

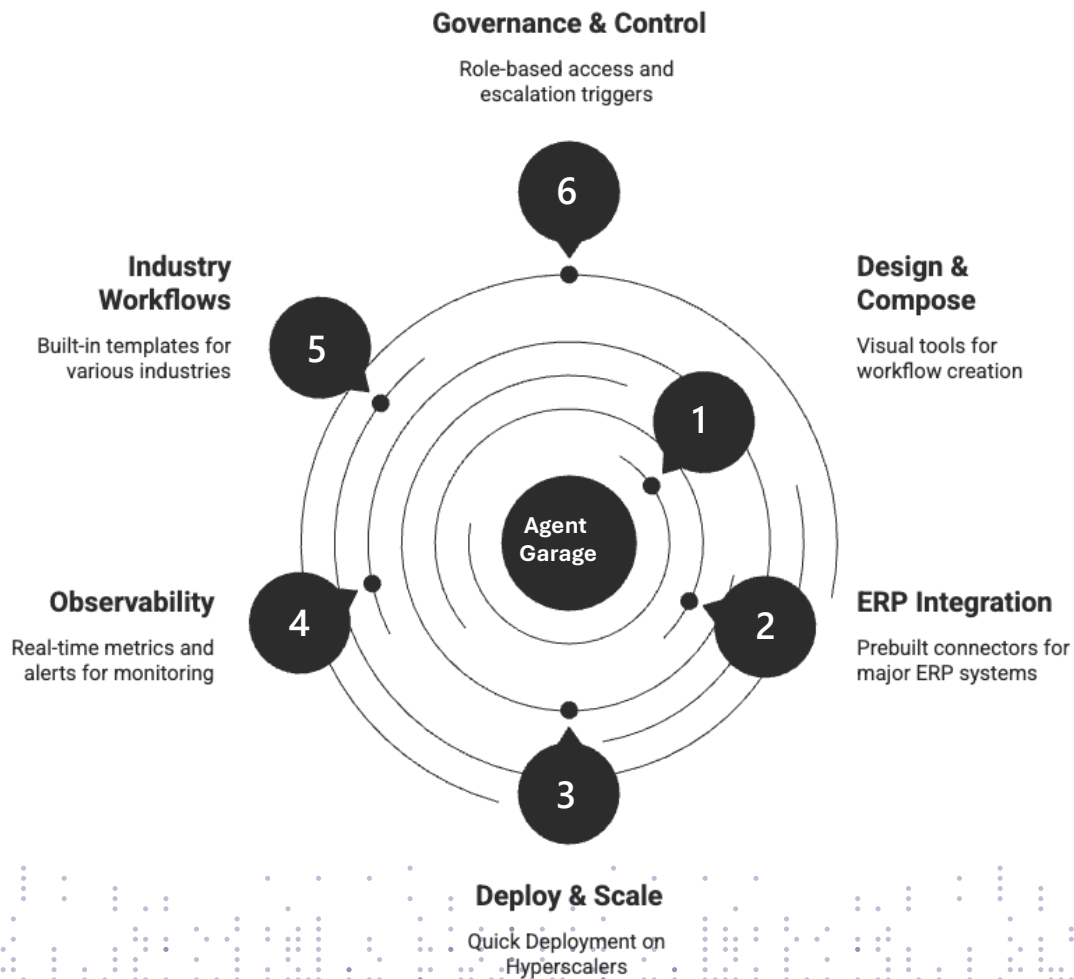
Introducing



AgentGarage.ai

Bringing Agentic AI into Enterprise Reality

Agent Garage is a next-gen enterprise AI platform that empowers secure, persona-driven intelligence through **autonomous agents**, **multi-modal RAG**, and **real-time retrieval over proprietary systems**.
It blends **Agentic AI architecture** with **embedded workflows** and **enterprise-grade observability**.



Accelerate process automation and boost productivity with a configurable library of base agents aligned to your enterprise needs

Execute complex workflows like:

- Contract-to-Billing
- Customer Onboarding
- Supplier Invoice Reconciliation
- Purchase Order Approval
- Sales Order Creation and many more...

Using Agents like:

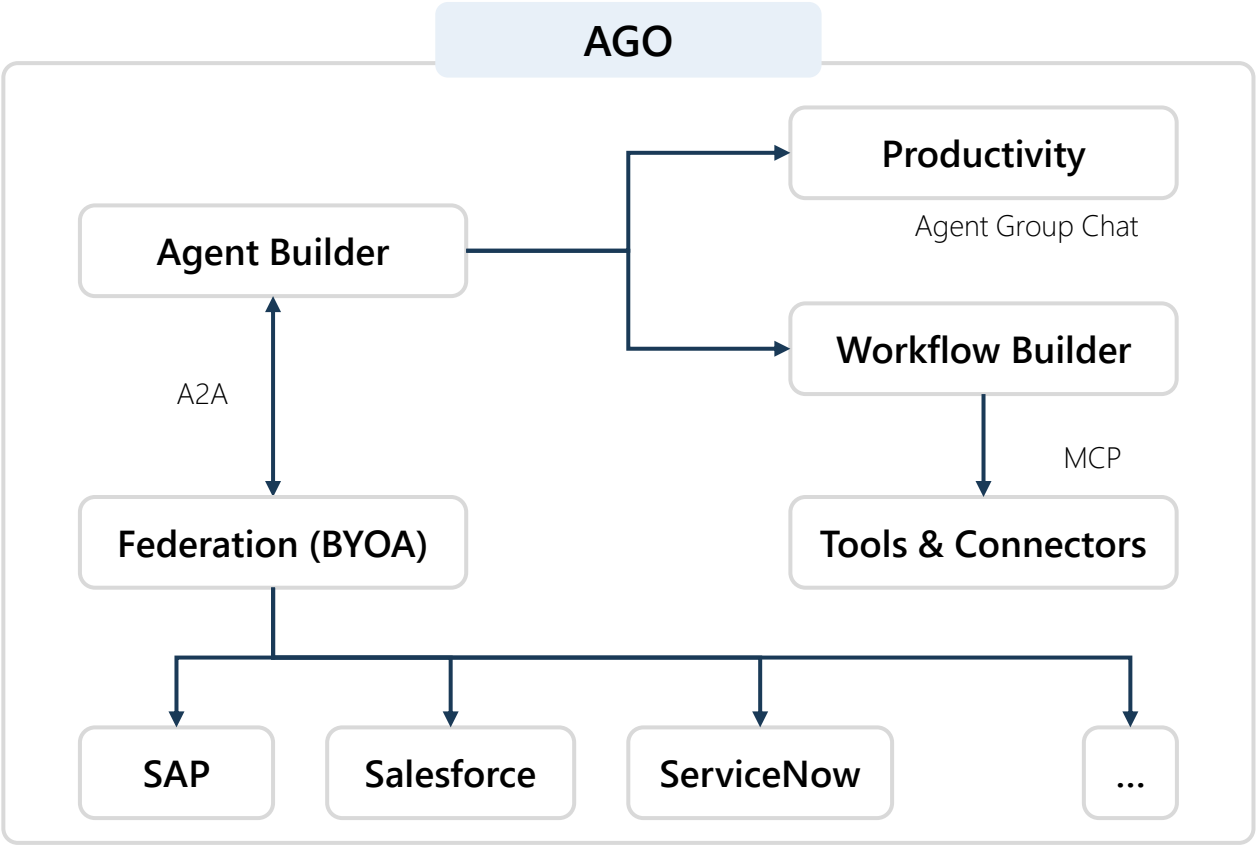
- Document Intelligence Agent
- SAP Entity Matching Agent
- Address Verification Agent
- Compliance Checker Agent
- Invoice Parser Agent
- Discrepancy Detection Agent
- Credit Check Agent

Boost Productivity by Streamlining tasks like:

- Retrieving information from ERPs/CRMs
- Knowledge Retrieval from documents
- Summarizing cross-functional meetings with linked SAP, Jira, and CRM updates
- Summarizing Documents
- Reading and triaging shared mailboxes
- New Hire Onboarding
- Comparing contract clauses

Using Agents like:

- ERP Agent
- RAG Agents
- Meeting Intelligence Agent
- Procurement Agent
- Guided Onboarding Agent



What our customers are saying?

“ This tool is a genuine Agentic AI masterpiece — a blend of advanced technologies that’s making a real difference in the day-to-day work of employees. It stands out as one of our most impactful Gen AI launches of the year.

- Sr. Director, GenAI & Application Integration

“ The launch has been a resounding success, with a Net Promoter Score of 95 from our beta users. This well-executed, collaborative engagement is driving AI literacy, increasing usage, and accelerating adoption across the enterprise.

- CIO, Global Fortune 500 Manufacturer

CT Why CT + AgentGarage.ai?

- ✓ Unified Orchestration Fabric
- ✓ Enterprise-Grade Governance
- ✓ Future-Proof Architecture
- ✓ Industry Depth
- ✓ Global Delivery Model
- ✓ Secure Multi-Agent Collaboration
- ✓ Rapid Time-to-Value
- ✓ Trusted Microsoft Data & AI Partner
- ✓ Accelerator-Led Delivery
- ✓ Innovation at Scale

Productivity Builder –

Document Search Structured & Unstructured files

Excel, CSV, Docs, PDF, Txt, Images, JSON, etc.

Deep Research

Large context data handling

YouTube Q/A

Summarization, Q/A, transcript generation, etc.

Process Reasoning

Context-aware answers for complex user queries

Private & Isolate workspace

Chats and documents remain private to the user

Library and Sharing

Users prompt library; chat & prompt sharing
functionality

Workflow Builder –

Drag & Drop Interface

Build workflows visually using modular nodes

Multi App Integration

Teams, Outlook, SAP, Databricks, SharePoint, etc.

Smart Triggers

Automate flows based on events, schedules

Conditional Logic & Branching

Build dynamic workflows with logics and loops.

Agent Driven Actions

Create custom AI agents as per the requirements.

ERP



Analytics



Document Stores



M365



Agent Garage

Empowering Agents with Seamless Access to Data, Insights, and Workflows for Smarter Interactions

- **Seamless ERP Integration:** Query, update, and reason over enterprise systems to drive real-time operational actions.
- **Analytics-Driven Intelligence:** Tap into live analytical data to identify trends, surface anomalies, and recommend next steps.
- **Smart Document Access:** Extract insights from documents, enabling smart Q&A and summarization.
- **Native M365 Connectivity:** Operate within M365 tools for diverse file support.

and many more to come...

Manufacturing



- Production scheduling and dynamic re-routing of assembly tasks
- Automate product designing and iterative improvements

Retail & CPG



- Personalized (headless) cart building through agents
- Manage Inventory and Replenishments

Energy



- Develop risk adjusted trading strategies
- Monitor boil-off gas and shift logs while detecting energy consumption anomalies

Financial Services

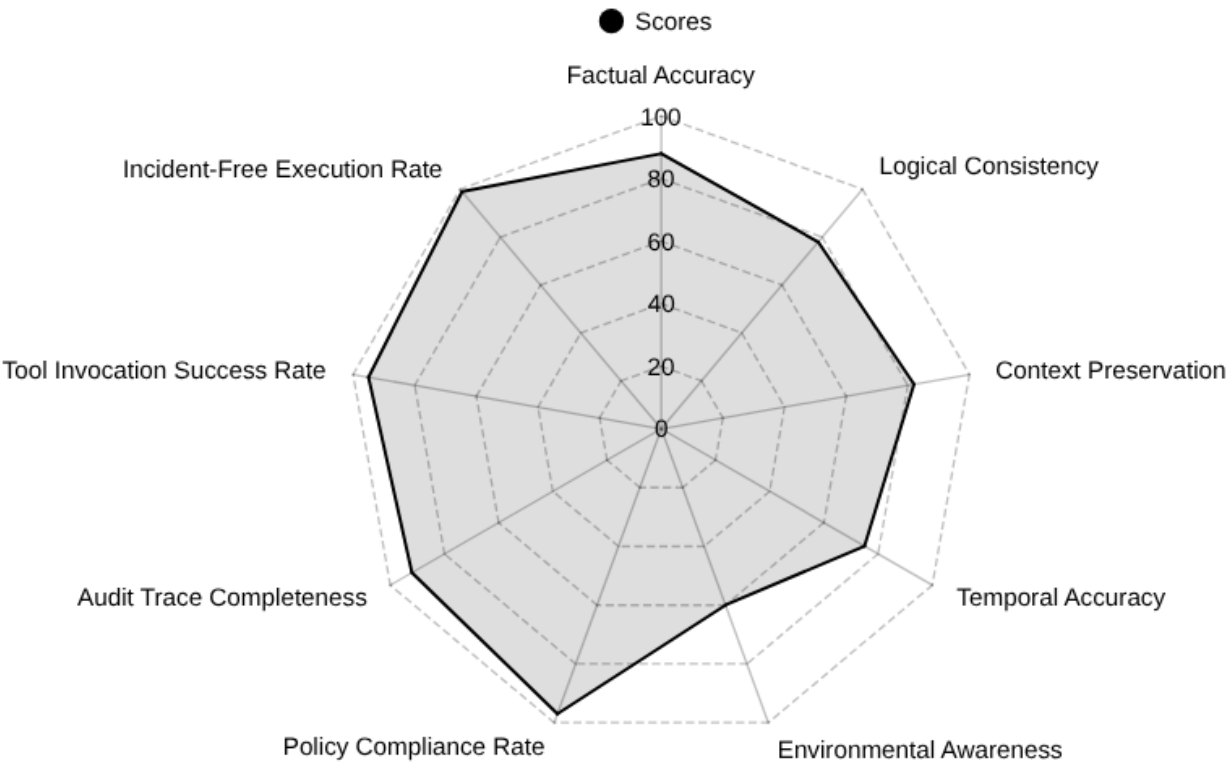


- Automated reach outs and request fulfillment for Relationship Managers
- B2B Customer risk profiling for Credit enquiries

Horizontal Scenarios



- Order to Cash Process
- Master Data enrichment through BYD and D&B datasets
- Deal Guidance and Quote Generation



Agent Timeline View

Expands per request: from prompt → retrieved context → model response → outbound API call or workflow transition.

Top-K Alerts Panel

Highlights anomalies: SLA violations, unexpected tool-use events, outlier behaviors flagged for operator review.

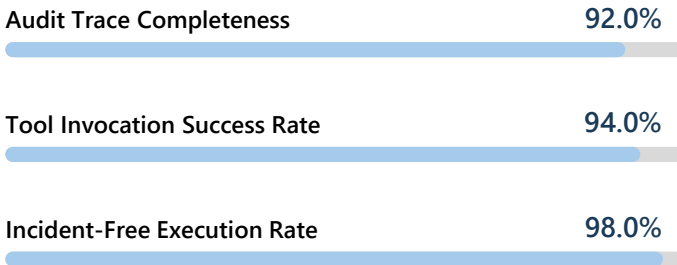
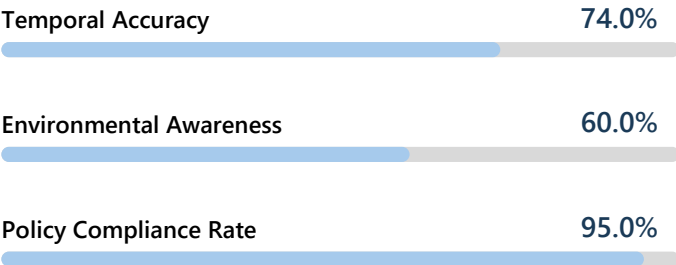
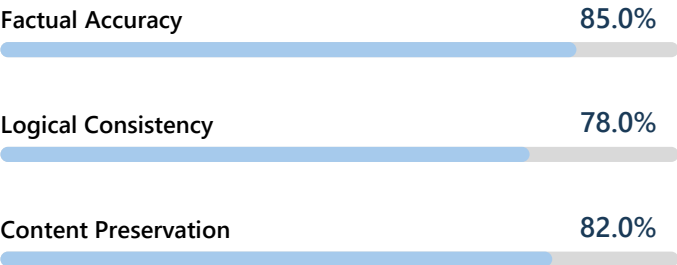
RAG Provenance Pane

Displays ranked source snippets with clickable links to original documents, chunk IDs, and retrieval confidence — enabling audit-ready traceability.

Agent Performance Leaderboard

Comparative view of agents by cost per request, success rate, mean resolution time, escalation frequency.

Detailed Component Scores





Data Quality & Governance

- **Provenance & Lineage:** Automatic capture of data source, ingestion path, transformations, and chunk IDs to enable source attribution and rollback.
- **Data Quality Gates:** Schema validation, freshness thresholds, provenance scoring, deduplication, and confidence scoring applied before retrieval or model invocation.
- **Model & Artifact Registry:** Maintains complete mapping of model versions, prompt templates, embeddings, tokenizers, and tool configurations per agent — integrates with experiment tracking for reproducibility.



Human-in-the-Loop (HITL) Oversight

- **Review & Approval Gates:** Low-confidence or high-impact agent actions are routed to human approvers before execution.
- **Continuous Feedback Loops:** HITL annotations feed model fine-tuning, retrieval curation, and prompt optimization pipelines.
- **Policy-Based Overrides:** Role-based control for critical workflows — finance, legal, HR — ensuring irreversible actions are manually vetted.



Red-Teaming, Safety & Compliance

- **Continuous Red-Teaming Pipeline:** Scheduled adversarial tests (prompt injection, data poisoning, permission escalation) using automated fuzzing and curated attack libraries.
- **Risk Taxonomy & Scoring:** Each agent gets a threat profile based on permission scope, data sensitivity, and external integration risk; remediation plans tracked in governance dashboards.
- **Safety Controls & Mitigations:** Content filtering, sandboxed tool calls, rate limiting, credential vaulting, and automated rollback on detected anomalies.



Why It Matters?

- Avoid Siloed Intelligence
- Cross-Platform Workflows
- Protect Existing Investments
- Unified Governance & Observability



BYOA (Bring Your Own Agents)

Onboard third-party or legacy agents — regardless of where they are built — into **AgentGarage.ai**'s orchestration fabric.

Powered by A2A (Agent-to-Agent) Protocol

Secure, standardized messaging for inter-agent communication across platforms, enabling intent sharing, context exchange, & action delegation.

Common Context Layer

Agents can share relevant session state, RAG context, and security tokens while respecting data boundaries.

Central Policy & Security Enforcement

Role-based access, rate limits, and sandboxing applied uniformly across internal and federated agents.



IT Service Management



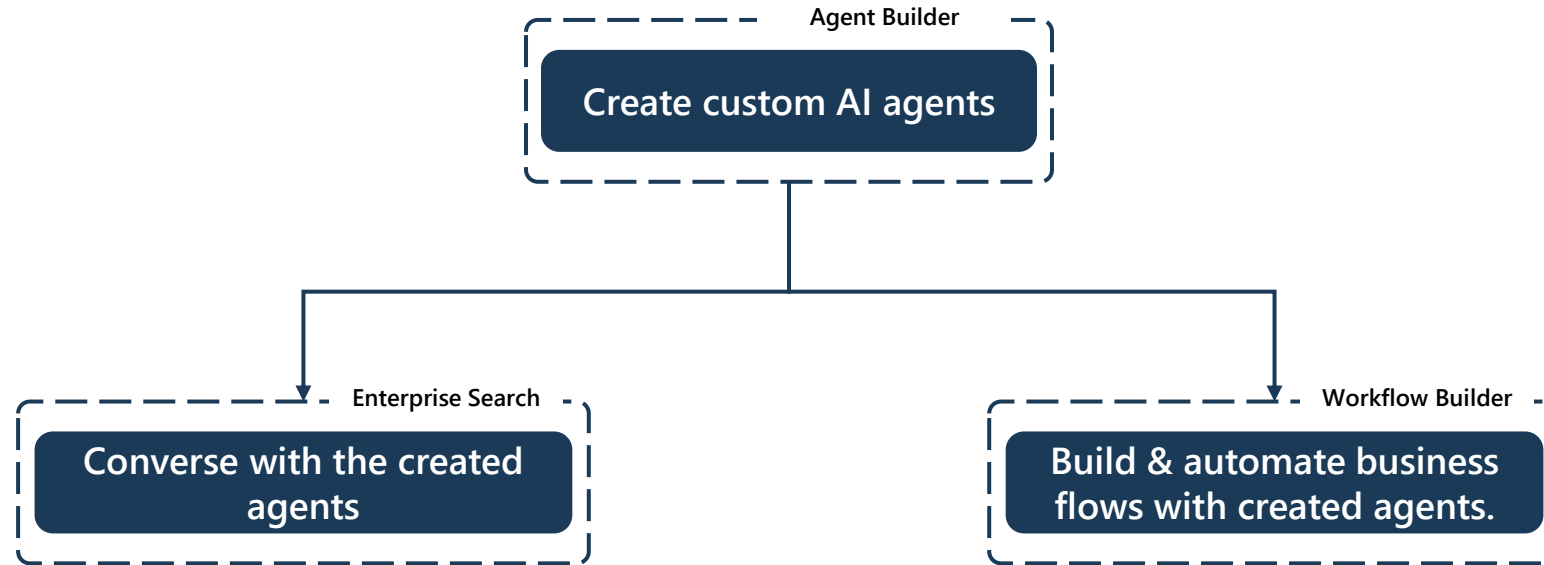
ERP + Procurement Automation



CRM + Marketing Automation



HR Onboarding



Application user segments

Admin - Full platform access and control

- Manages user permissions and role-based access
- Approves agents before organizational rollout
- Access to system settings, logs, and support tools

Builder Profile – Who can create custom agents

- Creates and configures agents for team/department use
- Submits agents for admin approval before activation

Basic User – Utilize the agents & Productivity features

- Can build and automate workflows with the published and pre-given agent
- Utilize the productivity module to get help in the daily tasks.

A unified approach combining openness, flexibility, and speed to deliver enterprise-ready AI agents.



1. Admin - Full platform access and control

- Manages user permissions and role-based access
- Approves agents before organizational rollout
- Access to system settings, logs, and support tools



2. Support Model

- Shared support with SLA-backed commitments.
- Onboarding assistance, solution co-design, and continuous optimization.



3. Workflow Builder Flexibility

- Buy the workflow builder product or use it as an accelerator for fragmented workflow automation

4. Intellectual Property (IP)

- Full customer ownership of workflows, data, and models.
- No proprietary data lock — assets remain with the enterprise.



5. Open Source

- Supports open-source models and frameworks for extensibility and community-driven innovation.
- Compatible with a wide ecosystem of connectors and libraries.



6. Time to Value

- Rapid deployment — from proof-of-concept to production in days.
- Prebuilt connectors, industry workflows, and reusable agent templates to accelerate ROI.



"Open, flexible, enterprise-ready — delivering intelligent agents at scale with measurable impact."

Customer Overview

- A Fortune 500 global leader in industrial tools, household hardware, & security products.
- Known for innovation & operational excellence, this company operates with a large workforce across multiple functions including, Procurement, Legal, Product Management & Engineering.

Challenges Faced

- Restricted Use of Public GenAI Tools
- Low Productivity for Knowledge Work
- Delayed Decision-Making
- Lack of Self-Service Capability

Highlights

- 95 NPS Score
- 1600+ Users
- 8+ Agents
- 25+ Features
- MS Teams Integration



Goals

The customer aimed to:

- Empower employees with secure, AI-driven self-service capabilities for document analysis, querying, and summarization.
- Enhance knowledge discovery and productivity through natural language access to proprietary data.
- Deploy a production-grade GenAI platform that meets security, compliance, and performance standards.



Solution

- **CT Agentic Spaces** – Developed and deployed by Celebal Technologies, a secure, enterprise-grade solution, specifically designed to enhance employee productivity, knowledge discovery, and self-service analytics.
- Key Solution Capabilities:
 - Real-Time File Upload & Notifications
 - Agentic Q&A
 - Self-Service Analytics: Includes summarization, translation, exploratory data analysis (EDA), and auto-visualizations.
 - Multi-Modal Retrieval-Augmented Generation (RAG)
 - Prompt Guardrails & Hallucination Control
 - Microsoft Teams Interface



Multi-Agent Architecture

Private RAG

Scalable Deployment

Customer Overview

- A global leader in integrated logistics & shipping solutions, the customer operates across 140 countries, providing end-to-end transportation services. Their expertise spans container shipping, supply chain logistics, port operations, and e-commerce solutions, driving innovation & operational efficiency in the logistics industry.

Challenges Faced

- Manual Customer Onboarding Process (72 hours)
- Data Inconsistencies
- Frontline Burden
- Comprehensive Checks: Multiple verification steps

Highlights

- Data Enrichment & Verification Automation
- Customizable Workflow for KYC and Compliance
- Address Triangulation
- Risk Scoring



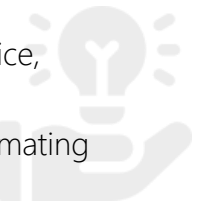
Data Variables Managed

- Business Verification Data (BVD) and D&B data points
- Company identity and verification
- Operational and industry-specific data
- Financial and risk data
- Contractual data (legal and compliance checks)



Solution

- **Agentic AI Platform – Multi-Agent Framework for Customer Onboarding**
- The Agentic AI platform enables multiple intelligent agents to work collaboratively, automating and streamlining the customer onboarding process, ensuring speed, accuracy, and consistency.
- Key Capabilities:
 - Data Enrichment & Verification Automation: The master agent orchestrates various agents for data verification, pulling in business verification data from BVD and D&B data points, ensuring accurate and compliant onboarding.
 - Multi-Modal Functionalities: Neural IVR was implemented for external customer verification via voice, adding convenience and ensuring data accuracy in real-time.
 - Automated Decisioning: The master agent orchestrates the flow of data across various tasks, automating the decision-making process to accelerate onboarding.



Multi-Agent Architecture

Neural IVR

External Data Integration



Thank You