

AI-Worker

● CURRENT STATUS: BUILDING MVP

Concept Note: Voice-First Intelligence

Version 1.0 • 2025

ai-worker.tech

INTRODUCTION

AI-Worker is a voice-first desktop workspace designed to revolutionize productivity by integrating Large Language Models (LLMs) with everyday applications and files using the **Model Context Protocol (MCP)**. We are currently in the **active MVP development stage**, providing high-performance orchestration via secure cloud-based LLM connectivity.

● Problem Statement

- AI assistants are siloed and text-heavy.
- Lack of seamless integration with enterprise tools.
- Privacy concerns with cloud-only data exposure.

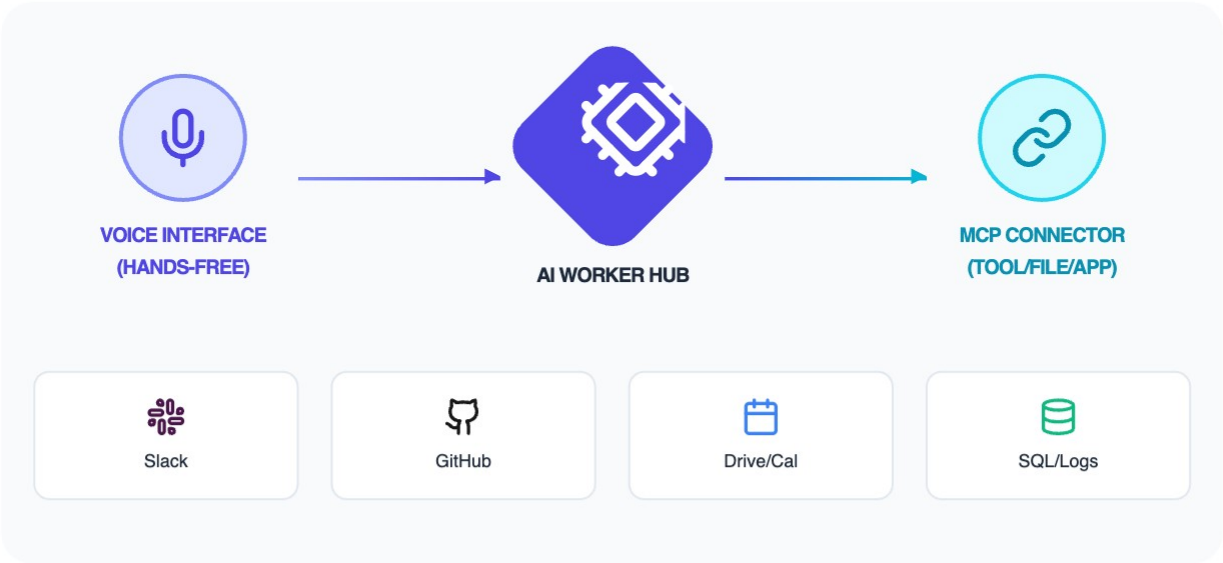
● The Solution

A universal bridge using **MCP** to connect state-of-the-art LLMs (Cloud) to local apps. This hybrid model ensures maximum capability today while architecting for a local-first future.

🛡️ COMPUTE STRATEGY

"If users' systems are capable of running local LLMs, and with the anticipated availability of lightweight machine-runnable LLMs (e.g., Chrome Gemini Nano or Phi models on Chrome and Edge browsers), AI-Worker will support fully privacy-focused operation locally at that time."

Workflow Integration Ecosystem



KEY FEATURES

MCP Connector
Bridge cloud brains to local tools and files.

Voice Native
Full system control via low-latency voice UX.

Hybrid Privacy
Zero Trust architecture for data processing.

Cross Platform
Native support for Mac, Win, and Linux desktops.

Agentic Workflows
Autonomous execution of complex tool chains.

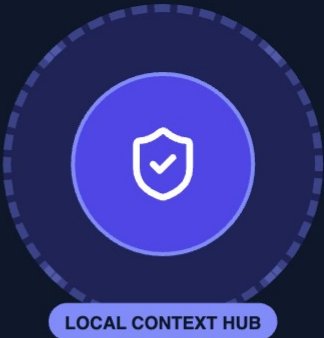
Secure Context
End-to-end encrypted model communications.

Architecting for Privacy

Secure Cloud integration today, Edge intelligence tomorrow.

Current: Hybrid Cloud
High-performance LLMs (Cloud) via secure MCP bridges.

Future: Local Edge
Gemini Nano / Phi on-device processing when available.



MARKET POSITIONING

STANDARD CHATBOTS		AI-WORKER (MVP)	
Interface	Text-Heavy	Interface	VOICE-FIRST
Context	Cloud-Only	Context	HYBRID BRIDGE
Workflow	Siloed	Workflow	MCP-INTEGRATED

STRATEGIC ROADMAP

- 1

Phase 1: Foundation & Cloud-Bridge MVP

CURRENT STAGE

Currently engineering the MVP. Utilizing high-performance Cloud LLMs connected via MCP to validate voice-native workflows and agentic capabilities.
- 2

Phase 2: Hybrid & Local Alpha

Experimental support for lightweight machine-runnable LLMs (Gemini Nano/Phi). Enabling fully privacy-focused offline operations for specific user tiers.
- 3

Phase 3: Edge Dominance

Production rollout of on-device intelligence. Fully autonomous, air-gapped workflows for enterprise security compliance.