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

ARGENT FOR SPORTS TEAMS

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 inside your own walls. In IBM's entertainment category, sports included, a breach averages $5.38 million; 92% of organizations with an AI-related breach lacked AI access controls.[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 SPORTS TEAMS ASK FOR FIRST

1	**Budget controls** Ticketing agents loop during an on-sale and run up a bill.	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.
2	**Data protection** An analyst pastes a player's diagnosis code into an AI.	Argent reads each request first and blanks out card and Social Security numbers. With the healthcare set on and the Sports pack in Enforce, labelled medical record numbers, diagnosis codes, ticket numbers and athlete IDs go too. The record names the kind of data, never the data.
3	**Auditing for auditors** A league partner asks which agent sent what, and when.	Every AI decision goes into a signed, tamper-evident record that cannot be quietly changed. An auditor or internal audit can check a package of it on their own computer and see whether anything was altered.
4	**Model control** A pricing agent runs on an AI model nobody approved.	Only models you approve are allowed; everything else is refused. Group them into model classes, such as approved for fan data and general use. A model can be swapped for an approved one without staff changing anything.
5	**Air-gapped** Player medical data must never leave the club's network.	Argent runs entirely inside your own organization, 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

ADA, 29 CFR 1630.14. Worker medical records stay confidential, in separate files; a large employer can owe up to **$300,000** in damages per person who sues.[2]

State breach laws. In Florida, Colorado and Washington, the people affected by a breach must be told within **30** days.[3]

HOW A CLUB OR LEAGUE 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: fan 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 CLUB'S OR LEAGUE'S OWN USE CASES.

NYEDIS.AI/DEMO

Sources. 1 IBM / Ponemon, Cost of a Data Breach Report 2026, July 2026 (entertainment average; AI access controls, all industries). 2 29 CFR 1630.14(b)(1) and (c)(1); 42 U.S.C. 1981a(b)(3)(D), Cornell LII, read 2026-11-19. 3 Fla. Stat. 501.171(4)(a); C.R.S. 6-1-716(2)(a); RCW 19.255.010(8), read 2026-11-14.