Confidential and Performant Processing for AI

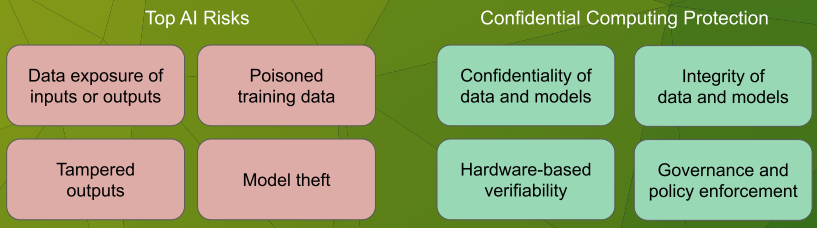
Powered by NVIDIA Confidential GPUs & Anjuna Seaglass

In today's data-driven landscape, the proliferation of AI technologies has brought about a pressing concern for enterprises: how to ensure the security and integrity of sensitive data processed by AI models.

NVIDIA and Anjuna are joining forces to usher in the era of the Confidential GPU. With the introduction of NVIDIA Blackwell and Hopper GPUs, the landscape has shifted, enabling the safeguarding of “data-in-use" during GPU processing. This includes data for training, inference, and the AI models themselves. By integrating with Anjuna Seaglass, the Universal Confidential Computing Platform, data confidentiality and integrity is ensured across the entire data lifecycle.

Mitigate Generative AI and Traditional ML Risks

Gartner describes Confidential Computing as a “core technology approach” to solving AI security risks. But what exactly are these risks, and how does Confidential Computing mitigate them?

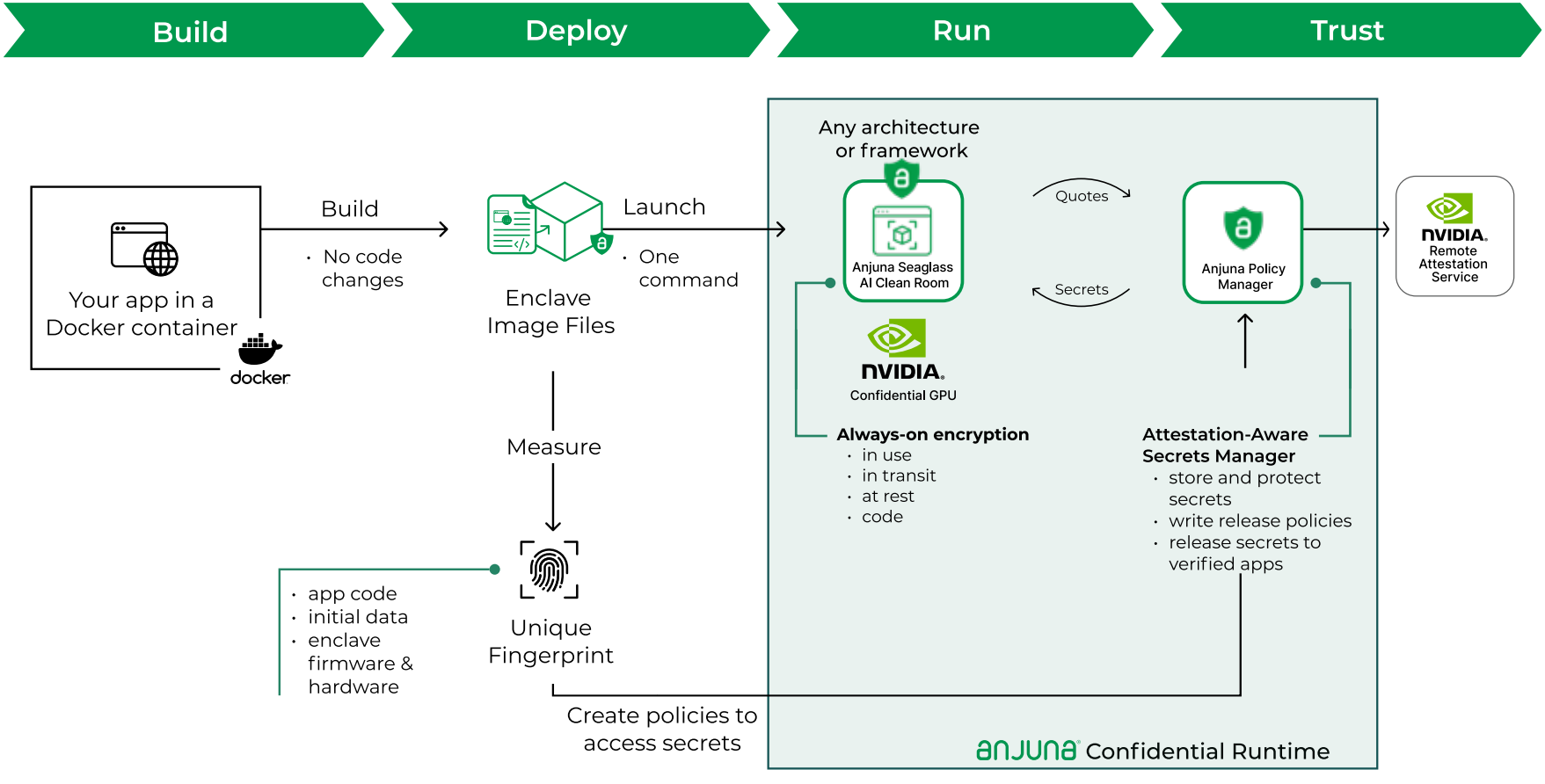


Sensitive data, especially PII and highly regulated, face risks in AI and ML systems, including LLMs. Breaches in confidentiality can expose sensitive data and models. Breaches in integrity result in counterfeit outputs or poisoned models, leading to potentially invalid results. The combination of these risks and current vulnerability to external attackers and insider threats severely restrict AI and ML use on sensitive data.

Enter Anjuna Seaglass: the easy path to secure and trustworthy hardware-accelerated AI workloads protected by Confidential Computing, powered by NVIDIA Confidential GPUs.

Want to discuss Confidential AI for your business?

Inside look at the Anjuna Seaglass platform with NVIDIA Confidential GPU



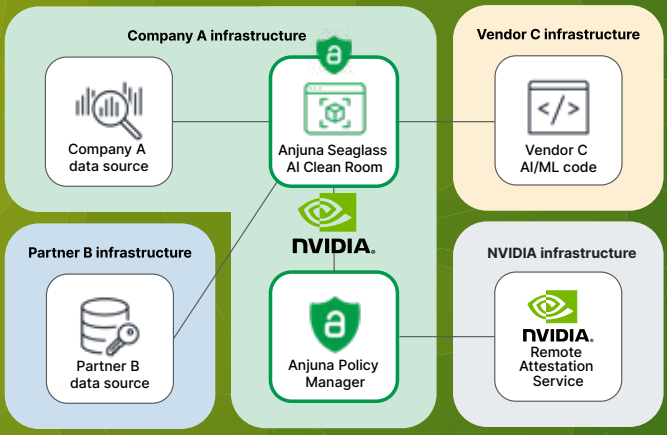
Universal Confidential Computing Platform

Want to discuss Confidential AI for your business?

Ensure Secure Multi-Party Collaboration

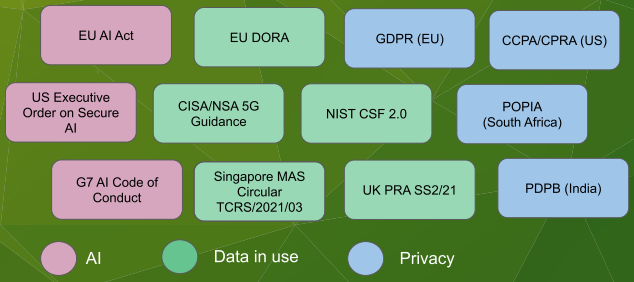
Confidential AI facilitates secure collaboration with partners while using proprietary data, algorithms, and AI/ML models. This unlocks use cases such as fraud detection, medical analytics, generative AI, and more.

Partners and other third parties can share datasets without compromising confidentiality. Organizations can collaborate on model training and evaluation, and benefit jointly from the resulting model. ISVs can sell direct access to their models, using Confidential Computing to protect valuable IP from unauthorized usage.



Facilitate Regulatory Compliance

Navigate strict data privacy and security regulations while harnessing the full capabilities of AI and ML. NVIDIA and Anjuna help you comply with the following regulations and more:



Earn your customers' trust by running secure, private, and performant AI and ML workloads, verifiably protected at the hardware level by NVIDIA Confidential GPU and Anjuna Seaglass.

©2024 Anjuna Security, Inc.