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

ARGENT AUDIT EVIDENCE

AUDITORS ASK WHAT YOUR AI DID. HAND THEM PROOF THEY CAN CHECK.

Argent Strategic Intelligence puts a checkpoint between your AI agents and the AI services they use, and writes a signed record of every decision it makes. Each record is linked to the one before it, so a changed record shows. When an auditor asks what your agents did last month, one click builds the evidence package.

The auditor checks it themselves. On their own machine, with no connection to Argent, they match the package's key against one their firm already holds, then run the verifier. Every record checks out, or the check fails and names the file. No screenshots, no spreadsheets, no taking your word for it.



SEE.
Every decision on traffic routed through Argent.



PROVE.
A signed package the auditor checks offline.



STOP.
By default, a request is refused if its record cannot be taken.

THE FIVE THINGS AUDITORS ASK FOR FIRST

1	**A signed record** Which agent sent what, and when?	Every decision Argent makes on traffic routed through it, and every admin change made in the console, is written as a signed record linked to the one before it. A record that cannot be signed is not written. Each UTC day is sealed.
2	**One-click package** The auditor wants last month, in one file.	On Evidence, Exports, the auditor picks a past period and sees what the package will hold: rows and files. One click on BUILD PACKAGE downloads a ZIP of signed records, keys, a signed manifest and a README.
3	**Offline check** Can't the vendor just hand over a clean file?	The auditor runs the verifier on their own machine, against a key confirmed from their own records. In a company package, a missing, extra, reordered or altered record fails the check and the file is named.
4	**Copies taken** Who took a copy of the evidence?	Building a package is recorded in the signed log before a byte leaves; if that record cannot be written, nothing is exported. Copies taken lists who, when, scope, rows, size and SHA-256.
5	**Read-only auditor** The external auditor needs access, not admin rights.	The Auditor role is read-only: it reads the record and builds packages for its own company only, whole company or one agent, up to 31 days. Rows that look like secrets are held back and listed.

WHAT AUDITORS ALREADY EXPECT

HIPAA Security Rule, 45 CFR 164.312(b). Covered entities must have mechanisms that "record and examine activity" in systems that contain or use electronic protected health information.[1]

NYDFS, 23 NYCRR 500.6. Covered entities must keep audit trails designed to detect and respond to cybersecurity events, and keep those records at least **3** years.[2]

HOW AN AUDIT RUNS

1. Grant access. Give the auditor a read-only Auditor account for your company.

2. Build. On Evidence, Exports: pick a past period, check the preview, click BUILD PACKAGE.

3. Check. The auditor confirms the key from their own records and runs the offline verifier.

BOOK A DEMO. WE WILL SHOW YOU A PACKAGE BUILT AND CHECKED, END TO END.

NYEDIS.AI/DEMO

Sources. 1 45 CFR 164.312(b), HIPAA Security Rule, Technical safeguards (law.cornell.edu, read 2026-11-19). 2 23 NYCRR 500.6, NYS DFS, Part 500 as amended 2023-11-01 (dfs.ny.gov, read 2026-11-19). Shown: AI traffic routed through Argent, for past sealed days.