DDX AiX Enterprise Platform

Technical Presentation

Self-Hosted, Secure, Governed AI Platform for
Regulated Environments

Your AI. Your Data. Your Control

DDX Business Solutions Limited

The company behind the AiX Enterprise Platform

- **Hong Kong-based** tech company established in 2023

- Helping organizations address **governance, data privacy, and AI adoption** challenges

- Developing secure and scalable **GenAI solutions** for modern enterprises

- **AiX** – our enterprise-grade GenAI platform using *your data with your control*

- Fully designed and developed in-house by **DDX** with 100% ownership of all source code and intellectual property

Your AI. Your Data. Your Control

Major Challenges of AI Adoption

Critical Barriers of Enterprises to Successful Implementation

DD X

Challenge 4

Difficulty Scaling AI

- Pilots works, but scaling is inconsistent and costly
- No standardized, reusable workflow automation framework
- High operational overhead managing tokens across solutions

Challenge 3

Governance & Vendor Lock-in Concerns

- Limited visibility into data usage, storage, and access
- Hard to enforce consistent governance and audits
- Closed platforms restrict model choice and hinder future migration

Challenge 2

Fragmented Data & Complex Integrations

- Information spread across emails, files, chats, and systems
- Lack of connectors for end-to-end automation
- Integrations require custom development and specialized skills
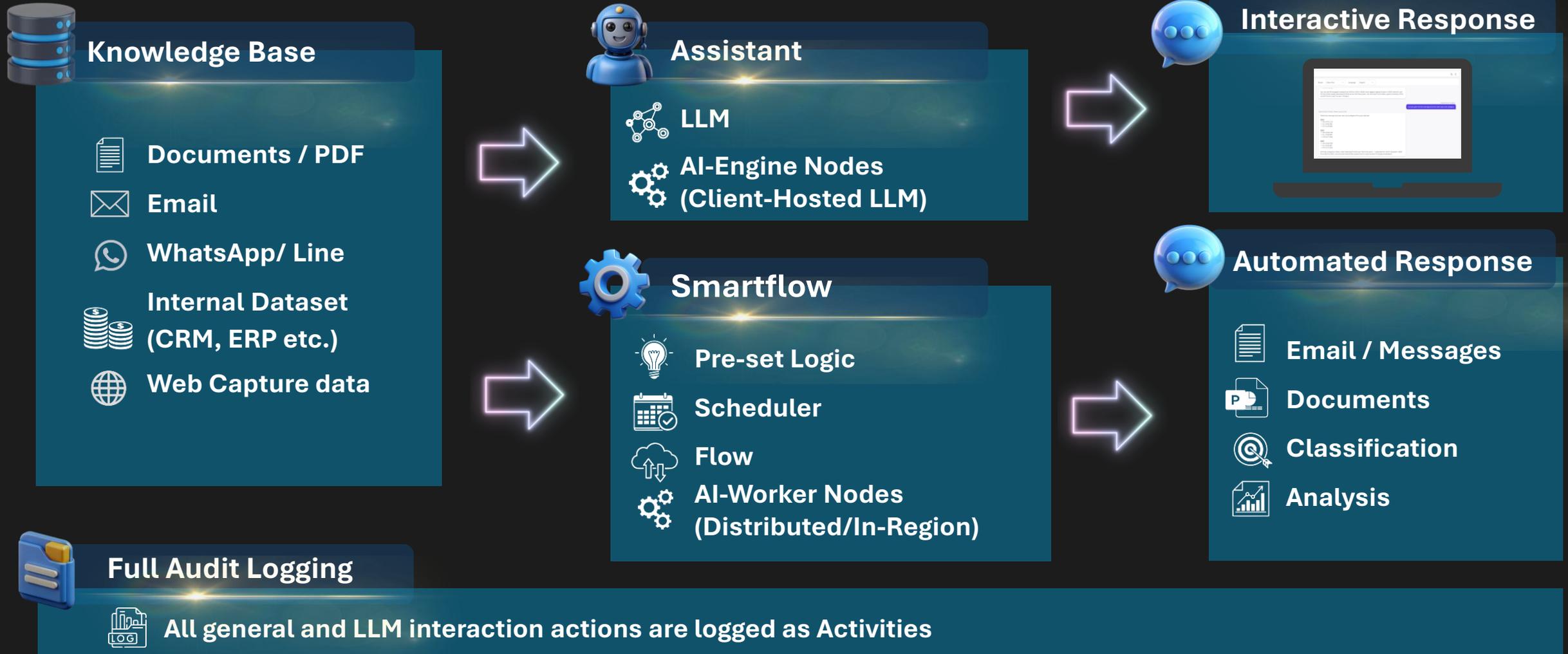
Challenge 1

Limited Technical Expertise & AI Skill Gaps

- Limited in-house AI and automation talent
- Business teams can't build or maintain AI workflows independently
- Heavy dependence on consultants slows adoption and drives up cost
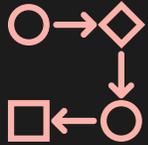
Your AI. Your Data. Your Control

What is Ai X

Self-hosted enterprise AI platform that transforms internal knowledge into actions & answers

Knowledge Base

- Documents / PDF
- Email
- WhatsApp/ Line
- Internal Dataset (CRM, ERP etc.)
- Web Capture data

Assistant

- LLM
- AI-Engine Nodes (Client-Hosted LLM)

Smartflow

- Pre-set Logic
- Scheduler
- Flow
- AI-Worker Nodes (Distributed/In-Region)

Interactive Response

Automated Response

- Email / Messages
- Documents
- Classification
- Analysis

Full Audit Logging

All general and LLM interaction actions are logged as Activities

Why AiX

Built for Business & IT with Your AI. Your Data. Your Control.

No Code Business Ready

- Business-friendly user interface, ready to use
- Drag-and-drop workflow building
- Prebuilt assistants & templates, no coding

Private, Secure Auditable

- Self-hosted, full data control
- Comprehensive audit logging with clear token usage
- Role-based access control for compliance

All-in-One Platform

- Chatbot, Knowledge Base, SmartFlow & Scheduler
- Integration with connectors
- Unified workspace for business & IT

Flexible AI Options

- Support Local, Cloud, or Hybrid AI Models.
- Mix and match AI providers
- Optimize cost, performance, compliance

Boost Efficiency with AI

- Automate repetitive, manual tasks
- Minimize errors and reduce rework
- Streamline and optimize with workflow approach

Your AI. Your Data. Your Control

Application Scenarios

Innovative, Practical, Flexible

Customer Emails Classification

- CRM teams spend significant time manually classifying email enquiries, often leading to delays and errors.

  SmartFlow can integrate with Outlook to classify and tag emails using LLM.

Order Data Extraction

- Sales teams spend significant time extracting order details from messages, emails and attachments.

  Whatsapp or other IM services can be integrated for order extraction with LLM.

Internal Chatbot

- Chatbot development is time-consuming and many IT teams lack the know-how on testing the "knowledge".

  Users can create their own knowledge base and assistant with custom prompts.

Legal Documentation Research

- High volume and repetitive document reviews and comparison drain Legal teams' effort.

  Users can upload legal documents for QnA and Knowledge Base.

Notification & Memo Drafting

- HR/Admin teams spend time drafting notices (e.g. Job postings, Internal notices) with templates and tones.

  SmartFlow can be built by uploading requirements and using LLM prompts.

Product Searching

- Customers often provide vague or incomplete queries, making it hard to find the right product.

  Pin SmartFlow with Chat and let users find products using incomplete details.
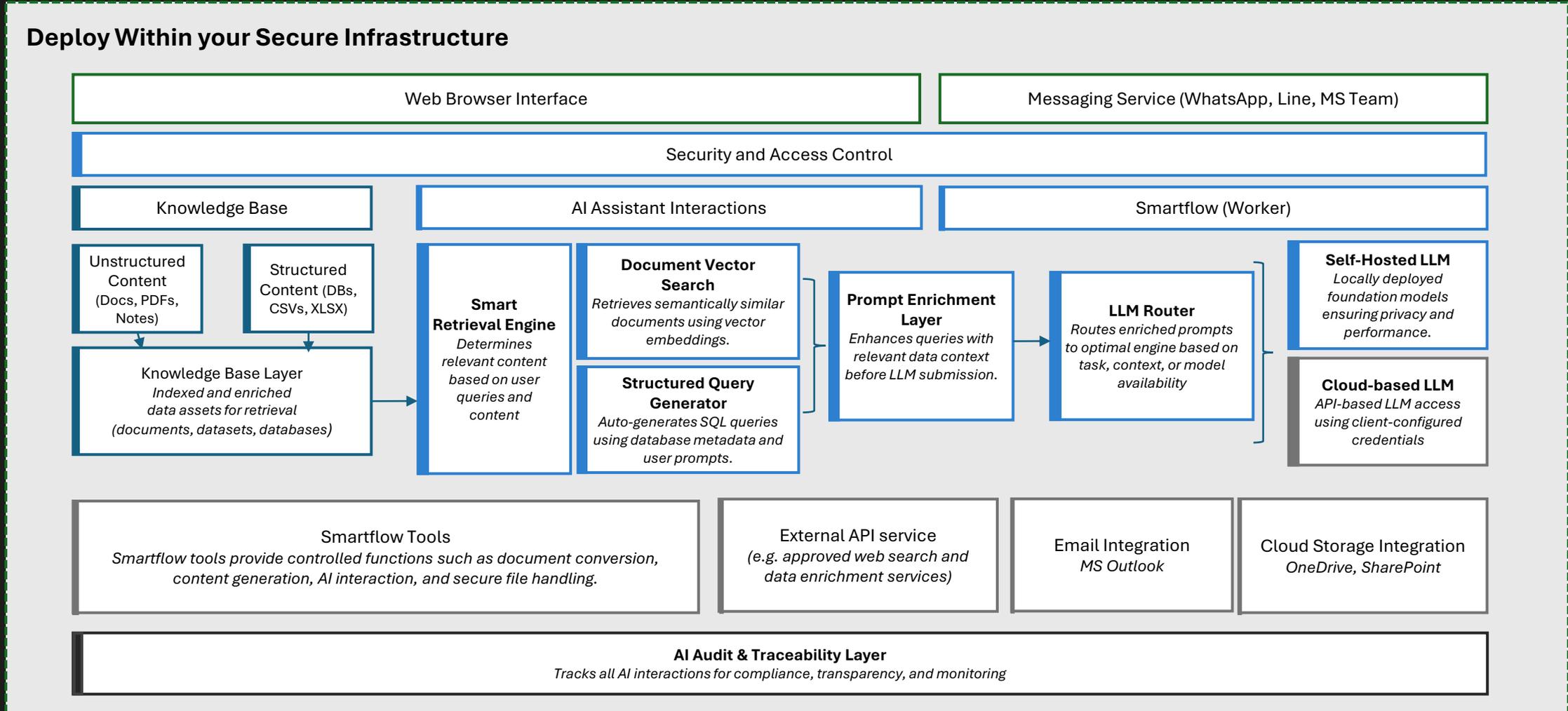
Your AI. Your Data. Your Control

Thank You

enquiry@ddxbiz.com

Architecture Overview

A self-hosted, layered AI architecture designed for security, governance, and full data control.

Deploy Within your Secure Infrastructure

Web Browser Interface	Messaging Service (WhatsApp, Line, MS Team)

Security and Access Control

Knowledge Base	AI Assistant Interactions	Smartflow (Worker)

Unstructured Content (Docs, PDFs, Notes)

Structured Content (DBs, CSVs, XLSX)

Knowledge Base Layer
Indexed and enriched data assets for retrieval (documents, datasets, databases)

Smart Retrieval Engine
Determines relevant content based on user queries and content

Document Vector Search
Retrieves semantically similar documents using vector embeddings.

Structured Query Generator
Auto-generates SQL queries using database metadata and user prompts.

Prompt Enrichment Layer
Enhances queries with relevant data context before LLM submission.

LLM Router
Routes enriched prompts to optimal engine based on task, context, or model availability

Self-Hosted LLM
Locally deployed foundation models ensuring privacy and performance.

Cloud-based LLM
API-based LLM access using client-configured credentials

Smartflow Tools
Smartflow tools provide controlled functions such as document conversion, content generation, AI interaction, and secure file handling.

External API service
(e.g. approved web search and data enrichment services)

Email Integration
MS Outlook

Cloud Storage Integration
OneDrive, SharePoint

AI Audit & Traceability Layer
Tracks all AI interactions for compliance, transparency, and monitoring

Component Overview

Clearly defined responsibility, ensuring secure operation, controlled data access, and scalable AI processing within enterprise environments.

Web
Provides the browser-based user interface for accessing AiX functionality.
- Supports business users and administrators
- Access to assistants, workflows, dashboards, and configuration views
- Enforces authentication and role-based access control

Console
Acts as the **platform control** for infrastructure and service management.
- Register and configure newly deployed nodes
- Manage service connectivity and trust relationships
- Control node lifecycle and environment configuration

AppServer
Serves as the **secure application gateway** to persistent data storage.
- Enforces access control and business rules
- Manages all read/write operations to the database
- Prevents direct database access by external or downstream services

Database
Provides persistent, auditable storage using PostgreSQL.
- Knowledge assets and metadata
- User activity and audit logs
- Workflow and execution state

MsgServer
Acts as a **secure webhook and ingestion service** for external messaging platforms.
- Receives events from WhatsApp, LINE, and Microsoft Teams
- Normalizes and forwards messages to the AppServer for persistence and processing
- Ensures controlled and auditable message ingestion
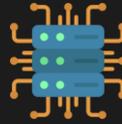
AiServer
Handles **AI asset processing and preparation** for downstream AI workflows:
- Document ingestion, extraction, and preprocessing
- Vectorization and embedding generation
- Controlled interaction with external LLM services via client-configured APIs

AiWorker
Executes **Smartflow workflows** in a controlled and scalable manner.
- Run predefined logic and scheduled workflows
- Perform distributed or in-region processing
- Scale horizontally based on workload demand

AiEngine
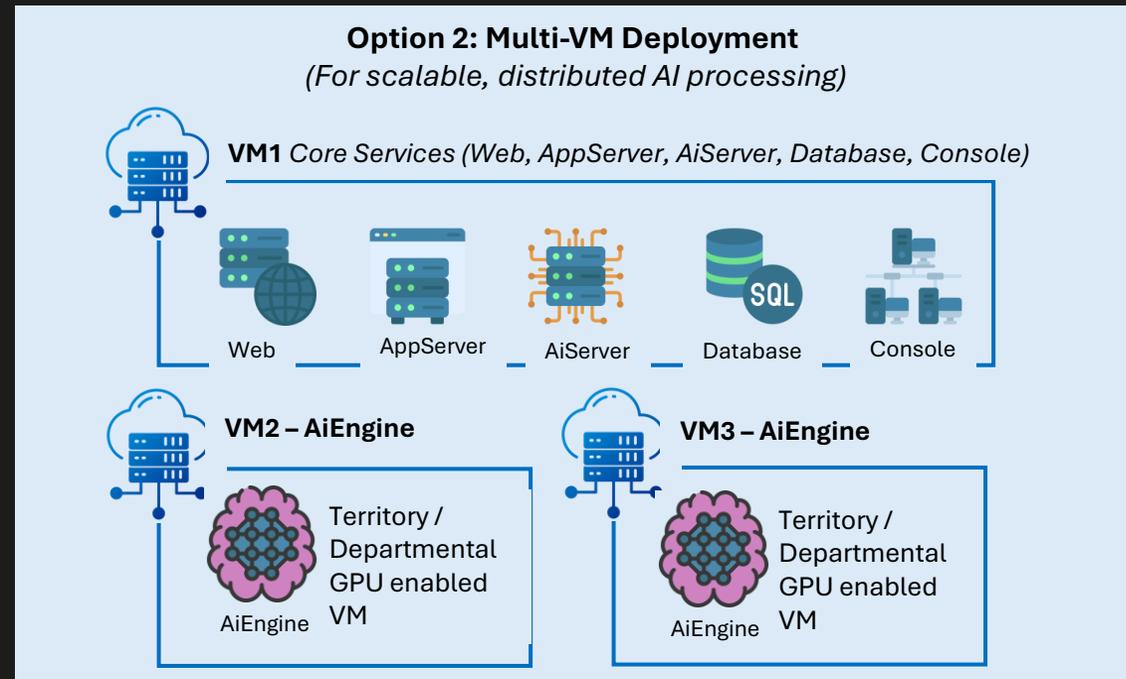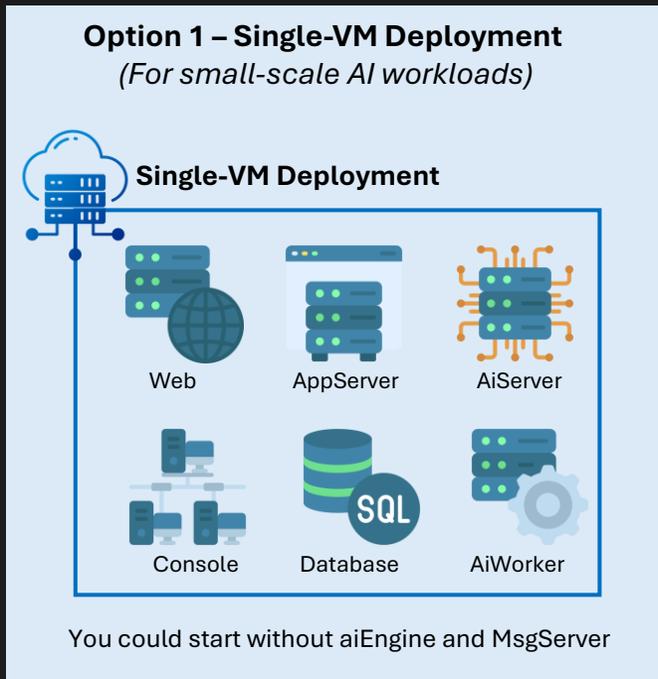Executes **locally deployed, GPU-accelerated LLMs** within the client environment.
- Hosts client-managed LLMs on GPU-enabled machines
- Provides high-performance inference for sensitive workloads
- Ensures data privacy and full infrastructure control

DDX AiX Enterprise is a modular, scalable AI platform designed to deliver governed, auditable AI outcomes while maintaining full client control over data and infrastructure.

Your AI. Your Data. Your Control

Deployment & Scaling

Start small and scale as your AI needs grow. Begin with a single machine and expand with additional AI-powered VM instances as demand increases.

Option 1 – Single-VM Deployment
(For small-scale AI workloads)

Single-VM Deployment

Web AppServer AiServer

Console Database AiWorker

You could start without aiEngine and MsgServer

Option 2: Multi-VM Deployment
(For scalable, distributed AI processing)

VM1 *Core Services (Web, AppServer, AiServer, Database, Console)*

Web AppServer AiServer Database Console

VM2 – AiEngine

AiEngine — Territory / Departmental GPU enabled VM

VM3 – AiEngine

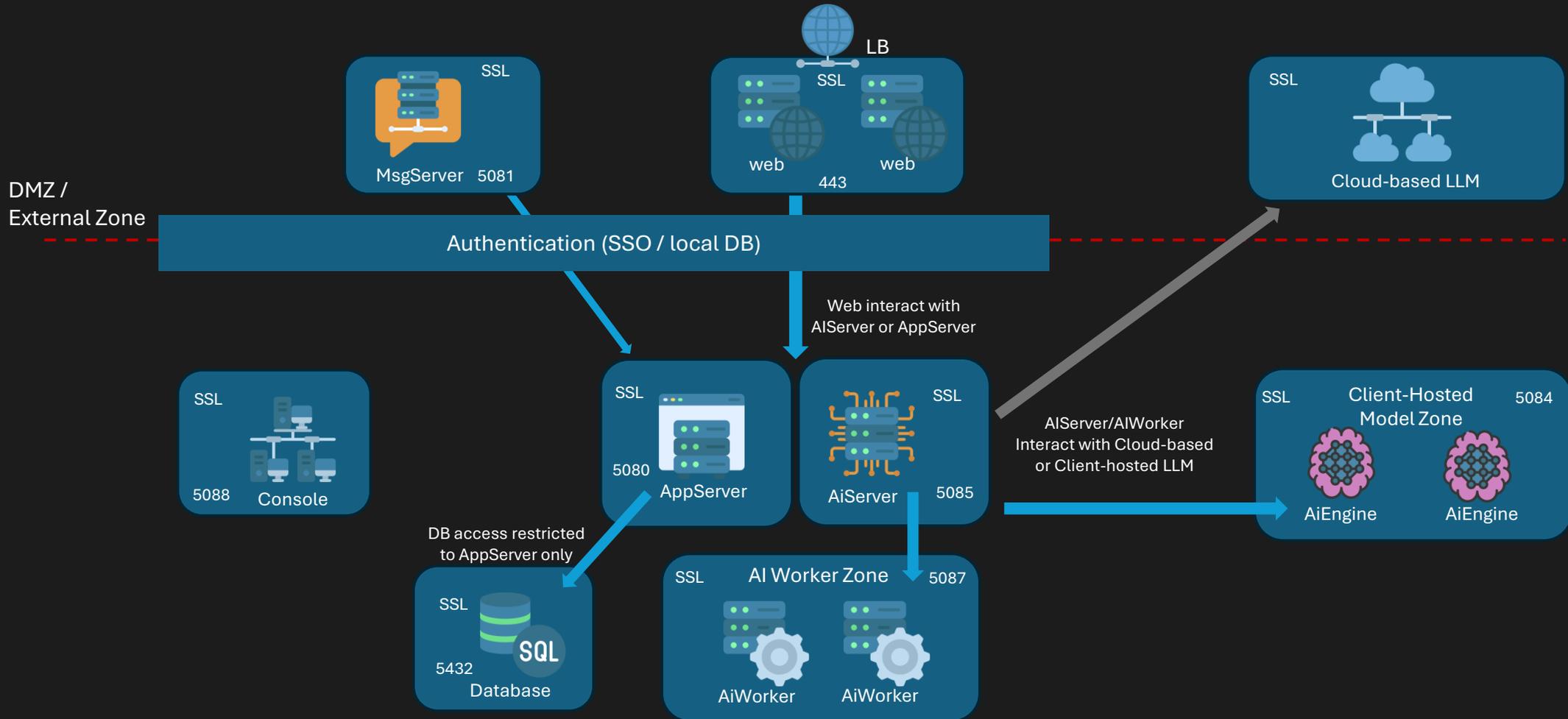AiEngine — Territory / Departmental GPU enabled VM

AI workloads can start with a single VM and expand into a multi-VM architecture, where additional AiEngine and AiWorker handle increased AI and Smartflow processing demands.

Network and Security Boundaries

Clear trust boundaries ensuring controlled access, secure data flow, and auditable AI interactions.

Supported Connectivity & AI Model Options

Enterprise Connectivity

- Identity & Access
  - Azure AD (SSO)
  - Local authentication (optional)

- Microsoft 365
  - Outlook (Email)
  - SharePoint
  - OneDrive

- Data Sources
  - File repositories
  - Databases (via controlled connectors)

AI Model Options

- Self-Hosted / On-Prem
  - Ollama with ollama supported models

- External LLMs (Optional)
  - OpenAI (ChatGPT)
  - Qwen
  - Grok
  - DeepSeek

All integrations and AI model usage are client-configured, authenticated, and auditable. No data is shared with DDX.

Summary

DDX AiX is an enterprise-grade, self-hosted AI platform designed for secure, governed, and scalable AI adoption in regulated environments.

- **Client-Controlled by Design**
  All data, models, and execution remain within the client-managed environment.

- **Secure & Governed Architecture**
  Clear network boundaries, role-based access, controlled service interactions, and end-to-end audit logging across all AI and user activities.

- **Modular & Scalable Platform**
  Start small with a single deployment and scale horizontally across AI engines and worker nodes as workload demand grows.

- **Flexible AI Strategy**
  Supports locally hosted, GPU-accelerated LLMs and cloud-based LLMs via client-configured, auditable access.

- **Enterprise Ready**
  Designed to support architecture reviews, security assessments, and compliance requirements.

Why Ai

Built for Business & IT with Your AI. Your Data. Your Control.

Limited Technical Expertise & AI Skill Gaps

- Shortage of in-house AI and process automation talent.
- Business teams cannot independently build or maintain AI workflows.
- Heavy reliance on external consultants slows down adoption and increases cost.

Fragmented Data & Complex Integrations

- Information scattered across email, files, chats, systems, and databases.
- Lack of connectors to automate end-to-end processes.
- Integrations often require custom development and specialized resources.

Governance & Vendor Lock-in Concerns

- Limited transparency over data usage, storage and access.
- Difficulty enforcing consistent governance and auditability.
- Closed platforms limit model choice, increase cost, and make future migration difficult.
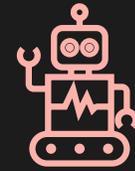
Difficulty Scaling AI Across the Enterprise

- Pilots work, but scaling across departments is inconsistent and costly.
- No standardized, reusable framework for automating business workflows.
- High operational overhead managing tokens multiple solutions.

Our Architecture Principal

Your AI. Your Data. Your Control.

- **Client-controlled, self-hosted** deployment with scalable performance

- **Data residency and boundaries** enforced by design

- **Explicit trust model** with no implicit data sharing across users or components

- Modular, extensible architecture supporting **hybrid AI models** based on client's selections

- End-to-end **governance and auditability** embedded into every workflow

Your AI. Your Data. Your Control

Our Architecture Principal

Your AI. Your Data. Your Control.

- **Client-controlled, self-hosted** deployment with scalable performance

- **Data residency and boundaries** enforced by design

- **Explicit trust model** with no implicit data sharing across users or components

- Modular, extensible architecture supporting **hybrid AI models** based on client's selections

- End-to-end **governance and auditability** embedded into every workflow

Single-VM Deployment
(For small-scale AI workloads)

Single-VM Deployment

Web AppServer AiServer
Console Database AiWorker