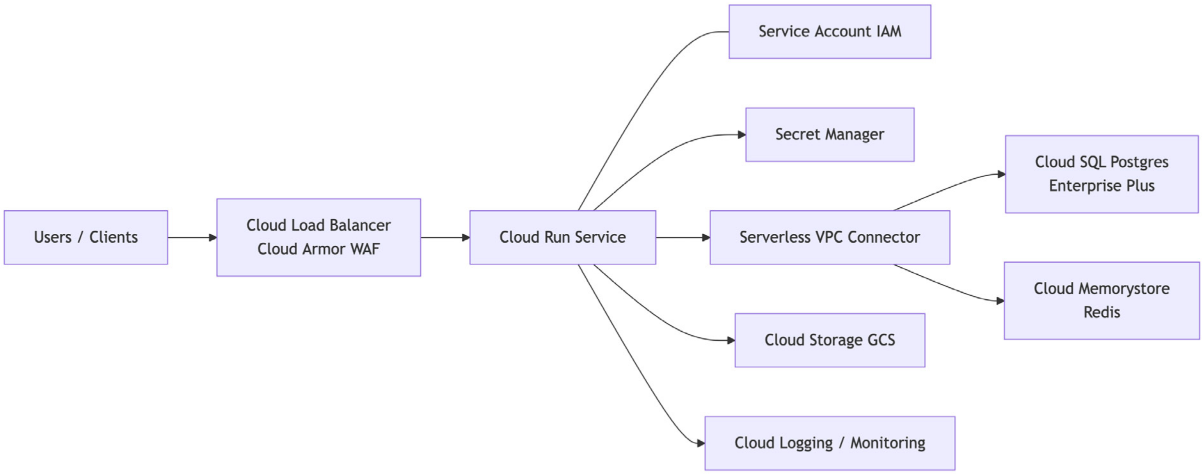


Figure 1: Platform architecture

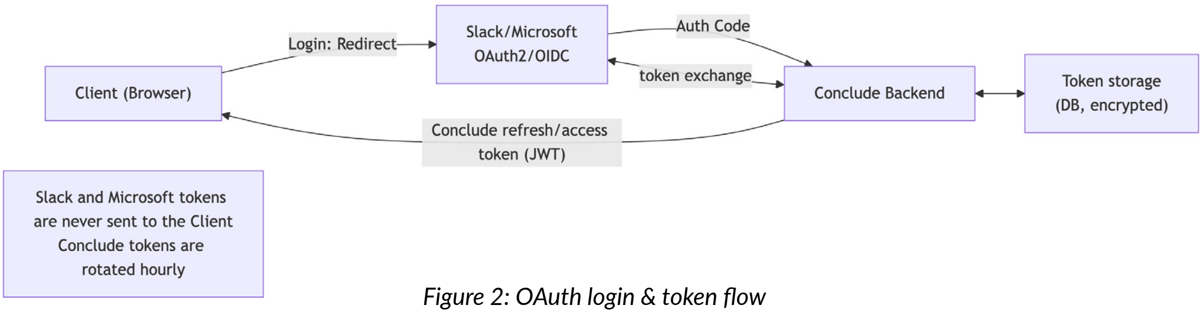

Client (Browser)
Login: Redirect
Slack/Microsoft OAuth2/OIDC
Auth Code
token exchange
Conclude Backend
Token storage (DB, encrypted)
Conclude refresh/access token (JWT)
Slack and Microsoft tokens are never sent to the Client Conclude tokens are rotated hourly

Figure 2: OAuth login & token flow

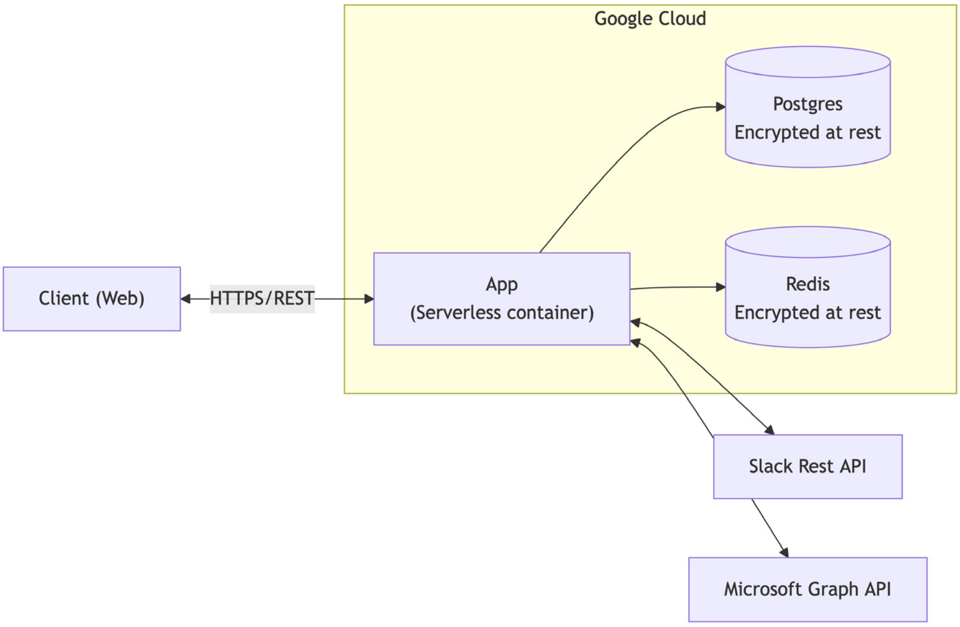


Figure 3: Data flow overview

Data Flow & Data Handling

- All client traffic uses HTTPS (TLS 1.2+; TLS 1.3 preferred where supported). OAuth2/OIDC with Slack and Microsoft—no user passwords stored by Conclude.
- Messages/files are processed pass-through for syncing with Conclude Connect; **no long-term storage of message or file content.**
- Minimal metadata retained (workspace/channel IDs, basic user profile info, timestamps, usage logs) for reconciliation, debugging, and auditability.
- File security remains enforced by Slack/Teams; Conclude does not host customer files.

Data categories

- **Public, Internal, Customer data,** Company data - handled per classification with controls appropriate to sensitivity.
- Customer data (incl. customer/user PII) access is strictly role-based and monitored.

***Data residency:** Primary production in GCP us-central1 (Iowa); regional options can be discussed case-by-case.*

Cryptography

- **In transit:** HTTPS/TLS 1.2+ for all client and service-to-service communications; **TLS 1.3** enabled where supported
- **At rest:** AES-256 on managed storage (Cloud SQL, Redis persistence, Cloud Storage)
- **Keys & secrets:** managed via GCP Secret Manager; access controlled by
- IAM and least-privilege service accounts

Identity, Access & Permissions

Customer identity & SSO

- Authentication via Slack/Microsoft (OAuth2/OIDC). MFA policies are enforced by the customer IdP. Conclude issues short-lived session tokens (rotated automatically); refresh/access tokens are JWT-based.

Least privilege

- Conclude requests only the minimal scopes needed for enabled features. Internal production access is role-based, time-bound, and logged. Access to customer data is limited to a **Core Security Team (CST).**

Approvals & SDLC

- All changes are peer reviewed, regression tested by CI, QA/UAT and approval steps; production is separated from dev/test; approvals are tracked.

Platform Permissions

- Microsoft Teams permissions (RSC & delegated):

https://conclude.io/doc/developer/permissions-microsoft-teams/

- Slack permissions (bot & user token scopes):

https://conclude.io/doc/developer/permissions-slack/

Compliance & Assurance

SOC 2 Type II—Security

- Scope covers the Conclude Platform and controls mapped to the AICPA Trust Services Criteria (Security, Confidentiality and Availability).
- Independent auditor's opinion: controls were suitably designed and operated effectively during the assessment period.
- Period: **Sept 1, 2024** - **Aug 31, 2025**, report date **Oct 2025.**

HIPAA

- Conclude implements safeguards aligned to HIPAA for handling PHI in supported use cases (BAA can be discussed where appropriate).

GDPR

- Conclude supports data subject rights (access, rectification, erasure) and acts as a processor where applicable. **Data Processing Agreement (DPA)** is publicly available: *https://conclude.io/data-processor/*

Terms of Service

- *Our Terms of Service, including data handling and acceptable use references, are public:*

  https://conclude.io/terms-of-service/

Vanta Trust Center

- Current control posture, policies, and select evidence are available in our Vanta Trust Center

Note: *The full SOC 2 report is a restricted-use document. We provide it under NDA upon request.*

Logging, Monitoring & Telemetry

- Centralized Cloud Logging with alerting for significant threats and anomalies
- Logs include user activities, exceptions, faults, security events; protected from tampering and restricted by IAM
- Health metrics, uptime monitoring, and alerts; daily automated backups for data stores

Vulnerability Management & Secure SDLC

- Automated dependency scanning and unit/integration tests in CI/CD; peer review for all code changes
- Static/dynamic security testing in CI/CD (incl. regular web app scanning); **staging** validation before production
- Annual **penetration testing**
- Patch management with severity-based SLAs

Incident Response & Breach Notification

- Formal IR Plan with roles, runbooks, communications, and evidence handling
- Monitoring with automated alerting and defined escalation procedures; incidents are triaged promptly during support hours, with critical events escalated per our IR plan
- Customer notification without undue delay if a breach affects their data

Recent history: *No security breaches reported in the last 24 months.*

Business Continuity & Disaster Recovery

- Managed backups (encrypted) with point-in-time recovery for data stores; monitored for completion and exceptions.
- Multi-zone, auto-healing serverless architecture; stateless app layer behind a global load balancer and WAF.
- Documented RTO/RPO with periodic tests.

Data Retention & Deletion

- Minimal metadata retained for operations and auditability
- No long-term storage of message or file content
- **Standard deletion:** within **30 days** of contract end (hard delete) or on request.

FAQs

What data is collected and how long is it stored?

We collect only what's necessary to operate Conclude and provide syncing:

- **User info:** name, avatar, email (when accessible via the customer's IdP/platform permissions)
- **Team/channel info:** names, IDs, and member lists
- **Message metadata:** identifiers and mapping needed to sync edits/deletes across platforms
- **Message content (text, images, attachments) is not stored**—it is processed ephemerally to perform the sync

Retention: *Data is retained for the duration of the customer agreement and deleted* ***upon request or within 30 days of termination*** *(hard delete), whichever comes first.*

Where is the data stored and processed?

All production data is hosted on **Google Cloud Platform (GCP) in us-central1 (Iowa, USA).** Processing occurs within this region. Data accessed via Slack/Microsoft/Jira/Zendesk APIs is subject to each provider's regional processing and your tenant configuration.

Is Conclude Connect secure?

Yes.

- **In transit:** TLS 1.2+ (TLS 1.3 preferred where supported)
- **At rest:** AES-256 encryption on managed GCP storage
- **No long-term message storage:** only minimal metadata is retained
- **Least privilege:** minimal scopes/permissions; role-based, time-bound internal access
- **Assurance:** SOC 2 Type II (Security) attested; HIPAA-aligned safeguards; continuous monitoring via **Vanta**; annual penetration testing

What data does Conclude store?

Minimal metadata necessary for service operation (workspace/channel identifiers, basic user info, timestamps, and usage logs). This enables reconciliation, debugging, and auditability. No long-term storage of message/file content.

Does Conclude Connect store user messages or files?

No. We do not store message bodies or files. We keep only the metadata required to mirror content between platforms.

What data does Conclude collect from connected platforms (Slack, Teams, Jira, Zendesk)?

Workspace names, user contact info (if authorized), channel/team data, actions within channels, and usage statistics - limited to what's required for the enabled features. Collection is authorization-based and governed by the scopes you approve.

How does Conclude handle messaging access on Slack?

Conclude can only view messages in channels/DMs where the app is a member. If the app is not present, no content is accessible. Conclude must be a member of a synced channel to mirror messages to Microsoft Teams.

How does Conclude handle messaging access on Microsoft Teams?

Conclude subscribes only to required Teams/chats. If the Teams app is installed in a team or chat, Conclude receives notifications about new messages there. Data not required for service delivery is ignored and immediately discarded. For connected channels/chats, only conversation metadata is stored.

How is data secured against potential breaches?

Defense-in-depth: encryption in transit/at rest, Google WAF, least-privilege IAM, secrets in GCP Secret Manager, centralized logging/alerting, vulnerability management and testing. No breaches reported in the last 24 months.

What happens if there’s an interruption in service?
The platform is designed for resilience (stateless services behind global load balancing, managed databases with PITR, autoscaling). We maintain runbooks for failover and recovery, and we communicate promptly during incidents.

Where can I see your current control posture?
Our **Vanta Trust Center:** *https://app.eu.vanta.com/conclude.io/trust/a3rjyink43zoeein0677tc.*
We provide the full SOC 2 report under NDA.

conclude

☎ +47 930 67760

✉ info@conclude.io

in /conclude