EINPRESSWIRE

XMPro Named a Sample Vendor for Agentic AI in the Gartner® Hype Cycle™ for AI and Cybersecurity, 2025

XMPro, selected as a Sample Vendor for Agentic AI, believes this recognition highlights our focus on secure, governed, and explainable agentic AI.

Press Release
XMPro Named a Sample Vendor for Agentic AI in the Gartner® Hype Cycle™ for AI and Cybersecurity, 2025
XMPRO

XMPro Named a Sample Vendor for Agentic AI in the Gartner® Hype Cycle™ for AI and Cybersecurity, 2025

DALLAS, TX, UNITED STATES, August 25, 2025 /EINPresswire.com/ -- XMPro, a provider of industrial AI software, today announced Gartner named it a Sample Vendor for Agentic AI in the "Hype Cycle for AI and Cybersecurity, 2025" report published August 7, 2025.

The report warns that “but this rapid enterprise adoption of emerging AI features, applications and agents, fueled by large language models (LLMs) and other AI models, outpaces the maturity of security controls and challenges existing best practices”, while noting that “the frenzy of AI messaging — sometimes coined as ‘AI washing’ and ‘AI agent washing’ — is showing in every area of cybersecurity, with technology providers quickly shifting their message from ‘cybersecurity AI assistants’ to ‘agentic AI’.”

In our opinion, XMPro's recognition underscores its alignment with Gartner's analysis: that enterprises adopting agentic AI must address governance, trust, and security from the outset to avoid the risks of uncontrolled autonomy and "agent washing."

Gartner positions agentic AI "At the Peak" with a "Transformational" benefit rating, noting "the agentic AI trend has seen a rapid surge of interest, with AI-agent-related inquiries increasing by 750% in 2024. " (1) The report emphasizes the need for AI Trust, Risk and Security Management (AI TRiSM) and warns that "the increased autonomy of AI agents means they present a series of new risks above and beyond the ones that come with using stand-alone AI models and GenAI assistants. "

XMPro's APEX (Agent Platform EXperience) provides the enterprise-grade orchestration layer for agentic AI, centralizing governance, observability, and lifecycle management. APEX enables supervisory control tower views so enterprises can monitor agent performance, enforce policies, and ensure reliable, explainable operations at scale. XMPro's Multi-Agent Generative Systems (MAGS) framework addresses these AI TRiSM requirements through cognitive agent teams with bounded autonomy, explainability, and separation of intent from action, ensuring safe and reliable performance in cyber-risk-sensitive environments.

> “
>
> Our APEX and MAGS frameworks address these AI TRiSM requirements by embedding bounded autonomy, explainability, and oversight into agent teams”
>
> *Pieter Van Schalkwyk - XMPro CEO*

"In our opinion, Gartner's research highlights that the increased autonomy of AI agents creates new risks that require robust governance and oversight," said Pieter van Schalkwyk, CEO of XMPro. "Our APEX and MAGS frameworks address these AI TRiSM requirements by embedding bounded autonomy, explainability, and oversight into agent teams — making them safe and reliable for mission-critical operations."

According to Gartner: “AI security posture management extends the traditional cloud security posture management tooling to AI workloads. When involved early in the development cycle, cybersecurity leaders can mandate good data security governance practices, and work with AI teams to see how they can leverage synthetic data to minimize privacy and confidentiality risks.” (1)
XMPro addresses this through a layered approach built into its decision intelligence architecture, which integrates directly with OT and enterprise systems.

• Architectural Guardrails: Governed data pipelines (via Data Stream Designer) and deterministic policy rules constrain what data, tools, and actions agents can access.
• Collaborative Safeguards: MAGS enforces team-level consensus, approval and override flows, and separation of decision intent from execution to keep autonomy bounded.
• Supervisory Oversight: APEX Control Tower views provide continuous monitoring, intelligent alerting, and full audit trails so agent behavior remains transparent, compliant, and within defined limits.

Together, these mechanisms ensure that XMPro’s agents operate predictably and safely in cyber-risk-sensitive environments, delivering the trust and accountability that Gartner identifies as critical for scaling agentic AI.

According to Gartner, “AI governance platforms are emerging as a distinct market that combines traditional governance, risk and compliance product capabilities with automating and enforcing essential governance rules to verify that AI is safe, valuable and performing as intended.” (1)
XMPro's approach helps organizations embed governance and explainability into AI-driven operations from the design phase rather than retrofitting security controls after deployment.

XMPro is helping enterprises move from AI pilots to governed, production-scale autonomy — setting the standard for secure, explainable, and trustworthy AI adoption across industries where security and reliability cannot be compromised.

(1) Source: Gartner, Hype Cycle for AI and Cybersecurity, 2025, Jeremy D'Hoinne, Manuel Acosta, Josh Murphy, 7 August 2025.

Gartner Disclaimer: Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

About XMPro
XMPro provides intelligent business operations solutions that help asset-intensive industries optimize performance through AI-powered decision support and autonomous operations management. The company's Intelligent Business Operations Suite (iBOS) combines agentic AI with real-time data integration to deliver autonomous operational intelligence and decision-making capabilities. XMPro's APEX platform enables the creation and management of specialized AI agent teams that can perceive, decide, and act autonomously in complex industrial environments. XMPro serves Fortune 500 companies across manufacturing, mining, energy, utilities, and other asset-intensive sectors. Headquartered in Dallas, Texas, XMPro has been solving complex challenges for global industrial companies since 2009.

Media Contact:

Wouter Beneke - Marketing Lead
XMPro
email us here
Visit us on social media:
LinkedIn
Facebook
YouTube
X