Solution Brief
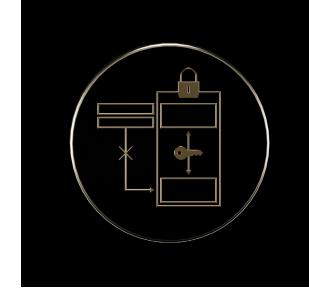

Anjuna Seaglass and Public Sector

Confidential computing secures LLM deployment to advance data insights across the public sector.

Introduction

The rise of generative AI models has attracted interest for a number of different applications. As a result, both businesses and individuals increasingly rely on cloud-based services while training and deploying AI, which increases the risk of security breaches and data leaks. Anjuna Seaglass has built a foundational technology that makes the process of sharing data confidentially seamless for developers and engineers in the process of testing, securing, deploying, and executing code in real time.

Applications

A member of **NVIDIA Inception**, a program for cutting-edge startups, Anjuna is collaborating with NVIDIA to advance GPU-accelerated confidential AI for enterprises. By integrating Anjuna Seaglass with the latest **NVIDIA Hopper and Blackwell architecture** GPUs, organizations are able to accelerate deployment of high-performing large language models (LLMs) without compromising trust, security, and privacy.

Leveraging **NVIDIA LaunchPad**, the U.S. Navy successfully tested Llama3 LLMs on confidential NVIDIA H100 Tensor Core GPUs. The seamless integration with Anjuna Seaglass enabled the U.S. Navy to create and deploy confidential environments in less than one hour, a remarkable feat, while obtaining high-speed processing with maximum performance. This integration yielded several key benefits for the U.S. Navy:

> Security without compromise: High processing speed enabled maximum performance of NVIDIA confidential GPUs with full privacy.

> Trust fully verified: The integrity and trustworthiness of LLMs were validated through attestation reports.

> Complete data privacy: Malicious entities were protected against in all three states: in use, in motion, and at rest.

Key Points

> Deploy secured LLMs in less than an hour to confidently share across data silos.

> Hardware compatibility concerns are a worry of the past with the Anjuna Seaglass technology.

> Public sector entities, such as the U.S. Navy has successfully tested secure LLMs.

"We believe in democratizing secure computing, data privacy, and trustworthy AI. Our work with NVIDIA signifies a formidable step towards achieving our vision. With their proven processing power and our flexible Seaglass platform, we're poised to ensure universal access to Confidential Computing for businesses worldwide"

Ayal Yogev, CEO and Cofounder of Anjuna Security

Ready to Get Started?

To learn more, visit **www.anjuna.io/partners/nvidia**