NEWS RELEASE

92% of Indian organisations had an AI agent security incident in the past year; only 36% of them contained it within 24 hours

2026-11-18

Leaders describe their agentic security as “established”. The controls behind it tell a different story.

INDIA, Wednesday, 18th November 2026: 92% of Indian organisations experienced an agentic security incident in the past year, yet only 36% of those organisations contained it within 24 hours, according to ServiceNow's new research, **Deployed but Ungoverned: The State of Agentic Security in India**, a survey of 500 security leaders.

“AI agents are now part of how Indian enterprises operate, but security has not kept pace. You can't secure or govern what you can't see. Every agent should be registered, owned and visible in one place, with controls enforced automatically and responses at machine speed, so security teams can detect problems and contain them in time,” said Kulmeet Bawa, GVP & Managing Director for India & SAARC at ServiceNow.

Security confidence is running ahead of control

Half of Indian security leaders describe their agentic security as established, yet the research shows that its foundations remain uneven:

- Only 19% have a single named individual accountable for agentic AI security governance
- Only 18% have unified, single-interface visibility into their agents
- Only 30% enforce an automated deployment gate that blocks agents until they pass security checks

- Only 47% can produce a complete evidence package on demand

Detection is automated, but response is still manual

Human oversight remains an important safeguard, but it cannot be the only line of defence where AI agents operate continuously and at machine speed. About half of Indian organisations (51%) have automated real-time detection for anomalous AI agent behaviour. However, 67% cannot automatically act when an agent behaves anomalously, which highlights the gap between identifying a threat and responding to it.

Only 46% bring in security before agent development begins, so many agents are designed and built before security has shaped the controls around them. The exposure also reaches beyond IT: 83% of organisations run AI agents in or interacting with operational technology (OT) or physical environments, and only 29% have a separate governance framework designed for them.

The “Shadow AI” problem

37% of organisations discovered AI agents running in production in the last 12 months that were never registered or known to security teams. These unregistered agents are a critical blind spot: organisations cannot govern what they cannot see.

CERT-In's (Indian Computer Emergency Response Team) October 2026 advisory on AI agents (CIAD-2026-0049) has put agent visibility and control on the agenda for Indian organisations.

The ServiceNow study looks at how well organisations can see and govern their own agents. Under CERT-In's 2022 directions, Indian organisations must also report cyber incidents within six hours of becoming aware of them.

Organisations that run agentic security on a unified platform, 43% of those surveyed, fare better than those that don't: 62% have automated real-time alerts for anomalous agent behaviour (versus 43% of others), 45% automatically remediate agent policy violations (versus 24%) and 51% capture evidence continuously (versus 43%).

Closing the gap starts with knowing what is running. Organisations need a complete record of their AI agents, one view across agents and identities, and a named leader responsible for governing them. To explore the full findings of the report, click here - **Deployed but Ungoverned: The State of Agentic Security in India**.

Methodology

Deployed but ungoverned: the state of agentic security, was conducted by ServiceNow in conjunction with Phronesis Partners. The study surveyed more than 3,700 senior security and technology decision makers, VP level

and above, across 20 countries, including 500 security leaders in India. The global study included 1,201 respondents across APAC.

About ServiceNow

ServiceNow (NYSE: NOW) is the Super Intelligence Control Tower for business reinvention. The ServiceNow platform integrates with any model, any cloud, and any data source to orchestrate, govern, and secure work across the agentic enterprise. ServiceNow gives customers the enterprise context and control to build and scale confidently. With more than 100 billion workflows running on the platform each year, ServiceNow helps organizations turn fragmented operations into coordinated, autonomous work for IT, CRM, Security, Employee Experience, and more. Learn how ServiceNow puts AI to work for people at **www.servicenow.com**.

Media Contact

Prerana Channe - ServiceNow

prerana.channe@servicenow.com