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

ARGENT WATCHES FIRST

SEE WHAT EACH CONTROL WOULD DO. THEN ENFORCE IT.

Argent Strategic Intelligence puts a checkpoint between your AI agents and the AI services and tools they use. Twelve of its controls each have their own WATCH / ENFORCE switch. In watch, a control runs its full check, sends the request on unchanged and signs what it would have refused or changed. A new tenant starts with every control in watch.

Evidence before every switch. NIST asks teams to analyze a change's security and privacy impact before making it.[1] The Rollout page shows that impact on your own traffic: for each control, what it would have refused or changed, which agents it touched, and samples your admins mark right or wrong.

SEE.
Would-refuse and would-change counts per control.

PROVE.
Signed record of what controls would do, and each switch.

STOP.
Enforce one control at a time, by passkey.

FIVE THINGS TO KNOW ABOUT WATCH MODE

1	**Untouched traffic** An agent drafts a loan summary holding a customer's SSN.	In watch, DLP (Data Loss Prevention) finds the number exactly as it would in enforce, and the model receives the agent's original request. The signed record names the kind of data and the count, never the value.
2	**The Rollout page** The CISO asks what DLP would have caught this week.	For each control: would-refuse and would-change counts, a trend, the agents it touched and sample events, with BEFORE and AFTER text where prompt capture is on. A check that could not run reads could not measure, never clean.
3	**Right or wrong** A sample was flagged that should not have been.	Admins mark each sample RIGHT or WRONG, and each label is a signed admin event. After five labels the page shows how often that control was wrong, and the enforce dialog repeats how many labelled samples were marked wrong.
4	**Passkey flips** DLP is ready; the other controls are not.	Before enforcing, the dialog states what the control would have refused in the last 7 days. A fresh passkey check signs every change, in both directions, and it applies live. The other eleven controls keep watching.
5	**Still enforced** Someone asks whether watch opens the doors.	People keep every restriction. Revoked keys and disabled agents are refused; quarantine, the kill switch and the emergency spend cap still hold; the Audit Ledger signs every decision whatever mode a control is in.

THE PRACTICE IT SUPPORTS

NIST SP 800-53, control CM-4. "Analyze changes to the system to determine potential security and privacy impacts prior to change implementation."[1]

Shadow AI is growing. IBM found security incidents involving unapproved AI more than doubled, to **43%** from **20%**; **92%** of organizations with an AI-related breach lacked proper AI access controls.[2]

HOW A TEAM STARTS

1. Watch. Route agents through Argent. Every control starts in watch, and Rollout fills with what each would have done.

2. Judge. Read seven days of your own traffic and mark the samples right or wrong.

3. Enforce. Flip one control at a time by passkey, with a signed record of every flip.

BOOK A DEMO. WE WILL SHOW YOU WATCH MODE WORKING ON YOUR OWN USE CASES.

NYEDIS.AI/DEMO

Sources. 1 NIST SP 800-53 Rev. 5 (Update 1), control CM-4 Impact Analyses, csrc.nist.gov. 2 IBM / Ponemon, Cost of a Data Breach Report 2026, July 2026 (602 organizations, March 2025 to February 2026).