NEWS RELEASE

ServiceNow launches Autonomous Security & Risk, integrating Armis and Veza to govern every AI agent, identity, and connected asset

2026-05-05

Armis delivers continuous asset intelligence across code, IT, OT, IoT, and connected devices; Veza brings fine-grained permission visibility, intelligence, and governance for every human and non-human identity

The ServiceNow AI Platform offers one of the most complete security, risk, and compliance platforms in enterprise AI

LAS VEGAS--(BUSINESS WIRE)-- Knowledge 2026 — Today, at ServiceNow's annual customer and partner event, **Knowledge 2026**, **ServiceNow** (NYSE: NOW), the AI control tower for business reinvention, launched **Autonomous Security & Risk** to govern every AI agent, identity, and connected asset. Armis delivers continuous asset intelligence across code, IT, OT, IoT, and connected assets. Veza provides fine-grained visibility, intelligence, and governance for human and non-human identities. The result of this combination is one of the most complete security, risk, and compliance platforms in enterprise AI.

Security and risk crossed $1 billion in annual contract value (ACV) for ServiceNow last year, making it one of the fastest-growing sources of demand on the ServiceNow AI Platform. The pressure is compounding as AI exponentially multiplies identities, permissions, connected assets, and decisions that require governance. AI agents acquire access, execute decisions, and operate at machine speed – and the non-human identities behind them already vastly outnumber human ones. Who approved that access, why it exists, and whether it remains valid are questions most enterprises cannot answer. Disconnected security tools cannot close this gap; a platform approach can.

“Today’s CISOs have to operate at two speeds: neutralizing threats in real time while reporting risk to the board with conviction,” said John Aisien, senior vice president and general manager, Central Product Management, Security & Risk, ServiceNow. “Autonomous Security & Risk replaces that fragmented stack with a single graph that maps every identity, every permission, and every connected asset, so prevention, detection, and response happen at machine speed.”

Every AI agent is an identity, with most ungoverned

Every AI agent that acts inside an enterprise does so through an identity. It accesses systems, reads data, and executes workflows under a set of permissions that were almost certainly designed for human actors, rather than the speed, scale, or autonomy of AI agents. Closing the identity visibility, intelligence, and governance gap is critical.

Veza's Access Graph provides a continuous, real-time map of every access relationship across an enterprise environment, including what has access, what it can do with that access, and how these change as context shifts, systems evolve, and agents multiply. With Veza now integrated into the ServiceNow AI Platform, this capability governs both human and non-human identities within a single operational framework: surfacing risk, enforcing least privilege at the point of action, triggering downstream remediation, and building the traceable institutional memory that auditors and regulators require. ServiceNow Veza works in concert with ServiceNow’s existing vulnerability, exposure, and incident management capabilities to close pre-breach & post-breach exposure: governing who and what has access and continuously identifying and remediating permission-related vulnerabilities.

You cannot secure what you cannot see

Asset visibility has always been a foundational requirement of enterprise security, along with a persistent failure point. The environments enterprises operate in today span pre-compiled code, IT infrastructure, operational technology, connected devices, cloud workloads, medical equipment, and now AI agents, interacting across boundaries that no single tool was ever meant to fully see.

Once integrated into ServiceNow, **Armis** will deliver real-time, contextual awareness of every connected cyber asset, including the devices and systems conventional tools had no visibility into. Armis will monitor network traffic without agents, without disrupting operations, and enrich every asset record with device type, classification, firmware version, behavioral data, and real-time risk posture. This intelligence flows directly into the ServiceNow CMDB, turning a hitherto static inventory into a live picture of the actual attack surface. When an asset is found to be vulnerable, misconfigured, or behaving anomalously, ServiceNow responds at machine speed, in accordance with prevalent environmental context.

Together, Veza and Armis boost ServiceNow's standing as a platform that knows what exists in the environment and who or what is permitted to interact with it. This real-time asset intelligence feeds directly into ServiceNow's security incident response workflows, so the same context used to assess risk before a breach is immediately available to contain it after.

The blueprint for trusted AI

When AI acts inside an enterprise, it must do so with the full business reality behind every decision, including governed permissions, continuous oversight, and an audit trail that holds under scrutiny. That is what Autonomous Security & Risk delivers. Asset intelligence, identity governance, risk management, and workflow automation operating as a single system, with AI running across all of it. Two new AI specialists, **announced today** as part of ServiceNow's autonomous workforce expansion, handle vulnerability resolution and security operations end to end, autonomously addressing unresolved vulnerability backlogs and investigating phishing incidents alongside human teams.

The **ServiceNow AI Control Tower** governs agents, ensuring they are inventoried from the moment they appear, risk-scored continuously, and least privilege enforced in real time. Evaluations score agents as they run. If something drifts, the AI Control Tower is able to catch it before it compounds. A2A and MCP interoperability means any agent, on any platform, operates within a governed framework that connects decisions to context and accountability to action. That same governed framework extends across ServiceNow's partner ecosystem, so the third-party security tools enterprises already rely on feed into a continuously updated picture of enterprise posture. ServiceNow's own security operations team runs Autonomous Risk & Security, handling incidents seven times faster than prior workflows using AI agents, with every action documented and every decision traceable.

Organizations are already seeing results on the **ServiceNow AI Platform**. A global energy company operating across 70+ countries saved 1.2 million hours by automating security operations and cut the time it takes to contain threats by 97%. A major U.S. financial services institution eliminated 96% of dormant non-human identities, turning least privilege from a policy goal into an enforced reality. A Fortune 100 aerospace manufacturer reduced the time to complete control attestations by 75% and close compliance gaps by 85%, replacing manual audit prep with evidence that captures itself.

Enterprises that establish this foundation of complete visibility, governed identities, integrated risk, and autonomous response will be decisively ahead as AI accelerates further. ServiceNow gives security and risk leaders a single view of how exposure, incidents, and identity decisions translate to enterprise risk posture in real time, with the audit trail regulators require.

What customers and partners say about Autonomous Security & Risk

Fortinet

"As the attack surface expands, real-time visibility and control over every asset is non-negotiable. ServiceNow's acquisition of Armis enables a powerful three-way partnership with Fortinet, advancing cybersecurity into an AI-driven, autonomous system that helps organizations continuously understand assets, prioritize threats, and execute response in real time," said John Whittle, chief operating officer at Fortinet. "With Fortinet's industry-leading AI-driven innovation at scale, combined with our long-standing relationships and deep integrations across both platforms, we can drive ServiceNow security workflows with precision—delivering faster, closed-loop protection and more consistent, accurate response for our customers."

About ServiceNow

ServiceNow (NYSE: NOW) is the AI control tower for business reinvention. The ServiceNow AI Platform integrates with any cloud, any model, and any data source to orchestrate how work flows across the enterprise. By unifying legacy systems, departmental tools, cloud applications, and AI agents, ServiceNow provides a single pane of glass that connects intelligence to execution across every corner of business. With more than 100 billion workflows running on the platform each year, ServiceNow helps organizations turn fragmented operations into coordinated, autonomous workflows that deliver measurable results. Learn how ServiceNow puts AI to work for people at **www.servicenow.com**.

Forward-looking statements

This press release contains "forward-looking statements" about the expectations, beliefs, plans, and intentions relating to ServiceNow's AI platform innovations. Such statements include statements regarding future product capabilities and offerings and expected benefits to ServiceNow. Forward-looking statements are subject to known and unknown risks and uncertainties and are based on potentially inaccurate assumptions that could cause actual results to differ materially from those expected or implied by the forward-looking statements. If any such risks or uncertainties materialize or if any of the assumptions prove incorrect, ServiceNow's results could differ materially from the results expressed or implied by the forward-looking statements made. ServiceNow undertakes no obligation, and does not intend, to update the forward-looking statements. Factors that may cause actual results to differ materially from those in any forward-looking statements include: (i) delays and unexpected difficulties and expenses in executing the product capabilities and offerings, (ii) changes in the regulatory landscape related to AI and (iii) uncertainty as to whether sales will justify the investments in the product capabilities and offerings. Further information on factors that could affect ServiceNow's financial and other results is included in the filings ServiceNow makes with the Securities and Exchange Commission from time to time.

Media Contact

Courtney Johnson
925.405.2446
press@servicenow.com

Source: ServiceNow