AI SECURITY

works

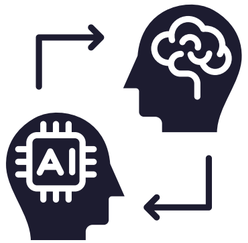
OBJECTIVE

This document outlines Wxrks' comprehensive approach to AI security.

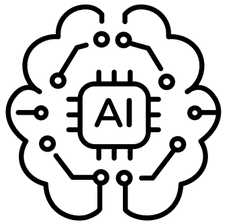
Table of Contents

CORE COMPONENTS OF AI SECURITY

Platform Security



Interaction with AI Models



Governance of AI Models

SOC 2 Type 2 Certification

Wxrks is a SOC 2 Type 2 certified company, undergoing annual third-party audits to maintain stringent data security standards.

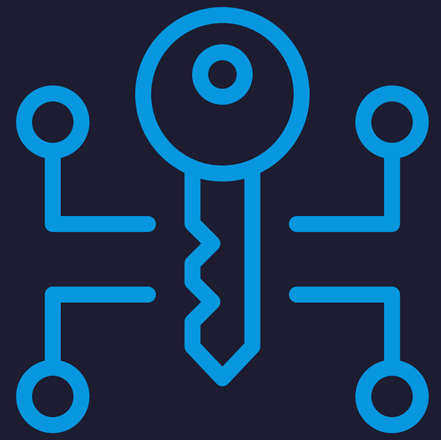
Copies of our latest audit reports and internal policies are available upon request.

Account and Data Isolation

- **Siloed Accounts:**Each user account operates in an isolated environment, ensuring no cross-account data visibility.
- **Granular Permissions:** Access to data is restricted based on roles, ensuring data is accessible only to authorized personnel.

Data Storage & Encryption

All data is stored in AWS us-east-1, encrypted at rest using AES-256 encryption with keys hosted separately.



Audit Trails

Comprehensive audit logs are maintained for three months and are available free of charge for analysis and compliance requirements.

HOW WXRKS INTERACTS WITH AI

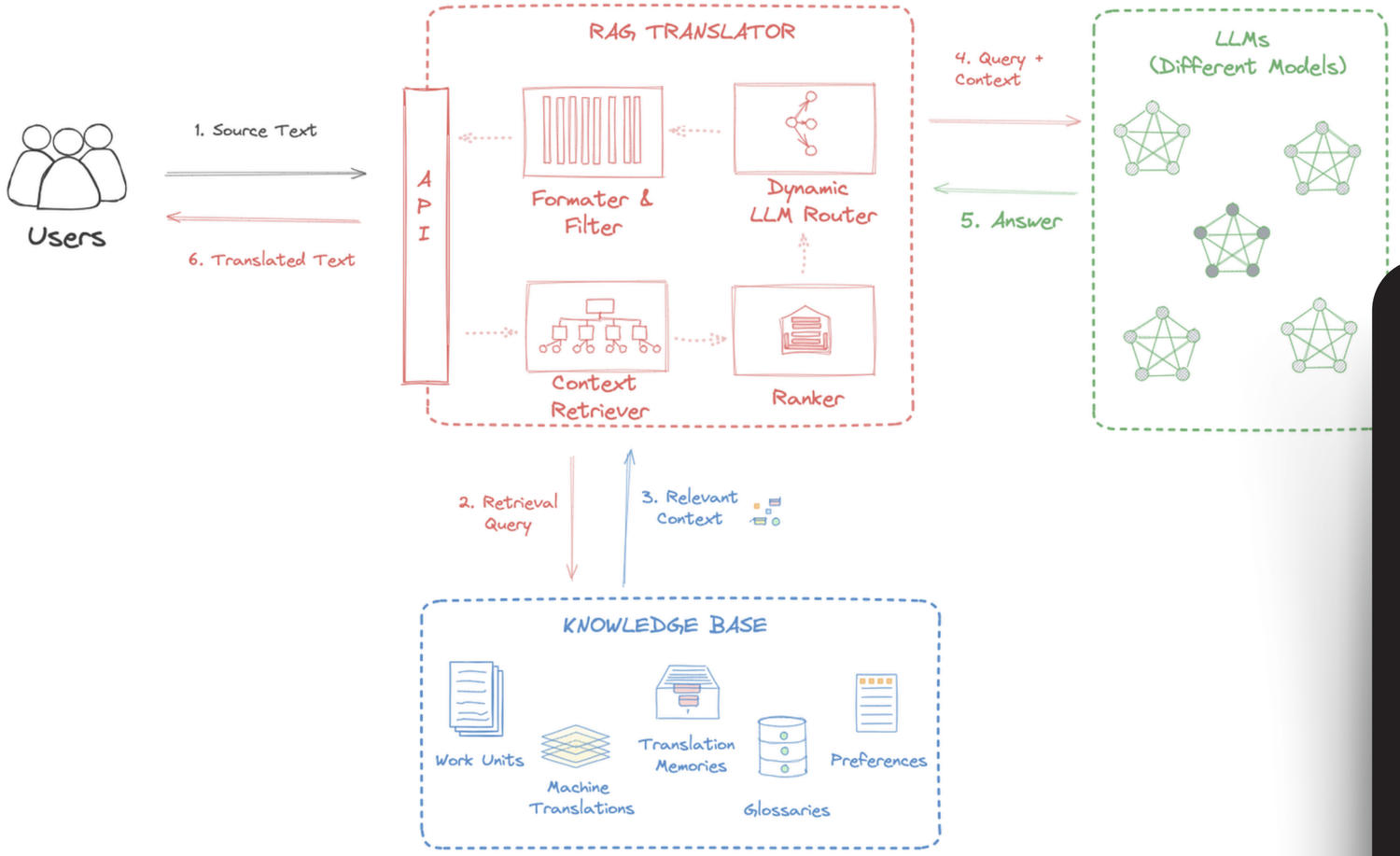
Wxrks emphasizes **secure, efficient, and predictable** AI interactions.

Stateless Interactions

By default, Wxrks interacts with stateless models, ensuring no data persists within these models unless otherwise directed by the Subscriber.

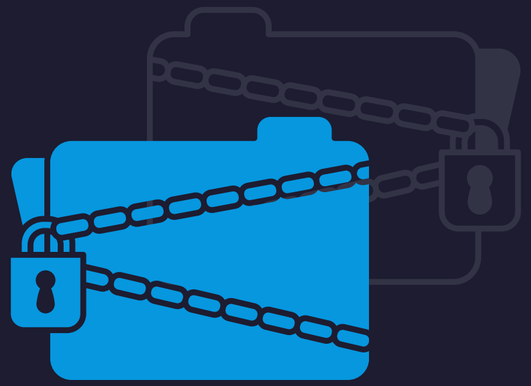
Few-Shot **Learning**

Leveraging a proprietary Retrieval-Augmented Generation (RAG) framework, Wxrks employs context-sensitivity to deliver precise responses.



Benefits of RAG Optimized Few-Shot Learning:

- Reduced computational expense.
- Optimized prompts for greater response accuracy.
- Enhanced predictability and user-aligned experiences.



Data Residency and Ownership

- Data generated through interactions resides exclusively within Subscriber’s Wxrks account unless explicitly configured to interact with Subscriber-specific models.
- Wxrks uses anonymized, aggregated metadata (e.g., project volumes, average task completion time) solely for platform optimization.

Context Sensitivity

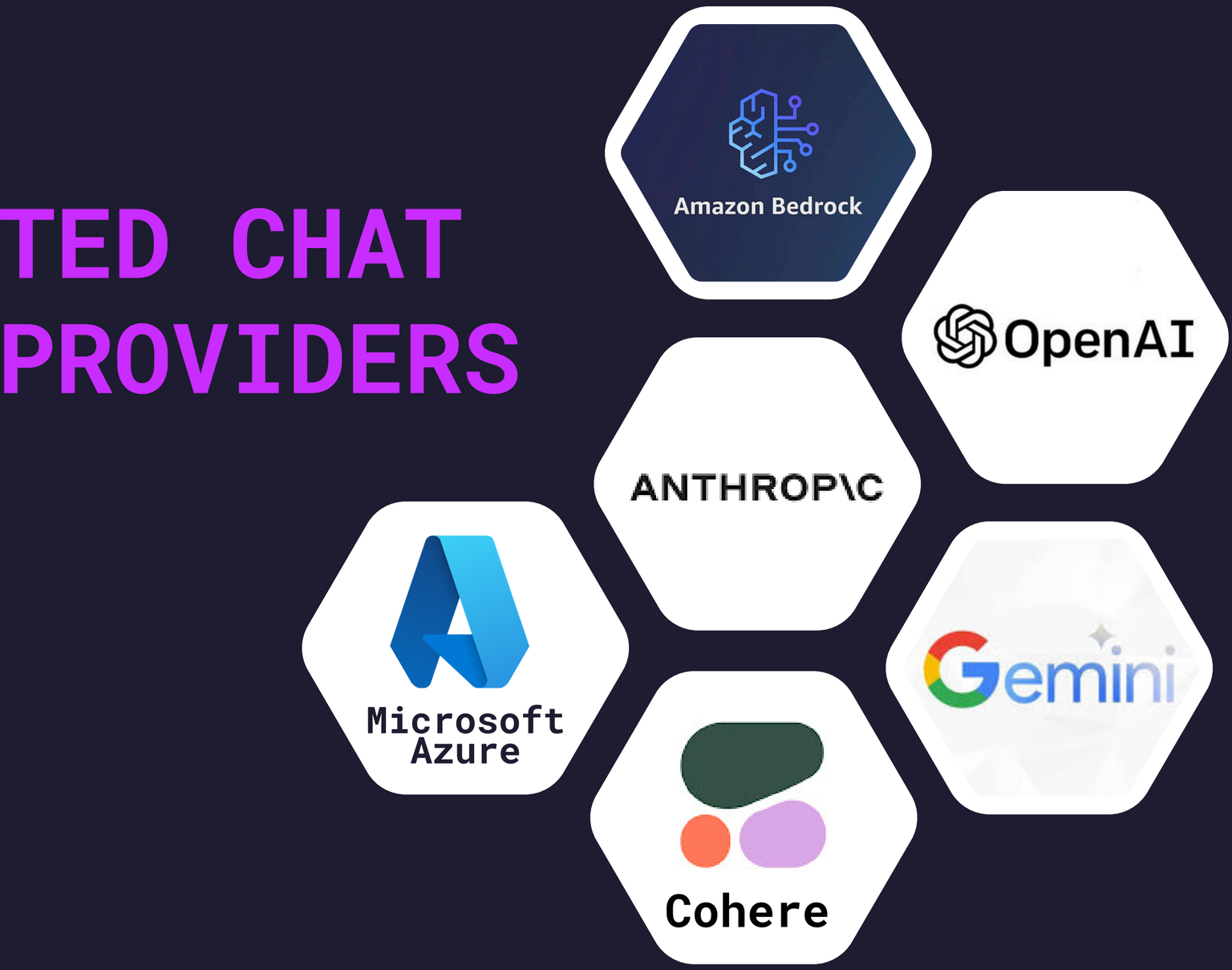
All translation interactions use a few-shot training approach, maintaining alignment without relying on model retraining.

Wxrks guarantees that the Subscriber retains exclusive ownership of its data, ensuring it is not utilized for external training or analysis.

GOVERNANCE OF AI MODELS

Wxrks supports seamless integration with leading AI models, ensuring flexibility and security

SUPPORTED CHAT MODEL PROVIDERS



MODEL SECURITY PROTOCOLS

Models integrated with Wxrks must adhere to the following principles:

- **Encryption:** Data stored temporarily must be encrypted for security purposes.
- **Retention Policy:** All temporary data must be permanently deleted within 30 days unless otherwise directed.

These principles can be overridden by the Account Owner if using proprietary Subscriber models.

Stateless by Design

Wxrks enforces stateless configurations
across integrated models
to enhance data privacy.

DIFFERENTIATORS

01

PROPRIETARY AI FRAMEWORKS

Wxrks combines RAG frameworks with AI augmentation for a context-sensitive user experience.

02

ALIGNMENT WITH SUBSCRIBER STANDARDS

Wxrks customizes AI workflows to align with Subscriber’s internal AI strategies and security expectations.

03

CUSTOMER-CENTRIC SECURITY

All interactions, integrations, and data policies prioritize the Subscriber’s sovereignty over its data.

CONCLUSION

Wxrks' AI security strategy balances flexibility, innovation, and stringent security protocols.

By combining robust platform security with stateless and context-sensitive AI integrations, we deliver a scalable, secure, and user-focused AI experience tailored to Subscriber's unique requirements.

If you have additional requests for specific security or integration needs,Wxrks remains committed to accommodating and customizing solutions for Subscribers.

Please write to us at architecture@wxrks.com


MAKE IT
wxrks
wxrks.com