



Solution Guide

The Enterprise AI Identity Security Platform

Saviynt Zuma – The Control Plane for AI and NHI



Modern enterprises rely on far more than their human workforce. Behind the scenes, countless AI agents and non-human identities are continuously accessing systems, moving data, and executing tasks around the clock. Securing them requires more than static permissions – it requires continuous visibility, runtime control, and end-to-end governance.

Zuma: Purpose-Built Identity Security for AI & NHI

Saviynt Zuma is the enterprise AI identity security platform that enables organizations to confidently adopt and scale AI. It discovers every AI and non-human identity and uncovers shadow AI across the enterprise, protects your environment with runtime control for agent access to enterprise apps and data, and manages accountability across the lifecycle of AI and non-human identities – helping you move from AI sprawl to AI confidence.

Discover

Gain complete visibility into AI agents, non-human identities (NHIs), and their surrounding ecosystem. Zuma automatically discovers AI agents and NHIs across your enterprise, inventories what they can access, and surfaces security and governance risks to eliminate blind spots. Visualize agent/NHI interactions with critical applications, data, and tools through detailed access maps, prioritize risks with continuous posture insights, and track every action and lifecycle event through a comprehensive timeline view.

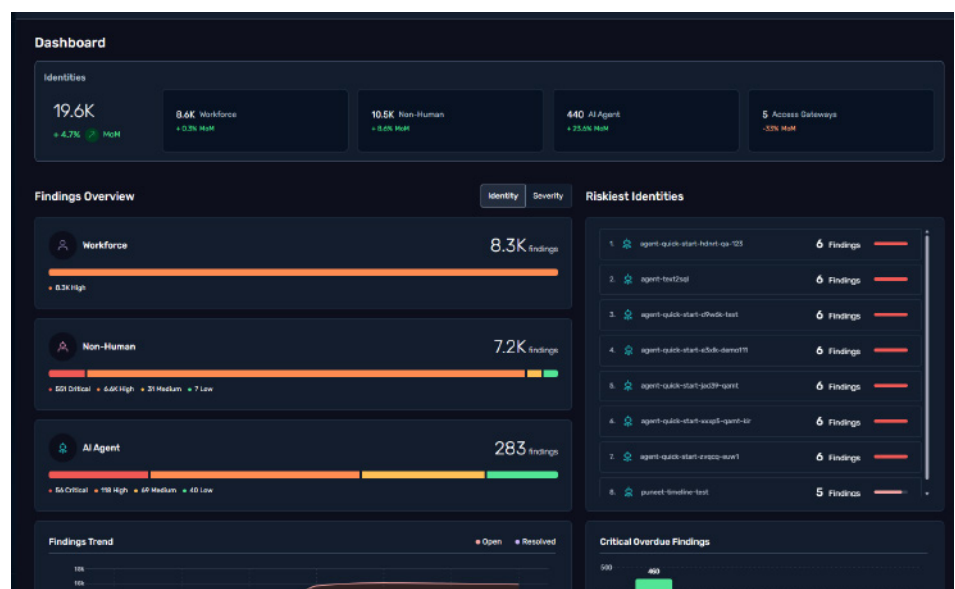
Access

Every AI agent action should be verified before it is executed. Through Saviynt's Agent Access

Gateway, Zuma continuously evaluates identity, intent, context, risk, and policy at runtime to authorize access and enforce Zero Standing Privilege. With intent-aware authorization, custom policy enforcement, and fine-grained application controls, organizations can ensure AI agents operate securely and perform only approved actions.

Manage

Register, govern, and maintain ownership of NHIs and AI agents across their entire lifecycle. Saviynt streamlines agent onboarding, automates ownership and succession management, and governs both



Saviynt Zuma delivers in-depth discovery, access, and management of all AI and non-human identities within your environment.

human-to-agent and agent-to- resource access. Quickly disable or remove unmanaged or orphaned AI agents before they create risk. By continuously identifying orphaned and unmanaged agents and enabling rapid offboarding, Saviynt ensures every AI agent remains accountable, governed, and secure from creation through retirement.

Zuma provides complete AI and NHI security through Discovery, Protection, and Management of all identities.

Zuma Insights

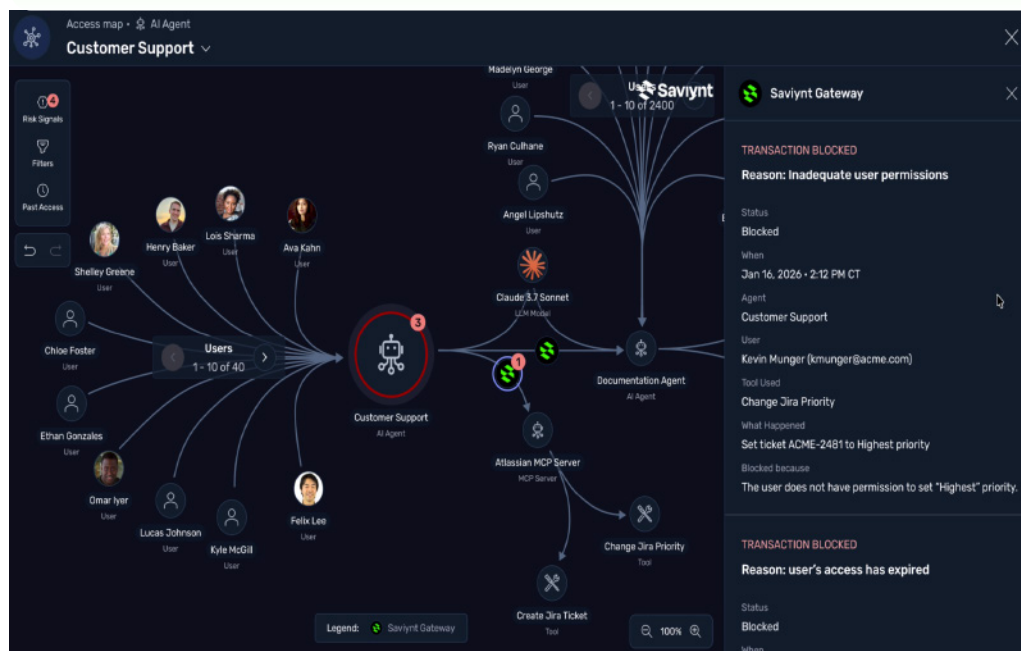
- **Discovery & inventory:** Detect newly created agents and provide a centralized view across NHIs, AI agents, models, and tools.
- **Risk findings:** Identify high-risk AI agents, including orphaned agents or agents operating without appropriate guardrails.
- **Access Map:** Visualize how NHIs/AI agents access applications, data, and tools.
- **Timeline:** A centralized and chronological view of agent access and lifecycle events.

Zuma Access

- **Authentication Context:** Determine whether an agent is acting independently or on behalf of a human or another agent.
- **Intent-Aware Authorization:** Continuously evaluate identity, intent, context, risk, and policy at runtime to authorize every AI agent action.
- **Fine-Grained Access Control:** Enforce granular authorization within applications to ensure agents perform only approved actions.
- **Agent Access Gateway SDK:** Developers can use it to handle policy decisions and enforcement during build time.

Zuma Governance

- **Registration:** Bring every AI agent under governance through a few clicks or API-based onboarding.
- **Ownership management:** Maintain continuous ownership through automated recommendations and succession management.
- **Access Governance:** Streamline request and approval workflows for each human-to-agent and agent-to-resource access.
- **Offboarding:** Quickly disable or remove unmanaged or orphaned AI agents before they create risk.



Zuma's Agent Access Gateway provides intent-aware runtime authorization for all agent actions.

About Saviynt

Saviynt's AI-powered identity platform manages and governs identity 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.

Next Steps

- Visit www.saviynt.com
- Request a [Demo](#)
- [Trial Zuma](#) for 30 days