sysdig

Your visual guide to

Detecting and governing shadow AI



Shadow AI is any artificial intelligence an organization uses or runs without security visibility or governance. It spans the tools employees adopt, the models developers build, and the agents that act on their own. But when AI use is invisible, breaches involving it are harder to catch and slower to contain.

The good news: Shadow AI doesn't have to stay invisible. In this guide, we'll walk you through how to detect shadow AI in your environment and how to govern it effectively.

Why shadow AI evades detection



Software

Detection expects a discrete app to inventory. Shadow AI is a feature **inside an already-approved tool**, so there's nothing new to flag.

Data

Detection watches where files live and move. Shadow AI's data **rides inside a prompt**, inside an encrypted request file-focused tools don't read.

Location

Detection watches the network. Shadow AI may run **on a local device or deep in a workload** and barely touch the network.

Identity

Detection assumes a person signs in. Shadow AI authenticates as itself, **a non-human identity**, and those identities multiply faster than teams can track.

How to detect shadow AI

EASY

Network edge

Watch DNS and traffic to known AI services.

✓ Catches — *Confirms AI is being reached*

✕ Misses — *What was sent or returned*

Gateways

Secure web gateway and cloud access broker flag connections to AI apps.

✓ Catches — *The AI people deliberately use*

✕ Misses — *Embedded features and personal accounts*

Identity

Audit the identity provider for broad Auth grants, service accounts, and API keys tied to AI.

✓ Catches

One of the few ways to surface agents before they act

Built layer

Scan code, secrets, package manifests, and pipelines for AI keys, libraries, and calls.

✓ Catches

Inventories what teams created, not just what was downloaded

Runtime

Watch it run. A model processing data, an agent assuming a role and calling systems — behaviors, not artifacts.

✓ Catches

Everything the static layers can't. ***None of it appears in a static inventory.***

HARD

How to govern shadow AI

ENABLEMENT

Make the safe path the easy one

Beat shadow AI on convenience

A sanctioned enterprise AI option that matches the speed people want without the exposure

Keep your data yours

Doesn't train on your data by default

Hand admins the controls

Gives admins control over access and retention

\+

ENFORCEMENT

Constrain what runs anyway

Route AI requests through a gateway so you can inspect them and apply policy in one place.

Scope agent identities so no agent inherits more access than it needs.

Require human approval before an agent takes a consequential or irreversible action.

Set rate limits so a runaway agent can't do much damage before anyone notices.

Ban it

A ban accomplishes neither half of the model. It doesn't earn the choice, and it doesn't constrain what runs. It only takes away what you had.

People keep wanting AI, so the shadow usage continues anyway — now against the rules.

The usage that continues now happens where you can't see it.

sysdig

INFOGRAPHIC

COPYRIGHT © 2026 SYSDIG, INC.
ALL RIGHTS RESERVED.

ING-014 REV. A 09/26

Want to learn more?

Read the full article on shadow AI and how to secure it.

READ THE ARTICLE →