okta

What's Auth0 for AI Agents?

The Challenge: Getting AI Agents into Production Without Slowing Down

As your teams move quickly to build AI agents, the real challenge isn't getting started—it's getting those agents into production where they can take meaningful action.

Today, companies are excited to use AI agents to get work done, but they get stuck because managing the security and digital "IDs" for AI agents is way more complicated and expensive than expected. Using hard coded credentials or API keys gets agents up and running, but it's only suitable for development and testing.

Figuring out enterprise-grade security and risk management stalls projects and drains budgets. When an agent needs to talk to 60 different tools and make 30,000 requests a day, legacy security models become a black hole for your team's time.

For those responsible for delivering product-ready AI agents, this presents several significant challenges:

Slow Time to Market: Your most expensive engineers are burning half the week rotating secrets and hardcoding permissions instead of building features that drive revenue.

Stagnant Growth: Most AI projects never hit profitability because the cost of keeping them running safely is too high.

Unpredictable Scaling: Every month an agent sits in "pilot phase" because you cannot scale complex workflows confidently with built-in human approvals and precise permissions for every agent.

Teams often end up rebuilding authentication, authorization, and access controls for every new use case—slowing delivery and increasing operational overhead.

This leaves key questions unanswered:

01 **How will your AI agents identify your users and connect to their apps and APIs?**

02 **How do you maintain oversight and build in human approval for critical actions?**

Without a clear approach, what starts as a fast-moving AI project can quickly turn into delays, rework, and stalled progress.

okta

The Solution: Auth0 for AI Agents — Ship at the pace of AI, not identity.

Auth0 for AI Agents lets your agents log in, call APIs, and connect to MCP servers securely, all with fine-grained controls and just a few lines of code. Instead of rebuilding identity infrastructure for every new use case, your teams can offload the complexity and move from prototype to production in days, not months.

If you're building AI agents, we allow you to:

- Instantly identify the user interacting with the agent so it can act with the correct history, preferences, and permissions.
- Empower agents to complete real-world tasks—like scheduling meetings or processing orders—by securely connecting to third-party apps on behalf of the user.
- Give users control at the exact moment it matters, allowing them to approve high-stakes actions like financial transactions or document sharing.
- Apply fine-grained policies so agents only access the specific data and tools they are authorized to use, minimizing the risk of data oversharing.
- Ensure agents only invoke specific MCP servers and data sources authorized for that specific user, whether they are an internal employee or an external customer.

How Auth0 for AI Agents Can Support Your Use Case

User Authentication: Connect AI Agents to Users and Their Data

Auth0's User Authentication (via Universal Login or Embedded Login) allows your AI agents to identify users and access the right data and APIs on their behalf.

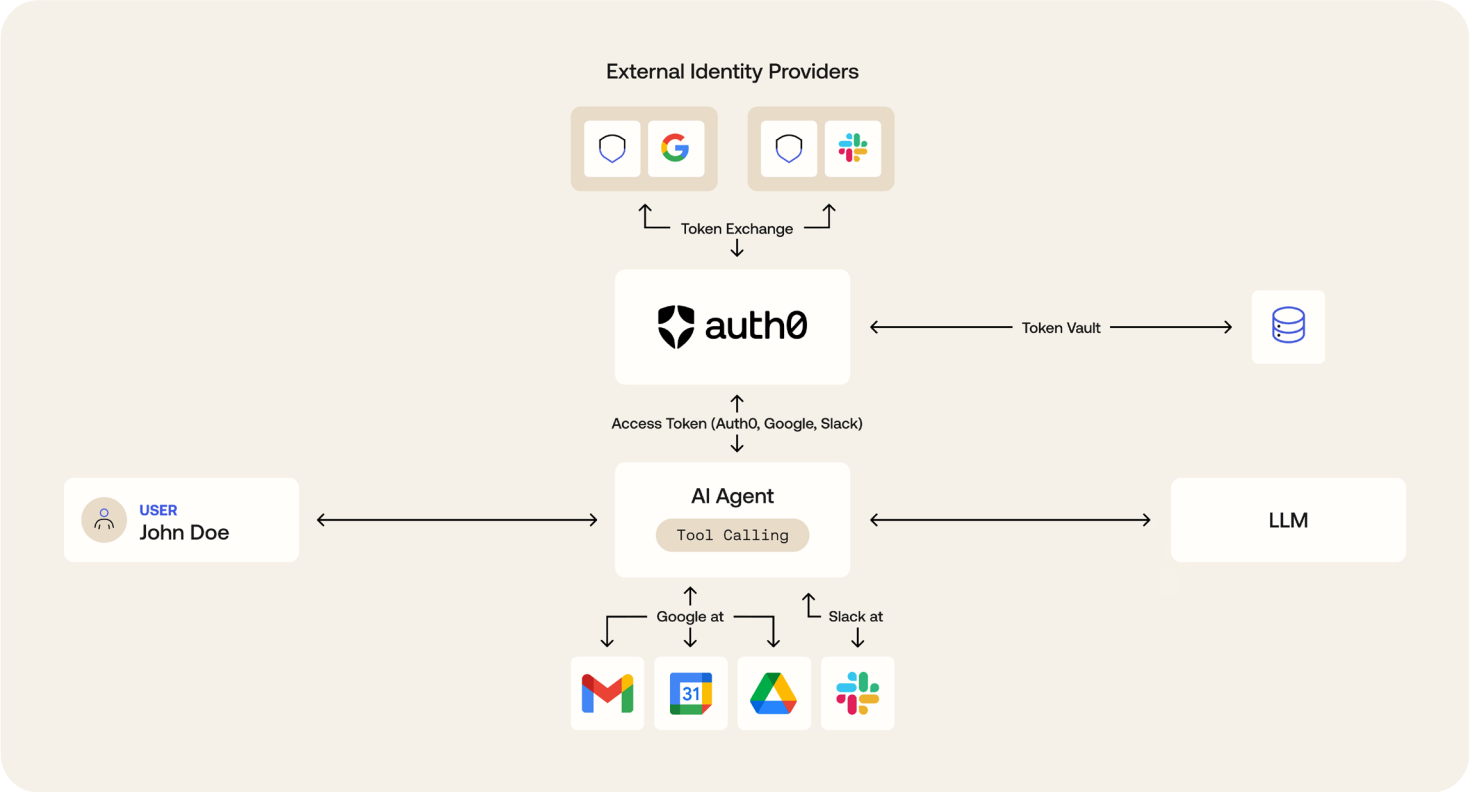
Instead of just answering questions, a customer support agent can identify a logged-in user, pull their specific order history, and take meaningful action.

okta

Token Vault: Connect to External Systems Without Managing Credentials

Token Vault acts as a secure, centralized authorization layer that integrates your AI agents with third-party APIs and external systems, such as Google Drive, Jira, or Slack.

Auth0 automatically stores and refreshes OAuth tokens, so your team doesn't have to build custom credential management. You can empower a productivity agent with 35+ pre-built app integrations without increasing engineering overhead.

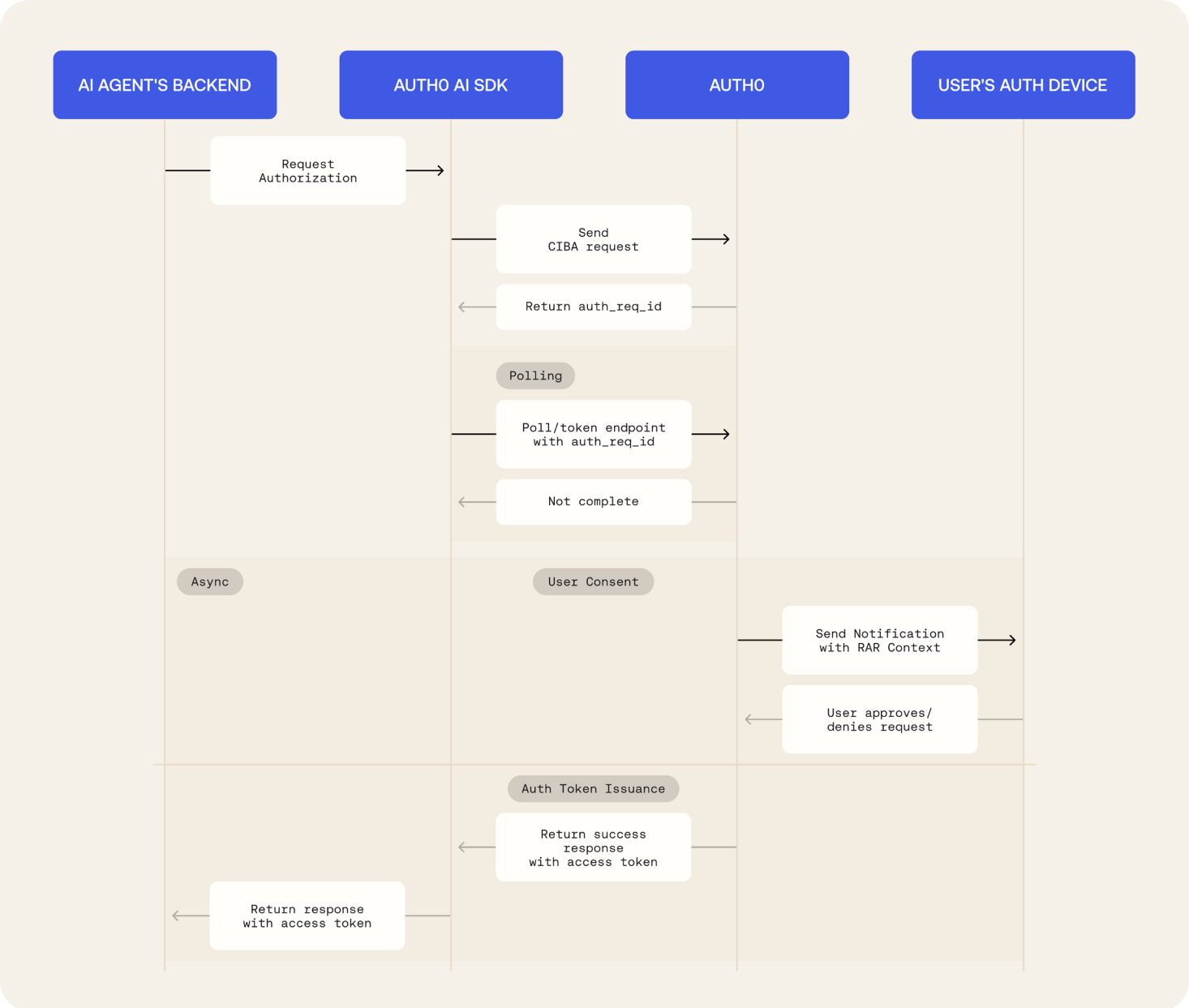


okta

Asynchronous Authorization: Human-in-the-Loop Without the Friction

Auth0 for AI Agents enables AI agents to asynchronously authorize users using Client-Initiated Backchannel Authentication (CIBA) flow, so agents can work in the background and only interrupt the user when a high-value approval is required.

If an agent needs to make a purchase, it doesn't have the permission to do so alone. It triggers a rich consent prompt to the user's device. The agent only receives the necessary token after the user approves, enabling secure transactions without blocking the workflow.

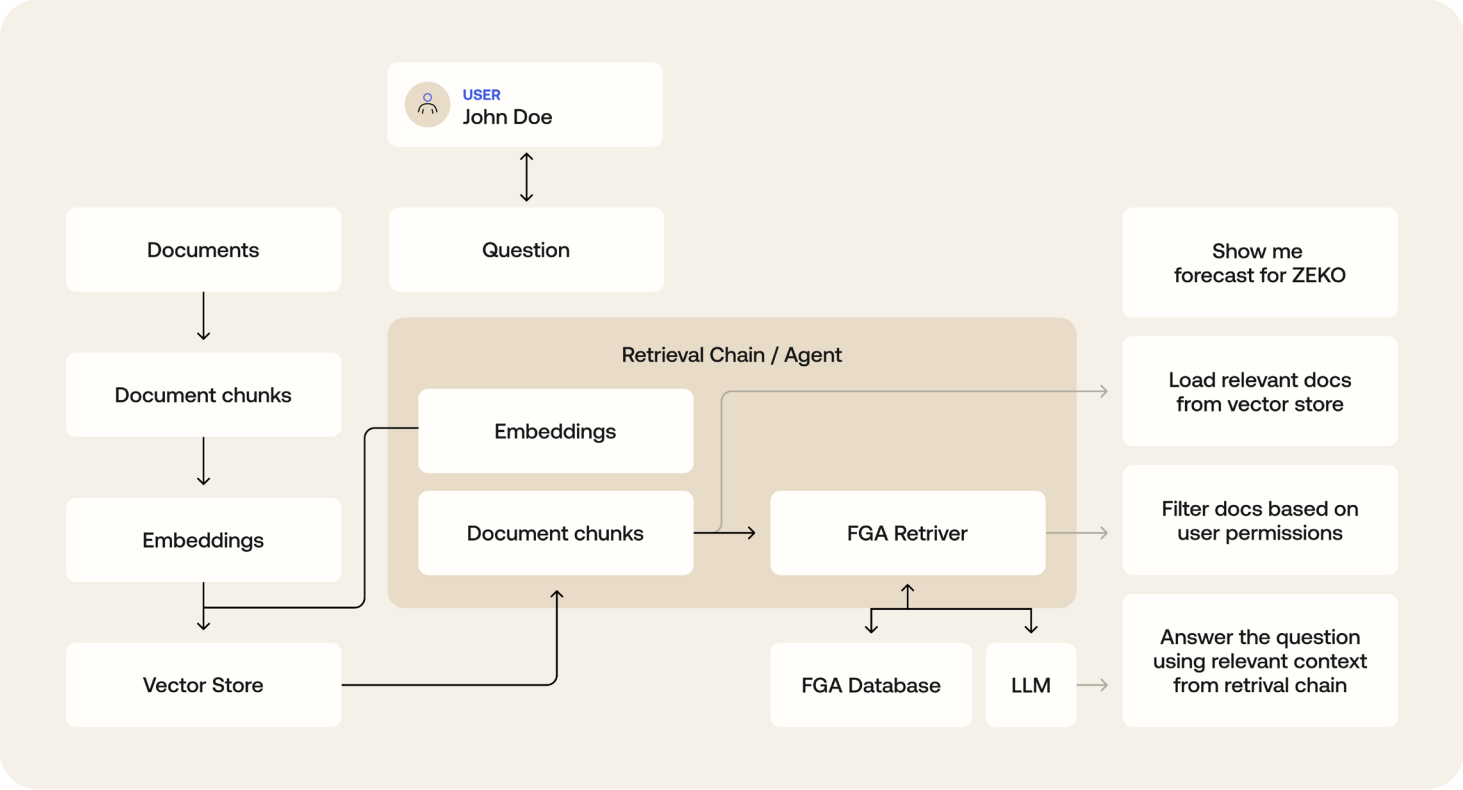


okta

Fine-Grained Authorization for Retrieval Augmented Generation (FGA for RAG): Apply Access Controls to AI Memory

Auth0 for AI Agents enables AI agents to implement Fine-Grained Authorization (FGA) for RAG pipelines to ensure that when an agent retrieves data to answer a query, it only sees and returns information the specific user is authorized to access.

A sales agent can search company-wide competitor intel but is automatically restricted from surfacing sensitive HR or payroll documents, even if they are in the same vector database.

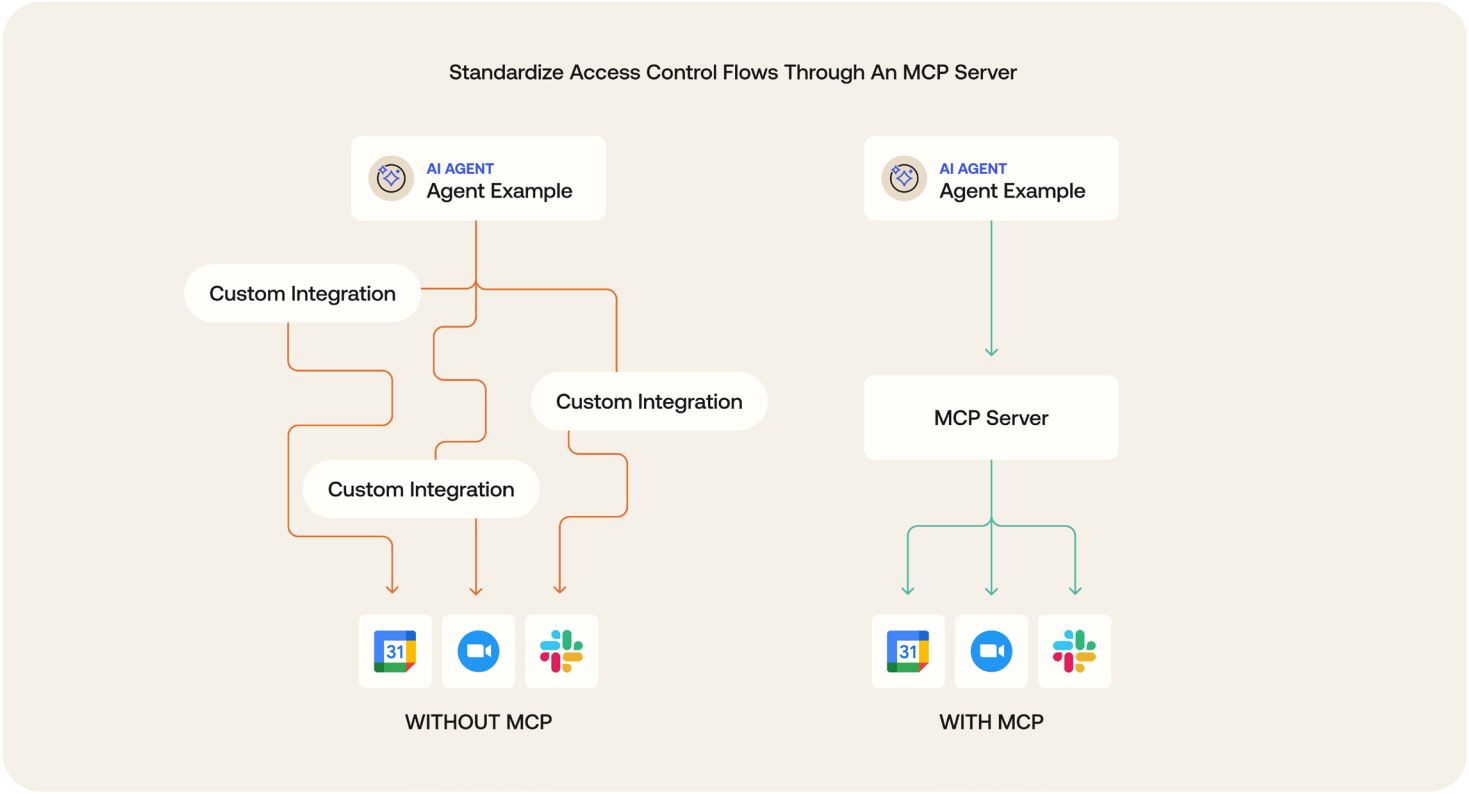


okta

Auth for MCP: Secure the Model Context Protocol

Auth0 for AI Agents enables a standardized way to add authentication and authorization to any MCP server with Auth for MCP, giving you granular control over who (and what) can access your data.

If you expose your inventory data via an MCP server for customers to use, Auth0 ensures that every interaction is locked down with real credentials and scoped permissions, preventing unauthorized data harvesting.



The Bottom Line: Stop rebuilding the basics and start scaling

The window to lead the agentic era is open, but for most engineering teams, the path to production remains blocked. Don't let your AI roadmap stall in a cycle of custom identity plumbing and manual security reviews. With Auth0 for AI Agents, you can offload the back-end complexity to a platform built for 10 billion monthly authentications—reclaiming 40% of your development capacity for core innovation. Move beyond the pilot phase today and start shipping trusted, production-ready AI experiences that act on behalf of your users with absolute accountability.

About Okta
Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.