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

ARGENT FOR HIGHER EDUCATION

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 AI services they use. It checks every request before it leaves and runs inside your own university. 94% of higher-education staff surveyed had used AI for work; only 54% knew a policy for it,[1] and an education breach averages $4.15 million.[2]

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 UNIVERSITIES ASK FOR FIRST

1	**Budget controls** A research lab's agent runs up a large bill overnight.	Set spend caps by team, person and agent. An agent that hits its cap is stopped; its owner asks for more, and a manager must approve, in Argent or through your ServiceNow or Jira tickets. Project cost tracking shows AI spend by project or department.
2	**Data protection** An aid advisor pastes an award letter into an AI.	Argent reads each request first and blanks out Social Security, card and labeled bank account numbers before anything leaves, and student IDs once you add your ID format as a pattern. The record notes the kind of data, never the data.
3	**Auditing for auditors** The provost 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** Staff start using an AI model nobody approved.	Only models you approve are allowed; everything else is refused. Group them into model classes, such as approved for student data and general use. A model can be swapped for an approved one without staff changing anything.
5	**Air-gapped** Research data must never leave the building.	Argent runs entirely inside your own university, 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

GLBA Safeguards Rule, 16 CFR 314.4. Federal-aid colleges must tell the FTC within **30** days of discovering that unencrypted data of **500+** customers was taken.[3]

FERPA, 34 CFR 99.31. A school must use reasonable methods so its staff reach only the student records they have a legitimate educational interest in.[4]

HOW A UNIVERSITY 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: student data, budgets, models, then tools.

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

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

NYEDIS.AI/DEMO

Sources. 1 AIR with EDUCAUSE, NACUBO and CUPA-HR, AI at Work in Higher Education survey, Jan 2026. 2 IBM / Ponemon, Cost of a Data Breach Report 2026, July 2026. 3 16 CFR 314.4(j)(1), eCFR, read 2026-11-14; Federal Student Aid Handbook 2026-27, Vol. 2 Ch. 7. 4 34 CFR 99.31(a)(1)(ii), eCFR, read 2026-11-14.