Agentic AI Raises Infrastructure Considerations Around Action Authorization

mEinstein explores how human-controlled, revocable permissions can govern AI agents, ensuring every automated action has legitimate authorization.

BOSTON, MA, UNITED STATES, November 4, 2026 /EINPresswire.com/ -- As artificial intelligence moves from answering questions toward taking actions, a new infrastructure challenge is emerging: how AI systems obtain human authorization when enterprise workflows reach an individual.

AI agents can increasingly reason, call software tools, retrieve information, prepare transactions and execute workflow steps. But capability alone does not establish authority.

> Agentic AI needs a Human Trust & Action Layer, A trusted boundary where machine intelligence can meet human context without overriding human agency."
>
> *Prithwi R. Thakuria, Founder & CEO of mEinstein*

"AI agents are getting very good at figuring out what to do," said Prithwi Thakuria, Founder & CEO of mEinstein. "That is not the same as having the right to do it."

The distinction is particularly important in regulated and personal workflows such as healthcare, financial services, clinical research and mobility, where AI may require access to private context or approval to take an action.

mEinstein refers to this challenge as the human permission problem.

Traditional digital consent is typically expressed through terms of service, privacy notices and checkboxes. Agentic AI may require a more granular system capable of defining who is requesting access, what information or action is needed, for what purpose, for how long, and whether that authorization can later be revoked.

“A checkbox is not a permission architecture for agentic AI,” Thakuria said. “Agents need purpose-bound, revocable and auditable authority.”

mEinstein is developing a Human Intelligence Infrastructure architecture that connects enterprise workflows to a user's private, on-device Algorithmic Self-Portrait through a governed permission bridge.

The architecture allows enterprise requirements to be translated into Human Context Contracts specifying purpose, requested context, actions, retention and other terms. AI can assist in interpreting the request, while deterministic rules govern execution.

The company summarizes the principle as: “AI interprets. Rules govern. Device executes.”

One potential benefit of this model is data minimization. Enterprise systems may not always need access to raw personal information. In some cases, a workflow may only require a verified answer, qualification result, proof or authorized action.

“The enterprise often does not need the person's entire data footprint,” Thakuria said. “It may need one verified answer, one approved context packet or one authorized action.”

mEinstein's current architecture includes live core contract-to-device capabilities, while agent-native intake, richer contract intelligence, permission binding and additional automation remain areas of productization.

The broader question extends beyond mEinstein as the AI industry shifts toward increasingly autonomous systems.

The first generation of AI focused on whether machines could understand information. Agentic AI increasingly asks whether machines can act.

The next infrastructure question may be whether AI systems can prove that their actions are grounded in legitimate human authority.

Prithwi Thakuria
mEinstein
+1 703-517-3442
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
TikTok

X

This press release can be viewed online at: https://www.einpresswire.com/article/954383554

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.