SailPoint Research Highlights Rapid AI Agent Adoption, Driving Urgent Need for Evolved Security

May 28, 2025

Key findings:

- 96% of tech professionals view AI agents as a growing security risk, yet 98% of organizations plan to expand adoption
- AI agents are viewed as a greater security risk than traditional machine identities
- Lack of governance and visibility over AI agents is putting sensitive enterprise data at risk
- Experts urge AI agents be managed like human identities, with clear access controls and accountability

AUSTIN, Texas--(BUSINESS WIRE)--May 28, 2025-- SailPoint, Inc. (Nasdaq: SAIL), a leader in unified identity security for enterprises, today released a new research report titled *'AI agents: The new attack surface. A global survey of security, IT professionals and executives.'* The report highlights an urgent need for improved identity security as AI agents gain widespread adoption.

According to the report, 82% of organizations already use AI agents, but only 44% of organizations report having policies in place to secure them. The report also presented a striking paradox: 96% of technology professionals consider AI agents a growing risk, even as 98% of organizations plan to expand their use of them within the next year.

The terms "AI agent" or "agentic AI" broadly encompass autonomous systems that perceive, make decisions, and take action to achieve specific goals within an environment. These agents often require several different machine identities to access needed data, applications and services, and they introduce additional complexities like self-modification and the potential to generate sub-agents. Notably, 72% state AI agents pose a greater risk than machine identities. Factors contributing to AI agents as a security risk include:

- AI agents' ability to access privileged data (60%)
- Their potential to perform unintended actions (58%)
- Sharing privileged data (57%)
- Making decisions based on inaccurate or unverified data (55%)
- Accessing and sharing inappropriate information (54%)

"Agentic AI is both a powerful force for innovation and a potential risk," said Chandra Gnanasambandam, EVP of Product and CTO at SailPoint. "These autonomous agents are transforming how work gets done, but they also introduce a new attack surface. They often operate with broad access to sensitive systems and data, yet have limited oversight. That combination of high privilege and low visibility creates a prime target for attackers. As organizations expand their use of AI agents, they must take an identity-first approach to ensure these agents are governed as strictly as human users, with real-time permissions, least privilege and full visibility into their actions."

Today, AI agents have access to customer information, financial data, intellectual property, legal documents, supply chain transactions, and other highly sensitive data. Yet respondents reported deep concerns over the ability to control the data AI agents can access and share, with an overwhelming 92% stating that governing AI agents is critical to enterprise security. Alarmingly, 23% reported their AI agents have been tricked into revealing access credentials. Additionally, 80% of companies say their AI agents have taken unintended actions, including:

- Accessing unauthorized systems or resources (39%)
- Accessing or sharing sensitive or inappropriate data (31% and 33%)
- Downloading sensitive content (32%)

AI agents are not just part of systems; they are a distinct identity type. With nearly universal plans (98%) to expand their use of agentic AI in the next year, comprehensive identity security solutions that not only govern human identities but also AI and machine identities are essential. These solutions must have the ability to discover all AI agents within the environment, provide unified visibility, enforce zero standing privilege and ensure auditability—helping organizations strengthen security and meet regulatory requirements. In an era of widespread data breaches, poorly governed AI agents only increase risk.

Read the full 'AI agents: The new attack surface. A global survey of security, IT professionals and executives' report.

Methodology

IT professionals responsible for AI, security, identity management, compliance, and operations at enterprise companies representing all seniority levels were invited to participate in a survey on their company's use of AI agents. A total of 353 qualified participants completed the survey, which was conducted by Dimensional Research, an independent third-party. All participants had enterprise security responsibilities. Participants were from 5 continents, providing a global perspective.

About SailPoint

At SailPoint, we believe enterprise security must start with identity at the foundation. Today's enterprise runs on a diverse workforce of not just human but also digital identities—and securing them all is critical. Through the lens of identity, SailPoint empowers organizations to seamlessly manage and secure access to applications and data at speed and scale. Our unified, intelligent, and extensible platform delivers identity-first security, helping enterprises defend against dynamic threats while driving productivity and transformation. Trusted by many of the world's most complex organizations, SailPoint secures the modern enterprise.

View source version on businesswire.com: https://www.businesswire.com/news/home/20250528829358/en/

Media Relations for SailPoint
Samantha Person
Senior Manager, PR & Corporate Communications
512-923-4053
Samantha.Person@SailPoint.com

Source: SailPoint, Inc.