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

ARGENT FOR AD AGENCIES

AI AGENTS NOW ACT LIKE STAFF. PUT A CHECKPOINT IN FRONT OF EVERY ONE.

Argent Strategic Intelligence puts a checkpoint between your AI agents and the outside AI services they use. It checks every request before it leaves, and it runs entirely inside your own agency. IBM puts ad agencies in an industry whose breach costs rose 20% to $4.71 million,[1] and 43% of incidents now involve unapproved AI.[1]

One pane of glass for your entire agent ecosystem: every agent, model, tool, owner and dollar in one view. **No rip and replace.** Argent works with what you already run: your identity provider (Okta, Microsoft Entra, LDAP), your own secrets vault (HashiCorp Vault, AWS Secrets Manager, CyberArk Conjur) and the AI tools your staff already use.



SEE.
Every agent, its owner, where it sends data.



PROVE.
A signed record of every decision.



STOP.
Unapproved models, tools and leaks are refused.

THE FIVE THINGS AGENCIES ASK FOR FIRST

1	**Budget controls** A pitch agent loops overnight on a paid model.	Set spend caps by team, person and agent. An agent that hits its cap is stopped; its owner asks for more, and nothing is granted until a manager approves, in Argent or through your ServiceNow or Jira tickets. Project cost tracking shows what each campaign or pitch spends on AI.
2	**Data protection** A copywriter pastes a brand's customer list into an AI.	Argent reads each request first and blanks out email addresses, phone numbers and card numbers before anything leaves the agency (a brand's own customer list too, where you register it). The record notes what kind of data, never the data itself.
3	**Auditing for auditors** A brand's lawyer asks which agents touched its customers.	Every AI decision goes into a signed, tamper-evident record that cannot be quietly changed. A client's auditor can check a package of only that client's records on their own computer and see if anything was altered.
4	**Model control** A creative team sends a brief to a model nobody approved.	Once you approve a list, only those models run; everything else is refused. Each brand client can keep its own approved list. A model can be swapped for an approved one without staff changing anything.
5	**Air-gapped** A client's data must never leave your network.	Argent runs entirely inside your own agency, even on a fully air-gapped network. The install bundle is checked at every step as it crosses into your closed environment.

WHAT REGULATORS ALREADY EXPECT

FTC, 16 CFR Part 465. Fake reviews and testimonials, such as AI-generated ones, are banned; the FTC warns of penalties up to **$53,088** per violation.[2]

California CCPA. Fines up to **$2,663** per violation, or **$7,988** if intentional or involving consumers the business knows are under **16**.[3]

HOW AN AGENCY STARTS

1. Watch mode. A real-time audit and view of what your AI is doing today. Nothing is blocked.

2. Enforce mode. Switch on blocking one area at a time: client data, budgets, models, then tools.

3. Inside your walls. Runs on your own hardware or in your own cloud VPC. Nothing leaves the perimeter without your explicit approval.

BOOK A DEMO. WE WILL SHOW YOU ARGENT WORKING ON YOUR AGENCY'S OWN USE CASES.

NYEDIS.AI/DEMO

Sources. 1 IBM / Ponemon, Cost of a Data Breach Report 2026, July 2026 (communications industry, incl. advertising agencies). 2 FTC, final rule banning fake reviews and testimonials, Aug 2024; FTC release, Dec 2025. 3 California Privacy Protection Agency, CCPA penalty amounts from 2025-01-01, read 2026-11-19.