NEWS RELEASE

ServiceNow completes Armis acquisition, closing the gap between asset visibility and cyber risk

2026-04-20

Armis adds real-time cyber asset discovery, prioritization, and protection across IT, OT, IoT, medical devices, physical AI, critical infrastructure, code, and cloud

The Armis acquisition is expected to more than triple ServiceNow's market opportunity for security and risk solutions

SANTA CLARA, Calif.--(BUSINESS WIRE)-- **ServiceNow** (NYSE: NOW), the AI control tower for business reinvention, today completed its acquisition of Armis. Armis, a leading cyber exposure management and security company, delivers a comprehensive AI-powered solution that sees, protects, and manages cyber risk across every connected asset — from OT, IoT, medical devices, physical AI to code and cloud — in real time. The acquisition extends ServiceNow's security platform into the physical and operational layers of the enterprise, adding the cyber asset intelligence foundation and business context that enterprises need to deploy agentic AI with trust and control at scale.

The close follows ServiceNow's completion of the **Veza acquisition** in March 2026. Veza brought AI-native identity intelligence to the ServiceNow AI Platform, giving enterprises continuous visibility into who and what has access to every digital, connected resource. With the Armis acquisition, ServiceNow’s identity intelligence and cyber exposure management capabilities distinctively power critical pre-breach and post-breach security outcomes as enterprises deploy agentic AI at scale. Together, Armis delivers real-time visibility and protection across every connected cyber asset, while Veza maps every permission and access path across human, machine, and AI agent identities.

Closing the gap between visibility and cyber risk

Security teams operating across fragmented, point solution stacks have long faced a structural challenge. Historically, the tools that manage risk cannot execute on remediation actions, and the tools that remediate cyber risk cannot see the full picture. The result is a widening gap between detection and response, a gap that exponentially increases the risk of security incidents in the agentic AI era.

Stolen credentials remain the dominant entry point for attackers[1] and this problem is accelerating. Machine identities now outnumber human identities by more than 80 to one, and nearly half carry sensitive or privileged access rights that most organizations cannot fully see or control, leading to lateral movement attacks.[2] As enterprises accelerate agentic AI, their attack surface has expanded further to encompass autonomous agents, unmanaged OT devices, and other connected systems across manufacturing, healthcare, and critical infrastructure that conventional security tools were never built to handle.

ServiceNow's advantage is architectural. Armis provides continuous, real-time visibility, management, and security across every connected cyber asset through non-invasive discovery, tracking nearly 7 billion devices in real time, including OT, IoT, medical devices and physical AI, code, and cloud. Veza's Access Graph provides cross-system visibility into every permission held by every human, machine, and AI agent identity. Both graphs power ServiceNow's Context Engine — the organizational intelligence that grounds every AI action in business reality, mapping assets and identities to the services, processes, teams, and policies that depend on them. Risk prioritization becomes automatic. Remediation becomes autonomous. Every action is auditable and bounded by policy. The result is a platform that doesn't just sense risk across the enterprise — it decides what matters most, acts through automated workflows, and governs every step with a full audit trail.

"Most security platforms stop at the alert. ServiceNow closes the loop," said Amit Zavery, president, chief operating officer, and chief product officer at ServiceNow. "Armis gives us real-time, contextual awareness into the cyber risk of every connected asset, including the devices and systems that conventional tools were never built to see. Combined with Veza's identity intelligence, that signal flows into ServiceNow's Context Engine and AI Control Tower, turning exposure into automated remediation with governance and a full audit trail built in at every step."

"We built Armis to solve the toughest cybersecurity challenges of organizations globally, protecting all their assets across IT, OT, IoT, medical devices, code, and cloud that are at the heart of manufacturing, healthcare, and critical infrastructure," said Yevgeny Dibrov, co-founder and CEO, Armis. "Joining ServiceNow, with Veza already on the platform, enables us to address this mission tenfold to keep the world’s largest and most complex enterprise environments safe and secure.”

What this means for customers and partners

For current Armis customers, Armis Centrix™ now operates with the full support of ServiceNow's product, engineering, and global go-to-market organization. It is integrated with the ServiceNow AI Platform today and remains available as a standalone solution, with deeper integration expected over time.

Customers of both ServiceNow and Armis can immediately begin leveraging their combined capabilities, with broader availability coming soon. Partners of ServiceNow and Armis can immediately accelerate revenue by tapping into growing customer demand from organizations looking to deploy agentic AI with trust and control at scale.

ServiceNow establishes global hub to pioneer autonomous cyber defense

ServiceNow is establishing an AI Center for Cyber Defense — a global hub dedicated to building the next generation AI security stack and pioneering the transition from reactive security to autonomous, agentic cyber defense. The center will bridge the gap between AI research and practical cybersecurity solutions, serve as a definitive resource for enterprise security leaders transitioning from legacy frameworks to AI-native security postures, and develop the expertise needed to anticipate and neutralize AI-driven attacks before they occur.

Strength building on strength

In the four months since the acquisition was announced, Armis has continued to operate as an independent company, consistently being recognized as a Leader. Armis was recently named a Leader in the 2026 Gartner® Magic Quadrant™ for CPS Protection Platforms for the second consecutive year. Armis was also named a Leader in The Forrester Wave™: IoT Security Solutions, Q3 2025 and The Forrester Wave™: Unified Vulnerability Management Solutions, Q3 2025. Armis Centrix™ was named “Best Solution” for Cyber Exposure Management in The Global InfoSec Awards at RSAC™ 2026 Conference.

The companies already maintain multiple integrations connecting Armis' asset intelligence to ServiceNow workflow action, making this integration acceleration, not initiation. Armis is trusted by nine of the Fortune 10 and more than 35% of the Fortune 100, as well as by public sector organizations and government agencies globally. Many of these organizations are already ServiceNow customers, reinforcing the complementary nature of both companies’ capabilities and the demand that already exists for their combined capabilities.

"Stronger cyber resilience starts with visibility across the entire network," said Rex Thexton, chief technology officer, Accenture Cybersecurity. "At Accenture, we help clients align this critical security foundation with real business outcomes. By leveraging solutions like ServiceNow and Armis, organizations can accelerate automated asset protection so they can scale securely, build the visibility needed to be resilient, and stay ahead of cyber threats."

"As the attack surface expands, real-time visibility and control over every asset is non-negotiable," said John Whittle,

chief operating officer, Fortinet. "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. 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."

With Armis employees joining ServiceNow, the combined organization brings deep expertise in cyber-physical security and risk to the ServiceNow AI Platform, accelerating its roadmap for autonomous, proactive cybersecurity. ServiceNow closed its largest quarter ever for OT in Q4 2025 and its security and risk business crossed $1 billion in annual contract value in Q3 — organic growth that established the foundation Armis now extends.

Armis, together with Veza, is expected to more than triple ServiceNow's addressable market for security and risk solutions.

To learn more about our security and risk platform vision, read our full **blog post**.

Transaction details

ServiceNow completed the acquisition of Armis for approximately $7.75 billion in cash, funded through a combination of cash on hand and debt. Tidal Partners served as ServiceNow's lead financial advisor. J.P. Morgan Securities LLC and Barclays also served as financial advisors to ServiceNow.

[1] Verizon, 2025 Data Breach Investigations Report

[2] CyberArk, 2025 Identity Security Landscape

Gartner Disclaimer

Gartner, 2026 Gartner® Magic Quadrant™ for CPS Protection Platforms, Katell Thielemann, Wam Voster, Ruggero Contu, Sumit Rajput, March 3, 2026. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Forrester Disclaimer

Forrester does not endorse any company, product, brand, or service included in its research publications and does not advise any person to select the products or services of any company or brand based on the ratings included in such publications. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change. For more information, read about Forrester's objectivity **here**.

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 85 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**.

Use of forward-looking statements

This press release contains "forward-looking statements" about the expectations, beliefs, plans, intentions, and strategies relating to ServiceNow's acquisitions of Armis and Veza. Such forward-looking statements include statements regarding future product capabilities and offerings and expected benefits to ServiceNow and its partners. 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, our results could differ materially from the results expressed or implied by the forward-looking statements we make. We undertake no obligation, and do 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, without limitation, any inability or delays in assimilating or integrating acquired technology into our platform; challenges retaining employees or customers of acquired companies; or any unanticipated obligations or liabilities related to the legacy businesses of those acquired companies. Further information on factors that could affect our financial and other results is included in the filings we make with the Securities and Exchange Commission from time to time.

Media Relations

Ryan Moore

press@servicenow.com

Investor Relations

Darren Yip

925.388.7205

ir@servicenow.com

Source: ServiceNow