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

ARGENT FOR NONPROFITS

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 organization. 55% of nonprofits are using or piloting AI,[1] and across industries 43% of security incidents now involve AI nobody approved.[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 NONPROFITS ASK FOR FIRST

1	**Budget controls** A fundraising agent runs up a large bill nobody funded.	Set spend caps by department, 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 project or department spends on AI.
2	**Data protection** A caseworker pastes a family's case details into an AI.	Argent blanks out Social Security, card and account numbers, emails and phones before a request leaves (donor IDs, grant IDs and case numbers too, with the Nonprofits pack). The record keeps the kind of data, never the data itself.
3	**Auditing for auditors** A funder asks which AI saw the families' data.	Every AI decision goes into a signed, tamper-evident record that cannot be quietly changed. A funder's reviewer or your auditor can check a package of it on their own computer and see whether anything was altered.
4	**Model control** A donor file goes to an AI model nobody approved.	Only models you approve are allowed; everything else is refused. Group them into model classes, such as approved for donor data and general use. A model can be swapped for an approved one without staff changing anything.
5	**Air-gapped** Beneficiary case files must never leave your network.	Argent runs entirely on your own network, even a fully air-gapped one. The install bundle is checked at every step as it crosses into your closed environment.

WHAT FUNDERS AND REGULATORS EXPECT

Federal award rules, 2 CFR 200.303(e). A federal award requires "reasonable cybersecurity and other measures" to safeguard information, including personal data.[3]

New York, Gen. Bus. Law 899-aa. Tell affected New Yorkers within **30** days of discovery; a knowing or reckless failure can cost up to **$250,000**.[4]

HOW A NONPROFIT 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: donor and family 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 ORGANIZATION'S OWN USE CASES.

NYEDIS.AI/DEMO

Sources. 1 Salesforce, Nonprofit Trends Report, 7th edition, 2025. 2 IBM / Ponemon, Cost of a Data Breach Report 2026, July 2026, all industries studied. 3 2 CFR 200.303(e) and 200.1, eCFR, read 2026-11-19. 4 N.Y. Gen. Bus. Law 899-aa(2) and (6)(a), NY State Senate, read 2026-11-14.