Cognizant Launches Secure AI Services to Help Enterprises Safely Scale Agentic Systems

New offering delivers AI-powered defense across the enterprise and supports the practice of provable trust for AI systems

TEANECK, N.J., May 7, 2026 /PRNewswire/ -- Cognizant (NASDAQ: CTSH) announced the launch of Cognizant Secure AI Services, a new integrated offering designed to help enterprises secure, govern and scale AI and agentic systems across their operations.

As AI systems move into enterprise-wide deployment, organizations are embedding AI into decision-making, automation, customer engagement and core workflows. Increasingly, these systems bring autonomous and agentic capabilities that can reason, act and interact with enterprise data, APIs and external applications. While this shift has the potential to unlock transformative value, it also introduces new security, governance and run-time risks that traditional cybersecurity models were not designed to address.

Traditional security was built for deterministic software. AI systems are probabilistic and context-driven, and they can be manipulated in ways legacy tools were never designed to detect. Manipulated models, poisoned prompts and corrupted agent behavior can trigger confidently wrong actions at scale.

The offering is designed to help enterprises move from assumed trust toward "provable trust" – an approach grounded in evidence, traceability and continuous assurance. Cognizant engineers trust twice, first at build time, by securing models, data and pipelines before deployment, and then at run time, by monitoring AI behavior in production to detect manipulation, help manage and mitigate unsafe actions and preserve audit-supporting evidence.

"AI is fundamentally changing how enterprise systems behave," said Vishal Salvi, Global Head of Cognizant's Cybersecurity Service Line. "These systems are adaptive, context-driven and increasingly autonomous – and securing them requires continuous assurance across build and run-time environments. With Cognizant Secure AI Services, we are helping enterprises engineer trust into AI systems from day one and to sustain that trust as those systems evolve."

Cognizant Secure AI Services is built on three foundations:

- A secure Agent Development Lifecycle (ADLC) that embeds protection across design, build, test, deploy and change of AI systems;
- Cognizant Neuro® Cybersecurity, a consolidated control plane that unifies AI and enterprise signals for threat response, correlation and audit-supporting evidence;
- Responsible AI, a continuous trust and assurance layer delivered through Cognizant Trust™ that provides traceability, policy enforcement and supports compliance alignment based on client-defined requirements as AI systems scale.

Together, these capabilities span model security, data protection, AI DevOps security, identity and access management, agent behavior controls and generative AI risk management, aiming to enable enterprises to secure AI systems across their stages of operation.

Cognizant is already working with 250+ global enterprises across regulated industries to assess, secure and operationalize digital transformation programs, including AI deployments. Early engagements address some of the most consequential risks organizations face today, from deepfake-driven fraud and model tampering to securing autonomous agents and generative AI systems operating across enterprise workflows, while establishing the governance and audit frameworks, in collaboration with clients, required to scale AI responsibly in regulated environments.

Arjun Chauhan, Practice Director, Everest Group, said: "In today's rapidly evolving landscape, organizations are increasingly looking for a more holistic approach to AI security that moves beyond siloed solutions. There is a growing need for unified frameworks that can address risks across both the build phase and the run-and-operate lifecycle. Additionally, the ability to integrate best-of-breed technologies into a cohesive, operationalized model is becoming critical to drive real-world impact. Platforms that offer a strong, unified cybersecurity foundation, while seamlessly extending to AI-specific security capabilities, are likely to be positioned well to deliver scalable and enterprise-ready outcomes."

Built for enterprise integration, supporting regulatory alignment and operational resilience, Cognizant Secure AI Services helps organizations scale AI with the practice of provable trust. For more information, visit Cognizant Secure AI Services

About Cognizant
Cognizant (Nasdaq: CTSH) is an AI Builder and technology services provider, bridging the gap between AI investment and enterprise value by building full-stack AI solutions for our clients. Our deep industry, process and engineering expertise enables us to build an organization's unique context into technology systems that amplify human potential, drive tangible outcomes and keep global enterprises ahead in a fast-changing world. See how at www.cognizant.com or @cognizant.

For more information, contact:

U.S.
Name Ben Gorelick
Email benjamin.gorelick@cognizant.com

Europe / APAC
Name Sarah Douglas
Email sarah.douglas@cognizant.com

India
Name Vipin Nair
Email Vipin.nair@cognizant.com

SOURCE Cognizant Technology Solutions
