Dickson Research

MARKET INTELLIGENCE

ANALYST BRIEF

ServiceNow Goes All In on Governing Every AI Agent

What CISOs need to know about ServiceNow's October 2026 bet that it can govern every AI agent in the enterprise, whoever built it.

PREPARED BY
Frank Dickson

DATE
November 6, 2026

EXECUTIVE SUMMARY

Bottom line

In October 2026, ServiceNow went all in on AI agent governance, betting that the control plane over everyone's agents matters more than the agents themselves. The headline is AI Passport: signed, scoped credentials checked at runtime, for ServiceNow and third-party agents alike. Around it sit shadow AI discovery, kill switches, cost controls, and an 11-member Control Tower Alliance.

DICKSON RESEARCH VERDICT

The direction is right, and the architecture is credible, but most of it is not generally available yet. CISOs should treat ServiceNow as a strong candidate for the AI governance system of record, especially where it already runs the CMDB and GRC, while keeping enforcement anchored in identity and security tools they already trust.

THE ANNOUNCEMENTS / 01

What ServiceNow announced

Five October announcements, taken together, extend ServiceNow's reach from its own agents to everyone's. Most ship in Q4 2026 or later.

DATE (2026)	ANNOUNCEMENT	SECURITY RELEVANCE	AVAILABILITY
Oct 28	Control Tower Alliance	11 founding members (Anthropic, AWS, Cisco, HiddenLayer, Kong, NVIDIA, Okta, OpenAI, Stripe, WitnessAI, Zenity) building certified integrations into the Control Tower. Okta supplies a kill switch that blocks new agent tokens; Cisco AI Defense feeds AI asset and security findings	Program launched; integrations rolling out
Oct 28	OpenAI partnership expansion	Security and Risk solutions powered by OpenAI cyber models; voice-driven governance and risk assessment in the Control Tower	Security early access Jan 2027, GA Q2 2027; Control Tower voice Q1 2027
Oct 21	Arc with NVIDIA	Personal long-running agent governed by the Control Tower and enforced by NVIDIA OpenShell, with hardware-backed (BlueField) runtime policies and kill switch	GA announced Oct 22
Oct 15	AI Passport	Cryptographically signed credential per agent and MCP server, checked at each step of multi-agent workflows; scope derived from CMDB, GRC policy, and workflow approvals; graduated responses up to a kill switch; built on open specifications	Expected Q4 2026
Oct 15	Control Tower expansion	Shadow AI detection for unapproved agents; discovery across IT, OT, cloud, and third parties (400+ out-of-box connectors); autonomous remediation; AI Cost Management; rename to Super Intelligence Control Tower	Rolling out

MARKET SIGNAL / 02

Why it matters

These moves reflect four shifts every CISO's AI program will have to absorb.

1. **Agent identity is the new perimeter.** AI Passport gives each agent an attested record of its authority, including its scope, who authorized it, and a full audit trail. The key idea is that third-party agents no longer rely on their own claims about permissions; the Control Tower issues a verifiable record instead.
2. **Authorization moves from login to runtime.** Permissions are checked at every step of a workflow, not once at sign-in. Responses are graduated, from redirect to restrict to kill, with a recorded reason when an agent is restored.
3. **Business context becomes a security input.** ServiceNow's differentiator is scoping agent authority from the CMDB, GRC policies, and workflow approvals. Its 2026 acquisitions of Veza (identity and access mapping, closed March) and Armis (asset visibility across IT, OT, and IoT, closed April) deepen that context. An identity provider knows who the agent is; ServiceNow claims to know what the agent should be doing right now.
4. **No single vendor governs the whole estate.** The Alliance concedes that discovery, identity, runtime enforcement, and model security live in different tools. ServiceNow wants to be the neutral layer that orchestrates them rather than replaces them.

COMPETITIVE LANDSCAPE / 03

Competitive context

ServiceNow is entering a crowded field where every major platform now claims to be the agent control plane. Its edge is business context and cross-vendor reach; its weakness is that, beyond its own platform, it relies on partners to block third-party agents.

VENDOR	APPROACH TO AGENT GOVERNANCE	WHERE IT IS STRONGEST	OVERLAP WITH SERVICENOW
ServiceNow	Super Intelligence Control Tower + AI Passport; partners enforce at runtime	Business context (CMDB, GRC, workflows); cross-vendor inventory	N/A
Microsoft	Agent 365 control plane + Entra Agent ID, with Defender, Purview, and Intune; Agent 365 ~$15/user/month or in M365 E7 (2toLead)	Owns identity, endpoint, and data enforcement in Microsoft-centric estates	High: both want to be the agent registry and governance plane
Okta	Okta for AI Agents (GA Apr 30, 2026): agent registry, Agent Gateway, Universal Logout kill switch; Blueprint Alliance announced at Oktane (diginomica)	Identity-native, vendor-neutral, token-level enforcement	Partner and competitor: Okta supplies ServiceNow's kill switch, yet Passport moves into authorization
Salesforce	Einstein Trust Layer, Agent Fabric, and Guardian, governed inside its Trust Boundary (Cyntexa)	Deep controls for agents inside Salesforce	Moderate: strong in-platform, weaker across other vendors' agents
CrowdStrike / Palo Alto Networks	Falcon AIDR and shadow AI governance; Prisma AIRS 3.0 with an AI Agent Gateway (CRN Asia)	Runtime detection and network/endpoint enforcement	Low to moderate: they detect and block; ServiceNow governs and remediates
AI security specialists	HiddenLayer, Zenity, WitnessAI, and others focused on agent and model security	Purpose-built threat detection	Mostly partners via the Alliance

Alliance membership overlaps by design: ServiceNow is a founding member of Okta's Blueprint Alliance, Okta is a founding member of ServiceNow's Control Tower Alliance, and AWS sits in both. Because Passport is built on open specifications, these layers can complement each other, but CISOs still need to decide which one is the system of record.

ANALYST PERSPECTIVE / 04

Dickson Research take

Going all in is the right call. Microsoft owns more of the enforcement stack, but ServiceNow brings business context and vendor neutrality that Microsoft cannot easily match. Whether the bet pays off depends on enforcement ServiceNow does not control.

Strengths

- **Context-aware authorization.** Tying agent scope to the CMDB, GRC policy, and approvals is a real differentiator. Identity vendors cannot easily replicate that business context.
- **Third-party coverage.** Issuing passports to agents ServiceNow did not build addresses the hardest problem: the agents nobody inventoried.
- **Open specifications.** Building Passport on open specs lowers lock-in risk and makes it plausible as a cross-vendor standard.
- **Ecosystem breadth.** The Alliance spans model labs, cloud, identity, network, and AI security, which few rivals can match.

Gaps and risks

- **Timing.** AI Passport is expected in Q4 2026; most Alliance integrations are still commitments, not shipping code. CISOs are buying a roadmap.
- **Dependent enforcement.** Beyond its own platform, kill switches run through Okta tokens and NVIDIA OpenShell. ServiceNow decides; others block. Seams between them are where failures hide.
- **Overlapping control planes.** Customers on Microsoft 365 E7 or Okta for AI Agents may end up with two or three agent registries. Conflicting policies are a new risk.
- **Cost and complexity.** Governance tied to the full platform favors existing ServiceNow shops. Armis Centrix remains available standalone and Passport's open specifications ease the dependency, but context-aware scoping still relies on CMDB and GRC data that live on the ServiceNow platform.

Open questions to put to ServiceNow

- Which enforcement points honor AI Passport at GA, beyond NVIDIA?
- How does Passport interoperate with Entra Agent ID and Okta's registry, and which system wins when policies conflict?
- What is the pricing model for Passport, shadow AI detection, and cost management?
- How quickly does a kill switch take effect on in-flight sessions, not just new tokens?

WHAT TO DO NOW / 05

Recommendations for CISOs

Act on the principles now and the products later: inventory, identity, and kill-switch readiness pay off whichever vendor wins.

1. **Inventory every agent this quarter.** Include third-party and shadow agents, coding agents, and MCP servers. Whatever tool you use, you cannot govern what you have not found.
2. **Give every agent an identity and a named human owner.** Stop running agents on shared service accounts. This is the common ground across ServiceNow, Microsoft, and Okta.
3. **Pick one system of record for agent governance.** Decide deliberately between ServiceNow, Microsoft Agent 365, and Okta based on where your CMDB, identity, and productivity stack live. Avoid running parallel registries by accident.
4. **Test the kill switch end to end.** Confirm it cuts active sessions, not just new tokens, and measure time to containment. Make it part of incident response tabletop exercises.
5. **Scope agents to tasks, not roles.** Push for runtime, least-privilege authorization tied to the workflow, the model AI Passport promotes.
6. **Pilot before you commit.** If you run ServiceNow, pilot AI Passport and shadow AI detection on one high-risk workflow at GA. Get pricing and interoperability answers in writing first.
7. **Track AI cost as a security signal.** Unexpected token spend often flags a rogue or compromised agent; tie cost monitoring into security alerting.

COPYRIGHT NOTICE

This Dickson Research document was published as part of Dickson Research's independent market intelligence coverage. Visit dicksonresearch.com to learn more about Dickson Research. Please contact Dickson Research at frank@dicksonresearch.com for information on reprints, web rights, or permission to cite this research in external materials.

This document is provided for informational purposes only. It is based on sources Dickson Research believes to be reliable, but Dickson Research makes no warranty as to its accuracy, completeness, or fitness for any particular purpose and accepts no liability for decisions made in reliance on it. Opinions reflect Dickson Research's judgment at the time of publication and are subject to change without notice. Nothing in this document constitutes investment, legal, or financial advice.

Dickson Research's analysis is independent. References to specific vendors, products, or services do not constitute an endorsement.

All product and company names mentioned in this document are trademarks or registered trademarks of their respective owners.

Copyright © 2026 Dickson Research. Reproduction is forbidden unless authorized. All rights reserved.