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

ARGENT FOR MEDIA COMPANIES

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 walls. Entertainment breaches now cost $5.38 million on average, up 18% in a year,[1] and 43% of incidents involve AI nobody approved.[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 MEDIA COMPANIES ASK FOR FIRST

1	**Budget controls** A trailer agent loops overnight on a paid model.	Set spend caps by team, person and agent. An agent that hits its cap is stopped; nothing more is granted until a manager approves, in Argent or through your ServiceNow or Jira tickets. Project cost tracking shows what each title spends on AI.
2	**Data protection** An analyst pastes a subscriber email list into an AI.	Argent reads each request first and blanks out email addresses, phone numbers and card numbers before anything leaves the company (your title codes and cast lists too, where you register them). The record notes what kind of data, never the data itself.
3	**Auditing for auditors** Business Affairs asks which agent had the script, and when.	Every AI decision goes into a signed, tamper-evident record that cannot be quietly changed. Counsel or internal audit can check a package of it on their own computer and see whether anything was altered.
4	**Model control** A data agent sends a table to a model nobody approved.	Once you approve your models, everything else is refused. Group them into model classes, such as approved for unreleased work and general use. A model can be swapped for an approved one without staff changing anything.
5	**Air-gapped** An unreleased season must never leave the building.	Argent runs entirely inside your own company, 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

Video Privacy Protection Act. A person whose video viewing records are wrongfully disclosed can sue, and a court may award at least **$2,500** in damages.[2]

FTC children's privacy rule (COPPA). Parents must consent before data is collected from a child under **13**; a knowing violation can cost up to **$53,088** each.[3]

HOW A MEDIA COMPANY 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: subscriber 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 COMPANY'S OWN USE CASES.

NYEDIS.AI/DEMO

Sources. 1 IBM / Ponemon, Cost of a Data Breach Report 2026, July 2026 (entertainment industry; shadow AI across all industries). 2 18 U.S.C. 2710(c), U.S. Code, GovInfo, read 2026-11-13. 3 16 CFR 312.5 (COPPA Rule) and 16 CFR 1.98(d) (FTC civil penalties), eCFR, read 2026-11-13.