

Amadeo Pérez, CEO of XTechAI: AI Agents Need Stronger Enterprise Controls

Amadeo Pérez warns that AI agents need strict permissions, human oversight and security controls as they move from answering to acting.

MÁLAGA, SPAIN, October 6, 2026 /EINPresswire.com/ -- Artificial intelligence is moving beyond systems that simply generate answers and toward AI agents capable of using tools, accessing business software and executing actions.



Amadeo Pérez CEO XTechAI

Amadeo Pérez, founder and CEO of [XTechAI](#), believes this transition could unlock major productivity gains, but also create a new category of enterprise risk if companies give AI systems excessive access to email, CRM platforms, databases, servers or other critical systems.

“

The question is no longer only what AI can do, but what we are allowing it to do.”

Amadeo Pérez, Founder & CEO of XTechAI

“The question is no longer only what AI can do, but what we are allowing it to do,” Amadeo Pérez said.

AI Is Moving From Answering to Acting

Traditional generative AI usually follows a simple model: a user makes a request, the system generates an answer and a person decides what to do next.

AI agents introduce a different model. An agent can receive an objective, determine which tools it needs, consult information and execute a sequence of actions.

In a commercial workflow, for example, an agent could analyze an incoming inquiry, locate a customer in a CRM, review previous interactions, prepare a proposal and update an opportunity.

“The biggest change will not simply be that artificial intelligence answers better. It will be that it

starts acting,” Amadeo Pérez said.

XTechAI works across artificial intelligence, automation, IT consulting and [custom software development](#), areas that Amadeo Pérez believes will increasingly converge as AI becomes integrated into enterprise infrastructure.

AI Agents Should Follow the Principle of Least Privilege

Amadeo Pérez argues that companies should apply a principle already familiar to cybersecurity teams: least privilege.

An AI agent should receive only the permissions required to perform its specific role.

A system that needs to read information does not automatically need permission to modify it. An AI agent preparing an email does not necessarily need authorization to send it, while a system working with a CRM may need access to specific records without having permission to delete them.

Sensitive operations can remain subject to human approval.

“Today, I am more concerned about an AI system with too many permissions inside a company than about a hypothetical conscious machine,” Amadeo Pérez said.

Human Oversight Will Remain Essential

Amadeo Pérez expects companies to deploy different levels of autonomy depending on risk.

Low-risk tasks may be completed automatically. Other actions can be prepared by an AI agent but require human validation before execution. Higher-risk operations involving sensitive data, financial systems, permissions or important decisions should remain under stronger supervision.

Companies will also need clear records showing what each agent has done, which information it accessed, which tools it used and who authorized important actions.

Logging, traceability and recovery mechanisms will become increasingly important as AI gains operational access.

AI and Cybersecurity Are Converging

As AI agents connect to real systems, artificial intelligence and cybersecurity become increasingly difficult to separate.

A system that generates text creates one type of risk. A system capable of interacting with credentials, databases, APIs, servers and enterprise software creates another.

The same AI technology that can help defenders identify vulnerabilities can also strengthen phishing campaigns, automate malicious activity or produce fraudulent content at scale.

Recent warnings from inside the AI industry have added urgency to the debate. Former Anthropic researcher Jacob Coxon resigned in September 2026 while publicly raising concerns about the safety and control of increasingly capable AI systems.

Amadeo Pérez believes such warnings should be taken seriously without automatically treating the most extreme scenarios as inevitable.

“There is a major difference between recognizing that a risk exists and assuming that it will necessarily happen,” Amadeo Pérez said.

AI, Automation and Employment

A report released by U.S. Senator Bernie Sanders warned that AI, automation and robotics could potentially replace nearly 100 million U.S. jobs over the coming decade.

Amadeo Pérez believes technological transformation and labor disruption can exist at the same time.

Some tasks will disappear, some professions will change and new roles will emerge. The central question is how workers and companies manage the transition.

“The problem is not using AI to eliminate repetitive work or increase productivity. The risk appears when the only objective is replacing people without considering how workers and companies will adapt,” Amadeo Pérez said.

Europe Faces the Challenge of Regulating AI Without Stopping Innovation

Europe is building a risk-based regulatory framework through the EU AI Act.

Amadeo Pérez supports distinguishing between different levels of risk rather than regulating every use of artificial intelligence in the same way.

Using AI to summarize a document is fundamentally different from allowing a system to make important decisions about people, manage highly sensitive information or interact with critical infrastructure.

Amadeo Pérez believes regulation will need to evolve alongside AI while avoiding unnecessary

barriers to European innovation.

AI Will Eventually Become Invisible Infrastructure

Over time, Amadeo Pérez expects companies to stop treating artificial intelligence as a separate product category.

AI will increasingly become part of CRM systems, internal applications, mobile apps, analytics platforms and custom software.

XTechAI's [artificial intelligence consulting](#) work focuses on practical use cases where AI can improve productivity, analysis or automation while maintaining appropriate levels of security and human oversight.

Its custom software development operations combine traditional software architecture, automation and AI to create business systems capable of interacting with increasingly intelligent tools.

Amadeo Pérez believes the competitive divide will eventually shift.

It will no longer be between companies that use artificial intelligence and companies that do not.

It will be between organizations that integrate AI with reliable data, strong security, well-designed processes and appropriate human oversight — and those that simply add AI without understanding why they need it.

About XTechAI

XTechAI is a Spanish technology holding company specializing in artificial intelligence, IT consulting, automation, custom software development and digital transformation.

Led by founder and CEO Amadeo Pérez, XTechAI helps businesses design, integrate and scale practical technology solutions.

Amadeo Pérez recently discussed AI agents, employment, cybersecurity, regulation and the future of artificial intelligence in an interview and article distributed by Europa Press in Spain.

Amadeo Pérez Mariscal

XTechAI

+34 643 93 21 21

amadeo.perez@xtechai.eu

Visit us on social media:

LinkedIn
Bluesky
Instagram
Facebook
YouTube
X
Other

This press release can be viewed online at: <https://www.einpresswire.com/article/947772237>

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.