FOR IT & PLATFORM TEAMS

You Don't Know What AI Your Employees Are Actually Using

Every IT team already fought this battle once for shadow SaaS. AI made it worse — anyone with a browser can run a model, install a coding assistant, or spin up an MCP server, and none of it shows up in your asset inventory. Customers running RuntimeAI's discovery typically find **3–10x more AI surface than they expected.**

Discovery **Shadow AI & Non-Human Identity Registry**

One continuous inventory of every AI agent and every non-human identity — service accounts, API keys, OAuth tokens, machine certificates — in your environment, registered or not.

THE PROBLEM

Shadow AI Is Shadow IT, Again

No Inventory, No Answer

When your CISO asks "what AI is running in our environment," most IT teams don't have a real answer — just a guess based on procurement records that miss anything self-serve.

It's Not Just SaaS Anymore

Local LLM servers, IDE coding assistants, MCP tool clients, and personal-account AI access all run on real endpoints — laptops, servers, VMs — completely invisible to cloud-only discovery tools.

Two Sprawls, One Blind Spot

AI agent sprawl and general non-human-identity sprawl (service accounts, API keys, tokens) are usually tracked in separate tools, if at all — nobody owns the whole picture.

WHAT RUNTIMEAI DOES

Discover, Classify, Control, Prove

STAGE	WHAT HAPPENS
Discover	Cloud environments, developer IDEs, browser extensions, container images, OAuth grants, SaaS integrations, DNS-layer AI traffic, VPC flow logs — plus a real host-level agent that scans any laptop, server, or VM for AI processes, local LLM servers, MCP configs, and exposed credentials
Classify	Every finding lands in one Agent Inventory Dashboard — owner, environment, risk tier, last-seen, sanctioned or not
Control	Hand off to your security team's policy layer with the inventory already built — no re-discovery needed
Prove	The same registry unifies AI agents and general non-human identities (API keys, OAuth tokens, service accounts) — one audit-ready answer, not two separate tools

BEFORE DISCOVERY

Unknown

"We think we know what AI tools are in use" — based on procurement records that miss anything self-serve, personal-account, or endpoint-installed.

→

AFTER A SCAN

3–10x more surface found

A real inventory — every agent and every non-human identity, with owner, risk tier, and last-seen — typically far larger than what procurement records showed.

ONE REGISTRY, NOT TWO

Most platforms treat "AI agent inventory" and "non-human identity governance" as separate problems, sold by separate vendors.

RuntimeAI unifies both — the same registry that tracks a rogue coding assistant on someone's laptop also tracks the orphaned API key nobody rotated in eight months. One dashboard, one owner, one audit answer.

Discovery is **read-only and non-disruptive** at this stage — it tells you what's there before anyone has to decide what to do about it. Control and enforcement are a separate, deliberate next step, handed off to your security team's own policy layer.

WHO THIS IS FOR

Platform & IT Admins
The team that gets asked "what's actually running" and has to answer for shadow IT, now shadow AI

SaaS Governance Owners
OAuth grants, browser extensions, and personal-account access to sanctioned SaaS tools

IAM / NHI Owners
Service accounts, API keys, and machine credentials that sprawl faster than anyone rotates them

Security Team Hand-Off
A ready inventory to govern — IT finds it, security governs it, one shared source of truth

WHY THIS MATTERS TO AN IT LEADER

5-Minute Answer

A new tenant — with RLS isolation, default policy, budget, and RBAC all configured — provisions in about 5 minutes, not a multi-day infrastructure request.

Host-Agnostic Scanning

The same agent that scans a laptop scans a server or a VM — no separate endpoint tooling to license and maintain for each environment type.

Built for the Hand-Off

Discovery output plugs directly into policy enforcement — the same inventory your security team uses to govern, with nothing to re-map or re-discover.

Run a free discovery scan

See your real AI and non-human-identity surface — read-only, non-disruptive, results in minutes.

Roshan Shaik
Founder & CEO · RuntimeAI
roshan@runtimeai.io
www.runtimeai.io
calendly.com/roshan-runtimeai/30min