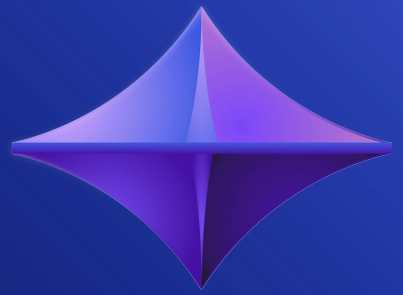
Okta secures AI



Michel Duong
Principal Solutions Architect EMEA,
Office of the Field CTO, Okta

okta

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.

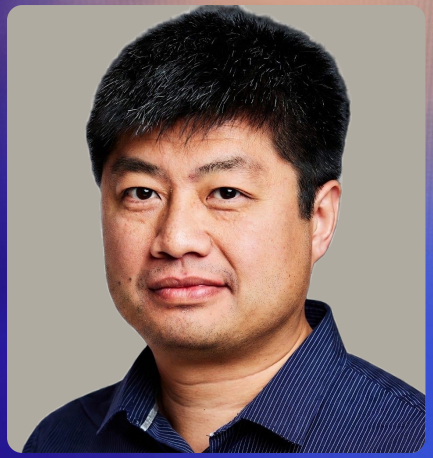
Privacy & Security Disclaimer

These materials and any recommendations within are not legal, privacy, security, compliance, or business advice. These materials are intended for general informational purposes only and may not reflect the most current security, privacy, and legal developments nor all relevant issues. You are responsible for obtaining legal, security, privacy, compliance, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein.

Okta is not liable to you for any loss or damages that may result from your implementation of any recommendations in these materials. Okta makes no representations, warranties, or other assurances regarding the content of these materials. Information regarding Okta's contractual assurances to its customers can be found at okta.com/agreements.

Use of Fictitious Information

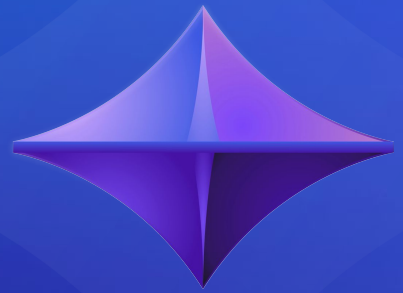
These materials may include companies, organizations, domain names, email addresses, account numbers, people, and events depicted which are fictitious. No association with any real company, organization, domain name, email address, account number, person, or event is intended or should be inferred from these fictitious companies.



Michel Duong

Principal Solutions Architect, EMEA
Office of the Field CTO, Okta


okta
The World's Identity Company

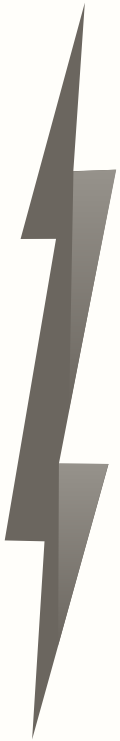


AI is the biggest platform shift since the internet

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*

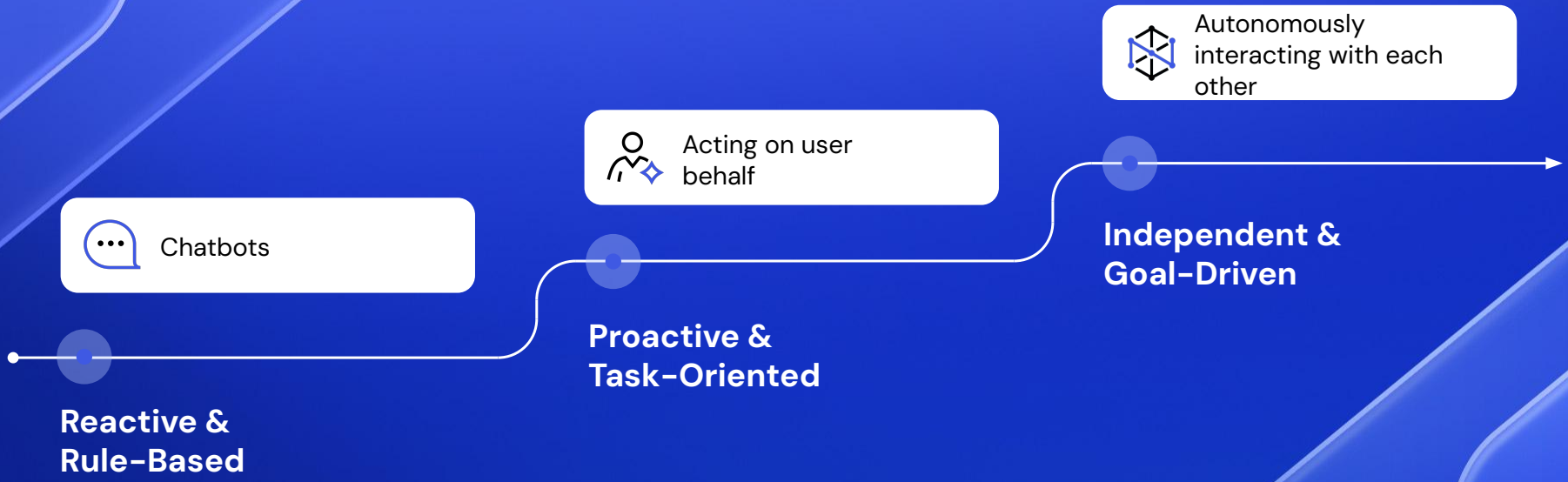
okta

Innovation

Security

Every organization struggles with this tension

AI agents are a powerful new identity type



AI agents are a powerful new identity type

LLMs are powerful. But unpredictable.

SAME PROMPT ×3

you "Should I approve this $5,000 vendor contract?"

RUN 1 · 9:00 AM

Approve

"Standard terms. Liability cap is reasonable at 2x contract value. Pricing is within market range. No red flags.

Recommend proceeding."

RUN 2 · 9:01 AM

Escalate

"The auto-renewal clause in Section 9 could lock you in for 3 years. Indemnity is uncapped. Needs legal review before signing.

Do not approve yet."

RUN 3 · 9:02 AM

Reject

"Critical: no data breach notification requirement. This violates GDPR and could expose the company to regulatory action.

Do not sign."

Three minutes. Three verdicts. Same contract.
Now imagine this happening 1,000 times a minute, across every department, with no human reviewing the output.

If you give an agent access to sensitive APIs '***just in case***,' it will ***eventually*** find a reason to use them.

Agentic task length is doubling every seven months

Source

LLM Release Date

Identities

Employees

Privileged users

Contractors

Partners

Customers

Agents

Downstream Agents

Infrastructure

Applications

Services

APIs

Resources

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.


AI security *is*
identity security

So what can we do?

How can Okta help?

Okta Secure Identity Commitment

Provide market leading secure identity products and services

Harden our corporate infrastructure

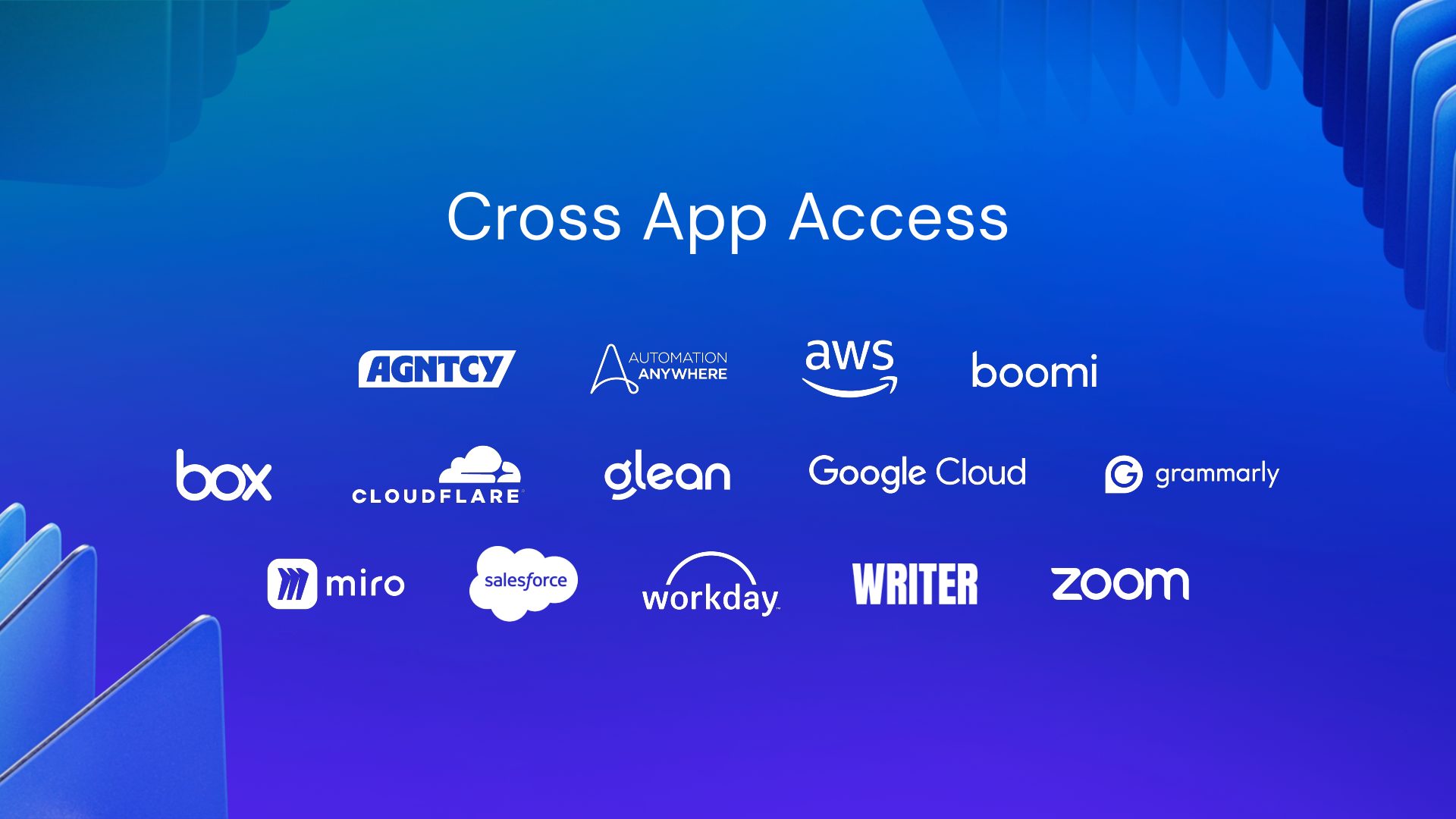
Champion customer best practices to help ensure they are best protected

Elevate our industry to be more protected from identity attacks

Okta continues to lead the industry

SAML | WS-Fed | OpenID Connect | IPSIE | Cross App Access

Cross App Access



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

Secure **every** agent by design

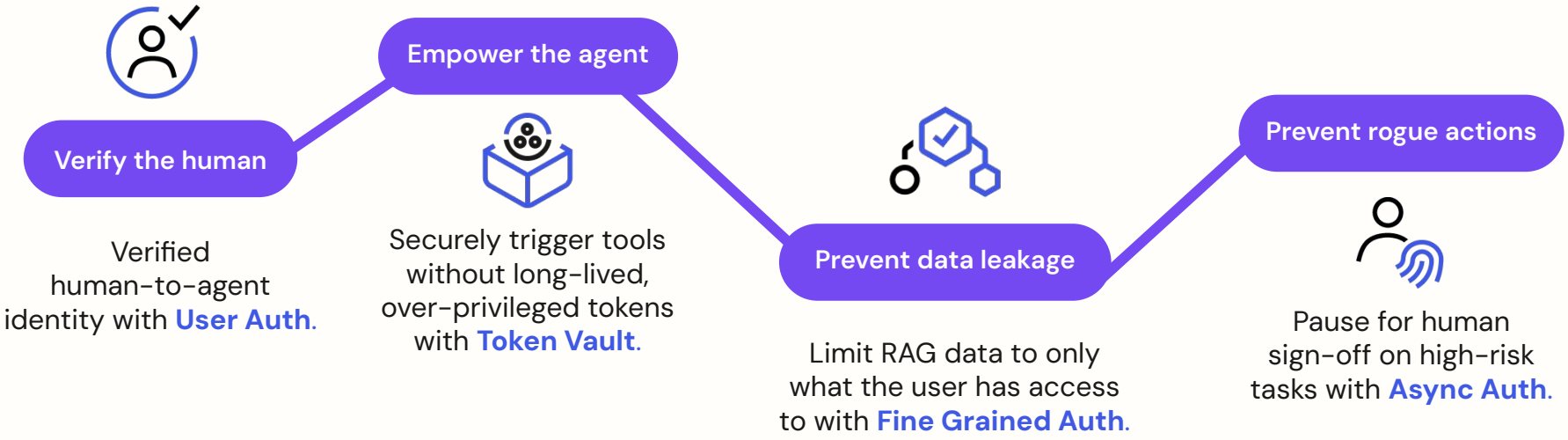
- Authentication
- Token Exchange
- Token Vaulting
- Data Security
- Tool Call Security
- Human in the Loop

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

- Agent registry
- Access control
- Governance
- Privileged credentials
- Agent detection
- Agent universal logout

Every agent secured from the first line of code

Save developer time and prevent security gaps with an identity-first agent journey.



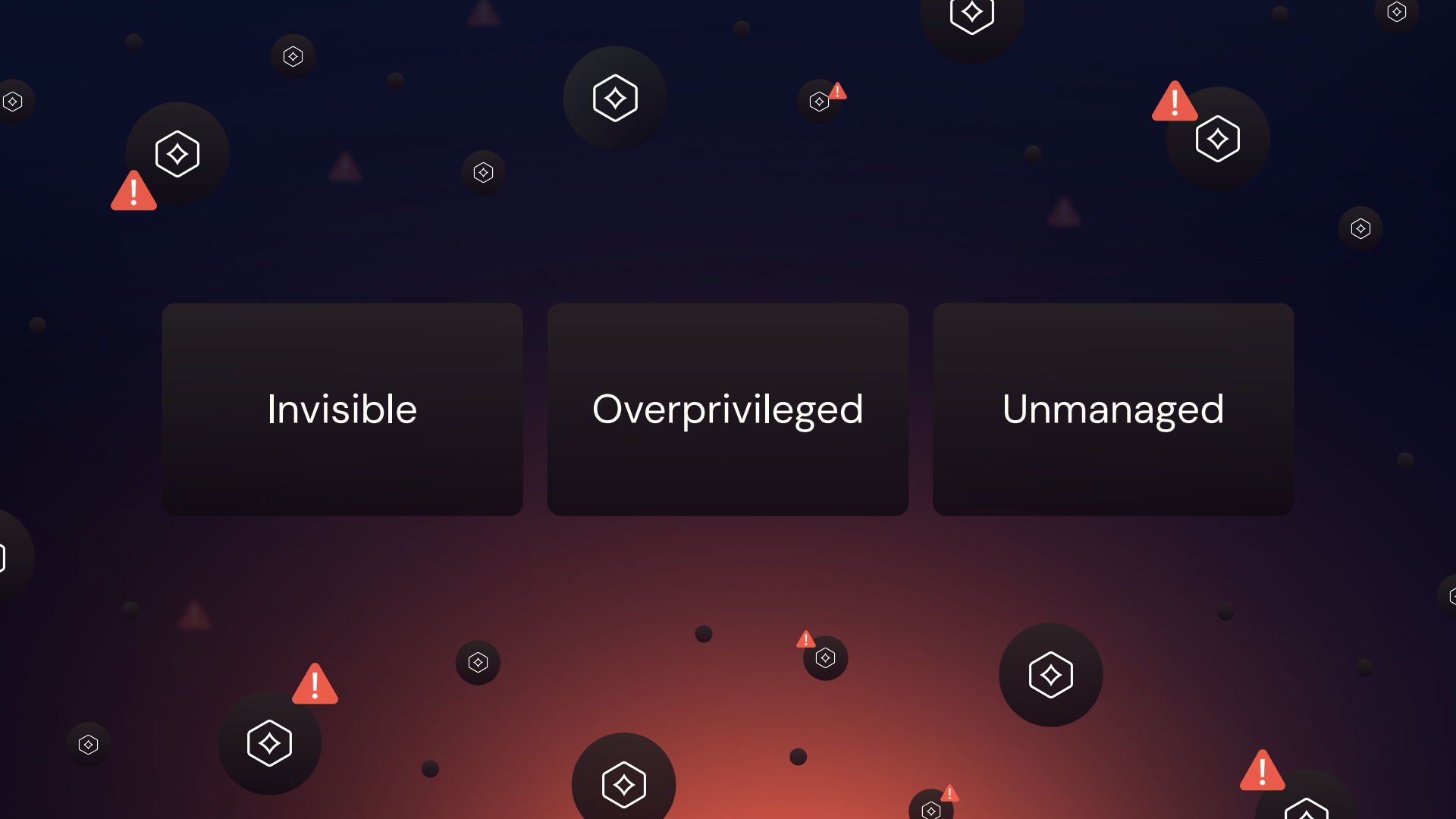
You need to secure **every** agent, and **all** agents

Secure **every** agent by design

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

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

- Agent registry
- Access control
- Governance
- Privileged credentials
- Agent detection
- Agent universal logout


Invisible
Overprivileged
Unmanaged

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?

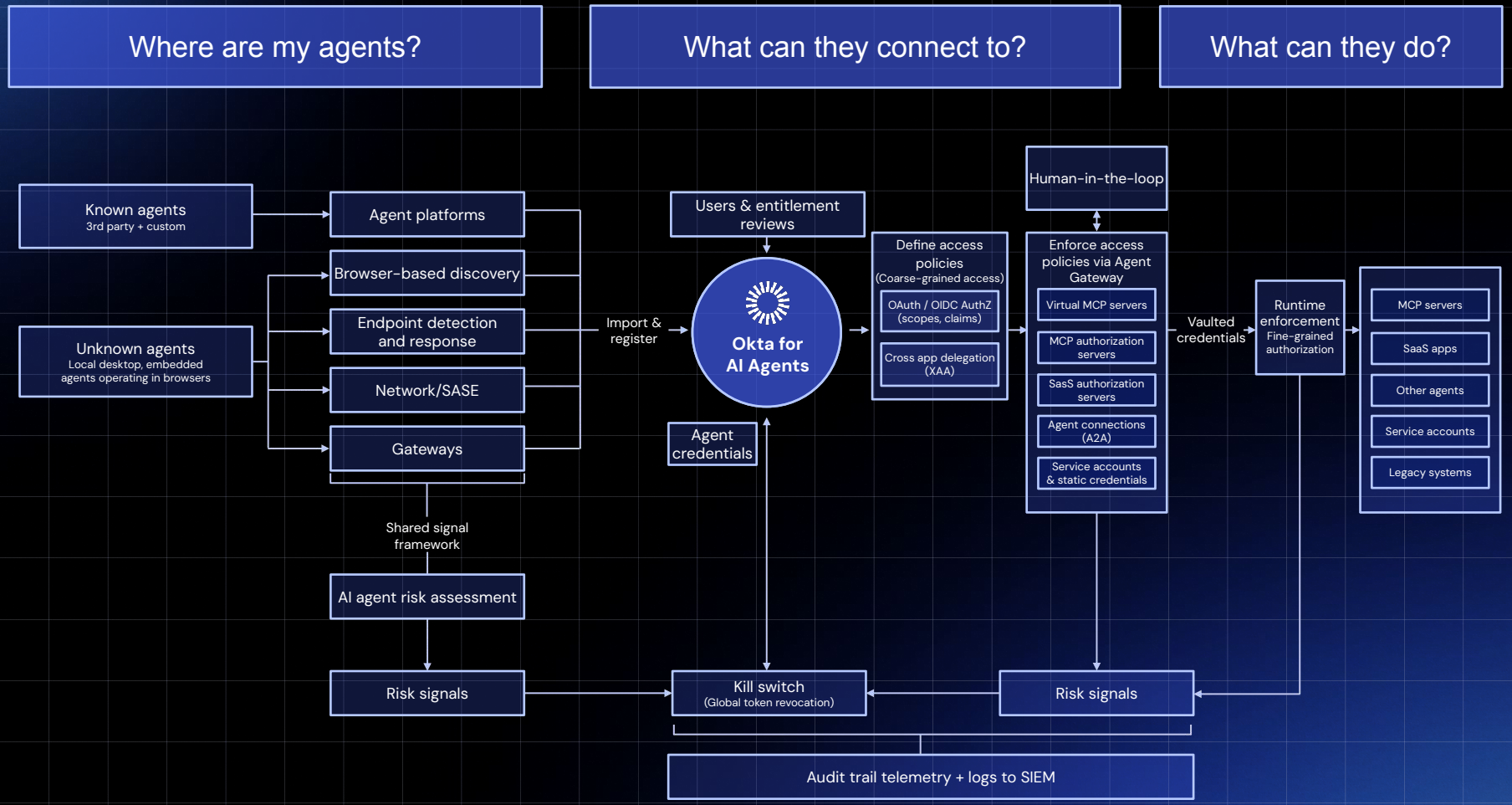
The blueprint for the secure agentic enterprise

CONCEPT
OKTA SECURES AI

DATE
2026

Where are my agents?	What can they connect to?	What can they do?
Agent integrations	MCP servers	Kill switch
Browser-based protection	SaaS services	Runtime enforcement
Endpoint detection	Agent-to-agent connections	Agent lifecycle management
Network detection	Service accounts	Human-in-the-loop
Gateway detection	Vaulted credentials	Audit logs and telemetry
AI agent risk detection		

OKTA 2026


Where are my agents?
What can they connect to?
What can they do?
Known agents
3rd party + custom
Unknown agents
Local desktop, embedded agents operating in browsers
Agent platforms
Browser-based discovery
Endpoint detection and response
Network/SASE
Gateways
Shared signal framework
AI agent risk assessment
Risk signals
Import & register
Users & entitlement reviews
Okta for AI Agents
Agent credentials
Define access policies
(Coarse-grained access)
OAuth / OIDC AuthZ (scopes, claims)
Cross app delegation (XAA)
Human-in-the-loop
Enforce access policies via Agent Gateway
Virtual MCP servers
MCP authorization servers
SasS authorization servers
Agent connections (A2A)
Service accounts & static credentials
Vaulted credentials
Runtime enforcement
Fine-grained authorization
MCP servers
SaaS apps
Other agents
Service accounts
Legacy systems
Kill switch
(Global token revocation)
Risk signals
Audit trail telemetry + logs to SIEM

Okta for AI Agents

Where are my agents?

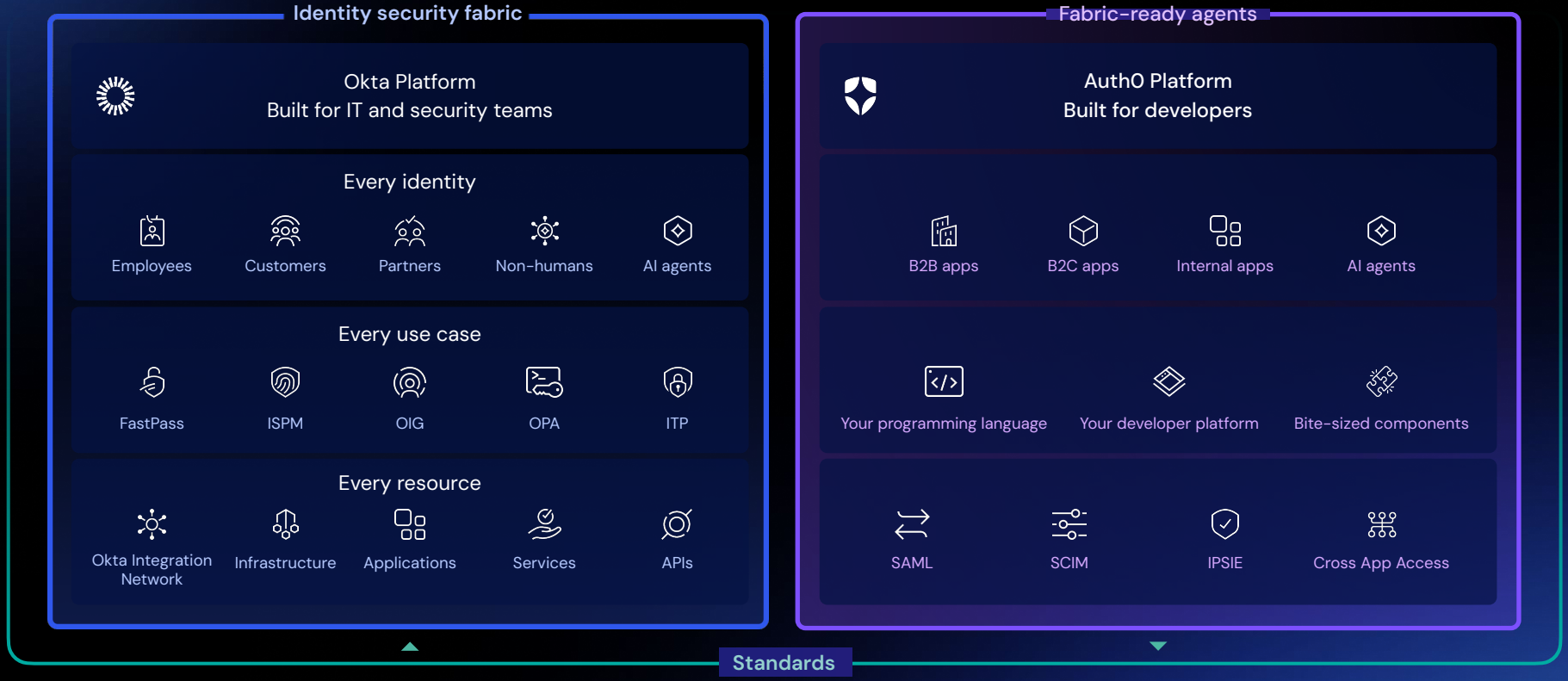
- **Agent integrations**
  Agent Integrations in Okta Integration Network
- **Browser-based protection**
  Shadow AI agent discovery
- Endpoint detection
- Network detection
- API gateway detection
- AI agent risk detection

What can they connect to?

- **MCP servers**
  Agent Gateway
- **SaaS services**
  Agent Gateway
- **Service accounts**
  Privileged Credential Management
- **Vaulted credentials**
  Secure Token Storage
- Agent-to-agent connections

What can they do?

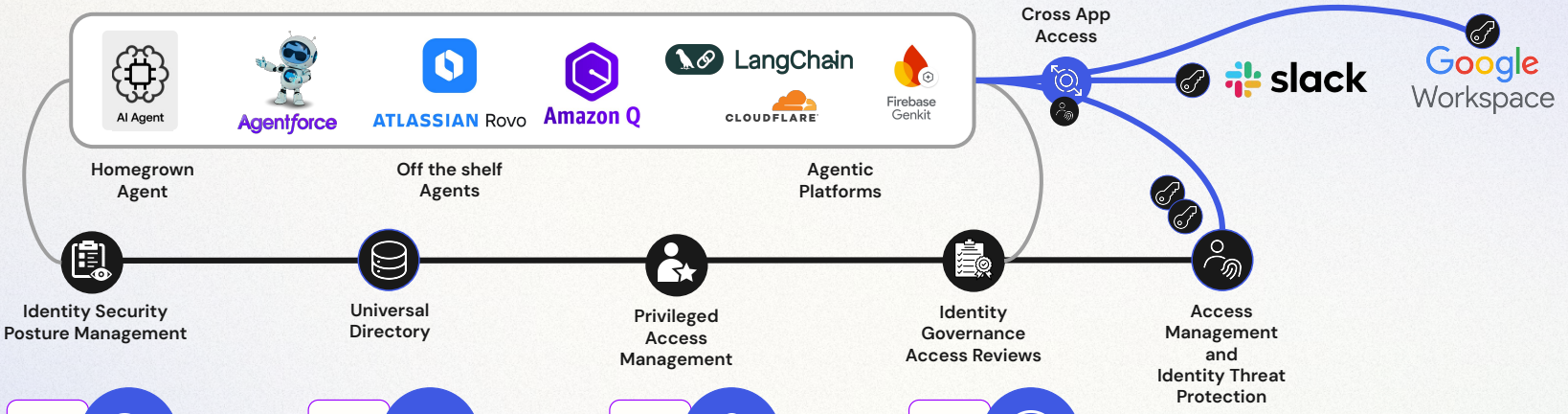
- **Kill switch**
  Universal Logout
- **Agent lifecycle management**
  Governance for agents as a resource
- **Audit logs and telemetry**
  System logs
- Runtime enforcement
  LLM Intent
- Human-in-the-loop



Thank you!

Identity Security Fabric

Agentic Pipeline: Secure by default



Detect & Discover

- Agent Discovery
- Risk Assessment
- Remediation Plans

Provision & Register

- Agent object creation
- Human Owner Assignment
- Credential Protection

Authorize & Protect

- Agent-Specific Policies
- Least Privileged Access

Govern & Monitor

- Access Certifications
- Activity Monitoring
- Continuous Threat Detection

oktane