Govern AI agents with confidence

Accelerate AI innovation without compromising your organization

AI agents help enterprises move faster and automate complex workflows — but they also introduce identity and security risks that are difficult to detect and contain. Scaling AI responsibly requires an identity-first approach that keeps every agent visible, governed, and accountable.

Why AI agents demand governance now

Unmanaged agents create risk across security, compliance, and operations:

- **Hidden access risk:** Agents operate across applications, data, and workflows with little visibility into what they can access or do.
- **Over-permissioning:** Agents often hold broader privileges than the people or processes they support, increasing exposure.
- **Limited visibility:** Most organizations lack insight into agent activity, system interactions, and how access is provisioned.
- **Unintended actions:** Agents can act outside their intended scope — accessing, sharing, or triggering things they shouldn't.
- **Compliance exposure:** When agent activity can't be traced, demonstrating regulatory compliance becomes significantly harder.
- **Orphaned agents:** Without clear ownership and lifecycle management, agents retain outdated access long after business needs change.

An identity-first framework for AI governance

Treat every AI agent as a managed identity. Here's how:

- **Discover and classify:** Identify agents across your environment and define them as non-human identities with clear access parameters.
- **Establish ownership:** Assign accountability, set policy frameworks, and keep agents within defined operational boundaries.
- **Use agent-specific authentication:** Implement authentication designed for machine identities, not inherited human credentials.
- **Monitor access and activity:** Track machine-to-machine interactions continuously to detect anomalies and emerging risks.
- **Manage the full lifecycle:** Review access regularly, adjust permissions as needs change, and decommission agents when they're no longer needed.
- **Build in auditability:** Maintain visibility into entitlements, connected systems, and activity histories to support investigations and compliance.

How SailPoint governs the agentic enterprise

SailPoint Agentic Fabric

SailPoint Agentic Fabric is an end-to-end identity security solution built for the age of AI. It gives organizations the visibility, governance, and real-time response needed to secure AI agents at scale — structured around three core pillars:

1

Discovery & Unified Registry

A single source of truth for all governed identities across your digital estate. SailPoint finds agents and contextualizes them within your broader identity landscape — including human identities and data.

2

Real-time Governance & Audit

Brings AI agents under centralized identity governance by treating them as first-class identities. SailPoint enforces ownership, governs access to agents, manages entitlements and machine identities, supports certification, and provides audit evidence — establishing a repeatable governance model for the agentic enterprise.

3

Authorize, Protect & Respond

Proactively detects and responds to AI agent risk through behavioral monitoring, drift detection, prompt security, and targeted remediation.

With SailPoint, AI agents get the access controls and governance they need — so your organization can innovate with confidence.

Scan to gain instant visibility of your AI landscape.
Free trial SailPoint Discovery Tool

About SailPoint

SailPoint (Nasdaq: SAIL) is defining the new era of adaptive identity security. In a world where non-human identities now significantly outnumber humans, our AI-powered platform unifies identity, security, and data intelligence to protect today's enterprise from advanced identity-based threats. We deliver the identity solution that spans both the breadth of identities and the depth of context needed to drive real-time access with confidence. Built on principles like zero-standing privilege and contextualized risk, our SailPoint platform transforms identity from a point of vulnerability into a powerful security advantage. Trusted by many of the world's leading organizations, SailPoint secures the enterprise with intelligent, autonomous identity security.

© 2026 SailPoint Technologies, Inc. All rights reserved. SailPoint, the SailPoint logo and all techniques are trademarks or registered trademarks of SailPoint Technologies, Inc. in the U.S. and/or other countries. All other products or services are trademarks of their respective companies.