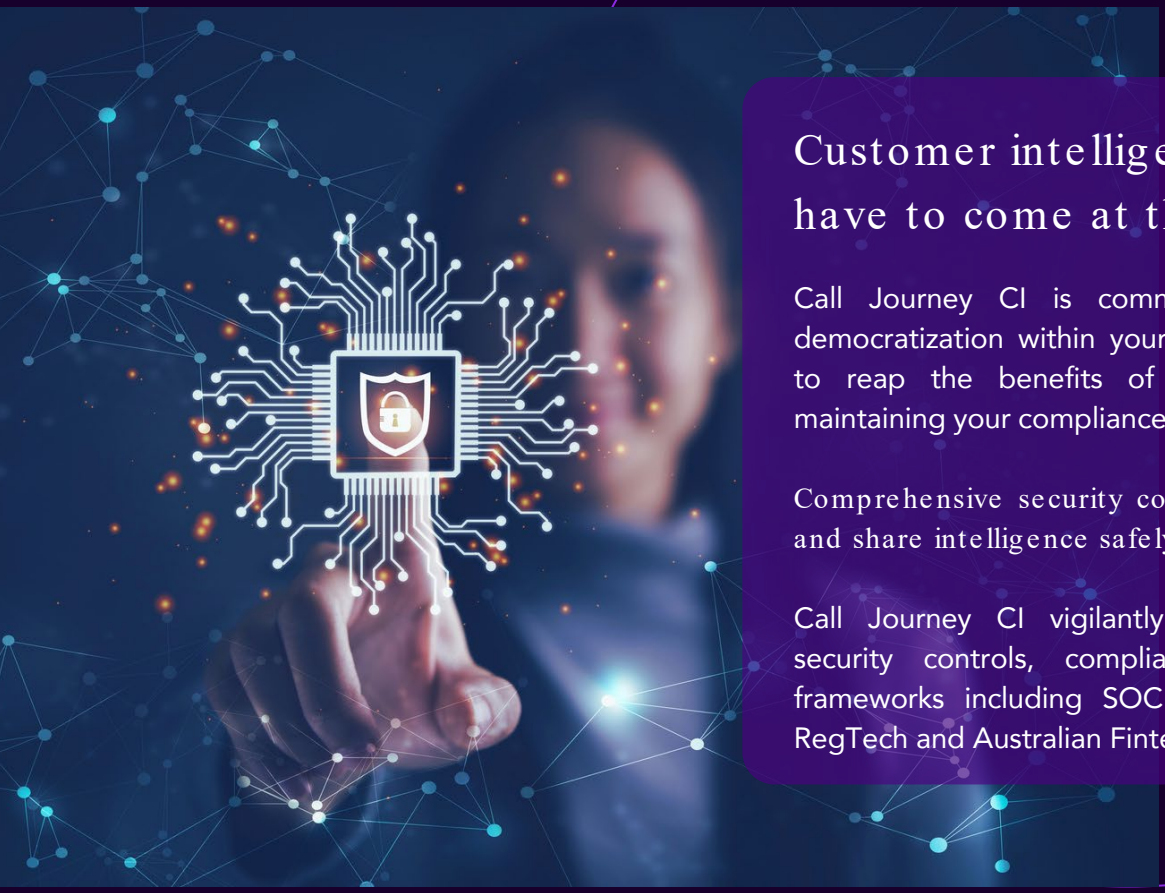
CALL JOURNEY ci

Security Controls



Customer intelligence doesn't have to come at the cost of trust

Call Journey CI is committed to improving data democratization within your organization, allowing you to reap the benefits of shared intelligence while maintaining your compliance obligations.

Comprehensive security controls allow you to access and share intelligence safely and securely.

Call Journey CI vigilantly maintains comprehensive security controls, compliant with leading security frameworks including SOC 2, HIPAA, GDPR, CCPA, RegTech and Australian Fintech.

About Call Journey CI

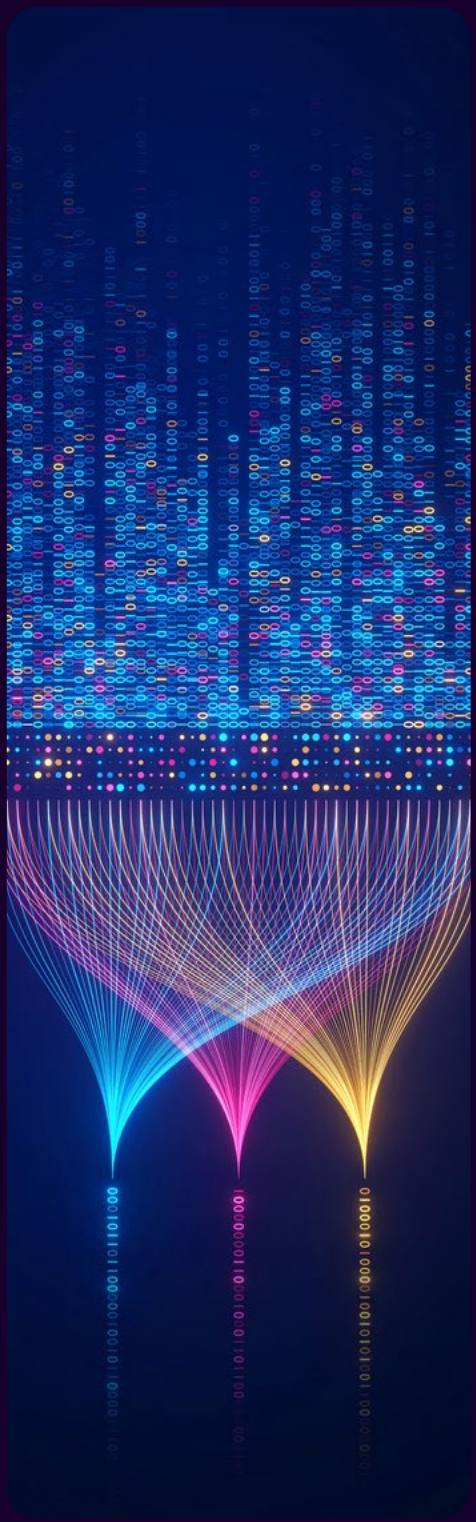
For truly customer-centric companies, conversation intelligence can be your greatest asset...provided you know how to harness it safely.

Call Journey CI is a highly secure analytical platform taking customer conversation excavation to new levels. It starts by digging deeper than anyone else, and ends as business intelligence gold right in the palms of your decision-makers.

We harness the best in NLP, deep machine learning, and the latest AI to create a deeply-layered understanding of the customer experience, including leading and lagging indicators of dissatisfaction and customer loyalty. We power the feedback loops that power your business.

Core Security Controls

Call Journey CI vigilantly maintains comprehensive security controls, compliant with leading security frameworks including SOC 2, HIPAA, GDPR, CCPA, RegTech and Australian Fintech.



This includes:

Encryption of data-at-rest and data-in-transit

- All data is encrypted in transit with TLS V1.2
- All data is encrypted at rest with 256-bit Advanced Encryption Standard (AES-256)

Secure access via SSO and MFA

- The Call Journey CI SaaS product supports SSO via OpenID implementations Azure Active Directory and Okta
- MFA is supported via integration with your SSO provider
- All production systems require MFA authentication.

Strict policies and procedures as part of preventative and proactive security measures

- Change and configuration management
- Vulnerability management program
- Incident response, DR and BCP
- Security event monitoring and alerting
- Employee and contractor training and access management
- Information Security management

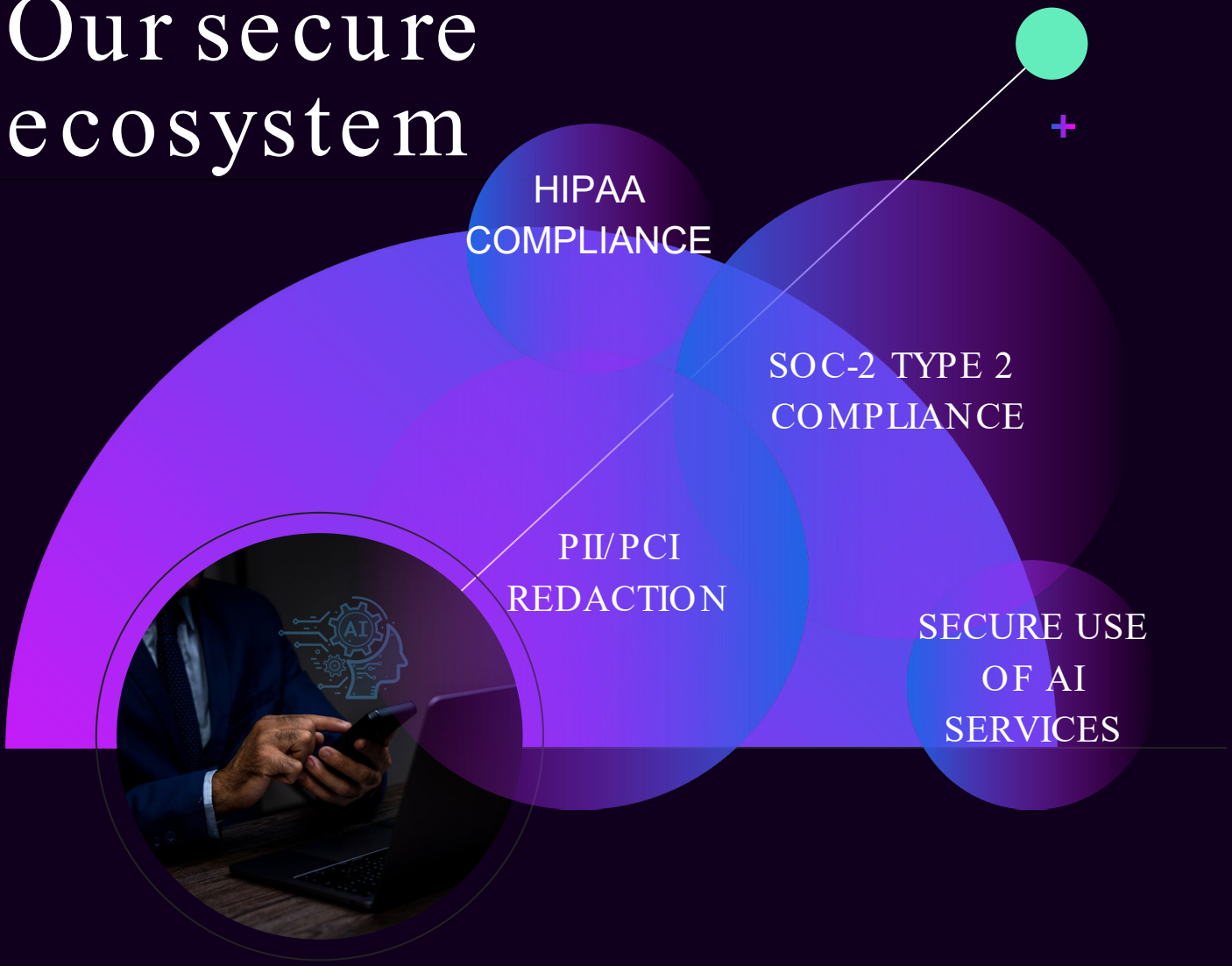
PII/PCI Redaction

- Redaction of personal information from transcriptions and audio
- Deployable either on-premise or via cloud

SOC 2 TYPE 2 · HIPAA COMPLIANT · GDPR READY · CCPA READY · RegTech · Australian FINTECH

CALL JOURNEY ci

Our secure ecosystem



Every component of our architecture is vetted for security as part of Call Journey CI's SOC-2 Type 2 compliance.

Call Journey CI does not integrate with any sources outside of our environment. Our ecosystem includes:

- AWS and Azure Cloud services
- A closed-source proprietary Large Language Model (LLM)

For any particular documentation or solutions involving our extended ecosystem, please contact us.

DATA SCIENCE

+ Use of Generative AI

Call Journey CI makes use of AWS & Azure LLMs and Generative AI capabilities. No customer-identifiable data is passed through to these services

+ Regional Capability

No data is stored out-of-region.

Introducing our Advanced PII/PCI Redaction

Deployable either on-premise or cloud, Call Journey CI's PII Redaction process protects your customers' identities, helping you fulfil your security commitments while maintaining the trust of your customers.

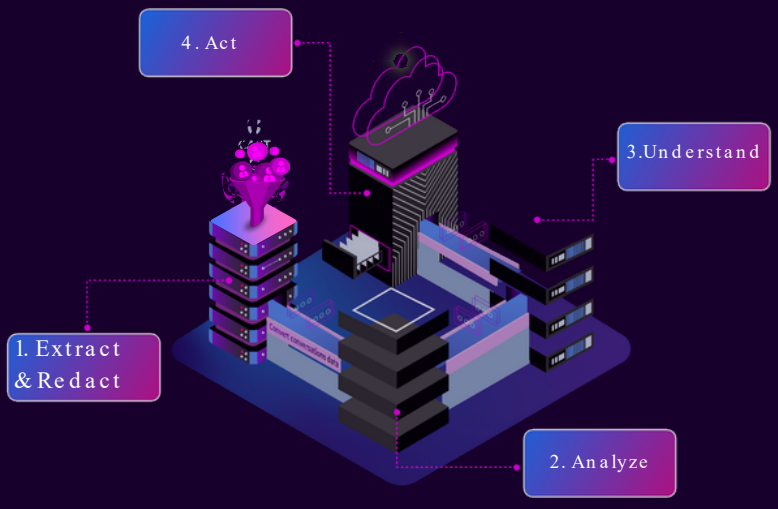
This includes:

- Names
- Email addresses
- Birthdates and other significant dates e.g. travel, transactions
- Significant numbers - credit cards, passwords, license, social security number, postal code
- Nationality
- Locations - mailing address, state, city, town, country
- Money amount

How it works

Call Journey CI uses AI, NLP and machine learning to remove personally identifiable information from voice transcriptions and audio files, ensuring the person is not identifiable and sensitive information is not visible in the transcription or audible in the audio.

This allows you to securely and safely analyze and act on customer intelligence, while remaining compliant.



SOC 2 TYPE 2 · HIPAA COMPLIANT · GDPR READY · CCPA READY · RegTech · Australian FINTECH

Extended Security Controls

Audit and Compliance
Call Journey CI maintains complete ongoing, validated compliance with the SOC-2 Type 2 Framework. Our ecosystem is also HIPAA Compliant and GDPR Compliant.

Anti-virus
All staff machines have anti-virus protection installed, and signatures are updated daily.

Background checks and NDAs for employees and contractors
Call Journey CI conducts background checks on all employees before employment and employees receive privacy and security training during onboarding as well as on an ongoing basis. All employees are required to read and sign our comprehensive information security policy covering the security, availability and confidentiality of our services.

Browser and client-side dependencies
The Call Journey CI suite is tested on Google Chrome. The latest version and one version lower are supported. No custom client-side libraries are required.

Change and configuration management
All systems that run the Call Journey CI SaaS product have configuration standards. Any change to the configuration of a production system goes through the change management process outlined in the Change Management Policy.

Data-at-rest encryption
All data is encrypted at rest with 256-bit Advanced Encryption Standard (AES-256)

Data-in-transit encryption
All data is encrypted in transit with TLS V1.2

Data center physical security
Call Journey CI operates services in the AWS and Microsoft Azure public clouds. To prevent unauthorized access to the physical servers and data centers, both cloud providers have implemented state-of-the-art physical security processes.

Data Sovereignty
Call Journey CI maintains data sovereignty through in-region storage, subject to the laws and governance structures of the nation where they are collected

Incident response plan
Call Journey CI has a formal incident response plan in place, based on NIST. Once 'containment, eradication & recovery' are completed, the incident will be communicated with 24 hours of its occurrence.

Independent third-party penetration testing
Call Journey CI's s in-house security team conduct penetration testing on all major releases or system changes. Penetration tests are also conducted annually; a summary report is available on request. Call Journey CI also makes its production environment open to penetration testing at any time. This excludes DDOS attacks.

Limited privileged access
Call Journey operates a least privileges model, where only Admin staff has admin permissions.

MFA
MFA is supported via integration with your SSO provider

MFA for administrative users and remote users
All production systems require MFA authentication.

Monitoring and alerting of security events
Call Journey CI logs all relevant user events and these logs are kept for 180 days. Logs are available upon request.

PII/PCI Redaction
Intelligent redaction of sensitive personal information both in the conversation transcript and the audio itself.

Security awareness
Per Call Journey CI's "Information Security Awareness Training Policy", all staff undergo security awareness training during onboarding and refresh the training annually.

Security certification
Call Journey CI has undergone an SOC 2 audit and a copy of the most recent report is available upon request from your Account Manager.

Secure coding
Call Journey CI follows the OWASP secure coding practices. Operating an agile SDLC, security is considered in the design, code reviews and testing.

SSO Integration support
The Call Journey CI SaaS product supports SSO via the Azure Active Directory provider.

Vendor management program
Call Journey CI partners with a select number of analytical vendors to enhance our capabilities. All vendors are audited and vetted on a recurring basis to ensure the utmost data protection.

Vulnerability management program
Call Journey CI operates the Azure Sentinel SIEM to monitor all systems and provide continuous vulnerability scanning and remediation.

We Do Not Sell Your Data
Customer data is only used to provide you with features and services within the Call Journey ecosystem. Call Journey does not use your data for any commercial gain beyond these services or make the data available for others to make commercial gain

Ready to safely and securely harness the power of conversation intelligence?

Contact us today:

sales@calljourney.com

SOC 2 TYPE 2 · HIPAA COMPLIANT · GDPR READY · CCPA READY · RegTech · Australian FINTECH