



NEWS RELEASE

ServiceNow delivers Autonomous Security, the industry's most complete security offering

2026-08-04

ServiceNow unveils six unified security solutions with AI Specialists to enable prevention-first, AI-native cyber defense that operates at machine speed

As the fastest-growing major enterprise cybersecurity company, ServiceNow's risk and security business unites exposure management, identity, cyber-physical, incident response, and compliance as one governed motion, with proof of what acted, why, and who is accountable

LAS VEGAS--(BUSINESS WIRE)-- ServiceNow, the AI control tower for business reinvention, today announced an acceleration of its Autonomous Security vision with six unified solutions that help deliver prevention-first, AI-native cyber defense across unified exposure management, continuous vulnerability detection, cyber-physical security, identity and access security, and agentic incident response, and cyber risk and compliance. With new AI Specialists that complete security workflows autonomously, including the Vulnerability Resolution AI Specialist, these capabilities enable enterprises to prevent, contain, and remediate risk at machine speed, before threats become breaches.

As enterprises adopt agentic AI, security teams face an emerging challenge: every new agent, identity, and line of code multiplies exposure faster than any human team, or any patchwork of disconnected tools, can respond to. Closing that gap requires governed autonomy at the same machine speed. The average enterprise runs more than 70 security tools, fragmenting insights across the extended attack surface, including endpoints, networks, cloud environments, and identities. Today, ServiceNow becomes one of the most complete and fastest-growing security companies built for the AI era by consolidating this complexity into one unified system where assets, identities, and agents are visible, contextualized, secured, governed and auditable in a single motion.

This is achievable through **Shift Zero**: the move from fragmented, reactive security to prevention embedded at every layer, where every system, identity, and agent is governed and secured in real-time as threats move at AI speed. In Shift Zero, the goal is zero exposure at all times with an enterprise able to answer, with proof, what every system is doing, why, and who is accountable, while AI moves as fast as the business needs it to.

"As AI exposures compound exponentially, security teams operate on a human clock," said Yevgeny Dibrov, SVP and GM, cybersecurity and risk, ServiceNow. "Machine identities double every 18 months. Fragmented security tools can't match the curve AI is creating. Organizations need autonomous security and governance that matches the scale, velocity, and unpredictability of the threats coming: where all assets, identities, AI agents, critical infrastructure, cloud environments and code are protected, and can adapt as fast as the ecosystem moves to detect and remediate threats in real-time. Security becomes an accelerant, not the brake."

Shift Zero: Prevention embedded at every layer

Autonomous Security moves companies from reactive, fragmented security to prevention-first, autonomously governed security that operates faster than AI creates risk. The Autonomous Security offerings stand on six solutions that integrate into ServiceNow's AI Control Tower.

Unified Exposure Management: Exposures pile up in silos, with security teams seeing vulnerabilities but not the assets that matter or which ones could be easily exploited. ServiceNow consolidates findings from any source and enriches data with business context and exploitation intelligence, enabling autonomous remediation at scale.

- Agentic Exposure Management consolidates vulnerability findings from every source into a single stream enriched by Early Warning threat intelligence and Fix Intelligence prioritized remediation.
- Vulnerability Resolution AI Specialist orchestrates triage and remediation at enterprise scale, executes low-risk patches, and turns exposure backlogs into closure pipelines.

Continuous Vulnerability Detection: The attack surface spans code, cloud, and infrastructure, but traditional tools only see one layer at a time. ServiceNow closes these gaps, enabling security teams to govern code, cloud, and infrastructure risks from a unified platform.

- Application Security extends threat modeling to AI-generated code and model dependencies with a new version that surfaces supply chain vulnerabilities before deployment.
- Dynamic Application Security Testing (DAST) validates runtime vulnerabilities in live applications and APIs.
- External Attack Surface Management (EASM) surfaces infrastructure exposure that attackers can exploit, showing a footprint the way threat actors see it.

Cyber-Physical Security: OT, medical devices, and IoT systems can be blind spots because legacy tools disrupt production and lack the behavioral understanding needed to catch risky activity. ServiceNow brings continuous visibility and compliance monitoring to operational environments without disruption.

- Agentic AI for Cyber Physical Security delivers agentless discovery across OT and medical networks, establishes behavioral baselines, validates compliance continuously in real time, and models attack paths, so security teams understand adversary movement. Automated remediation workflows execute across brownfield environments without custom engineering.

Identity & Access Security: Non-human identities, service accounts, cloud identities, and AI agents are everywhere and almost entirely ungoverned. ServiceNow enables security teams to see, control, and govern every identity across the enterprise under consistent least-privilege principles.

- AI Agent Access Security unifies access control for AI agents across any platform or model provider, closing the threat vector of ungoverned agents with escalated permissions.
- Non-Human Identity Remediation moves beyond risk scoring into active action: automated key rotation, deprovisioning, and permission revocation at scale across IT, OT, IoT, and medical networks; enables AI agents and service accounts to operate under identical identity governance as human users.

Agentic Incident Response: Incident response teams can lose hours stitching together threat intelligence, asset ownership, and identity data when they should be stopping threats. ServiceNow automates triage and investigation, freeing analysts to focus on sophisticated threats.

- Agentic Incident Response enables ServiceNow's Tier 2 SOC AI Specialist to autonomously build and execute multi-phase response plans for complex incidents, performing actions like enrichment, correlation, containment and blocking while escalating only high-risk decisions to human analysts.

Cyber Risk and Compliance: Compliance remains a pre-audit scramble. Evidence collection is manual, controls are monitored quarterly, and organizations are stuck playing catch-up. ServiceNow transforms compliance from a seasonal event into a continuous operational signal.

- Agentic AI for Continuous Control Monitoring transforms control evidence into a continuous operational signal. Automated agents evaluate segregation of duties, access rights, and configuration state across ServiceNow and external systems in real time, surfacing violations the moment they occur. Compliance-ready reports exist on demand across regulatory frameworks including SOC 2, ISO 27001, PCI-DSS, and HIPAA.
- Cryptographic Asset Compliance enables rapid migration from legacy cryptographic algorithms to quantum-resistant standards before the quantum threat window closes. ServiceNow delivers comprehensive discovery, AI-powered risk profiling, and guided migration workflows across on-premises and cloud environments, with

full integration to ServiceNow Integrated Risk Management and Governance, Risk, and Compliance (IRM/GRC) products for regulatory compliance evidence at enterprise scale.

What customers are saying about ServiceNow's security leadership

"For organizations operating complex industrial environments, effective cybersecurity starts with understanding risk and maintaining visibility across the enterprise," said Brandon Glaze, Sr. Director, Cybersecurity (OT/ICS) at Baker Hughes. "We've appreciated the collaboration and innovation from the ServiceNow (Armis) team as we continue working together to improve cyber resilience and support secure, reliable operations."

ServiceNow is building the world's most complete end-to-end security offering. Today's announcements are powered by ServiceNow's proven track record in security and risk and the depth of Armis and Veza now inside ServiceNow. Armis provides continuous, non-invasive visibility across every connected asset, tracking billions of devices in real time. Veza's Access Graph maps effective permissions across human, machine, and AI identities. Together, they feed ServiceNow's AI Control Tower, **Context Engine**, and orchestration layer with the unified business and operational intelligence that enables autonomous remediation with full governance and auditability.

Availability

Agentic Exposure Management, Autonomous Remediation Agents, Application Security, Dynamic Application Security Testing (DAST), External Attack Surface Management (EASM), Agentic AI for Cyber Physical Security, AI Agent Access Security, Non-Human Identity Remediation are available now. Tier 2 SOC AI Specialist, Vulnerability Resolution AI Specialist, Agentic AI for Continuous Control Monitoring, and Cryptography Asset Compliance are expected to be available in December 2026.

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.

Media Contact

Nicole Rosenberg

401.594.3673

press@servicenow.com

Source: ServiceNow