BUILT BY A TEAM THAT HAS SECURED MAJOR INSTITUTIONS WORLDWIDE FOR 25 YEARS.

ARGENT SHADOW AI DISCOVERY

YOU CANNOT GOVERN AI YOU CANNOT SEE. FIND IT FIRST.

Argent Strategic Intelligence finds the AI tools your people already use, from your proxy logs and managed machines, then lets you turn controls on one at a time, with proof of what each would do. Microsoft found **78%** of AI users bring their own AI tools to work,[1] and IBM found incidents involving unapproved ("shadow") AI rose to **43%** of organizations from **20%**.[2]

Three levels, each adding detail. Level 1 reads a copy of your web proxy's logs, with nothing installed. Level 2 adds managed machines. Level 3 registers an agent with a named owner.



SEE.
The AI your proxy logs and managed machines reveal.



PROVE.
Signed records of each sighting and each would-have-refused.



STOP.
Enforce one control at a time, after watching.

HOW SHADOW AI DISCOVERY WORKS

1	**Proxy log feed** Staff paste work into AI sites nobody approved.	**Level 1.** Your proxy sends a copy of its access log to Argent; nothing is rerouted. Argent keeps only visits to AI services in its catalog, drops every other line before anything is stored, and signs the rollups.
2	**Managed machines** A script sends files to an AI service every night.	**Level 2.** Your device management installs the Argent certificate and proxy settings once. Only machines from ranges an administrator approved are admitted. Traffic is tunnelled, never decrypted: Argent sees which AI service a machine reached, not what was said.
3	**Discovered inventory** Nobody can say who owns the coding assistant.	Anything Level 1 or Level 2 sees but nobody registered appears in the Agent inventory tagged **Discovered**, with how it was seen and, for log feeds, the login the proxy named. A quiet feed reads "No data received", never "no AI usage".
4	**Developer registration** A team wants its agent approved, not banned.	**Level 3.** A developer registers the agent with a named owner and installs its certificate. It now has an identity, an owner and a record of every request, and Argent flags it if it starts acting differently.
5	**Watch, then enforce** A control switched on blind refuses real work.	In a new tenant every control starts in **watch**: requests pass unchanged and what each control would have refused or changed is signed on the record. Admins mark samples right or wrong, then switch one control to **enforce** with a passkey check.

WHAT FRAMEWORKS ALREADY ASK FOR

NIST AI RMF, GOVERN 1.6. "Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities."[3]

NYDFS AI guidance (covered banks and insurers). Entities that rely on AI "should maintain an inventory of all such systems"; it adds no new requirements.[4]

HOW A ROLLOUT STARTS

1. Turn on Discovery. Add a log feed under Sources. Your proxy keeps running exactly as it does today.

2. Add machines, then agents. Managed machines from approved ranges, then developers register agents with an owner.

3. Watch, then enforce. Read what each control would have done, then switch them on one at a time.

BOOK A DEMO. WE WILL SHOW YOU ARGENT DISCOVERY WORKING ON YOUR OWN USE CASES.

NYEDIS.AI/DEMO

Sources. 1 Microsoft and LinkedIn, 2024 Work Trend Index Annual Report, May 2024. 2 IBM / Ponemon, Cost of a Data Breach Report 2026, July 2026. 3 NIST AI RMF Playbook, GOVERN 1.6, read 2026-11-19. 4 NYDFS Industry Letter, Cybersecurity Risks Arising from Artificial Intelligence, 2024-10-16.