IDSYNC LANDSCAPE REPORT · FIRST EDITION

The State of AI Agent Identity 2026

28 vendors, 8 acquisitions in 8 months, and the standards stack that emerged underneath it all — the definitive map of how enterprises give AI agents an identity, as of August 8, 2026.

Download the PDF

Free · no signup · cite with a link

Executive summary

AI agent identity went from a conference-talk topic to a consolidation-stage market in roughly eighteen months. This report maps the vendor landscape, the standards stack, and the open problems as they stand in August 2026.

8 deals / 8 months

The market consolidated before it matured: between December 2025 and July 2026, eight acquisitions removed most of the category's largest pure-plays — Veza (ServiceNow, ~$1.2B), Oasis (Cyera, ~$1B pending), Astrix (Cisco, reported ~$400M), SGNL (CrowdStrike, ~$740M pending), StrongDM (Delinea), Natoma (Snowflake),

3 buyer classes

Platform-security vendors (Palo Alto, Cisco, CrowdStrike), identity incumbents (Okta, SailPoint, Delinea, Twilio), and data/workflow platforms (ServiceNow, Snowflake, IBM, Cyera) all bought agent identity within twelve months — it is being treated as a control point, not a feature.

Entro (SailPoint), Permiso (Okta, ~$200M pending).

3-layer stack

A standards consensus emerged: SPIFFE/WIMSE for workload identity (what is this agent), OAuth 2.1 via the MCP authorization spec for delegated access (what may it touch), and the IETF Identity Assertion Authorization Grant — Cross-App Access — for enterprise brokering (who governs the delegation). OpenID's AuthZEN slots in as the fine-grained decision layer.

MCP 2026-07-28

MCP's July 2026 revision — its largest since launch — deprecated Dynamic Client Registration in favor of Client ID Metadata Documents, made the protocol stateless, and tightened token binding. Agent-auth architectures designed against 2025 assumptions now have migration work.

5 shared primitives

Product vocabulary converged across every segment: an agent registry, a human sponsor bound to each agent, short-lived scoped credentials, MCP-layer enforcement, and runtime (not login-time) authorization. Differentiation is now depth and ecosystem, not concept.

~25% of seed deals

Money kept arriving even as exits accelerated: Oasis raised $120M weeks before agreeing to be acquired, WorkOS closed $100M at $2B, and new entrants Oak ($60M), NewCore ($66M), and Keycard ($38M) left stealth with outsized rounds. AI/agent security took roughly a quarter of cybersecurity seed funding in Q2 2026.

1. Why agent identity became its own category

Enterprises have managed non-human identities — service accounts, API keys, workload identities — for decades, mostly badly. Machine identities already outnumbered human ones by an order of magnitude before LLM agents arrived, and the OWASP Non-Human Identity Top 10 (2025 edition, still current as of this writing) reads as a catalog of the resulting failure modes: secret leakage, long-lived credentials, improper offboarding, over-privileged accounts.

AI agents inherit every one of those problems and add four that traditional NHI tooling was never designed for:

- **Delegation.** An agent acts on behalf of someone. A service account's permissions are its own; an agent's legitimate authority is a function of who invoked it, for what task, and for how long. Static role assignment can't express that.
- **Dynamism.** Agents are spawned, forked, and retired at machine speed — sometimes spawning sub-agents of their own. Identity systems built around quarterly access reviews and manual registration don't fit workloads that exist for ninety seconds.
- **Intent drift.** An agent with valid credentials can still do the wrong thing. The newest products in this space evaluate behavior against declared purpose, not just token validity.
- **Tool-calling as the attack surface.** MCP turned "connect an LLM to your systems" into a standard pattern — and made the MCP connection itself the natural enforcement point. Half the products launched in the past eighteen months are, structurally, MCP-aware policy gateways.

The result: agent identity crystallized as a distinct buying category somewhere between February and May 2025, when nearly every serious vendor shipped its first dedicated product within a twelve-week window — Stytch Connected Apps (Feb 20), Permit.io AI Access Control (Feb 25), Clerk's agent toolkit (Mar 7), Okta's Auth for GenAI preview (Apr 9), CyberArk Secure AI Agents (Apr 10), Descope's Agentic Identity Hub (Apr 22), and Microsoft Entra Agent ID (May 19).

2. The consolidation wave

The defining structural fact of 2026 is how fast the category's independents disappeared.

WHEN	DEAL	PRICE	WHERE IT LANDED
Feb 2025	IBM closes HashiCorp acquisition	$6.4B	Vault → IBM's agentic runtime stack
Jul 2025 → Feb 2026	Palo Alto Networks acquires CyberArk (closed Feb 2026)	~$25B	PANW's identity security pillar
Aug 2025	Okta acquires Axiom Security	~$100M reported	Okta privileged access

WHEN	DEAL	PRICE	WHERE IT LANDED
Nov 2025	Twilio closes Stytch acquisition	$104.1M (10-K)	Twilio's identity layer for agents
Dec 2025 → Mar 2026	ServiceNow acquires Veza (closed Mar 2026)	~$1.2B (10-Q)	ServiceNow security portfolio
Jan 2026	CrowdStrike announces SGNL acquisition	~$740M	Falcon identity (close pending)
Jan → Mar 2026	Delinea acquires StrongDM (closed Mar 2026)	undisclosed	PAM + continuous authorization
~May 2026	Cisco announces Astrix acquisition	~$400M reported	Cisco Identity Intelligence / Duo
May 2026	Snowflake acquires Natoma	undisclosed	Cortex AI Gateway
Jun 2026	SailPoint closes Entro acquisition	undisclosed	SailPoint's NHI/secrets layer
Jul 2026	Cyera announces Oasis acquisition (close pending)	~$1B	Data security + agentic access
Jul 2026	Okta announces Permiso acquisition (close pending)	just under $200M	ITDR across human/NHI/agent

Three observations for buyers:

The acquirers came from three different directions. Platform-security consolidators (Palo Alto, Cisco, CrowdStrike) bought agent identity as a missing pillar. Identity incumbents (Okta, SailPoint, Delinea, Twilio, Ping via Keyless) bought speed. And — the most 2026 development — data and workflow platforms (ServiceNow, Snowflake, IBM, Cyera) bought it because agents touch their crown jewels and they'd rather own the control point than integrate someone else's. When Snowflake ships its own AI gateway with an identity-partner program, the platform layer is asserting that agent access control belongs to it.

Roadmap risk is now a real evaluation criterion. Four of the acquired products — Astrix's Agent Control Plane, Oasis AAM, Veza's AI Agent Security, StrongDM ID — were the category's most-cited independents a year ago. None disappeared, but all now serve an acquirer's platform strategy first. Buyers shortlisting in this category should weight the acquirer's integration record as heavily as the product; the Cloud Security Alliance published a research note on exactly this concentration risk after the Cisco–Astrix deal.

Independence is now a differentiator the remaining pure-plays actively sell. Aembit, Token Security, P0, Clutch, Corsha, Defakto, Keycard, and the newest entrants pitch neutrality — one identity layer across every cloud and platform — against suite lock-in. History (CASB, CSPM, ITDR) suggests a handful will stay independent long enough to matter; most will exit into platforms within two to three years.

3. The market map

We group the landscape into four segments by center of gravity. Many vendors straddle lines; we've placed each where its buyers actually meet it. Vendors with an IDSync directory profile are linked.

Segment A — Pure-play NHI and agent-identity platforms

The startups that made non-human identity a category, now extending discovery and governance roots into agent control planes.

Aembit — INDEPENDENT · $25M SERIES A (2024)

Workload IAM with a no-stored-secrets model. Its agentic push (October 2025) introduced Blended Identity — binding an agent's identity to its sponsoring human — and an MCP Identity Gateway for runtime policy enforcement. Named a Snowflake Cortex AI Gateway identity partner in July 2026, and the most standards-forward of the pure-plays (SPIFFE-aligned, active in WIMSE conversations).

Token Security — INDEPENDENT · $20M SERIES A (2025)

Machine-identity security whose March 2026 Intent-Based AI Agent Security is the clearest expression of the category's next idea: model what an agent is supposed to do, auto-generate

least-privilege policy from that intent, and flag out-of-intent behavior at runtime. RSAC 2026 Innovation Sandbox finalist.

P0 Security

INDEPENDENT · $15M SERIES A (2024)

Unified cloud IGA/PAM extended in June 2026 with Agentic Runtime Access Control: each agent action is evaluated against the invoking human's identity, the agent's own identity, tool authorization, and resource entitlements, with automatic revocation.

Clutch Security

INDEPENDENT · $20M SERIES A (2025)

NHI discovery and governance platform with an Agentic AI Governance module covering both sanctioned and shadow agents. Partnered with Simeio (August 2026) to push NHI and agent governance into managed-services channels.

Corsha

INDEPENDENT · $18M SERIES A-1 (2025)

The machine-identity provider (mIDP) for the industrial edge: machine-to-machine and agent identity for OT/ICS, defense, and robotics — a reminder that agent identity isn't only a SaaS problem. Booz Allen Ventures invested mid-2025.

Defakto (ex-SPIRL)

INDEPENDENT · $30.75M SERIES B (OCT 2025)

Founded by SPIFFE/SPIRE co-creators; rebranded from SPIRL in October 2025. Attestation-based, credential-less workload identity extended to AI agents — the closest thing to SPIFFE, productized for the agent era.

Keycard

INDEPENDENT · $38M SEED + SERIES A (OUT OF STEALTH OCT 2025)

Dynamic, identity-bound, task-scoped tokens designed to replace static API keys for agents. a16z, boldstart, and Acrew backing plus ex-Snyk/Okta founders made this the most-watched new entrant of late 2025.

Oak and NewCore

NEW ENTRANTS (2026)

Oak left stealth in July 2026 with a $60M seed to build an AI-native identity operating system spanning humans, machines, and agents; NewCore emerged in June 2026 with a $66M seed at a

reported $300M valuation. Seed rounds this size, this late in a consolidation wave, are the market's bet that the incumbents' agent stacks won't be enough.

Acquired and absorbing — Astrix (→ Cisco), Oasis (→ Cyera, pending), Entro (→ SailPoint), Natoma (→ Snowflake): see the consolidation ledger above. Each remains the agent/NHI capability inside its acquirer.

Segment B — Access infrastructure, secrets, and authorization

Vendors whose products govern access paths and policy decisions, now treating agents as first-class principals.

Teleport

INDEPENDENT · $110M SERIES C (2022)

Infrastructure access platform whose Agentic Identity Framework (January 2026) makes agents first-class identities alongside humans and workloads, built on SPIFFE and MCP. Its 2025 Secure MCP release put per-session, per-tool controls on MCP traffic; risk scoring and session summaries are in tech preview for fall 2026.

Akeyless

INDEPENDENT · ~$84M RAISED

Vaultless secrets management that moved earliest on secretless agent auth (SecretlessAI, July 2025) and added intent-aware runtime control (Agentic Runtime Authority, March 2026). Competes increasingly with both Vault and the pure-plays.

Permit.io

INDEPENDENT · ~$14M RAISED

Authorization-as-a-service (policy-based and fine-grained access control on OPA and Cedar). Its Four-Perimeter framework (February 2025) was an early, widely referenced blueprint for agent access control — prompt filtering, RAG protection, external access, response enforcement — plus human-in-the-loop approvals over MCP.

Cerbos

INDEPENDENT · ~$11M RAISED

Open-source policy decision point with MCP authorization in Cerbos Hub: per-agent, per-tool, per-session policy evaluation with audit logs. With AuthZEN standardizing the PDP/PEP interface, the open-source PDPs are positioned to become the neutral decision layer under agent stacks.

HashiCorp Vault

IBM (ACQUIRED FEB 2025, $6.4B)

The incumbent secrets platform announced native AI agent support in May 2026: an agent registry, ceiling policies, and ephemeral per-request authorization in JWTs, with public beta slated for summer 2026. Vault 2.0 under IBM added workload identity federation. The de facto starting point for any enterprise already running Vault.

Veza, StrongDM, SGNL

ACQUIRED (SERVICENOW · DELINEA · CROWDSTRIKE PENDING)

Veza's Access Graph and AI Agent Security (December 2025) now anchor ServiceNow's security portfolio. StrongDM's continuous Cedar-based authorization and StrongDM ID — verifiable agent identities, each linked to a human sponsor — sit inside Delinea. SGNL's zero-standing-privilege engine is headed into CrowdStrike Falcon.

Segment C — Developer auth and CIAM with agent capabilities

The auth-for-builders vendors racing to own how agent-facing apps authenticate agents — and how agents authenticate to everything else.

Auth0 / Okta

PUBLIC (NASDAQ: OKTA)

The most complete suite: Auth0 for AI Agents went GA in October 2025 (Token Vault for federated API tokens, async human confirmation via CIBA, fine-grained authorization for RAG), and Okta is the corporate engine behind Cross-App Access — the productization of the IETF ID-JAG draft — with an ecosystem push (AWS, Google Cloud, Salesforce, Box, Glean) announced June 2026. The Axiom (2025) and Permiso (2026, pending) acquisitions extend the story into privileged access and agent-aware threat detection.

WorkOS

INDEPENDENT · $100M SERIES C AT $2B (MAR 2026)

AuthKit as a turnkey OAuth 2.1 authorization server for MCP servers, with early support for Client ID Metadata Documents and fine-grained authorization from its Warrant acquisition. Raised explicitly to make agentic software secure by default.

Descope

INDEPENDENT · $88M TOTAL SEED

The most complete dedicated agent-identity product line among dev-auth vendors: Agentic Identity Hub (April 2025), 2.0 (January 2026 — agent identity profiles, credential vault, agent audit logs), and 2.5 (June 2026 — headless-agent management, step-up auth for agent actions).

Stytch

TWILIO (CLOSED NOV 2025, $104.1M PER 10-K)

Connected Apps (February 2025) lets any application act as an OAuth/OIDC identity provider for agents — the make-your-app-agent-ready pattern — now inside Twilio's identity layer.

Clerk

INDEPENDENT · $50M SERIES C (OCT 2025)

Component-first CIAM adding an agent toolkit, OAuth dynamic client registration and consent, MCP server support across Next.js and Express, and machine-to-machine auth. The Series C — co-led by Menlo Ventures and Anthropic's Anthology Fund — declared Agent Identity the strategic bet.

Segment D — Enterprise IAM, PAM, and platform incumbents

The platforms most enterprises already run, each now shipping agents as a native identity class.

Microsoft — Entra Agent ID

GA SPRING 2026

The gravitational center of enterprise agent identity: agents as a native directory object class, with identity blueprints, an owner/sponsor model, Conditional Access and identity-protection policies for agents, lifecycle governance through access packages, and federation for non-Microsoft agents (AWS Bedrock, Google Cloud, n8n). Delivered as the identity foundation of Microsoft Agent 365. For any Microsoft-standardized enterprise, this is the default the rest of the market must integrate with or displace.

Ping Identity

PRIVATE (THOMA BRAVO)

Identity for AI (GA March 2026): Agent IAM Core, Agent Gateway, and Agent Detection, extended in May 2026 with programmable identity via MCP/CLI/API and privileged access for desktop agents. Acquired Keyless (zero-knowledge biometrics, closed January 2026) for human-verification depth.

CyberArk

PALO ALTO NETWORKS (CLOSED FEB 2026, ~$25B)

Secure AI Agents went GA in December 2025 — privilege controls purpose-built for agents, atop the Venafi machine-identity portfolio. Now the identity pillar of the largest security platform, which changes the competitive math for every standalone vendor in this report.

SailPoint

PUBLIC (NASDAQ: SAIL)

Agent Identity Security (September 2025) treats AI agents as a third identity class alongside employees and machines: discovery, governance, certification, plus an MCP server and connectors for the major agent platforms (M365 Copilot, Bedrock, Vertex, Agentforce, ServiceNow, Databricks). The Entro acquisition (June 2026) supplies the NHI/secrets substrate.

1Password

INDEPENDENT

Came at agents from credential security: agentic autofill with Browserbase (October 2025), then 1Password Unified Access (GA March 2026) with launch partners including Anthropic, Cursor, GitHub, and Perplexity, adding privileged-access controls for agents and AI spend management by July 2026. The developer- and SMB-friendly on-ramp to agent credential hygiene.

4. Comparison matrix

Status and flagship agent capability per vendor, August 2026. "Sponsor binding" means the product formally links each agent to an accountable human owner. "Partial" means agent/MCP support exists but MCP-layer policy enforcement isn't the product's center. Dashes mean we found no formal capability as of the research date — corrections welcome via contact.

VENDOR	SEGMENT	AGENT-SPECIFIC PRODUCT (LAUNCH)	STATUS	S
Aembit	NHI/workload IAM	IAM for Agentic AI (Oct 2025)	Independent	Y I
Token Security	NHI security	Intent-Based AI Agent Security (Mar 2026)	Independent	Y
P0 Security	Cloud IGA/PAM	Agentic Runtime Access Control (Jun 2026)	Independent	Y I

VENDOR	SEGMENT	AGENT-SPECIFIC PRODUCT (LAUNCH)	STATUS	S
Clutch Security	NHI governance	Agentic AI Governance module	Independent	Y
Corsha	Machine IdP (OT/M2M)	mIDP for agentic AI (2025)	Independent	-
Defakto (ex-SPIRL)	Workload identity	SPIFFE-based agent identity (2025)	Independent	-
Keycard	Agent tokens	Task-scoped agent tokens (Oct 2025)	Independent	Y
Astrix Security	Agent control plane	Agent Control Plane (Sep 2025)	Cisco (2026)	Y
Oasis Security	Agentic access mgmt	Oasis AAM (Nov 2025)	Cyera (pending)	Y
Entro Security	NHI/secrets	Agentic AI & NHI platform	SailPoint (2026)	-
Natoma	MCP gateway	Enterprise MCP platform	Snowflake (2026)	-
Teleport	Infra access	Agentic Identity Framework (Jan 2026)	Independent	Y
StrongDM	Zero-trust PAM	StrongDM ID (Feb 2026)	Delinea (2026)	Y
Akeyless	Secrets/machine ID	SecretlessAI (Jul 2025) + Runtime Authority (Mar 2026)	Independent	-
Veza	AuthZ intelligence	AI Agent Security (Dec 2025)	ServiceNow (2026)	Y
Permit.io	Authorization	AI Access Control (Feb 2025)	Independent	I
Cerbos	Authorization (OSS)	MCP authorization in Hub (2025)	Independent	-

VENDOR	SEGMENT	AGENT-SPECIFIC PRODUCT (LAUNCH)	STATUS	S
HashiCorp Vault	Secrets	Native agent support (May 2026, beta)	IBM (2025)	-
Auth0 / Okta	CIAM/IAM	Auth0 for AI Agents (GA Oct 2025); XAA	Public	A
WorkOS	Dev auth	AuthKit for MCP (2025)	Independent	-
Descope	CIAM	Agentic Identity Hub 2.5 (Jun 2026)	Independent	Y
Stytch	Dev CIAM	Connected Apps (Feb 2025)	Twilio (2025)	-
Clerk	Dev CIAM	Agent toolkit + MCP support (2025)	Independent	-
Microsoft	Enterprise IAM	Entra Agent ID (GA 2026)	Public	Y
Ping Identity	Enterprise IAM	Identity for AI (GA Mar 2026)	Thoma Bravo	Y
CyberArk	PAM	Secure AI Agents (GA Dec 2025)	Palo Alto (2026)	Y
SailPoint	IGA	Agent Identity Security (Sep 2025)	Public	Y
1Password	Credential security	Unified Access (GA Mar 2026)	Independent	Y

5. The standards layer

The protocol work matured faster than most 2025 predictions allowed. What's emerged is a three-layer stack, with real running code at every layer.

Layer 1 — Workload identity: what is this agent?

SPIFFE/SPIRE (CNCF-graduated) is the consensus answer for cryptographic workload identity — short-lived, attestation-based credentials instead of static secrets — and 2026's reference architectures from HashiCorp, Stacklok, Teleport, and Defakto all place it under agent deployments. Its known friction point for agents: SPIRE's pre-registration model fits long-lived services better than dynamically spawned sub-agents.

IETF WIMSE (Workload Identity in Multi-System Environments) is where the plumbing is being standardized: the architecture draft (March 2026), workload credentials, and proof-of-possession tokens are active working-group documents, and agent-specific drafts have started arriving. Notably, there is still no dedicated IETF working group for AI agents — agent identity work is distributed across WIMSE and the OAuth WG.

Layer 2 — Delegated access: what may it touch?

The MCP authorization spec is the most consequential standard in this report because it ships in every serious agent platform. It is OAuth 2.1 with MCP servers as resource servers, mandatory separation from the authorization server, and RFC 8707 resource indicators binding tokens to specific servers. Two revisions matter for anyone building now: the **2025-11-25** release added OIDC discovery, incremental scope consent, and Client ID Metadata Documents (CIMD) as the recommended client-registration mechanism; and **2026-07-28** — the largest protocol revision since launch — formally deprecated Dynamic Client Registration in favor of CIMD, required issuer validation, bound client credentials to the issuing authorization server, and made the protocol stateless.

If your agent-auth architecture was designed against the mid-2025 spec, the DCR-to-CIMD migration is now on your roadmap. Anthropic's Claude connectors already support CIMD alongside legacy dynamic registration — a preview of where every MCP host is heading. MCP itself now lives under the Linux Foundation's Agentic AI Foundation (donated December 2025), with adoption across Anthropic, OpenAI, Google DeepMind, and Microsoft.

Layer 3 — Enterprise brokering: who governs the delegation?

The Identity Assertion Authorization Grant (ID-JAG) — productized as **Cross-App Access (XAA)** — is the enterprise answer to per-app OAuth consent sprawl: the corporate IdP exchanges an identity assertion for a scoped token to a downstream API, so agent access is brokered (and revocable) centrally. It reached draft -04 as an adopted OAuth WG

document in May 2026, authored by Okta's Aaron Parecki with Ping's Brian Campbell; Okta runs an ecosystem program around it and Keycloak documents an implementation. This is the draft to watch for anyone selling into IT-governed agent deployments.

AuthZEN (OpenID Foundation) standardizes the PDP/PEP interface — the request/response shape for "may this agent do this?" — and its 2026 drafts are explicitly framed for the agent era, with interop demonstrated at Identiverse 2026. It's how the authorization vendors avoid becoming N incompatible policy silos.

The rest of the map

- **A2A (Agent2Agent).** Agent-to-agent task exchange, under the Linux Foundation since June 2025 with a steering committee spanning AWS, Cisco, Google, IBM, Microsoft, Salesforce, SAP, and ServiceNow. v1.0 added JWS-signed Agent Cards — cryptographically verifiable agent capability advertisements. The Linux Foundation reported 150+ participating organizations and enterprise production use at the protocol's first anniversary (April 2026).
- **OWASP NHI Top 10.** Still the 2025 edition; the canonical risk vocabulary for this space.
- **Decentralized identity (DIDs) for agents.** Institutionally forming — W3C published DID 1.1, and an Agent Identity Registry Protocol Community Group was proposed in April 2026, explicitly coordinating with WIMSE — but thin in enterprise production against the OAuth/SPIFFE stack. Treat big adoption claims skeptically.
- **Agentic commerce.** Visa Intelligent Commerce and Mastercard Agent Pay both tokenize the agent as a payment principal — agent-held network tokens scoped by consumer-set mandates — with Google's AP2 as the emerging interop layer. Payments is building its own agent-identity registry ahead of the general-purpose standards; a fragmentation risk worth watching.
- **Government.** NIST moved fast by NIST standards: a January 2026 RFI on securing AI agent systems, then a full AI Agent Standards Initiative (February 2026) spanning industry standards leadership, open protocol co-investment with NSF, and agent security/identity research. No binding requirements yet — but the direction of travel is set.

6. What's still unsolved

1. Delegation chains

User → agent is handled (on-behalf-of patterns, Cross-App Access, Entra's sponsor model). User → agent → sub-agent → tool is not: semantics for attenuating authority down a chain of dynamically spawned agents are split across at least six competing individual IETF drafts, with no working-group-adopted answer. This is the biggest gap between what agents actually do and what the standards cover.

2. Registry fragmentation

Microsoft has an agent directory, Snowflake has one, the payment networks are building theirs, A2A signs Agent Cards, and W3C is incubating a DID-based registry protocol. Nothing federates them. “Which agents exist, and who vouches for them?” currently has a per-platform answer.

3. Intent verification at runtime

The 2026 product wave (Token Security, Akeyless, P0, Ping's Agent Detection) converges on evaluating agent behavior against declared purpose — but there is no shared standard for expressing intent, so every vendor's policy model is proprietary.

4. Offboarding at machine speed

OWASP's NHI1 (improper offboarding) gets worse when identities are created by the thousand per day. Lifecycle features exist — Entra's cascade deletion, SailPoint certification — but cross-platform revocation, killing an agent's access everywhere when its sponsor leaves, remains integration work rather than a protocol.

5. The human accountability boundary

Sponsor binding is now table stakes in products, but liability frameworks haven't caught up: when a sponsored agent misacts across three SaaS platforms via brokered tokens, audit trails exist and accountability standards don't. Expect the NIST workstream and sector regulators to land here first.

7. Twelve-month outlook

Where we'd put probability mass between now and August 2027:

1. At least two more of the remaining pure-plays get acquired. The acquirer classes that haven't yet bought (Google and AWS at platform level; Zscaler and Fortinet in security) all have gaps. Aembit, Token Security, Descope, and Keycard are the names we'd watch.
2. Client ID Metadata Documents become the default client-registration story for agents, and “supports MCP 2026-07-28” becomes an enterprise RFP checkbox the way “supports SAML” once was.
3. ID-JAG / Cross-App Access reaches RFC or near-RFC status, and enterprise IdPs beyond Okta (Entra, Ping) ship first-class support — making IdP-brokered agent access the assumed enterprise pattern.
4. A delegation-chain draft gets working-group adoption. The sub-agent problem is too central to stay unstandardized; expect the OAuth WG or WIMSE to adopt a consolidation of the current drafts.
5. The first public agent-identity incident report. Given the OWASP NHI breach pattern and the volume of newly minted agent credentials, a named breach with an agent credential as the initial access vector is more likely than not within the window — and it will do more for this market's budgets than any analyst report.
6. Agent-identity pricing consolidates into per-agent tiers. Platform bundling (“identity included”) will collide with the pure-plays' per-agent models; expect painful metering debates.

Methodology and sourcing

This report was compiled by IDSync in August 2026 from primary sources: vendor announcements and documentation, press releases, SEC filings (10-K/10-Q/8-K for acquisition terms), IETF datatracker records, official specification changelogs (MCP, A2A, SPIFFE), standards-body publications (OWASP, OpenID Foundation, W3C, NIST), and funding disclosures. Where only secondary reporting exists — for example, unconfirmed deal values — figures are marked "reported." Facts we could not verify against a primary source were excluded. Corrections: contact us — we fix and re-date.

IDSync is an independent, vendor-neutral buyer-research platform for identity, access, and authentication software, operated by TetraCore. **No vendor paid for inclusion or placement**

in this report. Some vendors listed appear in IDSync's directory and comparison pages; sponsorships, where they exist, are disclosed on the relevant pages and had no bearing on this report's content.

Compare the best AI agent identity tools →

Side-by-side comparison of the leading vendors from this report.

Get a personalized shortlist →

Tell us your stack and constraints; we'll narrow this landscape to 3–5 vendors worth your evaluation time.

IDSync

The buyer-focused platform for identity, access, and authentication software.

Platform

Home

IAM Stack Finder

Directory

Resources

State of AI Agent Identity 2026

Buyer Guides

Glossary

Newsletter

Newsletter Archive

Best of guides

All comparisons

All vendor alternatives

Best SSO tools

Best MFA tools

Best PAM tools

Best IGA tools

Best CIAM tools

Best passwordless auth

Best identity security

Best machine identity

Best SaaS access governance

Best developer auth

Best for startups

Best for enterprises

Best SCIM tools

Best for AI agents

Best NHI tools

Okta pricing explained

Auth0 pricing explained

Okta alternatives

Auth0 alternatives

For Vendors

Sponsor

Submit Product

Claim Profile

Partner

Company

About & Methodology

Contact