ZeroTrusted.ai Assessed “Awardable” for Department of Defense work in the CDAO’s Tradewinds Solutions Marketplace

ORLANDO, FLORIDA, USA, May 21, 2024 /EINPresswire.com/ -- ZeroTrusted.ai, a leading provider of AI Governance, today announced that it has achieved “Awardable” status through the Chief Digital and Artificial Intelligence Office’s (CDAO) Tradewinds Solutions Marketplace.

The Tradewinds Solutions Marketplace is the premier offering of Tradewinds, the Department of Defense’s (DoD’s) suite of tools and services designed to accelerate the procurement and adoption of Artificial Intelligence (AI)/Machine Learning (ML), data, and analytics capabilities.

ZeroTrusted.ai’s video introduces their LLM Firewall, a breakthrough in cybersecurity and AI security designed by our cybersecurity and AI research experts. It enhances Large Language Models (LLMs) for secure areas, addressing data privacy, security vulnerabilities, and accuracy—essential for defense. They are used by a wide range of businesses, including Fortune 500 companies, small businesses, and government agencies.

ZeroTrusted.ai's video is accessible only by government customers on the Tradewinds Solutions Marketplace. ZeroTrusted.ai was recognized among a competitive field of applicants to the Tradewinds Solutions Marketplace whose solutions demonstrated innovation, scalability, and potential impact on DoD missions. Government customers interested in viewing the video solution can create a Tradewinds Solutions Marketplace account at www.tradewindAI.com.

In today's data-driven environment, the deployment of Large Language Models (LLMs) raises significant security and privacy concerns, particularly within sensitive sectors such as defense

and national security. (link unavailable)'s latest solution innovatively addresses these issues by enhancing the security protocols around the usage of LLMs, ensuring that data integrity and privacy are maintained without compromising the quality of output received by the users.

ZeroTrusted.ai's system is designed to automatically recognize data security, privacy, and governance issues. It fictionalizes sensitive data and rectifies security or privacy-relevant events before the data is sent to the LLM and validates the results against multiple LLMs to ensure accuracy. This method helps in identifying hallucinations, potential copyright infringement or plagiarism, and protects against LLM injections and training attacks. Critically, this process operates seamlessly in the background, ensuring that the user's experience and report quality are not compromised, even adding sensitive information back once the query returns to the system.

One of the unique aspects of ZeroTrusted.ai's technology is the ability to encrypt and anonymize sessions to internal LLMs and anonymize sessions to third-party LLMs. This feature is particularly crucial for different communities of interest (COIs) that require the power of LLMs without risking data aggregation attacks or creating data spillage. For instance, if a COI is working on a sensitive program, dubbed "Tough Chihuahua", and multiple prompt queries contain similar information, the system ensures the AI does not learn and subsequently disclose details about the mission across different queries.

Furthermore, ZeroTrusted.ai's platform supports financial efficiency by allowing organizations to bring their own tokens or use existing LLM accounts, thus minimizing additional costs. Essentially, ZeroTrusted.ai serves as a robust security and privacy layer, enhancing existing investments in LLM technologies. Additionally, the platform provides a comprehensive chain of custody by logging any security or privacy-relevant interactions related to the session to and from the LLM. This protocol not only enhances operational transparency but also ensures that organizations retain complete control over their data and training processes.

This solution is a testament to ZeroTrusted.ai's commitment to advancing cybersecurity measures in step with the evolution of technology and threat landscapes. It ensures that defense and security entities can leverage the latest AI technologies safely and effectively, protecting national interests and operational integrity.

###

About ZeroTrusted.ai: ZeroTrusted.ai is at the forefront of Generative AI security, leveraging Zero Trust Architecture to safeguard corporate data within the LLM ecosystem. Our commitment to innovation and compliance drives us to provide unmatched security solutions, helping organizations navigate the complexities of AI and data privacy effectively. At ZeroTrusted.ai, we are committed to securing data and applications through reliable zero trust security solutions, utilizing the latest in AI, blockchain, and universal encryption technologies.

About the Tradewinds Solutions Marketplace: The Tradewinds Solutions Marketplace is a digital repository of post-competition, readily awardable pitch videos that address the Department of Defense's (DoD) most significant challenges in the Artificial Intelligence/Machine Learning (AI/ML), data, and analytics space. All awardable solutions have been assessed through complex scoring rubrics and competitive procedures and are available to Government customers with a Marketplace account. Government customers can create an account at www.tradewindai.com. Tradewinds is housed in the DoD's Chief Digital Artificial Intelligence Office.

For more information or media requests, contact: Success@tradewindai.com

Sharon Lam
ZeroTrusted.ai
+1 407-507-9350
contact@zerotrusted.ai
Visit us on social media:
Facebook
Twitter
LinkedIn
Instagram
