okta
The World's Identity Company

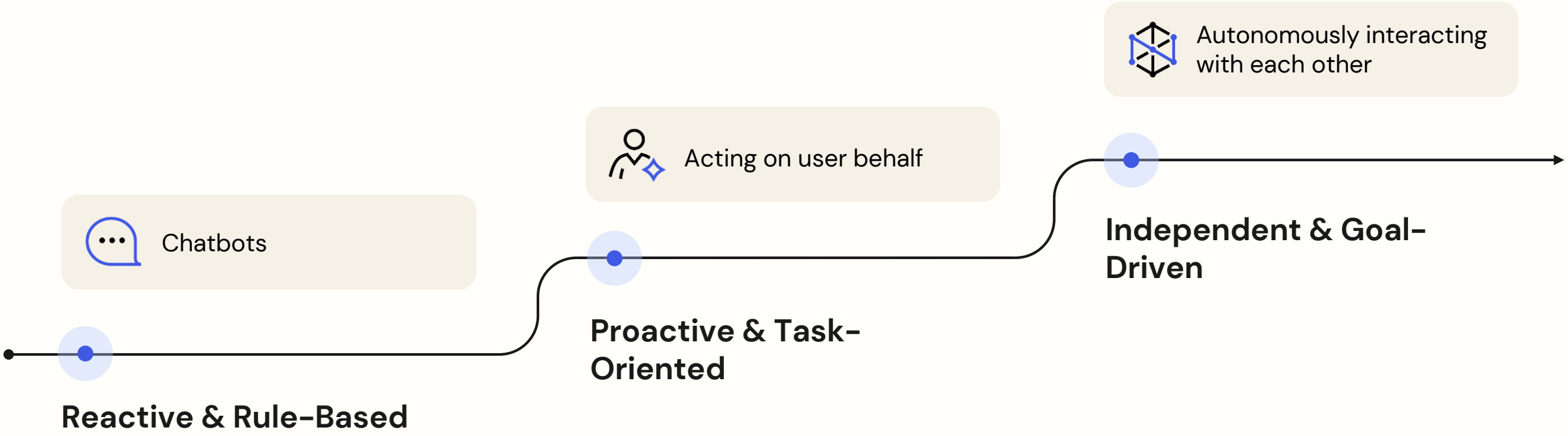
Okta Secures Agentic AI

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.

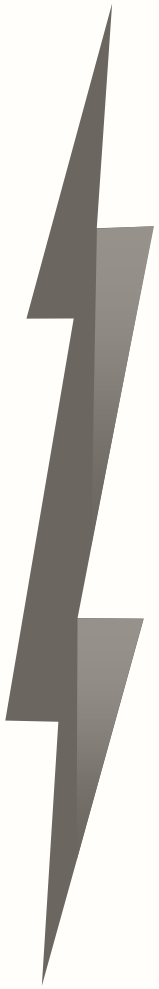
Any products, features, functionalities, certifications, authorizations, or attestations referenced in this presentation that are not currently generally available or have not yet been obtained or are not currently maintained may not be delivered or obtained on time or at all. Product roadmaps do not 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.

AI Agents are rapidly evolving, becoming more complex and introducing new risks



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

91% of organizations are already using AI agents [1]



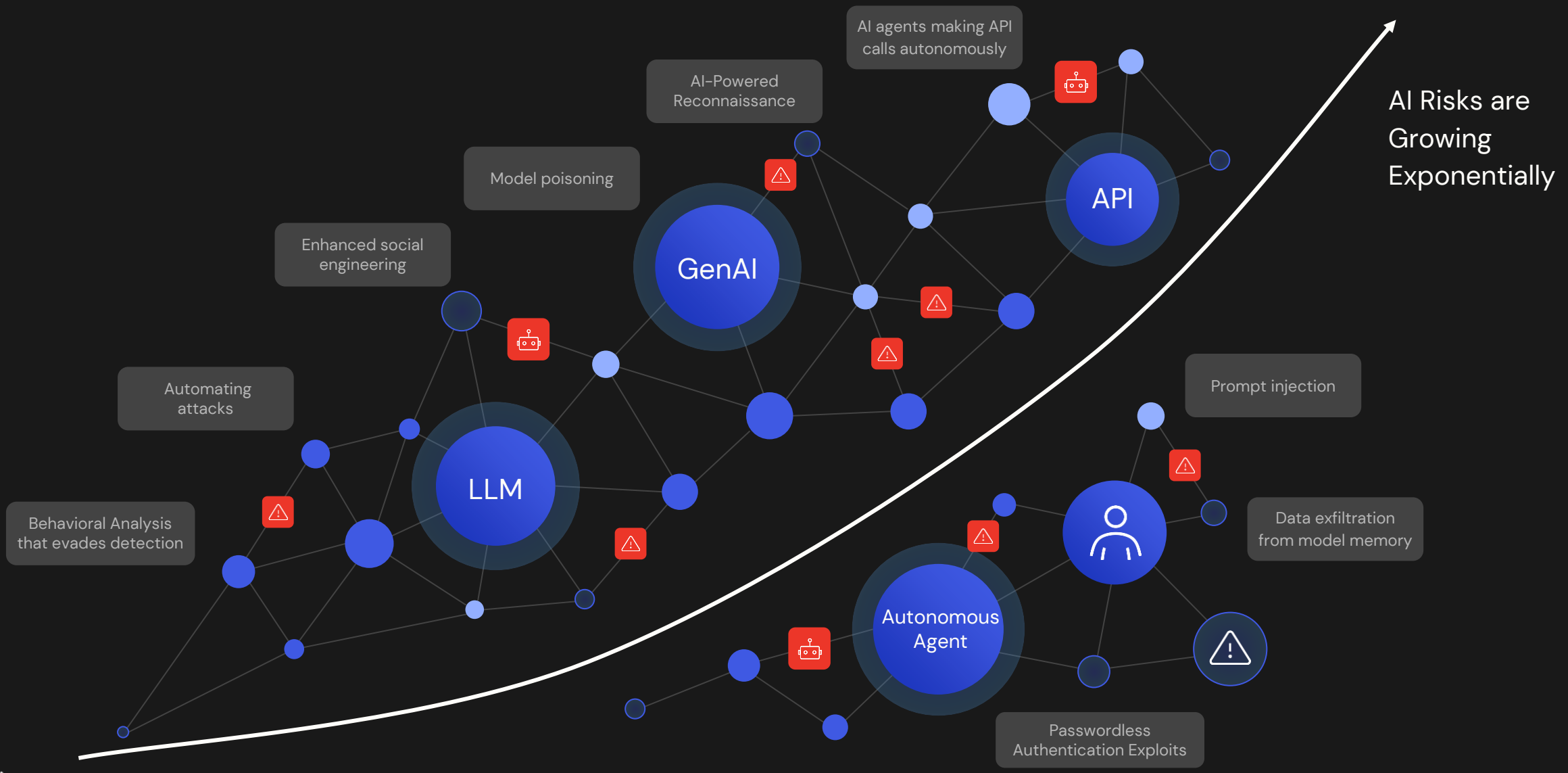
80% experienced unintended agent behavior [2]

23% report credential exposure via agents [3]

44% have no governance in place [4]

1 *Okta AI at Work 2025: Securing the AI-powered workforce*
2, 3, 4 *The Times, 2025*

AI is rewriting the attack surface



Agentic AI introduces major identity security risks

Unauthorized data access

Agents fetch data the user should never see.

Stale or over-provisioned permissions

Old roles or tokens can let agents with powers nobody tracks.

Compliance & audit gaps

Actions are not tied back to a real user or logged consent, so audits fail.

Weak or coarse-grained authorization

One-size rules let any agent run sensitive actions.

Secrets & credential leakage

Keys and tokens can show up in prompts where attackers can steal them.

Privacy & data-leak exposure

Personal data leaves safe zones and can land in the wrong hands.

You need to secure **every** agent, and **all** agents

Secure **every** agent by design

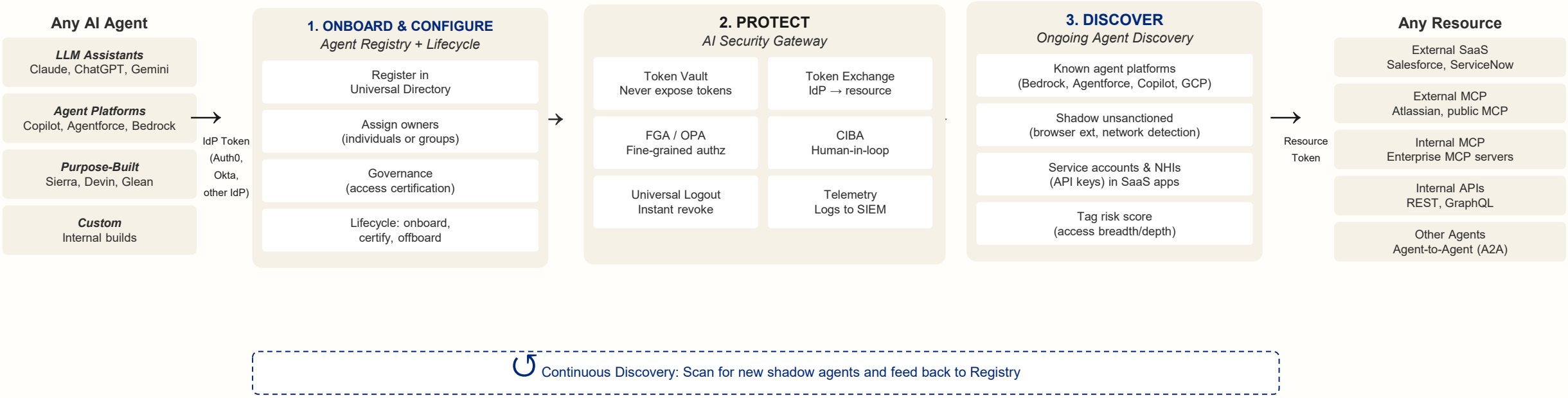
- Authentication
- Authorization
- Token Vaulting
- Data Security
- Tool Call Security
- Human in the Loop

Secure **all agents** from a single control plane

- Agent registry
- Access control
- Lifecycle management
- Privileged credentials
- Agent detection
- Agent universal logout

Okta for AI Agents: Onboard, Protect, Discover

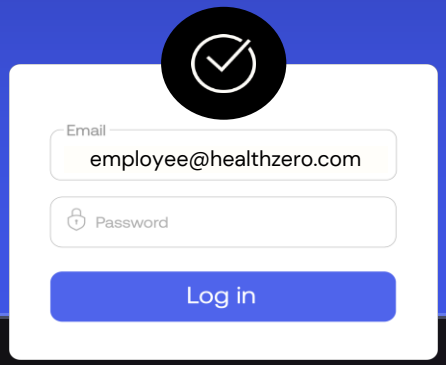
Gateway-Centric Architecture: Okta discovers & registers → AI Gateway protects runtime access



Agents need to be built secure by design

User Authentication

Agents need to **know who I am**

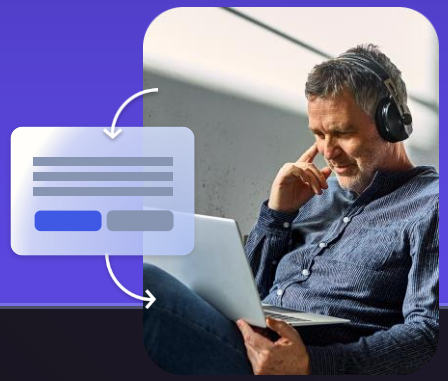


Token Vault

Agents should have **zero standing privileges**

Async Authorization

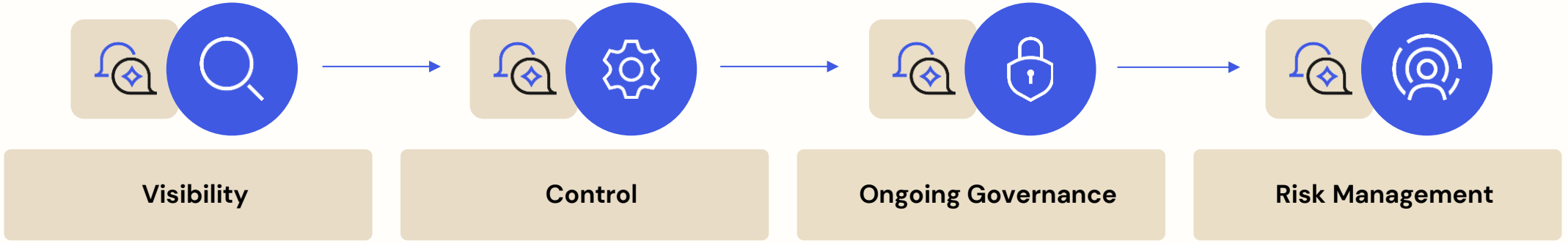
Agents should use **async interactions for sensitive actions**



Fine-Grained Authorization

Agents should only **access what they need**

Bring AI Agents into your identity security fabric



Secure Identity Products

Posture Management | Access Management | Universal Directory | PAM | Governance | Identity Threat Protection

Secure Identity Orchestration

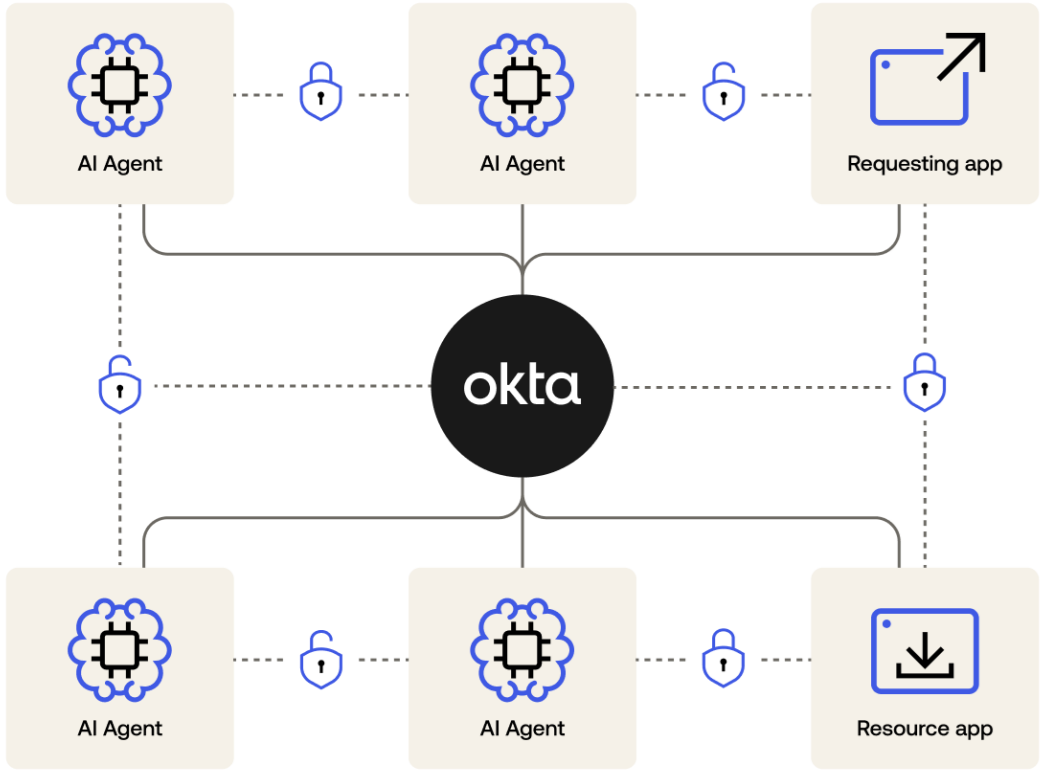
Secure Identity Integrations

Infrastructure	Applications	APIs	Authentication Frameworks
IaaS, On Prem Servers	Cloud Apps, On Prem Apps	Public, Private	A2A, Cross App Access

Cross App Access for AI Agents - make agents ‘fabric-ready’ from the get go

New 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**



OKTA PRODUCT DESIGN

Help shape the future of Okta: Share your perspective on securing AI

Be part of the conversation and help us understand what you need to secure AI at your company. Provide feedback on design concepts, share your experience with the beta or EA, and explain your current use cases and needs. No wrong answers, just insight from you, our customers!

During this hour, you'll meet with our UX and design teams to discuss your most critical needs, gaps in your current toolsets, and what you'd like to see next from Okta so we can build a more powerful and intuitive solution to secure AI.

WHEN

1 hour sessions in February, March, and April

Sign up here!

Sign up for the month that works best for you and we will schedule a 1 hour zoom call

Okta for AI Agents

Build and manage AI agents securely

Secure ‘every’ agent

Generally Available

Build agents to be secure-by-design

- Token Vault
- Fine-Grained Authorization
- Out-of-the-box support for Cross App Access
- Authentication for AI agents
- Async Auth

Secure ‘all’ agents

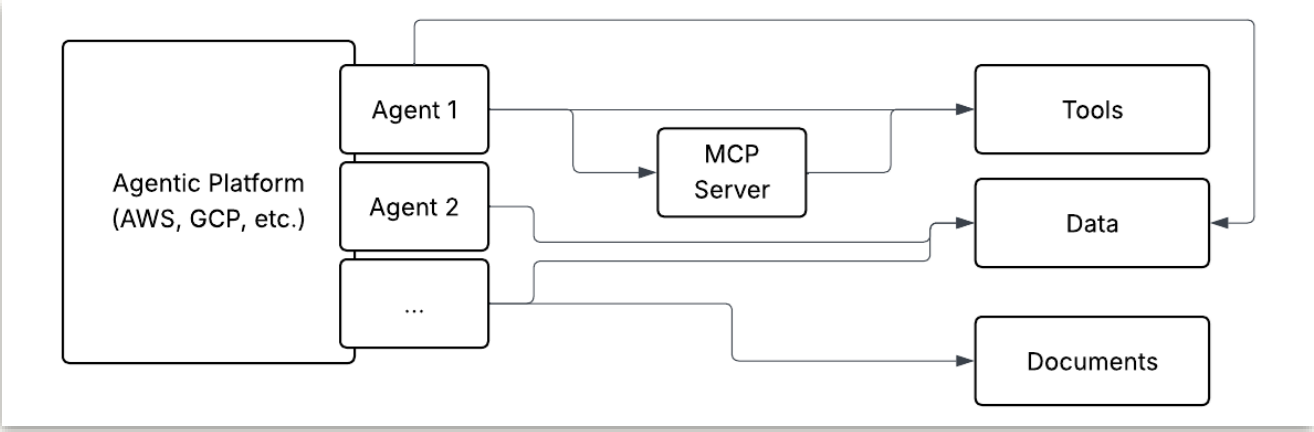
EA Q1 26

Manage and govern AI agents in your environment

- Agent registry in Universal Directory
- Agent detection with Identity Security Posture Management
- Agent governance and access certification with Okta Identity Governance
- Privileged account credential vaulting for agents with Okta Privileged Access
- Universal logout for agents

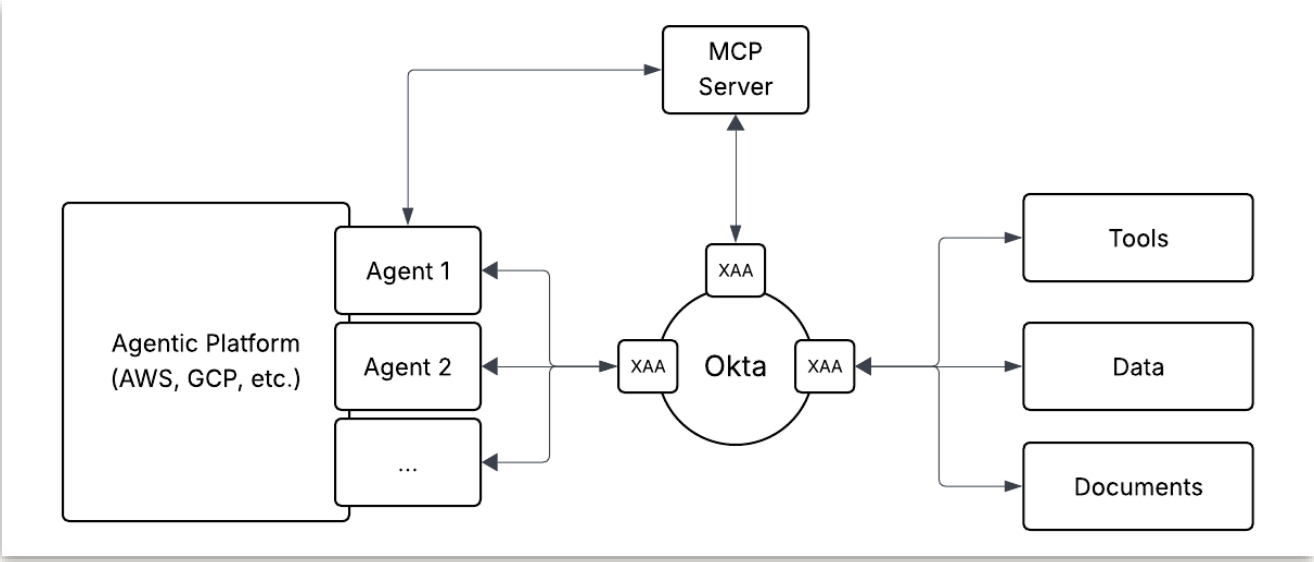
Thank you!

okta



✗ *Without Okta - dependent on agentic platform*

- **Direct connections** between agents/MCPs and enterprise resources → major risk
- **No single registry, governance and threat detection** → leads to sprawl, and cost overruns
- **Dependence on agentic platform for IAM** → vendor risk, breaks layered defense strategy

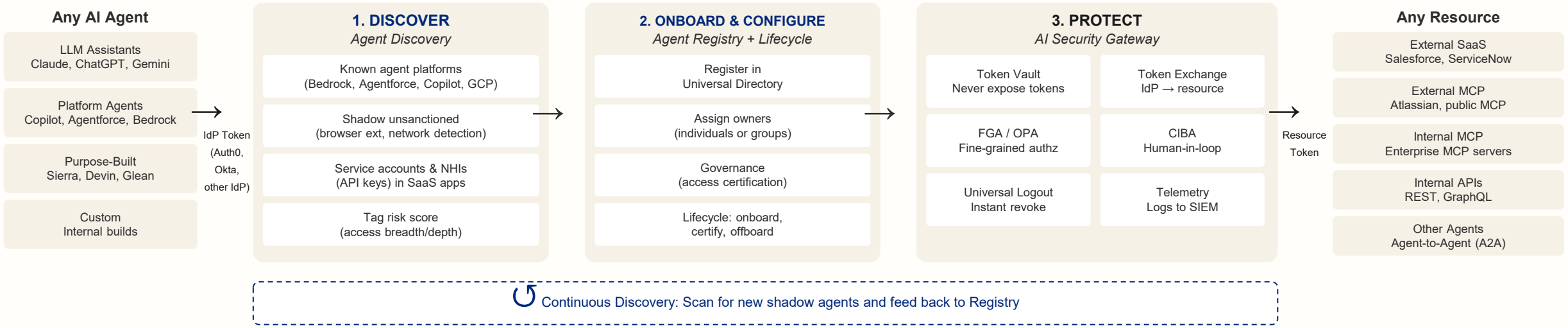


✓ *With Okta for AI Agents - central control plane*

- **All connections managed through Okta**, based on industry protocol of Cross App Access (XAA) → full access control in IT/Security's hands
- **Agentic control plane** → visibility, control and lifecycle governance
- **Built-in threat detection and response** → universal logout for agents
- **Central enforcement of IAM policies on agents**

Complete AI Security Stack: Discover, Onboard, Protect

Gateway-Centric Architecture: Okta discovers & registers → AI Gateway protects runtime access



How It Works

Discover: Scan agentic platforms (Bedrock, Agentforce, Copilot, GCP), detect shadow agents via browser/network, find NHIs in SaaS apps

Onboard: Register agents in Universal Directory with owners, risk scores, and metadata. Automate lifecycle with Workflows.

Protect: Gateway brokers all access. Token Vault holds credentials. FGA enforces fine-grained authz. CIBA for sensitive ops. Logs to SIEM.

Key: Discovery finds agents → Registry onboards them → Gateway protects runtime access. Discovery runs continuously to catch new shadow agents.

Okta for AI Agents - Roadmap

We have an aggressive roadmap over the next many *months* (not years) to help our customers build and manage agents securely

Available now

For agent builders

- Token vaulting for agents
- Human-in-the-loop flows
- Fine-grained authorization
- All of the above for MCP

For IT/Security

- Agent registry (universal directory, ownership and connections)
- NHI registry
- ISPM for humans and NHI

Early 26

For agent builders

- Partner dev portal
- Deeper agentic/payment platform integrations (e.g. AWS, OpenAI, Google, etc.)

For IT/Security

- Agent detection in ISPM (browser plugin & native app)
- Access certifications for agents
- Agentic access relay

Later in '26

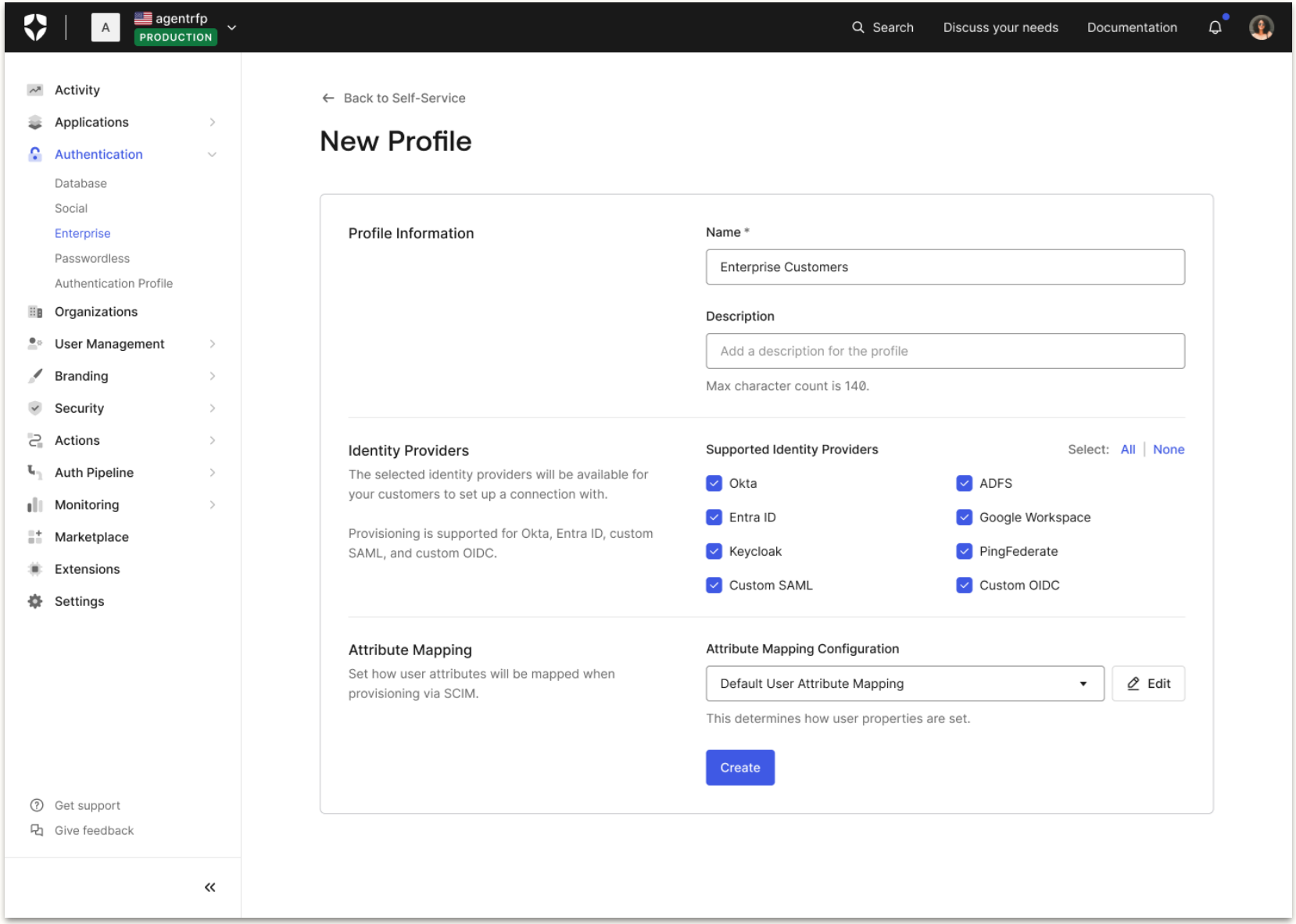
- Deeper integrations into security stack
- Agentic access relay enhancements - signal sharing, token revocation
- Continued agentic platform integrations

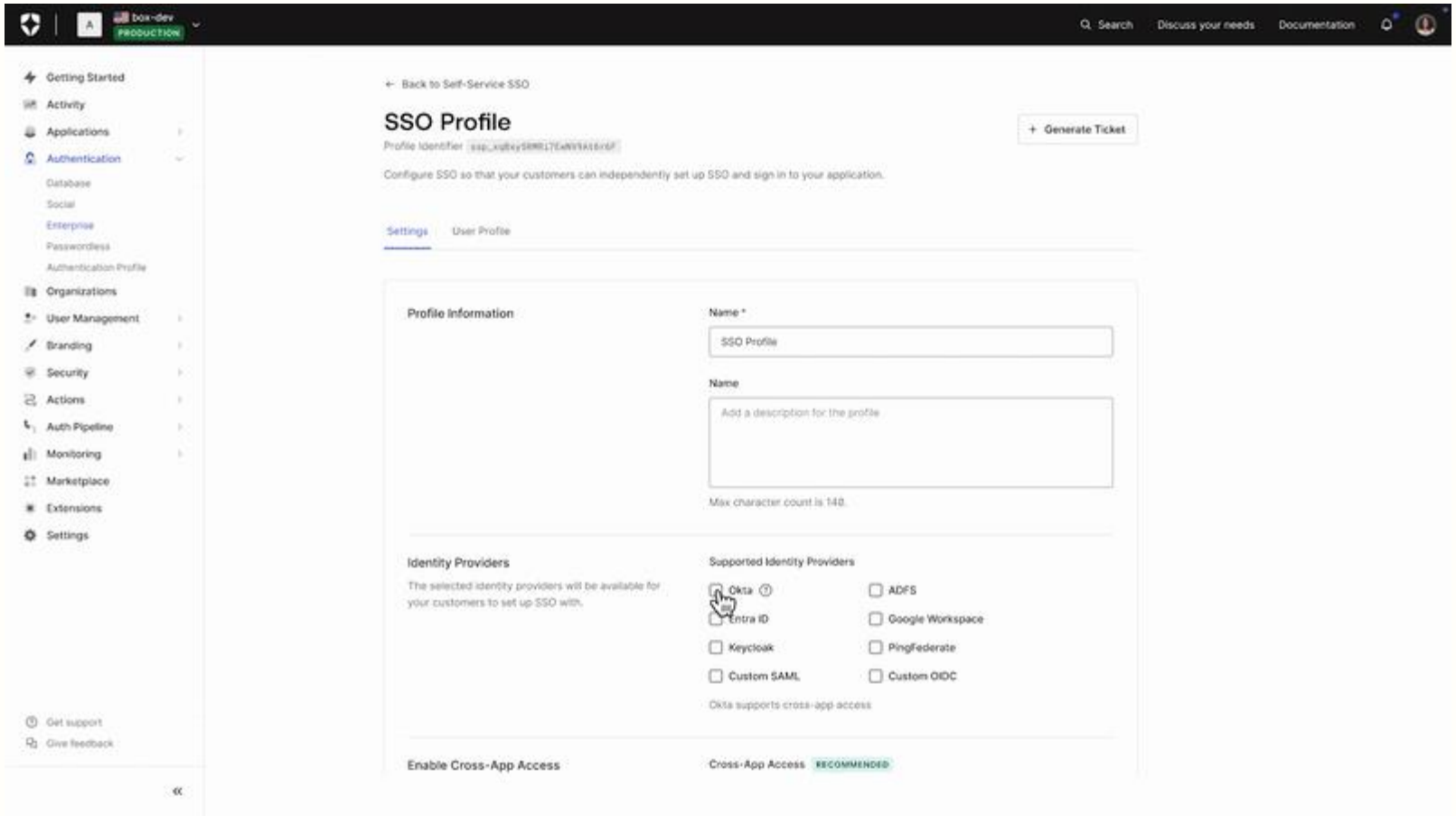
Ongoing work to increase standards adoption

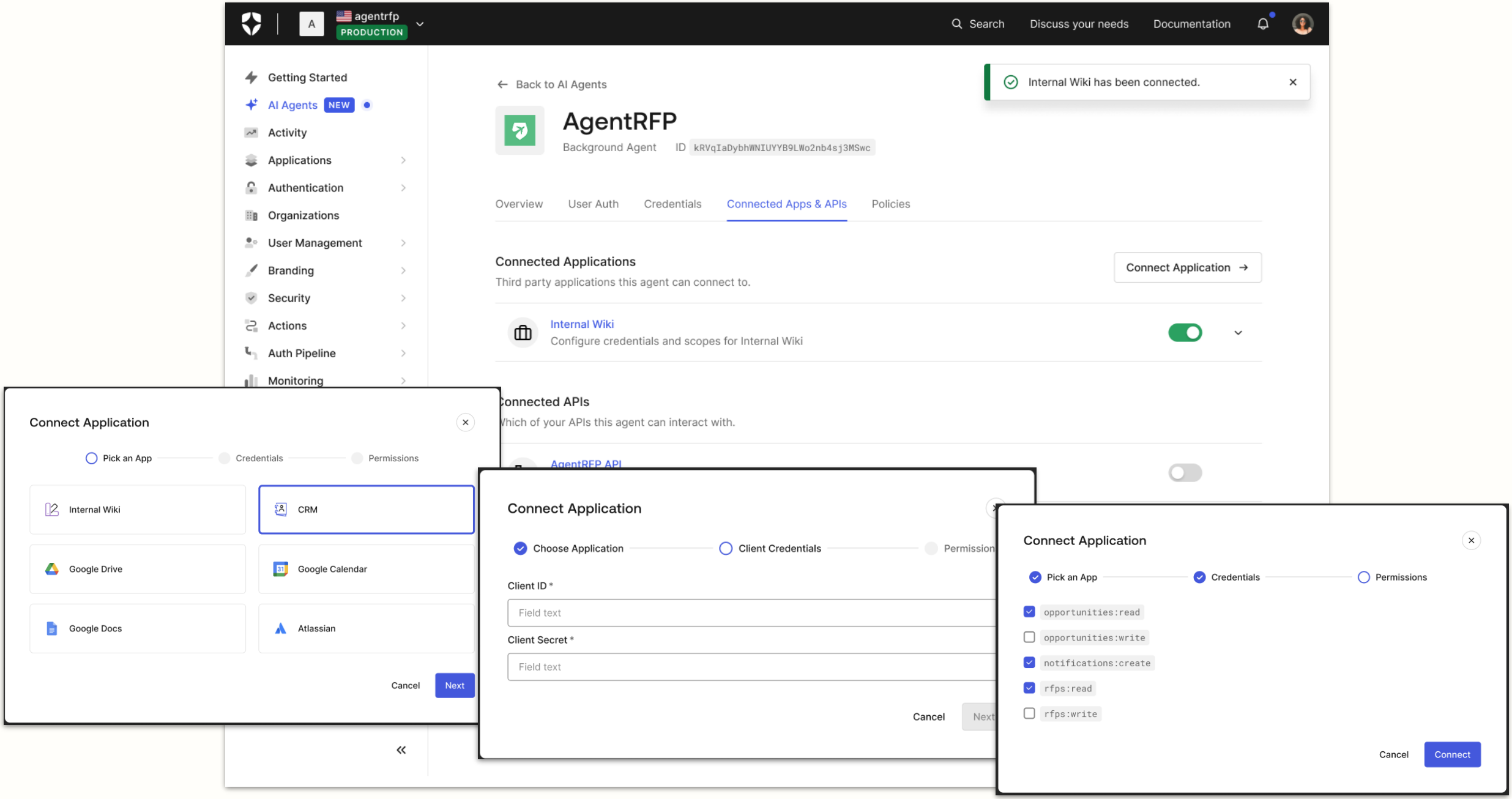
- Cross-app access support for requesting and resource apps
- Continued push to get ISVs to adopt XAA

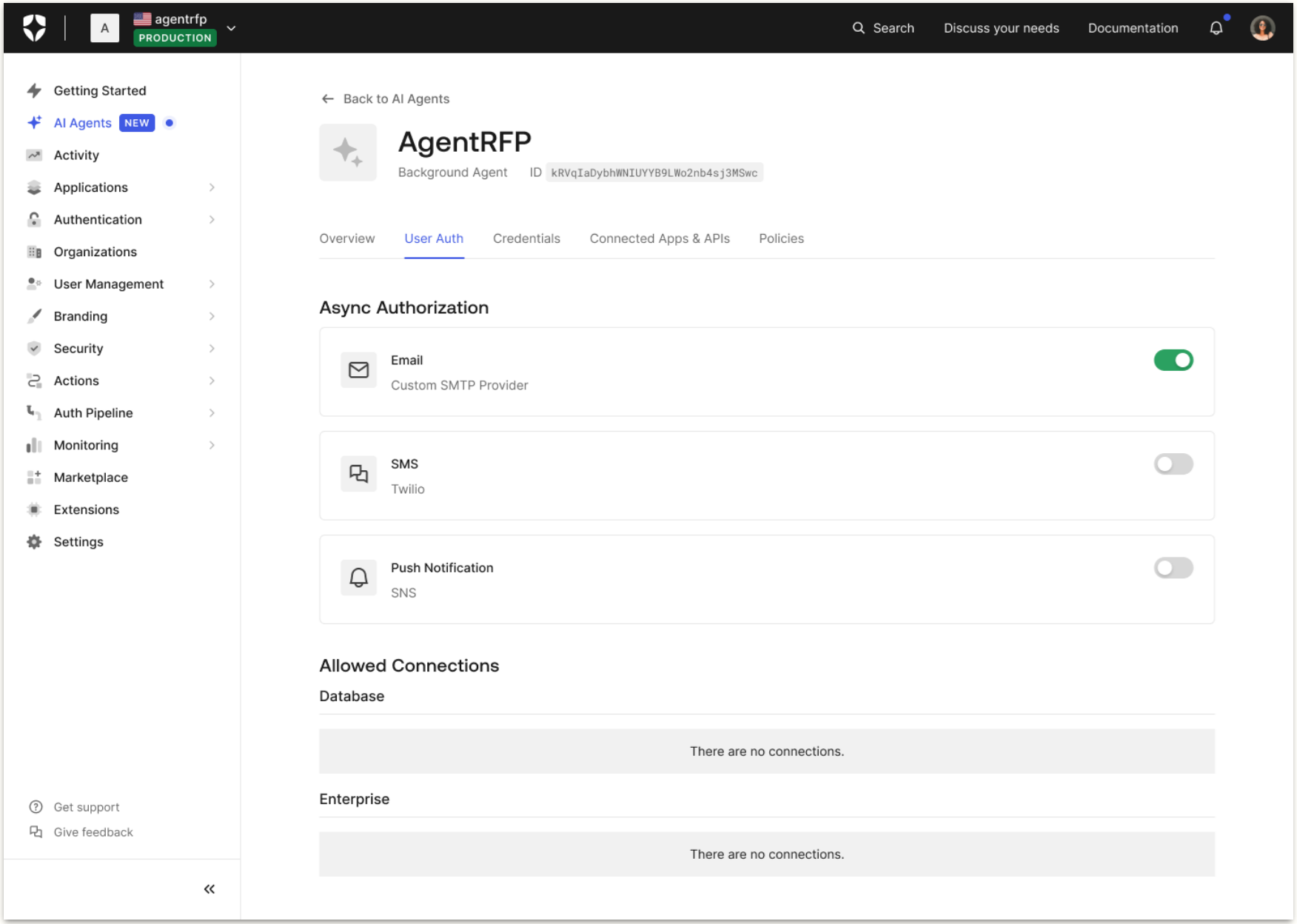
Clickthrough Demo

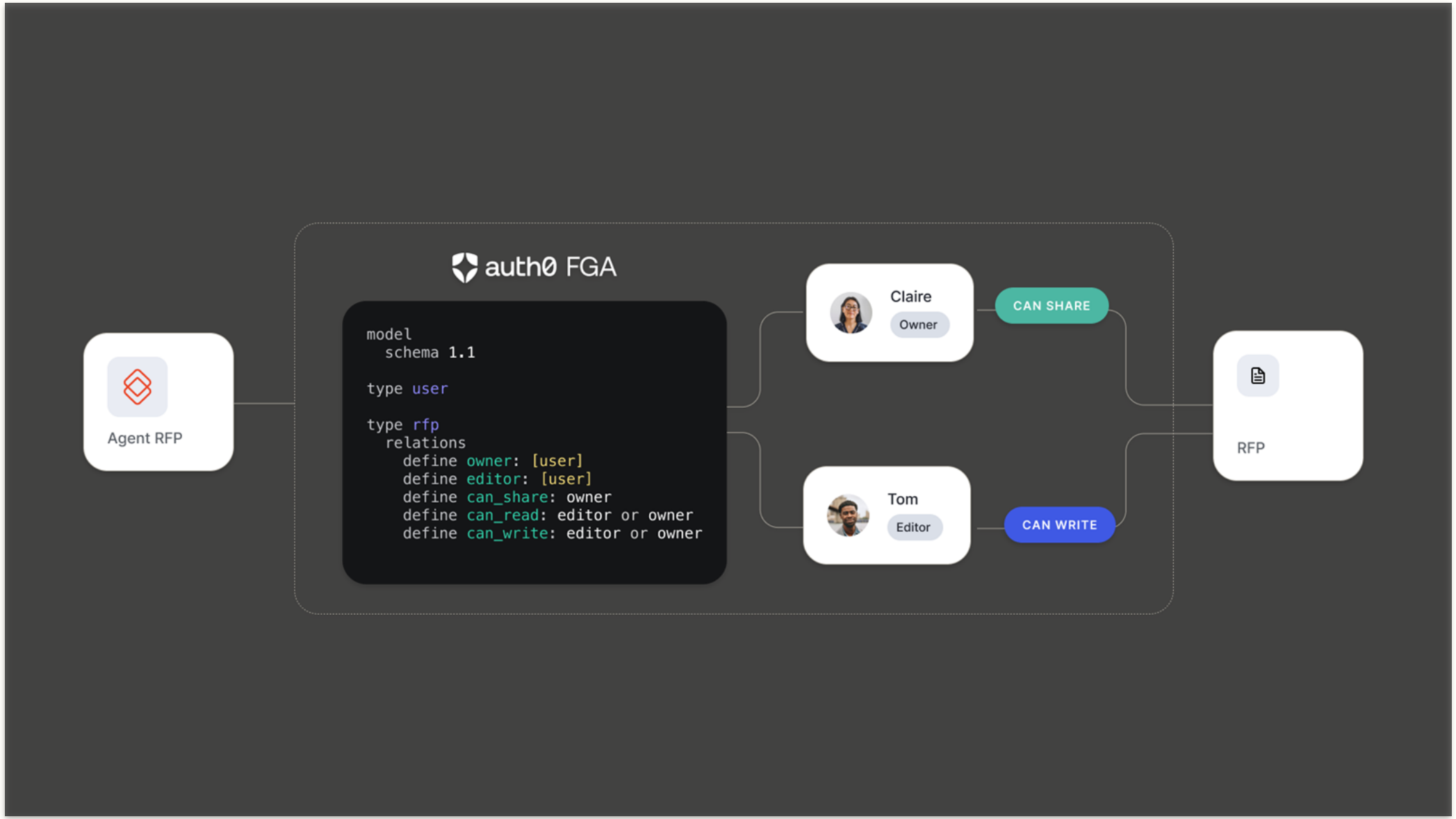
okta











Dashboard
Directory
People
Groups
Realms
AI Agents
Service Accounts
Devices
Profile Editor
Directory Integrations
Profile Sources
Customizations
Applications
Identity Governance
Security
Workflow
Reports
Settings

AI Agents

Manage the registration, access, lifecycle, and oversight of your AI agents.

Register AI Agent

Search...

NAME	STATUS	OWNER
Customer Service	ACTIVE	Group IT-Admins
SupportRocket	ACTIVE	Otto Waller, Mannix Jones, Dorian Morrison
Sales Investigator	INACTIVE	Group IT-Admins
Zoom AI Companion	ACTIVE	Brenda Dixon, Harlan Prince, Robert Burke, Ira Cochran
Glean AI Agent	ACTIVE	Group Glean App Owners
OpenAI Codex	ACTIVE	Group IT-Admins
Gemini	ACTIVE	Group IT-Admins
Lattice AI	ACTIVE	Group IT-Admins
Slack MCP	ACTIVE	Group IT-Admins
Insight Scribe	ACTIVE	Group IT-Admins

Rows per page 10 1-10 of 10 rows

Page 1

okta

Search...

mallory
Streamward

Admin

- Dashboard
- Directory
  - People
  - Groups
  - Realms
  - AI Agents
  - Service Accounts
  - Devices
  - Profile Editor
  - Directory Integrations
  - Profile Sources
- Customizations
- Applications
- Identity Governance
- Security
- Workflow
- Reports
- Settings

Back to AI agents

Create AI agent

Agent profile

Name

Customer Service

Description Optional

Agent owner

- Assign users
- Assign a group

Groups

Up to 5 groups can be assigned as owners

IT-Admins

Connected public client app

App Optional

Recommended actions

RISK REMEDIATION GUIDE

Register AI Agent in Universal Directory

Get step-by-step instructions to register an AI Agent, in Universal Directory.

The following admin roles have permission to complete this guide:

Super Admins

1. Configure Agent profile
2. Assign agent owners

   In the Agent owner section, select the users or groups as owners of the agent:

   - Choose the users whose access you want to review.
3. Connect public client app

Next Steps:

RISK REMEDIATION GUIDE
Configure Cross App Access

RISK REMEDIATION GUIDE
Create a Certification Campaign

Admin Console

- Dashboard
- Directory
  - People
  - Groups
  - Realms
  - AI Agents
  - Service Accounts
  - Devices
  - Profile Editor
  - Directory Integrations
  - Profile Sources
- Customizations
- Applications
- Identity Governance
- Security
- Workflow
- Reports
- Settings

Directory / AI Agents / SupportRocket

AI AGENT

SupportRocket

Your AI assistant for IT answers and insights. View Logs

Profile | Managed connections | Owners | Assignment

Authorization on behalf of user

Control what this AI agent can access and do for on behalf of a user. Manage connections to allow only approved actions and protect sensitive resources.

Create connections

RESOURCE	TYPE	ACCESS
Google Workspace	Agent-app connection	Only include: `drive.read-only`
Atlassian Jira	Agent-app connection	Only include: `read:jira-work` `write:jira-work`
Salesforce	Agent-app connection	Only include: `api` `read_only_accounts` `read_write_cases`
PagerDuty	Service account	svcAcct1@streamward.co, svcAcct2@streamward.co
Asana	Vaulted Secret (API Key)	`asana-support-key`

Admin Console

- Dashboard
- Directory
  - People
  - Groups
  - Realms
  - AI Agents
  - Service Accounts
  - Devices
  - Profile Editor
  - Directory Integrations
  - Profile Sources
- Customizations
- Applications
- Identity Governance
- Security
- Workflow
- Reports
- Settings

Directory / AI Agents / SupportRocket

AI AGENT

SupportRocket

Your AI assistant for IT answers and insights. View Logs

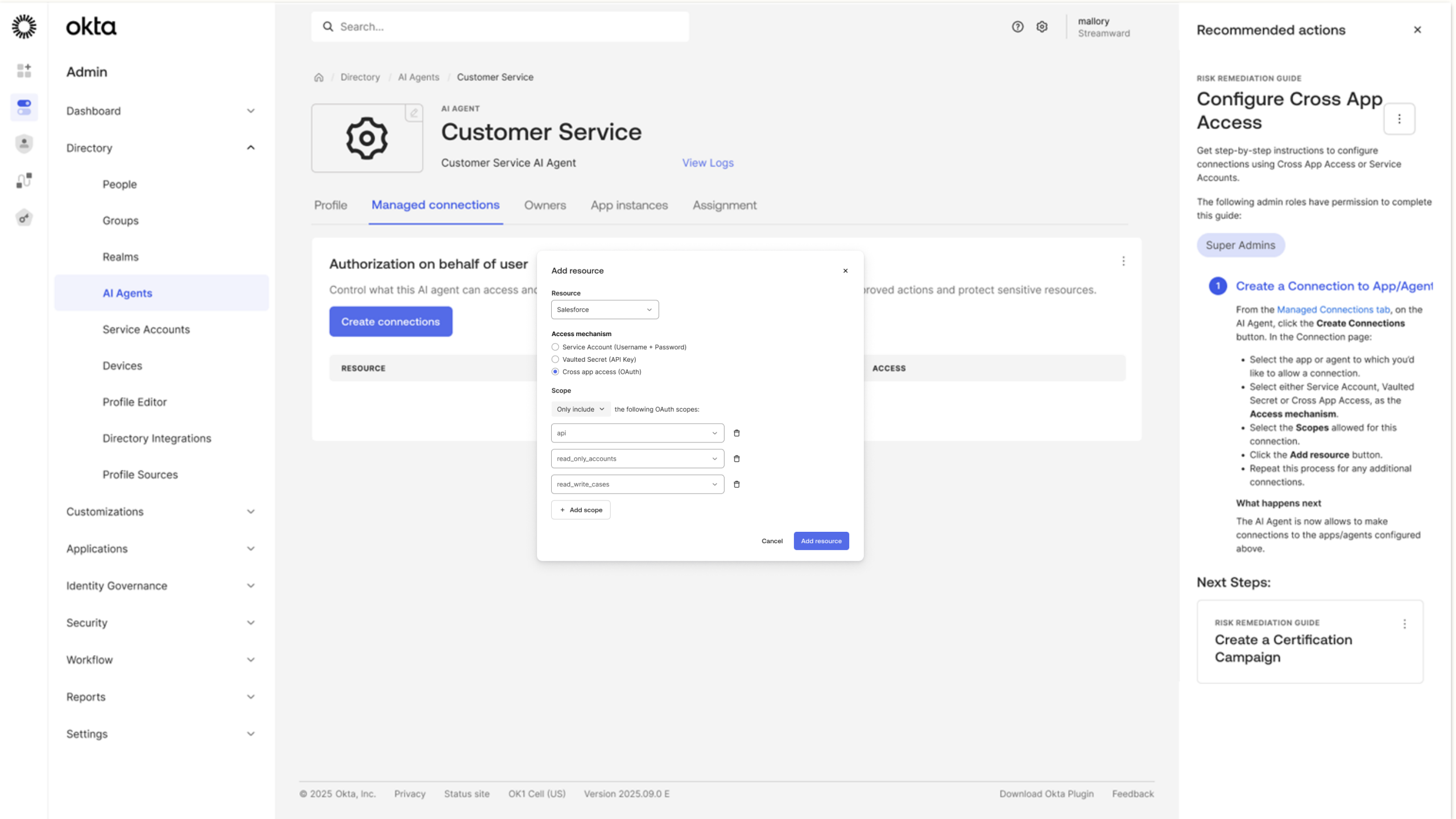
Profile | Managed connections | Owners | Assignment

Authorization on behalf of user

Control what this AI agent can access and do for on behalf of a user. Manage connections to allow only approved actions and protect sensitive resources.

Create connections

RESOURCE	TYPE	ACCESS
Google Workspace	Agent-app connection	Only include: `drive.read-only`
Atlassian Jira	Agent-app connection	Only include: `read:jira-work` `write:jira-work`
Salesforce	Agent-app connection	Only include: `api` `read_only_accounts` `read_write_cases`
PagerDuty	Service account	svcAcct1@streamward.co, svcAcct2@streamward.co
Asana	Vaulted Secret (API Key)	`asana-support-key`


okta
Admin
Dashboard
Directory
People
Groups
Realms
AI Agents
Service Accounts
Devices
Profile Editor
Directory Integrations
Profile Sources
Customizations
Applications
Identity Governance
Security
Workflow
Reports
Settings
Search...
mallory
Streamward
Directory / AI Agents / Customer Service
AI AGENT
Customer Service
Customer Service AI Agent
View Logs
Profile
Managed connections
Owners
App instances
Assignment
Authorization on behalf of user
Control what this AI agent can access and
roved actions and protect sensitive resources.
Create connections
RESOURCE
ACCESS
Add resource
Resource
Salesforce
Access mechanism
Service Account (Username + Password)
Vaulted Secret (API Key)
Cross app access (OAuth)
Scope
Only include
the following OAuth scopes:
api
read_only_accounts
read_write_cases
+ Add scope
Cancel
Add resource
Recommended actions
RISK REMEDIATION GUIDE
Configure Cross App Access
Get step-by-step instructions to configure connections using Cross App Access or Service Accounts.
The following admin roles have permission to complete this guide:
Super Admins
1
Create a Connection to App/Agent
From the Managed Connections tab, on the AI Agent, click the Create Connections button. In the Connection page:
Select the app or agent to which you'd like to allow a connection.
Select either Service Account, Vaulted Secret or Cross App Access, as the Access mechanism.
Select the Scopes allowed for this connection.
Click the Add resource button.
Repeat this process for any additional connections.
What happens next
The AI Agent is now allows to make connections to the apps/agents configured above.
Next Steps:
RISK REMEDIATION GUIDE
Create a Certification Campaign
© 2025 Okta, Inc.
Privacy
Status site
OK1 Cell (US)
Version 2025.09.0 E
Download Okta Plugin
Feedback

okta

Search...

mallory
Streamward

Admin Console

- Dashboard
- Directory
- Customizations
- Applications
- Identity Governance
  - Access Certifications
  - Access Requests
  - Resource Collections
  - Settings
- Security
- Workflow
- Reports
- Settings

← Back to access certifications campaigns

Salesforce Access Review

Description: Review of access to Salesforce.

Created by: Mallory (mallory@streamward.co) on 9/24/2025

Pending reviews	Approved	Revoked	Reassigned	Progress
5	2	4	0	60 %

Pending | Closed

Pending reviews

Approve or revoke access to resources for the users/agents. You can also reassign a review to another user. View best practices

Filters: No filters applied

Search by user

Reassign (0)

	Identity	Type	Resource	Reviewer	Entitlement	Actions
☐	Otto Waller	Individual	Salesforce	Mannix Jones	Permission Sets: M	Reassign
☐	Berk Holland	Individual	Salesforce	Mannix Jones	Feature Licenses:	Reassign
☐	Ira Cochran	Individual	Salesforce	Mannix Jones	Profile: System Ad	Reassign
☐	SupportRocket	Cross App Access	Salesforce	Otto Waller	api	Reassign
☐	SupportRocket	Cross App Access	Salesforce	Otto Waller	full	Reassign

Review details

last updated 09/25/2025 at 09:40 AM

Identity details

Identity	SupportRocket
Type	Cross App Access
Status	Active
Owner	Otto Waller

Entitlement details

Application details

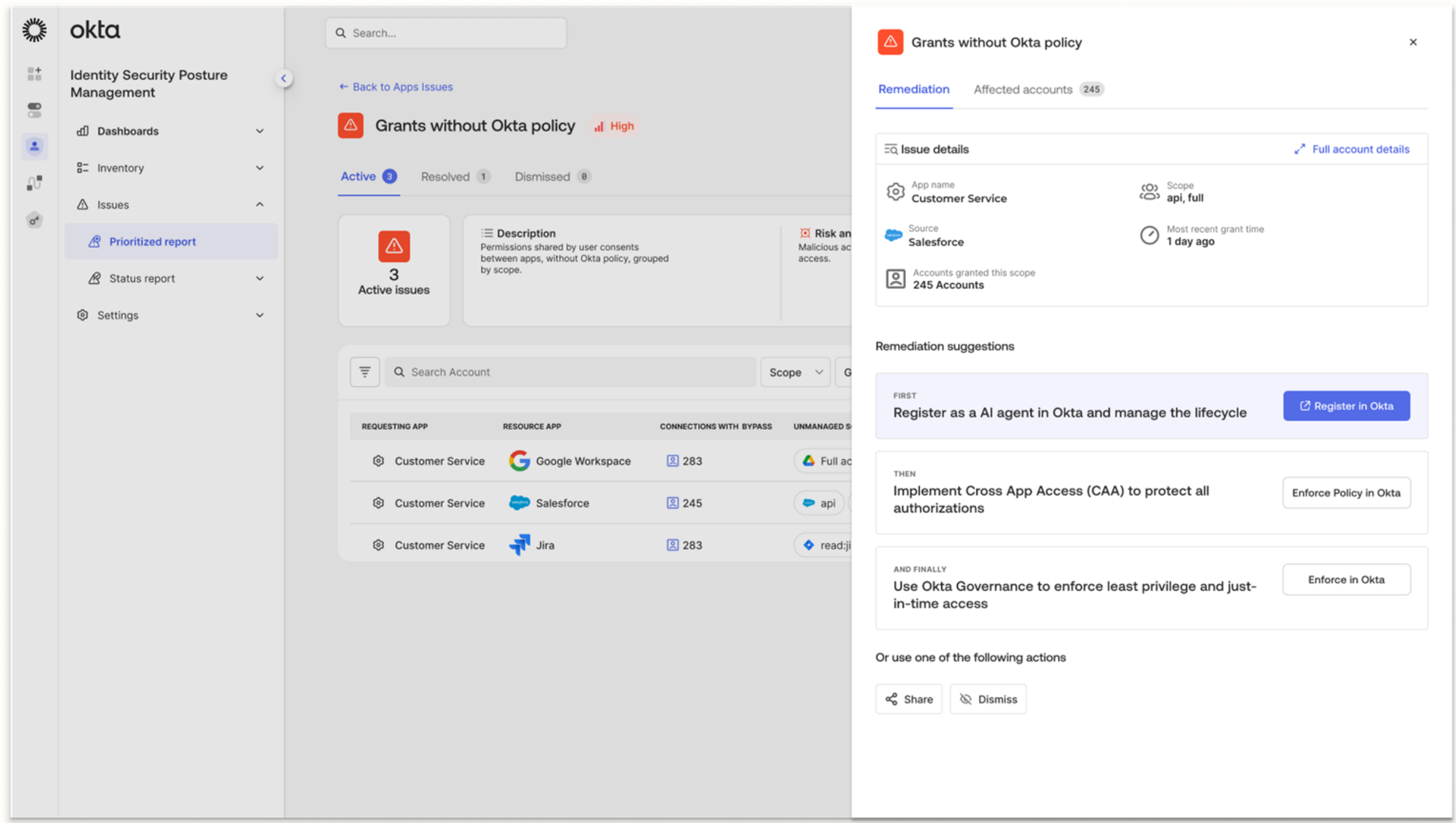
Risk level detail

Recommendation	Revoke
Overall risk level	High
Past governance decisions risk	Low
App assignment risk	High
Usage history risk	High
User profile change risk	Low

History

- 07/01/2025

  Otto Waller (o.waller@streamward.co) previously approved this item with the justification "still testing, but access should be removed when we're done".


okta
Identity Security Posture Management
Dashboards
Inventory
Issues
Prioritized report
Status report
Settings
Search...
Back to Apps Issues
Grants without Okta policy
High
Active 3
Resolved 1
Dismissed 0
3
Active issues
Description
Permissions shared by user consents between apps, without Okta policy, grouped by scope.
Risk an
Malicious ac
access.
Search Account
Scope
REQUESTING APP
RESOURCE APP
CONNECTIONS WITH BYPASS
UNMANAGED S
Customer Service
Google Workspace
283
Full ac
Customer Service
Salesforce
245
api
Customer Service
Jira
283
read:ji
Grants without Okta policy
Remediation
Affected accounts 245
Issue details
Full account details
App name
Customer Service
Scope
api, full
Source
Salesforce
Most recent grant time
1 day ago
Accounts granted this scope
245 Accounts
Remediation suggestions
FIRST
Register as a AI agent in Okta and manage the lifecycle
Register in Okta
THEN
Implement Cross App Access (CAA) to protect all authorizations
Enforce Policy in Okta
AND FINALLY
Use Okta Governance to enforce least privilege and just-in-time access
Enforce in Okta
Or use one of the following actions
Share
Dismiss

Appendix | Reference Slides

okta

Secure your agents today and tomorrow using a maturity model

01 Fundamental

Authorize and Protect AI Agents

Build a secure foundation by **creating policies** and **coverage** for AI agents

02 Advanced

Discover and Detect Risk

Strengthen your oversight by identifying critical artifacts and agent patterns, pinpointing existing errors and also providing clear remediation for risk

03 Scale

Provision and Register AI agent Access

Enhance your security posture by **defining both agent and human roles**. Import **static credentials** to fortify protection

04 Strategic

Govern and Monitor Agentic AI Behavior

Ensure **continuous security** and **compliance** by establishing regular access certificates and comprehensive reporting on agent-based action

Explore what’s next.

01

Start building with Auth0 for AI Agents

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 the Oktane 2025 Keynote: Okta Secures AI