

## ServiceNow + Armis: Strategic Rationale and Key Points

This morning, ServiceNow announced the acquisition of Armis (press release [here](#)).

AI and Agents are poised to create significant business value but also bring additional complexity and risks. The use of AI and Agents by cyber threat actors is pushing organizations to better understand and fix exposures at the speed of AI, requiring increased focus on remediation velocity. Organizations also face a growing challenge managing sprawling, hyper connected environments spanning IoT/OT devices, servers, applications, software components, identities, and now AI agents, all of which expand operational complexity and the attack surface. This scale and heterogeneity make it hard to even know what exists, let alone keep it inventoried, secured, and governed consistently across IT, security, and risk teams.

Armis will expand ServiceNow's security workflow offerings, provide leadership in cyber-physical security for critical infrastructure (OT, IoT, Cloud, and IoMT), and advance AI-native, proactive cybersecurity and vulnerability response across all connected devices. Together, ServiceNow and Armis will connect real-time asset discovery, threat intelligence, and risk prioritization with automated remediation and response workflows to accelerate security outcomes and strengthen security posture through continuous risk reduction.

Armis delivers an enriched view of an organization's assets as a network of connected entities (devices, services, applications, identities, and data flows) and the paths between them, powered by graph-based technology. With this comprehensive and connected graph view, organizations can see how a single misconfiguration on one node (for example, an exposed OT device or a mis-scoped identity) can propagate impact downstream into critical business services and processes, making it possible to prioritize fixes based on blast radius rather than just local severity. This graph understanding also helps validate that remediation plans actually break high risk attack paths instead of only addressing isolated symptoms.

For example, a customer operating numerous sites and networks could proactively detect and aggregate asset and vulnerability information across the entire IT and OT environment. Agentic AI-driven automation then turns prioritized, graph aware recommendations into concrete actions: AI agents can open, route, and enrich incidents, propose or execute remediation, trigger changes, and orchestrate containment of risky devices and services through ServiceNow workflows. This closes the loop from "see everything" (Armis Visibility), to "understand how it is connected" (Enriched Graph), to "decide what matters most" (Armis Exposure Management and Prioritization), to "act at scale and speed" (ServiceNow Agentic AI plus workflows), enabling organizations to manage complexity while materially improving security and operational outcomes.

Armis extends ServiceNow's security offerings in critical, fast-growing areas of cybersecurity and drives greater AI adoption by strengthening trust across a rapidly expanding threat surface. AI is creating massive new markets, and winning will require accelerating innovation to meet the moment. Companies

that move fastest will lead, while others risk falling behind. While AI is accelerating the pace of acquisitions across the industry, ServiceNow maintains a disciplined M&A strategy.

### **Key Points**

- ServiceNow has already established itself as a security leader. In 3Q25, ServiceNow's Security and Risk business became the company's fifth business to cross the \$1 billion annual contract value (ACV) threshold.
- The acquisition is expected to more than triple ServiceNow's market opportunity for security and risk solutions and accelerate the company's roadmap to autonomous proactive cybersecurity.
- Armis currently generates over \$340 million in annual recurring revenue (ARR), with over 50% y/y growth.
- ServiceNow remains fully capable of achieving previously established subscription revenue and Now Assist ACV targets without Armis. Recent acquisitions create incremental opportunities on top of ServiceNow's strong organic growth engine.
- Currently, management does not see any other large white spaces necessary to fill to complete ServiceNow's platform vision for Security.

### **Investor Relations**

Darren Yip

925.388.7205

[ir@servicenow.com](mailto:ir@servicenow.com)