

# Identity for the AI Era: Securing Customers, Employees, and AI Agents

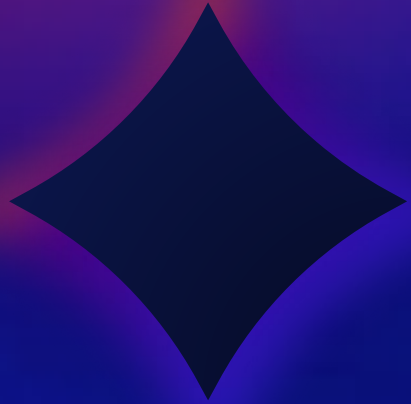


# Toby Allen

Senior Solutions Engineer, Okta

How many of you  
are using  
Generative AI  
everyday?

How many of you  
believe your  
machine identity &  
secrets controls are  
perfect?



Your agents are already running.  
Most of them without your permission.



# 100:1

machine-to-human  
identity ratio across  
enterprises

# 1.3B

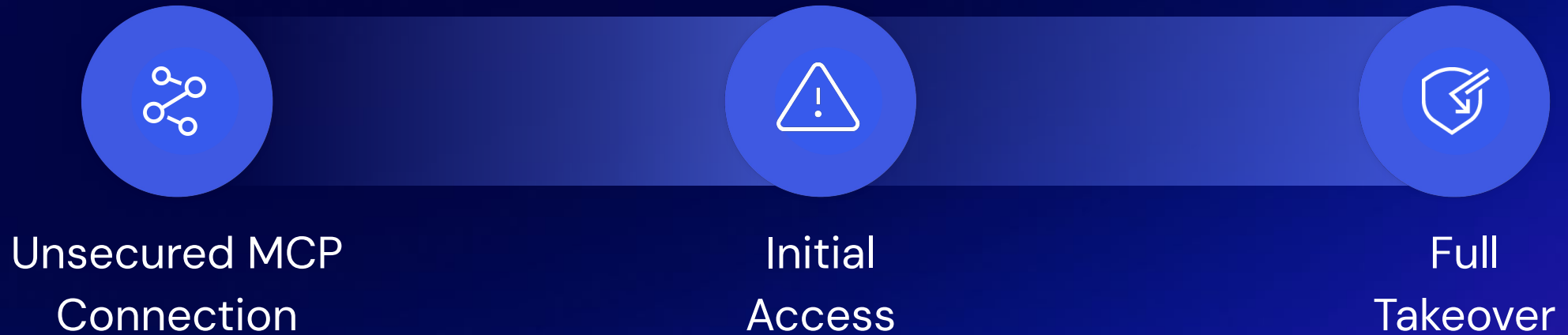
AI agents projected in  
enterprise environments  
by 2028



# 68%

of organizations cannot  
distinguish agent activity  
from human activity

# This is no longer theoretical



***One MCP connection. Total compromise.***



Amazon.com

+ Add to myFT

## Amazon holds engineering meeting following AI-related outages

Ecommerce giant says there has been a 'trend of incidents' linked to 'Gen-AI assisted changes'



Recent outages had a 'high blast radius', according to a company memo © Belga Mag/AFP via Getty Images

# Apologizes after its AI agent wiped a business test run and lied about it

THE DIG

FEBRUARY 25, 2026

## Single API Keys Weren't Secrets. But on Gemini Changed the Rules

Hacking McKinsey's AI Platform

UNAUTHENTICATED ACCESS TO PRODUCTION DATABASE

46.5M

728K

57.8K

95

Chat Mes

### History Repeats: Security in the AI Agent Era

Exclusive: Lab tests discover 'new form of insider risk' with artificial intelligence agents engaging in autonomous, even 'aggressive' behaviours

**Robert Booth** UK technology editor

You spent a decade securing humans. Agents are undoing it.

88%

of organizations report  
confirmed or suspected AI  
agent security incidents

97%

of AI breach victims had  
no formal AI access  
controls

The **S** in AI stands for  
security.

AI SECURITY HAS THREE LAYERS

# Security doesn't stop at the model layer.

The stronger models get, the more agent identity and data authorization become the critical layers.

## MODEL SECURITY

Is this model sanctioned and in bounds?

VISIBLE

↑ MOST STOP HERE

## AGENT IDENTITY

Is this agent authorized to act for this user?

GAP

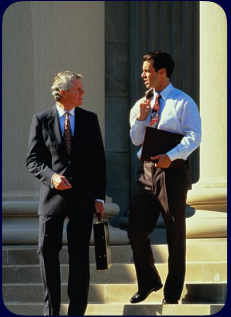
## DATA AUTHORIZATION

Should this action execute with these parameters, right now?

GAP



AI security *is*  
identity security





**Where are my  
agents?**



**What can they  
connect to?**



**What can  
they do?**



**Where are my  
agents?**

Anyone can spin up an agent. Agents spawn more agents. The ones you don't know about are the ones that pose the most risk.



**Known agents**  
Third party + custom



**Unknown agents**  
Local desktop + browser-embedded agents



**What can they  
connect to?**

The blast radius of a compromised agent is defined by its connections. All it takes is one connection to compromise your entire system.



Authorization servers



SaaS applications



Service accounts and secrets



MCP servers



**What can  
they do?**

Agents access resources at machine speed. If you cannot enforce governance in real-time, you have already lost control.



Kill switch



Access Requests



Human-in-the-loop

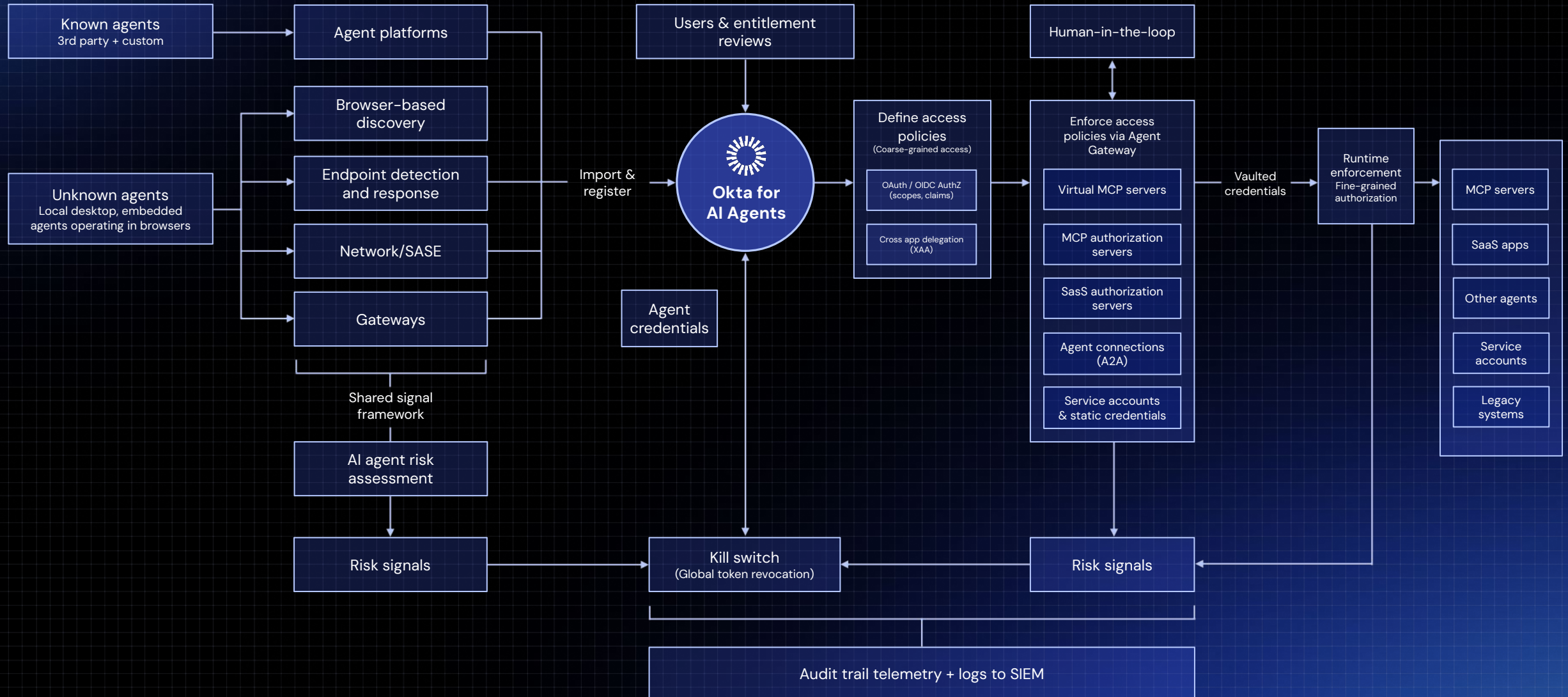


Access Certifications

## Where are my agents?

## What can they connect to?

## What can they do?





**Where are my  
agents?**



**What can they  
connect to?**

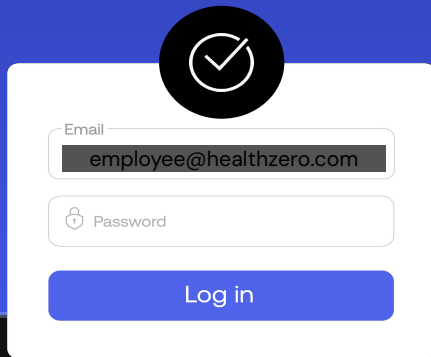


**What can  
they do?**

# Agentic Security for Applications

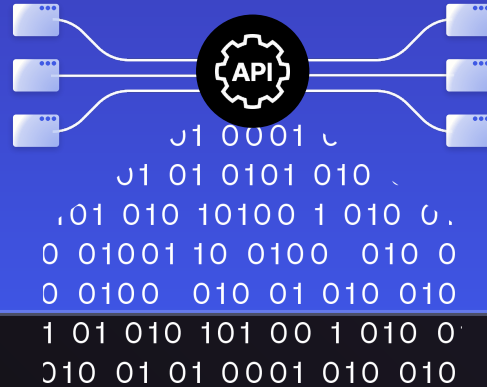
## User Authentication

AI needs to know who I am



## Token Vault

AI needs to call APIs on users behalf



## Async Authorization

AI uses async interactions



## Fine-Grained Authorization

AI data access must consider user permissions



# What are the main use cases?



## Deliver connected AI experiences

Integrate AI experiences into existing high-scale consumer applications and drive user adoption.

### AI Deployment Paths:

- ✓ Retail Concierge
- ✓ Personal Finance Manager
- ✓ Commerce Agent



## Build trusted, action-oriented products

Transform products into partners that act on a user's behalf across data silos and accelerate time to market.

### AI Deployment Paths:

- ✓ Workflow Automator
- ✓ Project Management Agent
- ✓ SRE and DevOps Agent



## Secure the agentic workforce

Standardize and secure specialized agents for workforce automation and eliminate shadow AI risks.

### AI Deployment Paths:

- ✓ Expense & Audit Agents
- ✓ Code Generation Assistants
- ✓ Travel and Logistics Agents

Q&A



# Unprecedented customer demand for security

