Saviynt™

Solution Guide

Identity Security for AI

Identity: The Control Plane for AI

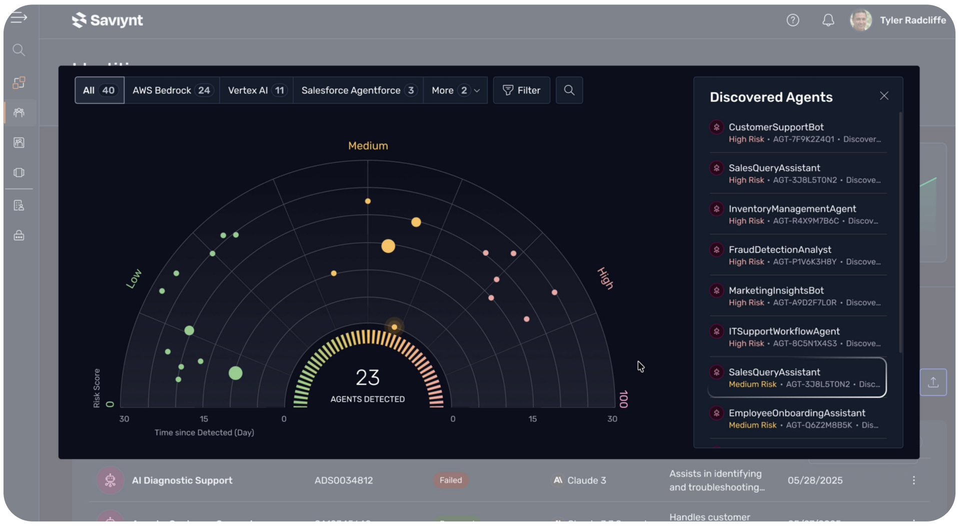
AI agents are contextual and autonomous, making dynamic decisions and accessing systems across the enterprise. Operating at machine speed and scale without direct human oversight, they introduce security challenges that traditional, human-centric identity solutions were never designed to address. Securing AI agents requires identity to evolve into a continuous control layer that provides visibility, governance, and policy enforcement for every action of AI agents. Saviynt delivers a purpose-built identity security platform designed for the speed, scale, and autonomy of AI.

A Purpose-Built Identity Security for AI Ecosystems

AI agents can interact dynamically across applications, other agents, models, and tools, at machine speed and scale. Securing them requires more than extending traditional identity security. Saviynt delivers a purpose-built approach for the autonomy, speed, and complexity of AI agents and their surrounding ecosystem.

Comprehensive Visibility across the Entire AI Ecosystem

Organizations need to comprehend the entire AI ecosystem before they can effectively protect its identities. Saviynt provides deep, platform-agnostic visibility across AI agents, models, MCP servers, tools, and applications, delivering fine-grained access insights and posture intelligence to identify risks and access paths, along with a timeline for agent lifecycle events.



Discovered Agents

- CustomerSupportBot
  High Risk • AGT-7F9K2Z4Q1 • Discover...
- SalesQueryAssistant
  High Risk • AGT-3J8L5T0N2 • Discove...
- InventoryManagementAgent
  High Risk • AGT-R4X9M7B6C • Discov...
- FraudDetectionAnalyst
  High Risk • AGT-P1V6K3H8Y • Discove...
- MarketingInsightsBot
  High Risk • AGT-A9D2F7L0R • Discove...
- ITSupportWorkflowAgent
  High Risk • AGT-8C5N1X4S3 • Discove...
- SalesQueryAssistant
  Medium Risk • AGT-3J8L5T0N2 • Disc...
- EmployeeOnboardingAssistant
  Medium Risk • AGT-Q6Z2M8B5K • Dis...

AI Diagnostic Support	ADS0034812	Failed	Claude 3	Assists in identifying and troubleshooting...	05/28/2025

Saviynt Identity Security for AI:

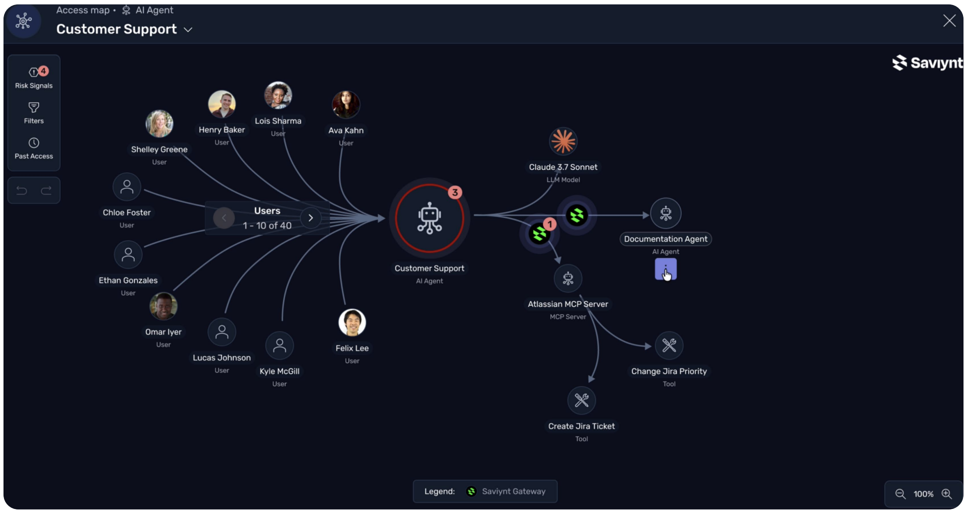
- ✓ **Purpose-built identity security for AI**
  A single, unified platform designed specifically for AI agents and their ecosystem — not an extension of legacy identity tools.
- ✓ **Full visibility across the AI ecosystem**
  Discover and understand agents, models, MCP servers, and tools with deep identity posture insights, including access paths and event timelines.
- ✓ **Fine-grained runtime access control**
  Authorize every AI agent action with application-level controls enforced in real time.
- ✓ **Automated lifecycle governance at AI speed**
  Policy-driven lifecycle management that keeps pace with the speed and scale of AI agents.

Automated, Policy-driven Lifecycle Management

AI agents are created and modified dynamically, which traditional manual governance approaches were never designed to handle. Saviynt automates ownership assignment, succession management, and lifecycle governance through policy-driven controls, ensuring every AI agent remains accountable and governed from creation through retirement.

Fine-grained, Application-level Access Control

AI agents execute actions at high speed across multiple systems, making static permissions insufficient. Saviynt enforces contextual, fine-grained authorization at the application layer, validating every access request in real time to ensure agents operate within approved policies and least-privilege boundaries.



Access Gateway

- **Authentication context:** Detect whether an agent acts independently or on behalf of a human or another agent
- **Access authorization at runtime:** Validate agent access to MCP servers, tools, and applications and enforce only approved interactions.
- **Access scope management:** Enforce fine-grained authorization within applications

Posture Management

- **Discovery & registration:** Detect newly created agents and automatically register discovered agents.
- **Inventory:** Provide a centralized view of identities and findings across AI agents, models, and tools.
- **Risk findings:** Identification of agents without owners and guardrails
- **Access Map:** Visualize how AI agents access applications, data, and tools.
- **Timeline:** Provide a chronological view of agent access and lifecycle events.

Lifecycle Management

- **Ownership management:** Automatically assign ownership (both business owners and technical owners) to specific human identities
- **Label management:** Classify agents and apply custom labels to drive policy enforcement

Next Step

- Vist our webpage www.saviynt.com
- Request a Demo

About Saviynt

Saviynt's AI-powered identity platform manages and governs human and non-human access to all of an organization's applications, data, and business processes. Customers trust Saviynt to safeguard their digital assets, drive operational efficiency, and reduce compliance costs. Built for the AI age, Saviynt is helping organizations safely accelerate their deployment and usage of AI today. Saviynt is recognized as the leader in identity security, with solutions that protect and empower the world's leading brands, Fortune 500 companies, and government institutions. For more information, please visit **www.saviynt.com.**

Saviynt™

Headquarters
1301 E El Segundo Blvd,
Suite D El Segundo, CA 90245
United States

310.641.1664
info@saviynt.com
www.saviynt.com