okta
The World's Identity Company

Okta Secures Agentic AI

Safe harbor

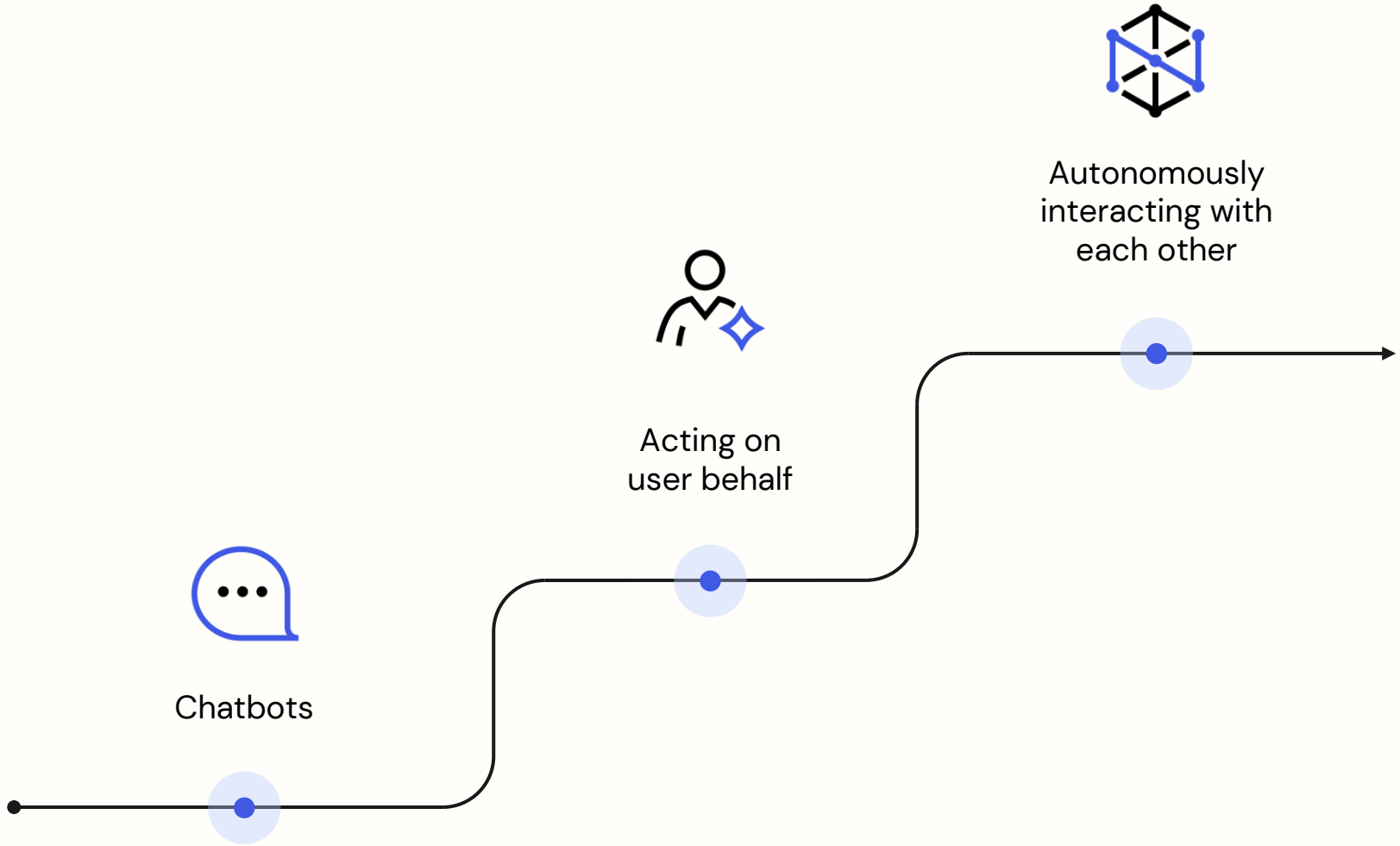
This presentation contains "forward-looking statements" within the meaning of the "safe harbor" provisions of the Private Securities Litigation Reform Act of 1995, including but not limited to, statements regarding our financial outlook, business strategy and plans, market trends and market size, opportunities and positioning. These forward-looking statements are based on current expectations, estimates, forecasts and projections. Words such as "expect," "anticipate," "should," "believe," "hope," "target," "project," "goals," "estimate," "potential," "predict," "may," "will," "might," "could," "intend," "shall" and variations of these terms and similar expressions are intended to identify these forward-looking statements, although not all forward-looking statements contain these identifying words. Forward-looking statements are subject to a number of risks and uncertainties, many of which involve factors or circumstances that are beyond our control. For example, global economic conditions have in the past and could in the future reduce demand for our products; we and our third-party service providers have in the past and could in the future experience cybersecurity incidents; we may be unable to manage or sustain the level of growth that our business has experienced in prior periods; our financial resources may not be sufficient to maintain or improve our competitive position; we may be unable to attract new customers, or retain or sell additional products to existing customers; customer growth has slowed in recent periods and could continue to decelerate in the future; we could experience interruptions or performance problems associated with our technology, including a service outage; we and our third-party service providers have failed, or were perceived as having failed, to fully comply with various privacy and security provisions to which we are subject, and similar incidents could occur in the future; we may not achieve expected synergies and efficiencies of operations from recent acquisitions or business combinations, and we may not be able to successfully integrate the companies we acquire; and we may not be able to pay off our convertible senior notes when due. Further information on potential factors that could affect our financial results is included in our most recent Quarterly Report on Form 10-Q and our other filings with the Securities and Exchange Commission. The forward-looking statements included in this presentation represent our views only as of the date of this presentation and we assume no obligation and do not intend to update these forward-looking statements.

Any products, features, functionalities, certifications, authorizations, or attestations referenced in this presentation that are not currently generally available or have not yet been obtained or are not currently maintained may not be delivered or obtained on time or at all. Product roadmaps do not represent a commitment, obligation or promise to deliver any product, feature, functionality, certification or attestation and you should not rely on them to make your purchase decisions.

Apps no longer wait for instructions. They act on your behalf.

Agentic AI is Redefining how Apps Operate

- → AI agents act independently
- → Apps now make decisions, connect across systems – without permission
- → Autonomy boosts productivity but creates new identity risks



Users are fueling agent sprawl using new tools.

AI is democratizing app creation.

→ AI turns users into developers

→ Every user can now build, connect and run apps

→ NLP is becoming the new programming language

Google

Gemini Code Assist and Vertex AI Agent Builder

ANTHROP\C

Claude API and Claude Code

Relevance AI

Relevance AI Platform

_zapier

Zapier Central

Microsoft

Copilot Studio

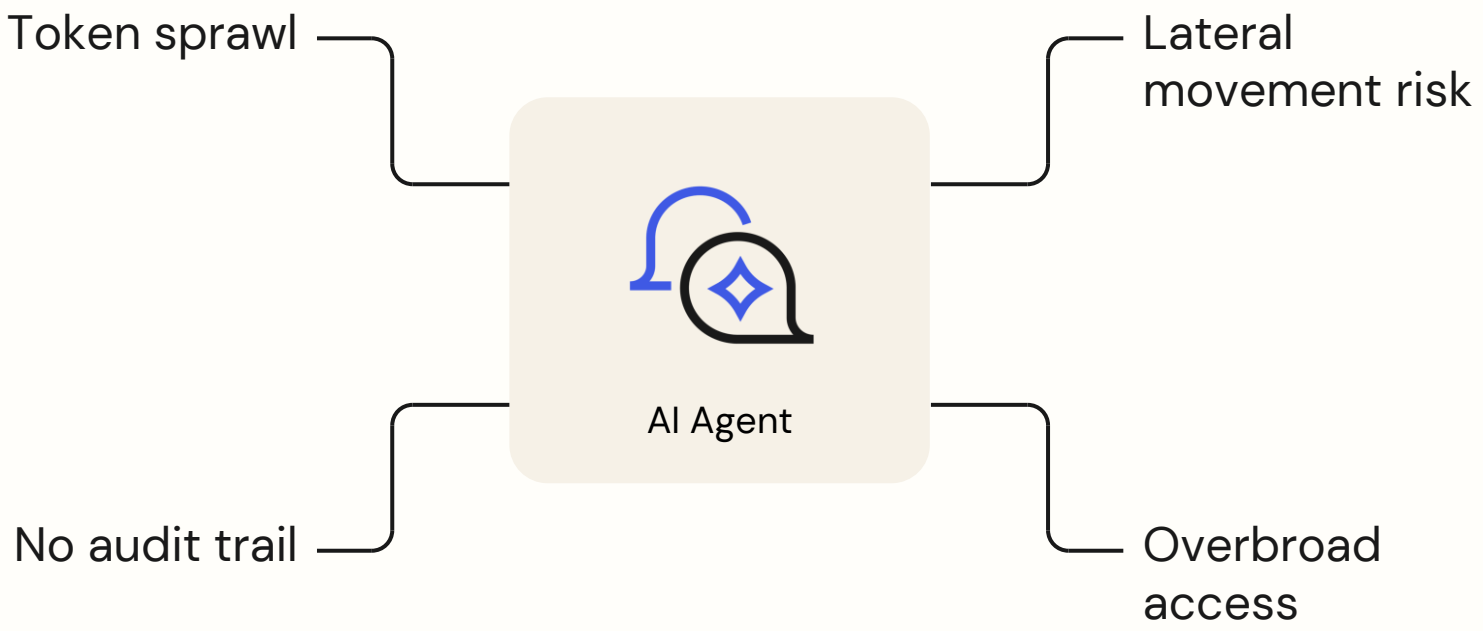
Glide

Glide Claude Integration

Every AI agent is a hidden attack vector.

Your Biggest Identity Risk Doesn't have a Username

- → Compromise in one app can cascade across your ecosystem
- → Lack of audit and control breaks compliance and obscures accountability
- → One token leak can unlock systemic compromise



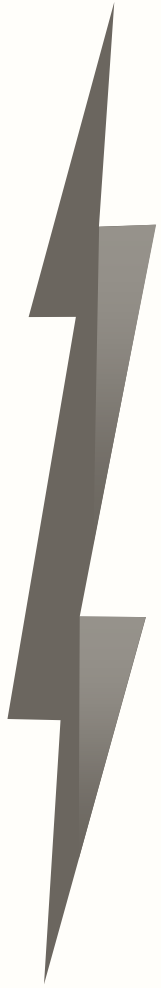
AI adoption is surging. But security and governance haven't kept up.

IT is Flying Blind with Autonomous AI Agents

- → Enterprises deploy agents faster than they can secure them
- → Security teams lack visibility into what agents can access and do
- → Legacy protocols weren't built to handle autonomous, app-to-app activity

51%[1]

of companies already use AI agents



80%[2]

experienced unintended agent behavior

23%[3]

report credential exposure via agents

44%[4]

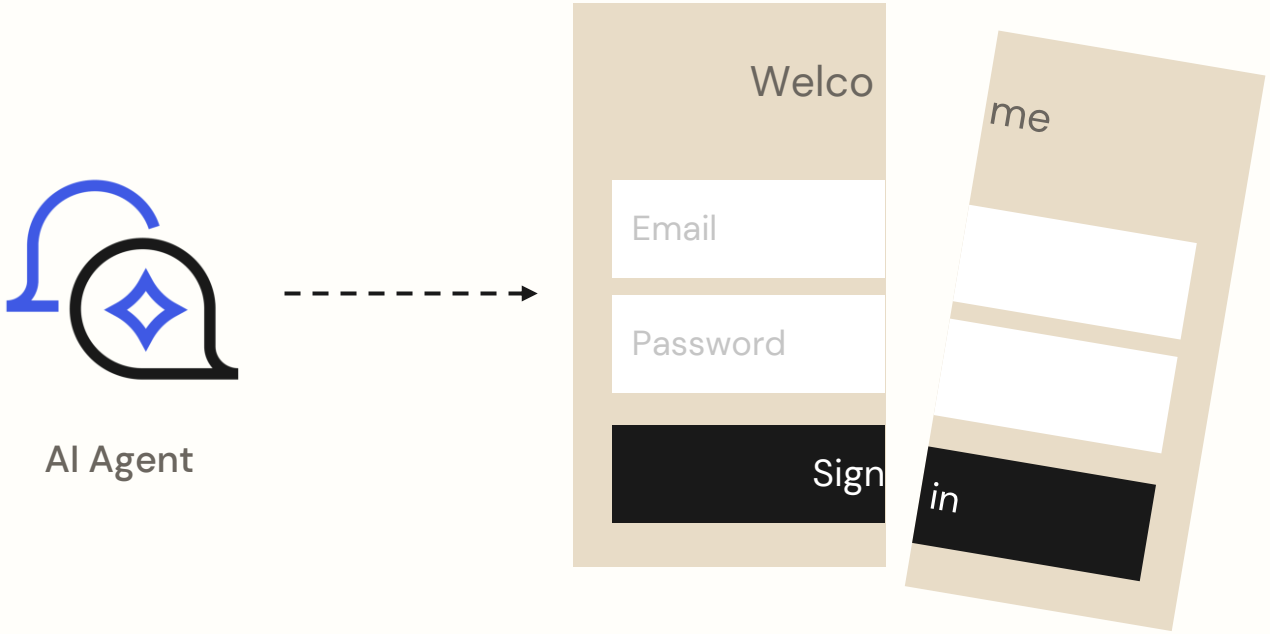
have no governance in place

1 Pager Duty, 2025
2, 3,, 4 The Times, 2025

Your identity tools were built for people. AI agents break them.

AI agents defy human identity guardrails.

- → Identity systems assume logins, sessions and passwords – none of which apply to agents.
- → Agents operate with broad, persistent access that can't be easily scoped or revoked.
- → Without agent-aware governance, organizations can't enforce policies or audit



Agentic AI needs a new approach to identity security – with identity as the control plane.

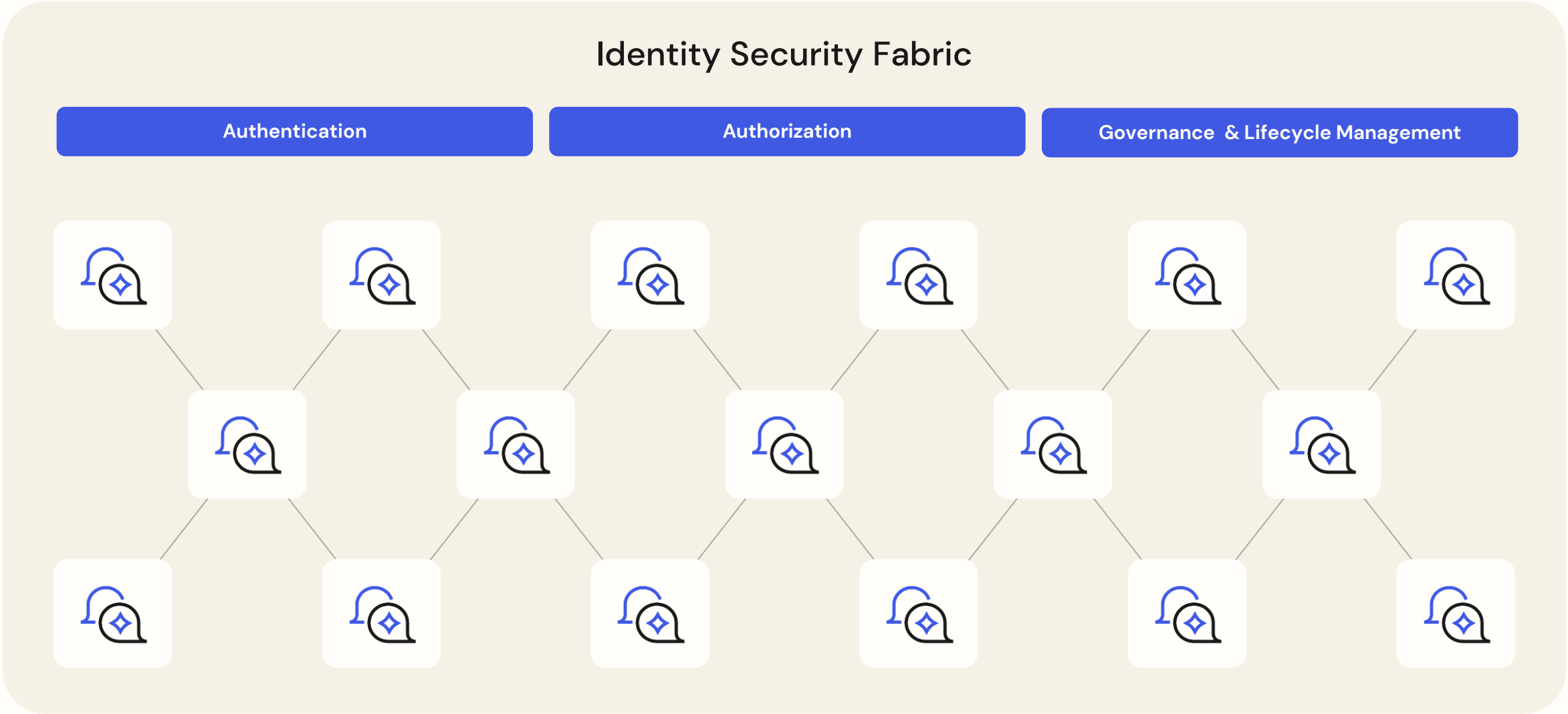
Auth0

Build agents to be secure by design

Okta

Bring agents into into a secure identity fabric

Okta’s identity security fabric covers the AI stack.



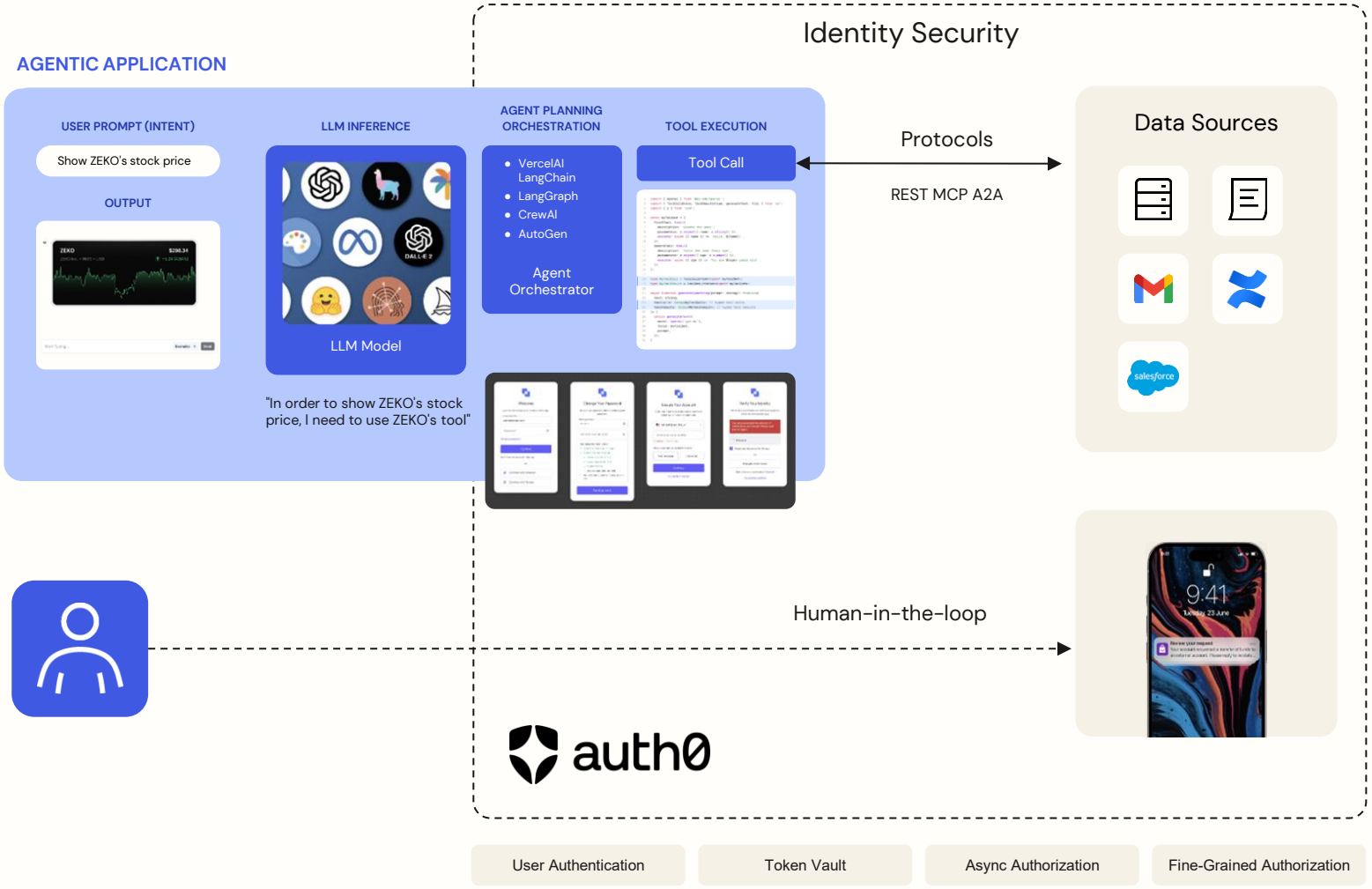
Auth for GenAI secures access, scoped permission & user oversight for SaaS builders.

Framework for Securing Agent Behavior Inside Apps

- → Secure login for agents (chatbots & workers)
- → Vaulted tokens + FGA for API & doc access
- → Human-in-the-loop approvals for async actions

So developer get:

- → Faster, safer GenAI development
- → Full policy control over agent behavior
- → Enterprise-grade security for AI features



Cross App Access provides visibility and control for enterprises.

Protocol for Securing App-to-App & Agent Access

→ Shifts control of apps/ agent access to the identity layer

→ Applies policies to every connection in real time

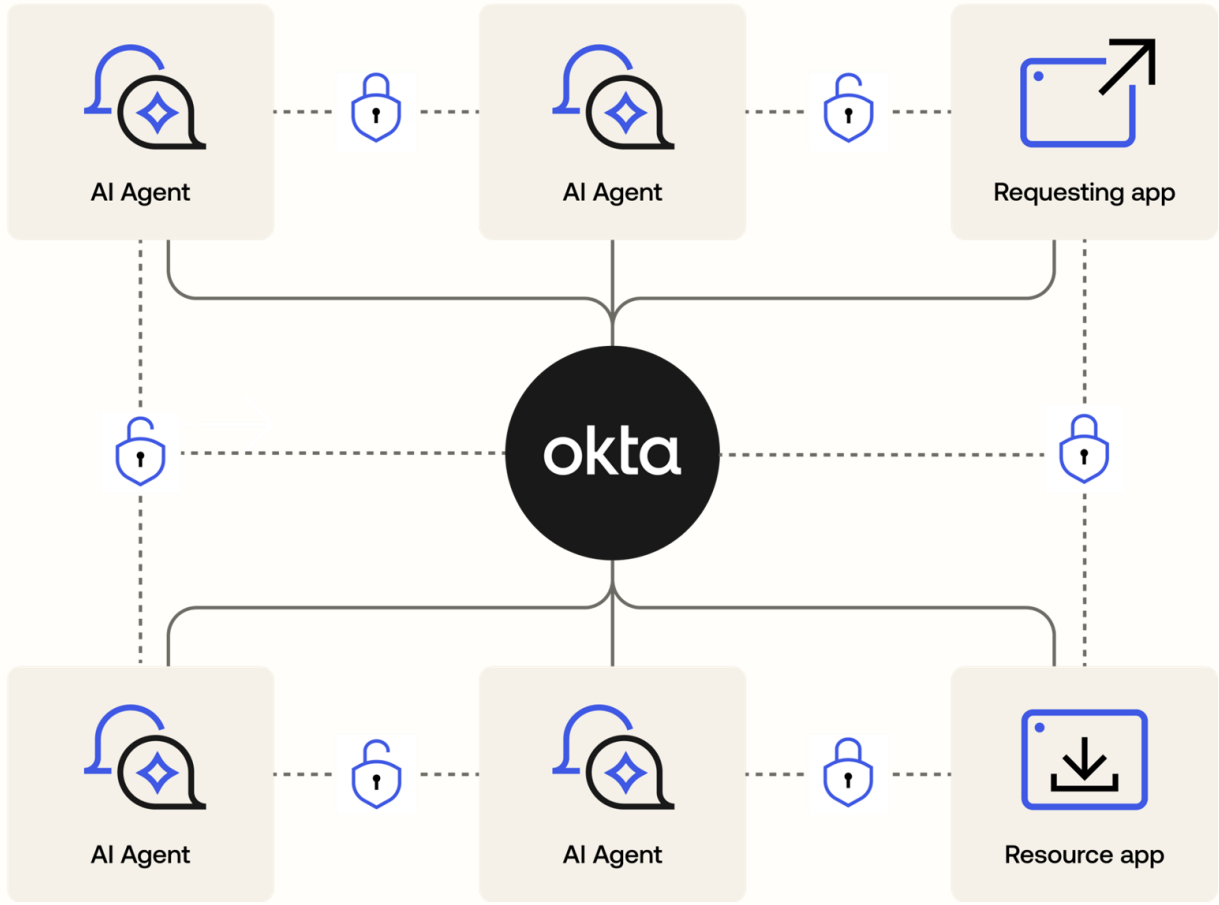
→ Standardizes how data is accessed across systems

So enterprises can:

→ See and control every agent and app interaction

→ Enforce least-privilege access across SaaS ecosystem

→ Eliminate risky credentials and unmanaged connections



The Okta Platform helps you continuously discover, manage, and monitor AI agents.

Unified security for AI agents

→ A consistent way to discover, manage, authorize, monitor and protect our customers using AI Agents— regardless of how they are implemented

→ A new E2E flow only made possible by the Okta Platform

So enterprises can:

→ Gain holistic visibility of human and non-human identities

→ Standardize AuthN & AuthZ

→ Enforce least privileged access and governance

→ Continuously evaluate and protect

The Vision

Discover all agent access in a customer's environment

Be the directory of AI Agents within an enterprise

Manage AI Agent access to resources with Okta

Standardize how AI Agents authenticate with resources

Control what level of access AI Agents have with applications

Just-in-time temporary elevated access for AI Agents

Certify AI Agent access to maintain compliance

Revoke AI Agent Access when high risk is detected

Explore what’s next.

01

Start building with Auth for GenAI

Securely add AI agent capabilities to your apps using trusted identity patterns.

02

Get Early Access to Cross App Access

Get governance over app-to-app and agent access ahead of general availability.

03

Watch *Securing Agentic AI*: An Industry-Wide Call to Action

Watch the digital event to see how Okta, ISVs and enterprises are coming together to define the next era of AI-powered access.

Thank you!

okta