

HALO™ Agent Studio by OmniTrust

Build, Operate & Scale Trust-Native Enterprise AI Agents
Any model. Any framework. Enterprise control and AI governance built in.

Halo Agent Studio is the business enablement offering within OmniTrust AI Lifecycle Management (ALM). It gives business teams a fast, secure way to build, deploy and operate AI agents using the models, frameworks, tools and enterprise data that best fit each workload. Built on the same Halo Enterprise AI Control Plane, every agent operates with identity, policy, data protection, runtime enforcement and cost controls already built in.

BUILD FASTER

Turn business use cases into working AI agents.

- Build agents in minutes
- Start from scratch or templates
- Connect tools, APIs & data
- Use any agent framework

OPERATE SECURELY

Enterprise control, built-in

- Agent identity & permissions
- Protect sensitive data & IP
- Control models, tools & APIs
- Enforce policy at runtime

OPTIMIZE AI ECONOMICS

Match models to workloads and use the best AI at the best cost.

- Track usage & cost
- Reduce unnecessary AI spend
- Hundreds of AI models available

Halo Agent Studio helps business teams move from AI ideas to production agents faster, while giving the enterprise consistent control over identity, data, execution, models and cost.



Build

Create & Launch Agents

Build visually, start from approved templates or bring existing agents and frameworks. Connect enterprise data, applications, APIs and tools and choose the right model for the task.



Operate

Run Securely Under Halo Control

Every agent operates with identity, permissions, protected credentials and data, approved model and tool access, runtime policy enforcement, cost controls and traceable activity.



Scale

Expand To Teams & Enterprise

Share agents and templates, reuse successful workflows, standardize approved patterns and scale across teams and business units without creating uncontrolled AI silos.

Need enterprise-wide AI discovery and control? [Halo Enterprise AI Control Plane](#), also part of OmniTrust ALM, discovers AI and Shadow AI across the enterprise, extending centralized policy, runtime enforcement, data protection + cost control across the fleet.

ALM™ ALM Expert Services

AI Strategy & Advisory

Executive workshops, AI strategy, agentic AI education, use-case discovery, workflow prioritization, operating-model development and enterprise AI roadmaps.

AI Foundry & Forward-Deployed Engineering

OmniTrust AI architects and engineers help teams identify high-value workflows, build agents and automations, integrate enterprise systems and move rapidly from idea to production.

Trust-Native Agent Architecture

Design agent identity, permissions, runtime enforcement, data protection, model and tool policy, infrastructure choices and operational trust into agents from the outset.

ALM QuickStart Program

A rapid 8–12-week engagement to identify high-value AI opportunities, deploy initial agents and automations, establish control and cost baselines, and build an enterprise AI roadmap.

HALO Agent Studio — Build, Operate & Scale Enterprise AI Agents

Halo Agent Studio operationalizes the Enable layer of OmniTrust AI Lifecycle Management, giving business teams one secure environment to build, deploy and operate AI agents across models, frameworks, tools and enterprise data - with the Halo Enterprise AI Control Plane enforcing identity, policy, data protection, runtime behavior and cost underneath.

BUILD

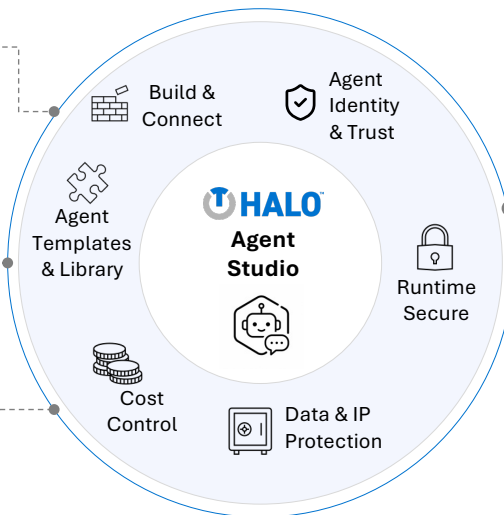
- Low / no-code agent creation
- Start from scratch or templates
- Existing agent frameworks
- Enterprise data, tools & APIs

OPERATE

- Secure agent runtime
- Identity & permissions
- Policy & data controls
- Activity & cost visibility

SCALE

- Share agents & workflows
- Reuse approved templates
- Expand across teams & BUs
- Standardize enterprise patterns



Built on:

Halo AI Control Plane

As teams scale, Halo can extend enterprise-wide discovery, policy, runtime enforcement and governance to AI, Security, CIO and IT leadership. Enabling them to **Discover, Control & Enable** Enterprise AI.

FINANCE & PROCUREMENT > Gain visibility into AI spend, optimize model economics, reduce unnecessary premium-model usage and preserve negotiating leverage through multi-model choice.

Secure, Multi-Model AI Infrastructure


**HALO
SECURE
AI CLOUD**

 Dynamic,
Multi-Model
Orchestration

 Secure AI
Infrastructure

 Cost
Intelligence
& Control

 AI Agility & Choice —
Model, framework,
cloud &
infrastructure

Use any model. Build with any framework. Run on approved infrastructure. Halo Agent Studio gives teams the freedom to choose the best AI for each workload based on performance, security and cost - while maintaining consistent identity, data protection, runtime and cost controls.



Control the AI. Control the cost. Keep the freedom to change.

 **OmniTrust**

www.OmniTrustHalo.com

© 2026 OmniTrust Security LLC.

OmniTrust secures the connected world, from silicon to cloud to AI - by delivering verifiable, enforceable trust across the full lifecycle. As the leader in Trust Lifecycle Management (TLM), OmniTrust protects over 2 billion devices and 3 billion software updates annually, extending trusted identity, security, and operational control from embedded systems to enterprise infrastructure and autonomous AI.