Oktane 2026 Product Announcements

Blueprint Alliance

For AI agents to drive better outcomes, they need to reason, act, and connect across model providers, data platforms, SaaS applications, networks, and infrastructure. This interconnected agentic stack requires vendors to come together to close an identity gap where shadow agents multiply, credentials cross trust boundaries, and agents execute beyond their intended scope.

Founding Alliance members have aligned toward a shared set of principles for securing AI agents. Guided by these principles, the Alliance evolved and expanded the blueprint for the secure agentic enterprise, first introduced in March 2026, into an open, multi-vendor reference architecture. It provides organizations with a standardized way to address four core challenges: **Where are my agents? What can they do? What are they doing? How do I respond?**

Announcement	What's new	Why it matters
Blueprint Alliance *Availability:* September 22	An industry coalition advancing an open, multi-vendor reference architecture to help organizations secure AI agents and govern the agentic stack. Founding members aligned on a set of principles for how agents should operate, and co-authored the new blueprint reference architecture. • Industry Leaders Form the Blueprint Alliance to Advance a Shared Architecture for Securing AI Agents	This blueprint gives tech leaders a concrete way to scale agentic deployments securely, addressing four core challenges: Where are my agents? What can they do? What are they doing? How do I respond?

Highlights across the Okta Platform

Whether you're securing your workforce, customers, or AI agents, Okta's newest innovations close governance blind spots and extend zero standing privilege across every identity—human, non-human, and AI agent. New capabilities across Okta Identity Governance, Okta Privileged Access, and identity threat detection and response (via the Permiso Security acquisition) give CIOs, CISOs, and AI leaders automated compliance and real-time control across their organization - accelerating AI adoption without compromising security.

Product	What's new	Why it matters

Okta for AI Agents
 	
Availability:
• **Shadow AI Agent Discovery for Endpoints (CrowdStrike):** EA now, GA Q4 CY26
• **Shadow AI Agent Discovery for Endpoints (Okta Verify):** EA Q4 CY26, GA Q1 CY27
• **Agent-to-Agent Connections:** GA now
• **Agent Gateway:** GA Q3 CY26
	• **Shadow AI Agent Discovery for Endpoints (CrowdStrike):** Enable discovery of local AI agents and MCP servers through EDR integration (CrowdStrike Falcon Discover), providing fleet-wide visibility into locally running AI workloads
	  ◦ Your endpoints are running AI agents you can't see
	• **Shadow AI Agent Discovery for Endpoints (Okta Verify):** It extends the device trust you already use for human authentication to scan for AI agents on managed devices
	• **Agent-to-Agent Connections:** Govern which agents can communicate, under what authority, with a complete delegation record
	  ◦ Securing your multi-agent workflows with Agent-to-Agent Connections
	• **Agent Gateway:** Okta-secured gateway sitting between AI agents (e.g., Claude, Agentforce) and enterprise tools. It aggregates MCP servers, injects credentials, and brokers every tool call through Okta
	  ◦ Introducing Agent Gateway: Runtime AI agent governance
		• **Shadow AI Agent Discovery for Endpoints (CrowdStrike):** Closes shadow AI blind spots before they become breaches by surfacing unmanaged agents on employee devices before they turn into exposure
		• **Shadow AI Agent Discovery for Endpoints (Okta Verify):** Provides fleet-wide visibility into shadow AI workloads, eliminating blind spots where unauthorized or unvetted AI agents could pose security and compliance risks across your enterprise infrastructure
		• **Agent-to-Agent Connections:** Enables secure delegation between AI agents with complete authority tracking and audit trails, allowing complex multi-agent workflows while maintaining governance and accountability for every handoff
		• **Agent Gateway:** Moves from after-the-fact logs to real-time enforcement by sitting directly in the execution path between an agent and its tool calls, enforcing policy and logging every interaction live

Product	What's new	Why it matters
• **Configuration Designer:** GA Q4 CY26 • **Agent Gateway based Kill Switch:** GA Q4 CY26 • **Okta for AI Agents capabilities for Okta Customer Identity:** GA Q4 CY26	• **Configuration Designer:** Visually maps agent-to-resource connections so every handoff is governed, scoped, and auditable • **Agent Gateway based Kill Switch:** For agents connected through Agent Gateway, the moment you deactivate, the gateway rejects every request carrying a token that agent already holds. No waiting for tokens to expire. No relying on downstream providers to cooperate. • **Extended capabilities for OCI:** We're extending Okta for AI Agents capabilities to Okta Customer Identity, enabling organizations to securely govern customer-facing AI agents with distinct identities, policy-based access, end-to-end auditing, and rapid agent deactivation, without disrupting customer experience	• **Configuration Designer:** Translates complex agent permission requirements into visual, auditable governance policies, making it faster and safer to deploy new agents while ensuring every resource access is scoped, governed, and traceable • **Agent Gateway based Kill Switch:** Enables instant containment when something goes wrong by instantly revoking every active token held by a compromised agent the moment it's deactivated—no waiting for tokens to expire or relying on downstream providers to cooperate • **Extended capabilities for OCI:** Extends governance to customers so that customer-facing agents stay locked to user permissions, partners onboard securely with no static credentials, and rogue access can be cut off instantly
Agent SSO *Availability:* • GA now	Brings the Cross App Access (XAA) open protocol into Okta's identity platform. It enforces least-privilege access, enables deeper audit records, and provides an easy path to scale to Okta for AI Agents for full-lifecycle governance.	• **Eliminates non-expiring keys:** Swaps long-lived API keys for short-lived, identity-governed tokens, closing off a major standing-credential risk • **Available today, at no extra cost:** Included in core Okta SSO now, so customers can turn it on immediately rather than waiting on a separate rollout • **A stepping stone to full governance:** Provides an easy path to scale up into Okta for AI Agents for full-lifecycle governance
Okta Identity Governance *Availability:* All capabilities EA by Q4	• **Advanced Entitlement Management for AWS:** Gives admins a granular view into the exact permissions a user, workload, or agent has, turning vague 'AWS access' into specific, governable entitlements. That precision means faster, more accurate access certifications and SoD enforcement, so developers keep the access they need while security gets true least-privilege control. • **Intelligent Request Recommendations:** Offers AI-driven at the point of decision, so approvers will not rubber-stamping a request. The result: faster, more confident approvals for employees and stronger, more consistent least-privilege enforcement for security • **Identity Reconciliation (Rogue Account Detection, Rogue Entitlement Remediation):** This gives IT, app owners, and compliance teams visibility into accounts created and entitlement changes outside the governance process. Teams can review, and take action on rogue accounts, and configure automatic detection and revocation of entitlements at the app level • **On-demand integrations:.** Building on Okta's catalog of more than 8,000 pre-built integrations, Okta now leverages AI to deliver new integrations for governance, privileged access, and beyond in as little as 48 hours (down from a manual process that took two to three months), enabling teams to rapidly unify and govern access for people, machines, and AI agents in one place. ◦ Now available: On-demand SaaS integrations from Okta	• **Advanced Entitlement Management for AWS:** Transforms opaque cloud permissions into precise, auditable entitlements, enabling security teams to enforce true least-privilege access across developers, workloads, and AI agents while maintaining the access they need to operate effectively • **Intelligent Request Recommendations:** Shifts approvals from blind rubber-stamping to informed decision-making by surfacing AI-driven context at the moment of approval, accelerating access decisions while strengthening least-privilege enforcement across the organization • **Identity Reconciliation (Rogue Account Detection, Rogue Entitlement Remediation):** Closes the governance blind spot by catching unauthorized accounts and entitlement drift the moment they occur, enabling teams to automatically remediate policy violations before they become security incidents • **On-demand integrations:** Eliminates months-long delays in governance coverage by using AI to rapidly build custom integrations, allowing organizations to extend centralized access control across their entire ecosystem—people, machines, and AI agents—without waiting for manual connector development
Okta Privileged Access *Availability:* • **Secure Privileged Access to Databases:** GA Q3 CY26	• **Secure Privileged Access to Databases:** Enables centralized access controls, account vaulting, and automated credential rotation for major database engines, including PostgreSQL, My SQL Server, Oracle Database, Microsoft SQL Server, and Mongo DB • **Non-Human Identity access (workloads):** Native AWS support lets workloads and machines authenticate dynamically without static, hardcoded keys, and new access to Active Directory accounts, SaaS service accounts, and vaulted secrets covers the same high-value targets workloads actually interact with	• **Secure Privileged Access to Databases:** Eliminates credential sprawl and automatically vaults and rotates database secrets to protect sensitive data against breaches, centralizing policy enforcement across servers, SaaS accounts, and Active Directory • **Non-Human Identity access (workloads):** Closes the standing-privilege gap by swapping long-lived static keys for dynamic, short-lived credentials, ensuring every action is traced back to the accountable human even as automated identities and CI/CD pipelines operate at machine speed

Product	What's new	Why it matters
• **Non-Human Identity access (workloads):** GA Q3 CY26 • **Secure Privileged Access to Kubernetes:** EA Q1 CY27	• **Secure Privileged Access to Kubernetes:** SSO-based Just-In-Time access to secure human access to K8s clusters • **Secure Privileged Access to Network Devices:** Agentless SSH access to protect routers, switches, and firewalls without installing agents	• **Secure Privileged Access to Kubernetes:** Eliminates long-lived credentials by enabling teams running autoscaling apps to avoid hardcoding service account tokens or manually rotating secrets when pods spin up, allowing businesses to scale without standing privilege risks • **Secure Privileged Access to Network Devices:** Non-Human Identity access (workloads): Closes the standing-privilege gap by swapping long-lived static keys for dynamic, short-lived credentials, ensuring every action is traced back to the accountable human even as automated identities and CI/CD pipelines operate at machine speed
Identity Threat Detection and Response *Availability:* EA Q4 CY26. Regions included: USA and Canada.	**Advancing ITDR via Identity Threat Protection with Permiso Security:** Beyond governing and securing access, organizations also need to detect and respond to identity risk as it emerges. Following Okta's recent acquisition of Permiso Security, Okta is broadening and deepening its existing identity threat detection and response capabilities. Permiso brings identity risk signals, behavioral analytics, and threat-informed detections across multiple identity providers, cloud environments, and SaaS applications. Together, Okta and Permiso will help organizations discover, monitor, and respond to identity threats across human, non-human, and AI identities.	• **Unified threat visibility:** Okta and Permiso together help organizations discover, monitor, and respond to identity threats across human, non-human, and AI identities • **Stops rogue agents in real time:** Expands ITDR features to stop rogue AI agents and validate tool calls against original session intent

Highlights across the Auth0 Platform

Every new customer touchpoint creates an opportunity to increase revenue, but also introduces new risks or complexity. The key to breaking that trade-off is a comprehensive identity layer that connects people, apps, APIs, data, and agents. Auth0 helps companies grow revenue while reducing risks. For consumer facing companies, Auth0 reduces friction and enables personalization, ultimately driving conversion. For business facing companies, Auth0 provides enterprise-grade identity without costly migrations, helping them grow customer acquisition. Auth0 then provides simplified multi-tenancy and onboarding, helping companies.

As AI agents increasingly transact on behalf of consumers and do work on behalf of employees, businesses have an opportunity to grow and meet customer needs. At the same time, the AI agents introduce a new risk surface. By securing agentic commerce, and introducing new ways to securely add agents into B2B workflows, Auth0 helps businesses turn the agentic era into a growth opportunity without compromising security or risk.

Product	What's new	Why it matters
Auth0 AI innovation *Availability:* • **AI Identity for Commerce:** GA now • **Auth for UCP:** EA Q4 CY26, GA Q1 CY27 • **Auth0 Agent Gateway:** EA Q1 CY27 • **Universal Components for AI Agents:** EA Q4 CY26	**AI Identity for Commerce** is a set of AI identity capabilities that enables retailers, travel and hospitality organizations to safely unlock a massive new revenue channel: agentic commerce. • Auth0 helps brands deliver standardized, secure agentic shopping experiences through **their own AI shopping assistants** and **popular AI assistants** like Chat GPT, Gemini and Claude. • Auth0 enables agents to **safely connect and checkout** on customer behalf and use identity linking to **inject personalized offers and loyalty context** into agentic shopping interactions **Auth for UCP**: Let agents securely connect, shop and checkout on behalf of users using the Universal Commerce Protocol (UCP). UCP standardizes the commerce journey so agents can interact with merchants to discover products, build shopping carts, and complete checkout and payment flows on behalf of users.	**AAI Identity for Commerce:** • **Buy through agents, grow revenue:** Empowers brands across B2C industries like retail, travel, and hospitality to secure their systems and verify customers across vital new commerce channels • **Security without sacrificing experience:** Sensitive data never has to be exposed directly to an agent—it stays within a secure identity component, outside the language model—so consumers get a seamless conversational flow while businesses keep control **Auth for UCP:** • Unlocks a new revenue channel by enabling frictionless, secure transactions directly inside AI agents like Google Gemini—letting customers discover, personalize their experience, and complete purchases without ever visiting your website

Product	What's new	Why it matters
	Auth0 Agent Gateway: A centralized hub that can securely connects agents to downstream MCP servers. You integrate once, and Auth0 Agent Gateway can handle access policies, credential injection, audit logging, and manages the Organization boundaries automatically. **Universal Components for AI Agents:** A secure interface framework that lets AI agents safely display pre-built UI components inside any AI surface—protecting sensitive data while delivering personalized, identity-aware experiences and actions without custom code.	**Auth0 Agent Gateway:** • Eliminates months of custom integration work by centralizing agent-to-MCP connections in one place, so builders ship faster while security teams maintain complete control over access policies, credentials, and organization boundaries **Universal Components for AI Agents:** • Keeps sensitive data out of the hands of AI agents by rendering secure identity components directly in the chat, so customers get a seamless conversational flow while businesses maintain control and compliance without requiring custom code
Auth0 for B2C *Availability:* • **Auth0 Identity Conversion Suite:** EA Q3 CY26	**Auth0 Identity Conversion Suite** bundles together two advanced identity capabilities for conversion optimization: • **Anonymous Sessions:** Increase conversions by giving every anonymous user an identity from their first visit and recognizing their cart and preferences when they return • **Experiment Center:** Perform A/B testing within Auth0 and gradually rollout capabilities for authentication flows, enabling organizations to identify which signups and sign-ins result in the highest conversion	**Auth0 Identity Conversion Suite:** • **Captures intent before login:** Businesses can track and recognize potential customers before they ever sign up, maintaining shopping cart and preference context across sessions • **Removes friction from the funnel:** Testing different auth experiences in parallel — from sign-up methods to login flows — means less guesswork and more customers making it through the funnel • **Drives measurable growth:** Together, these tools help businesses drive revenue through reduced friction and better customer experiences
Auth0 for B2B *Availability:* • **B2B Connect**: in beta now, EA in Q3 CY26 • **Tenancy-as-a-Service:** GA now	**B2B Connect:** Businesses can now layer enterprise-ready identity capabilities directly onto existing identity infrastructure without forcing a full user, app, or token migration. In 60 days or less, businesses can deliver enterprise SSO, federation and multi-tenant capabilities effortlessly without putting existing customer experiences at risk **Tenancy-as-a-Service:** Build your identity model once and scale it across every customer, delivering tailored experiences for each while maintaining strict isolation between customer environments.	**B2B Connect:** • **Wins bigger deals, faster:** The result is becoming enterprise-ready and activating customers in record time — checking every box on the RFP (SSO, SCIM, multi-tenancy) that 96% of enterprise buyers require, without pausing innovation to do it Auth0 • **Shrinks a multi-year effort into days:** Instead of forcing a costly platform migration, B2B Connect lets you layer Auth0's enterprise capabilities directly onto your existing stack — eliminating migration headaches and shrinking a risky multi-year effort down to days **Tenancy-as-a-Service:** • **Scale without added engineering overhead:** Enables business facing organizations to add more customers and to focus on innovation while Auth0 handles multi-tenancy requirements. • **One model, built once, isolated per customer:** This removes underlying complexity by letting businesses build their identity model once and delivering tailored experiences for every customer while maintaining isolation between environments. • **Self-service reduces support burden:** Customers can handle their own ongoing org management without opening support tickets, all underpinned by a standardized, multi-tenant identity foundation built to scale to thousands of enterprise customers

All dates are calendar year unless otherwise indicated.

Any products, features, functionalities, certifications, authorizations, or attestations referenced on this page 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.