Australia must strengthen security as rogue AI looms large

New research reveals that over a quarter of Australian organisations found AI agents running in production were unregistered or unknown

Sydney, 9 November 2026 - ServiceNow, the Super Intelligence Control Tower for business reinvention, today warned Australian organisations to crack down on rogue AI agents and strengthen governance, as new research reveals one in four (28%) Australian organisations found AI agents in production that were never registered or known. The warning comes as AI agents move out of pilots and into the systems that run hospitals, airports, manufacturing, financial institutions, and beyond.

Over half of Australian organisations (51%) are using agentic AI, but many are doing so without the governance foundations to keep those agents under control. ServiceNow's research – **Deployed but ungoverned: the state of agentic security** – found over half (57%) of organisations are only bringing in security after agent planning and design; less than half have proper frameworks, such as real-time monitoring (46%) or incident response (39%).

The research reveals that 91% of organisations had an agentic security incident in the last year, with 43% of them failing to contain agentic incidents within 24 hours (compared to 36% globally). Alarmingly, 79% had a security incident involving an AI agent that affected an Operational Technology (OT) system or physical security system.

"Since the arrival of Generative AI, the message has been to adopt AI or fall behind. But as the technology has advanced and rogue AI has become a threat, the biggest risk is now failing to build in governance and security from the start and instead bolting it on. And it's a threat that could go beyond just organisations to the core of Australia's economy and its critical infrastructure," said Pete Andrew, Group Vice President, Australia and New Zealand at ServiceNow.

Blind spots give rise to 'shadow AI'

"Governance and security are two sides of the same coin. Weak governance leads to severely compromised security outcomes for organisations and consumers too," said Mr Andrew.

"And while there are many unknowns about what the impacts could be, we've already had a taste. With incidents ranging from wiping gym bookings to getting unauthorised access to government data, mitigating these risks is essential. It's why ServiceNow's Autonomous Security is inbuilt with guardrails and an AI kill switch."

But as employees and teams deploy AI agents faster than organisations can identify, register and oversee them, a new form of 'shadow AI' is growing. This autonomous technology, operating inside

the enterprise without clear ownership, permissions or accountability, is creating a new governance challenge.

When asked to rate their security posture, leaders reveal a concerning blind spot:

- 58% say their current posture for securing Agentic AI is established, but most lack basic governance checks.
- Only 27% have a mandatory automated gate that blocks deployment until an agent passes security checks.
- 63% cannot act automatically when an agent behaves anomalously.

"Our research shows that most organisations are vastly overestimating how developed their agentic AI security is and that many lack basic governance and security checks," said Mr Andrew.

"Overconfidence is dangerous when it comes to rapidly developing technologies that can do serious damage to an organisation."

What is next for Australian organisations

AI is already delivering immense benefits, but like the shift to the cloud in the 2010s, organisations need to get their agentic governance and security basics right. Globally, most surveyed businesses (60%) had only a limited or emerging security posture, with only 13% of organisations having a defensive posture. The five moves for a defensible posture are:

1. Register every agent automatically at deployment, with a live map of what it can access.
2. Build security in before design and contain incidents within 24 hours.
3. Keep a complete, up-to-date inventory of all agents.
4. Capture agent evidence continuously, inside the system that generates it.
5. Give one person enterprise-wide governance accountability for the framework, gates, response plan and evidence, while each function owns the agents it runs.

"If you don't know what or where AI agents are operating inside your organisation, you can't govern what they're doing. And if you can't govern what they're doing, you can't help prevent security incidents," said Mr Andrew.

ENDS

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 300 in Australia.

© 2026 ServiceNow, Inc. All rights reserved. CONFIDENTIAL. ServiceNow, the ServiceNow logo, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc. in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

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 organisations 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

Phil Smith – ServiceNow
phil.smith@servicenow.com

Emily Saville – Vocal
emily@wearevocal.com.au

© 2026 ServiceNow, Inc. All rights reserved. CONFIDENTIAL. ServiceNow, the ServiceNow logo, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc. in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.