Workday Launches Agent Passport to Test, Verify, and Continuously Monitor Every AI Agent in the Enterprise

Agent Passport Measures Every Agent Against Industry Standards Including OWASP LLM Top 10, NIST AI RMF, and MITRE ATLAS

Cisco Joins as Launch Partner to Independently Test AI Agents in Workday Using Cisco AI Defense

Your browser does not support the video tag.

LAS VEGAS, June 2, 2026 /PRNewswire/ -- **Workday DevCon —** Workday, Inc. (NASDAQ: WDAY), the enterprise AI platform for HR, finance, and IT, today announced Agent Passport, which tests and verifies every AI agent, Workday-built or third-party, before it goes into production, and continuously monitors it after. Every attestation is tied to a public industry standard, such as OWASP LLM Top 10, NIST AI RMF, and MITRE ATLAS, so security teams have a signed, auditable record of what each agent has been tested for and who did the testing.

Agent Passport gives companies a verified record that every agent has been tested against the most serious risks before it goes into production, including prompt injection, jailbreak and goal hijacking, system prompt extraction, leaks of employee data, and unsafe outputs. Each test result is tied to a public standard and signed by the partner that performed it, so the record is independent, auditable, and comparable across agents from any vendor.

When an agent attempts to execute a task, Agent Passport will monitor in real time and either allow, block, or route the action accordingly. If a problem is discovered, a single revocation can automatically stop, limit, or otherwise restrict affected agents based on company policy.

"AI agents are now doing the most sensitive work in the enterprise, from onboarding employees to processing payments, and one insecure agent can leak employee data, break compliance, and put the company on the front page for the wrong reasons," said Dean Arnold, vice president, AI Platform, Workday. "Agent Passport gives companies confidence that every agent has been independently tested and verified, and the power to shut any of them down across the business the moment something changes."

A Shared Standard, Built with Industry Leaders

Most platforms that offer agent security testing do it themselves, which means customers receive a "safe" label from the same vendor that built the agent. Workday has built extensive trust with customers with its broad portfolio of AI solutions for HR and finance. The company is building on that trust through open standards and partnership with leading vendors in agentic security and regulatory compliance, so the testing is independent and open, and the results are comparable across agents from any vendor.

Each agent's record has three layers. The first covers the broad areas of trust that Workday defines and keeps current, such as protection against attacks, safe behavior at runtime, and human oversight. The second is a set of specific, testable claims tied to public standards, like resistance to known attack techniques. The third is the signed results from the partner that performed the testing, issued by verified, trusted attestors starting with Cisco.

Because every check is tied to a public standard, security teams can compare agents from different vendors on the same terms for the first time. If two agents carry the same check from two different partners, companies know they were held to the same bar.

Independent Attestations from Industry Leaders in Agentic Security

Cisco is the launch partner for Agent Passport, bringing Cisco AI Defense to independently test AI agents running in Workday against leading security standards before deployment and continuously protect them at runtime against prompt injection, data leakage, jailbreaks and unsafe actions.

Cisco AI Defense confirms the agent resists attempts to override its instructions, keeps its own instructions from being exposed, protects sensitive employee information from leaking, and blocks harmful or policy-violating responses before they reach a user. These validations are important for any agent, but are non-negotiable for agents operating on payroll, benefits, and financial data.

"Agents are going to be everywhere in the enterprise, and that only works if security teams have a clear, signed record of what each one has been tested for," said DJ Sampath, senior vice president and general manager, AI Software and Platform, Cisco. "Cisco AI Defense was built for exactly this kind of validation, and we're excited to partner with Workday to secure the agentic workforce."

Availability

Agent Passport will be available to early access customers in the second half of 2026, and general availability is projected before the end of 2026. The Workday and Cisco partnership is active today, with joint capabilities rolling out over coming quarters.

For More Information

- Discover how Workday and Cisco are partnering to define enterprise agentic security.
- Read how Workday Build is now agent-ready, empowering developers to build, connect, and verify AI agents for HR, finance, and IT.
- Learn how the latest expansions to Workday Data Cloud allow developers to securely bring live HR and finance data into their existing AI, analytics, and applications without rebuilding data pipelines.
- Explore the three paths to build AI apps and agents with Workday, without giving up control or safety.

About Workday

Workday operates at the heart of the enterprise – HR, finance, and IT – where the margin for error is effectively zero. By tightly coupling AI with the context, guardrails, and trusted processes that run the business, Workday goes beyond AI that assists work to agents that do the work and drive measurable outcomes. More than 11,500 organizations worldwide, including more than 65% of the Fortune 500, trust Workday to deliver. For more information about Workday, visit workday.com.

Forward-Looking Statements

This press release contains forward-looking statements including, among other things, statements regarding Workday's plans, beliefs, and expectations. These forward-looking statements are based only on currently available information and our current beliefs, expectations, and assumptions. Because forward-looking statements relate to the future, they are subject to inherent risks, uncertainties, assumptions, and changes in circumstances that are difficult to predict and many of which are outside of our control. If the risks materialize, assumptions prove incorrect, or we experience unexpected changes in circumstances, actual results could differ materially from the results implied by these forward-looking statements, and therefore you should not rely on any forward-looking statements. Risks include, but are not limited to, risks described in our filings with the Securities and Exchange Commission ("SEC"), including our most recent report on Form 10-Q or Form 10-K and other reports that we have filed and will file with the SEC from time to time, which could cause actual results to vary from expectations. Workday assumes no obligation to, and does not currently intend to, update any such forward-looking statements after the date of this release, except as required by law.

Any unreleased services, features, or functions referenced in this document, our website, or other press releases or public statements that are not currently available are subject to change at Workday's discretion and may not be delivered as planned or at all. Customers who purchase Workday services should make their purchase decisions based upon services, features, and functions that are currently available.

SOURCE Workday Inc.

For further information: Media@workday.com

---

https://newsroom.workday.com/2026-06-02-Workday-Launches-Agent-Passport-to-Test,-Verify,-and-Continuously-Monitor-Every-AI-Agent-in-the-Enterprise