VIJIL DISCOVER · DATA SHEET

Govern Shadow AI

You Cannot Govern Agents You Cannot See

Shadow AI was already pervasive. Agent sprawl is compounding it. Once frameworks like LangChain, LangGraph, CrewAI, Google ADK, Strands, or the OpenAI Agents SDK are approved internally, agents proliferate across repositories, notebooks, demo branches, cloud environments, and production — faster than governance can follow.

Most organizations have no reliable answer to the questions governance depends on:

- What agents exist, and where are they running?
- Who is accountable for them?
- What identities do they hold, and what tools can they reach?
- What system prompts guide their behavior?
- Which agents have been evaluated for trustworthiness?

The stakes are higher than with third-party GenAI apps. Rogue or compromised agents can cause real damage — but even sanctioned, legitimate agents produce **ungoverned actions**, such as performing inference on sensitive and regulated data.

Turn Agent Inventory Into Agent Governance

Vijil Discover continuously inventories AI agents and workloads across source code repositories and production infrastructure. It walks GitHub organizations to identify repositories using agent frameworks, introspects tools, prompts, and model configurations, then scans cloud infrastructure, Kubernetes services, host runtimes, API gateways, and network-exposed endpoints to find what is actually deployed.

Every discovered workload — inference servers, model APIs, LLM gateways, AI desktop applications, custom agents — is classified with a framework label, a confidence score, and the evidence behind its identification. Results aggregate in real time in the Vijil Console, where security and compliance teams review each finding, assign ownership, and decide whether an agent is banned, approved, or promoted into the Agent Trustworthiness Lifecycle.

Advantages

- **Deep:** Goes beyond SaaS integrations and cloud metadata with Kubernetes service discovery, host-runtime detection, and API gateway auditing.
- **Dual-mode:** Covers both the source and the destination of agents — development environments and runtime infrastructure alike.
- **On-prem deployment:** Runs inside the customer VPC as a scheduled scan. No proxy, gateway, or endpoint agent required.
- **Evidence-based:** Each finding carries a framework label, confidence score, and supporting evidence for review.
- **Accountable:** Attributes ownership so every agent has a named person or team responsible for it.
- **White-box:** Profiles the agent itself - code, tools, prompts, configuration - instead of treating it as a black box to be wrapped in generic guardrails.
- **Lifecycle:** Creates the governed population that GRC workflows and control frameworks depend on.
- **Fingerprint:** Issue cryptographic identity via SPIFFE/SPIRE X.509 SVIDs, not just retrofit IAM.

Close the Agent Visibility Gap

81%
of organizations are deploying or testing AI agents

14.4%
have full security approvals in place

Shadow AI

Unsanctioned third-party agents, embedded SaaS agents, GenAI apps, and custom agents running in production. Detect and stop rogue agents.

Ungoverned AI

Legitimate agents operating without visibility, ownership, or trustworthiness assessment. Profile and register them for the governance lifecycle.

Discovery Coverage

Development

- GitHub scanning
- Framework detection
- Tool introspection
- System prompt discovery
- Ownership attribution

Runtime

- Cloud API enumeration
- AI workload identification
- Endpoint probing
- Exposure analysis
- Shadow AI detection

Agent Trustworthiness Lifecycle

DISCOVER | REGISTER | EVALUATE | PROTECT | MONITOR | ADAPT

Deployment: install Vijil Discover on premises, generate a deploy ID and token, and deploy the scanner agent to your VPC. Example:

```
vijil discover --github-org acme-corp
```

BENEFIT

Vijil Discover is the registry and onboarding layer for the Agent Trustworthiness Lifecycle — the only AI discovery platform purpose-built to convert agent inventory into agent governance.

Gartner COOL VENDOR 2025

CB INSIGHTS AI 100 2025

© 2026 VIJIL