The agentic identity company.

We manage and protect every AI agent you run, on any platform, from creation to revocation.

THE CHALLENGE

AI agents arrived. Accountability didn't.

Most teams still can't answer:

01

Where are your AI agents, and who owns them?

Every platform keeps its own list. An agent on a shared key or someone else's token leaves no trace of an owner.

02

What are they allowed to do?

Access doesn't equal control. The same permission that lets an agent read an invoice lets it send a payment.

03

How do you stop a risky action before it runs?

Logs tell you what an agent did after the fact. By then, the damage is done.

WHAT WE DO

One platform to secure the entire agent lifecycle.

CREATION → REVOCATION

Detect	Create	Authenticate	Authorize	Secure	Revoke

Know your agents and their owners.

Find every agent on any cloud, platform or laptop. Give each one its own identity and an owner whose access is its ceiling. When the owner leaves, suspend the agent until you reassign or revoke it.

Control what each agent can access and do.

Write one natural-language policy for every connected platform, and test it against real sessions before it goes live.

Assess risk and escalate to a human when needed.

Evaluate each call against policy and security signals. Routine actions run, sensitive ones wait for approval, and risky actions are blocked.

HOW IT WORKS

Every agent gets its own identity. Every call proves it.

Every decision is recorded: which agent acted, for whom, what it asked, the policy enforced and any human decision.

1 · VERIFY THE AGENT

AGENT ID — Issued by NewCore

SR **Spend Reconciler**
`nc:agent/spend-reconciler`

Client	Claude
Owner	DL Dana Levi
Token	one per call · 9 min

Agents get access. They never hold your credentials.

2 · CHECK POLICY AND SIGNALS

NEWCORE POLICY ENGINE — Active

Finance guardrails

Every connected platform

WRITTEN AS

"Read invoices. Payments above $25,000 need approval. Never change payment details."

ENFORCED AS

Read invoices	Allow
Payments above $25,000	Ask
Change payment details	Deny

SECURITY SIGNALS

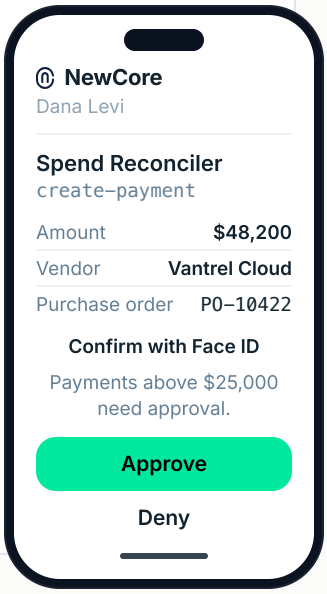
EDR / XDR · DLP · DSPM · Device trust · AI guardrails

3 · ENFORCE THE DECISION

Read invoices — Runs

Send a $48,200 payment

Held for approval



Change payment details — Blocked

WORKS WITH THE STACK YOU RUN

Microsoft Entra ID · okta · CROWDSTRIKE · WIZ · Microsoft Purview · cyera · splunk> by cisco · and more

> *It accelerates my speed to deploying agentic capabilities, and so that's the business value.*
>
> AM LAW 50 CISO

ABOUT NEWCORE

NewCore is the agentic identity company. We manage and protect every AI agent, on any platform, from creation to revocation. Founded by cybersecurity veterans and Unit 8200 alumni, and backed by Cyberstarts, Index Ventures and Evolution Equity Partners.

Secure every agent. Govern every action.

Book a Demo →