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

ARGENT AGENT BEHAVIOR WATCH

THE AGENT'S KEY STILL WORKS. ITS BEHAVIOR CHANGED.

Argent Strategic Intelligence learns what normal looks like for each AI agent from its own traffic: which tools it calls, how often, how many tokens, from which networks and clients. When an agent stops behaving like itself, Argent records it, shows what moved, and gives a person the next move. OWASP's 2026 Agentic Top 10 lists rogue agents as a top risk.[1]

It watches how an agent behaves, not what it says. The baseline holds counts and fixed names only, never prompts or content. Every agent that works through Argent is enrolled on its first request, with no setup per agent, and every verdict, hold and release is a signed record.



SEE.
What each agent normally does, and what moved.



PROVE.
A signed record of every verdict and hold.



STOP.
A person, or your chosen policy, holds the agent.

FIVE THINGS IT DOES FOR YOUR TEAM

1	**Learns normal** A claims agent calls the same three tools all day.	Each agent gets its own baseline over ten behaviors, including tools, request and token rates, hours active, scopes, networks, regions, client and credential. A new agent shows WARMING while it learns and is never called drifting too early.
2	**Spots drift** The same agent bursts into a payments export.	Two independent checks must agree, so one noisy signal does not raise an alarm. The agent turns DRIFTING on the Drift view, with up to three behaviors that moved, baseline versus now.
3	**First-seen alerts** An agent calls a tool it has never used.	The first time an agent uses a tool, network, region or client it has never used, Argent files one signed record, even when its counts look normal.
4	**Hold in one step** The security lead wants it stopped while they look.	A person holds the agent for 1, 4 or 24 hours or until released, with a required reason; in Enforce mode the gateway refuses its next request. If the change is legitimate, they accept it as the new normal.
5	**Automatic holds** A team wants drifting agents held without waiting.	Teams can choose to have Argent hold a drifting agent automatically. It releases slowly, only after sustained normal behavior, and a hold placed by a person is never lifted automatically.

WHAT SECURITY GUIDANCE ALREADY NAMES

OWASP Top 10 for Agentic Applications 2026. Lists rogue agents (ASI10), and identity and privilege abuse, where leaked credentials let agents operate far beyond their intended scope.[1]

NYDFS AI guidance, October 2024. Points DFS-regulated companies to monitoring for unusual query behaviors that might indicate an attempt to extract nonpublic information.[2]

HOW A TEAM STARTS

1. Watch mode. Argent learns each agent that works through it and records drift. Nothing is blocked.

2. Decide. People review the Drift view and hold, release or accept each change.

3. Enforce. Switch on refusals area by area, and opt in to automatic holds when ready.

BOOK A DEMO. WE WILL SHOW YOU ARGENT LEARNING YOUR OWN AGENTS' BEHAVIOR.

NYEDIS.AI/DEMO

Sources. 1 OWASP GenAI Security Project, Top 10 for Agentic Applications 2026, Dec 2025. 2 NYDFS Industry Letter, Cybersecurity Risks Arising from Artificial Intelligence, 2024-10-16. Shown: AI traffic routed through Argent; refusals only in Enforce mode.