Your agents have an identity crisis.

What verifies who they are and where they run?

WHY IT MATTERS

You can’t trust what you can’t name.

An agent moves money. Drops a table. Emails a customer. Your log shows a shared API key. Which agent? Which instance? No answer. The liability stays with you.

2,488

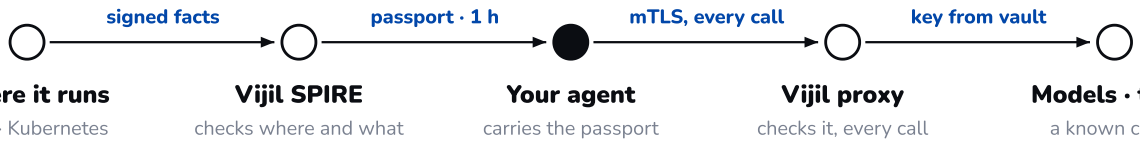
organizations hit by two poisoned LiteLLM releases in March 2026, per Hudson Rock.

October 2026: 49,000 instances potentially exposed all LLM keys and environment variables.

verified by vijil

HOW IT WORKS

Every agent carries a passport. Every call checks it.



Where it runs and what it runs, verified. A SPIFFE identity that dies in an hour. Checked on every call. No key in the agent.

FOR DEVELOPERS

Delete the key.

No secret to fetch. The agent's identity arrives over the SPIFFE Workload API, and any SPIFFE library reads it.

```
$ unset ANTHROPIC_API_KEY
from spiffe import WorkloadApiClient
svid = WorkloadApiClient().fetch_x509_svid()
```

FOR SECURITY LEADERS

One view.

Vijil Discover finds the agents already in your estate, from your identity provider’s consent logs. Then it tells you which ones can prove who they are.

STANDARD	RUNTIMES	PROVES WHERE	PROVES WHAT
SPIFFE, via SPIRE 1.14	EKS · EC2 · AgentCore	AWS-signed identity	Image **sha256** digest
CREDENTIAL	**MODEL KEYS**	**AUDIT**	**FOOTPRINT**
X.509 1 h · JWT 5 min	Secrets Manager, per team	Every call, by instance	One read-only IAM role

START FREE

Your first agent, free forever

READ THE TECH BRIEF

TALK TO US

contact@vijil.ai

vijil.ai