

OFFERING 01 / 06

AI Agent & Non-Human Identity Governance

Bring every AI agent, service account, API key and MCP server under ownership and least privilege.

THE CHALLENGE

AI agents, bots and service accounts are multiplying faster than any team can track — most with broad standing permissions, no accountable owner and no visibility in traditional identity governance. SailPoint research finds 97% of AI agents have access to sensitive data, yet only 2% of enterprises have identity security built to govern them.

YOU NEED THIS IF

- › Copilots, agents or MCP servers are rolling out faster than security can review them
- › Secrets, tokens and API keys are scattered across pipelines, vaults and SaaS tools
- › Auditors or the board are asking how AI usage is governed

THE JOINT SOLUTION

Persistent and SailPoint discover every AI agent and non-human identity, map each one to the credentials it uses and the data it can reach, and assign a human owner. Access is right-sized and governed across its lifecycle, with runtime controls to monitor prompts, redact sensitive data and stop rogue agents instantly. Persistent's LLM Firewall extends protection to the model layer.

SailPoint brings

- SailPoint Agentic Fabric — agent, MCP server and credential discovery, incl. shadow AI via endpoint and browser sensors
- Inline prompt security, redaction and agent kill switch
- Agent Audit — framework-aligned compliance evidence
- Entro credential lineage and secret discovery (in Agentic Fabric)

Persistent brings

- NHI and AI agent discovery assessment
- Ownership model and agent lifecycle runbooks
- Integration with CI/CD, vaults, cloud and SaaS sources
- LLM Firewall and Agentic AI Identity Governance (Persistent IP), plus ongoing governance operations

HOW IT WORKS

1 Discover

Inventory agents, MCP servers, service accounts and secrets.

2 Assign

Map credentials to owners and data; score blast radius.

3 Govern

Enforce least privilege, lifecycle policies and runtime controls.

4 Prove

Generate audit evidence and monitor continuously.

BUSINESS OUTCOMES

- ✓ An owned inventory of every AI agent and machine identity
- ✓ Smaller blast radius from over-privileged agents and secrets
- ✓ Confident, governed adoption of agentic AI
- ✓ Audit-ready evidence of AI governance

IDEAL FOR

Enterprises scaling copilots or agentic AI

Regulated industries — banking, insurance, healthcare, life sciences

Organizations with large DevOps and cloud estates

Start with an Identity Posture Assessment

Talk to Persistent's SailPoint specialists about this offering.

info@persistent.com →