THE EMERGENCE OF PRIVATE AI

Enable Privacy, Security & Compliance for Government Deployment of AI

"When you look at how Broadcom defines Private AI, we are extremely well aligned if not intertwined with the goals of the White House AI Executive Order, especially on privacy and security."

Chris Wolf,
Head of Global AI
at Broadcom

Private AI is a non-proprietary architectural approach that works in any environment. It aims to balance the operational gains from AI with the practical privacy and compliance needs of an organization.

Generative AI (GenAI) has taken hold and governments across the globe are assessing its power to dramatically impact government agencies' processes and programs.

> "We have found over 180 instances where such generative AI tools could add value for us, with oversight."*
>
> **— Deputy Secretary of Defense Kathleen H. Hick**

While many government agencies are looking to take advantage of GenAI, there are concerns with keeping sensitive, private data from being shared externally and ensuring complete control over access to their AI models.

Concerns With Government Deployment of GenAI

Many of the concerns government agencies have with deploying GenAI focus on security and privacy of the data. Specifically, those concerns are:

- **Security Risk:** There are significant privacy and business operational risks that could arise from deploying GenAI, including data and intellectual property leakage, security, model accuracy, data privacy, and lack of transparency.
- **High Cost and Complexity:** Publicly available AI models are highly complex and costly deployments that require accelerators like GPUs and require libraries from varied sources for development.
- **Data Privacy Risk:** Agencies need to ensure sensitive data won't be shared publicly, and maintain complete control over access to their AI models.
- **Constituent Distrust of GenAI:** In general, the public has a great deal of concern about governments using GenAI when working directly with them, especially given the public nature of the GenAI models that the public interacts with.

Controlling and Securing GenAI Models through Private AI

Governments worldwide are seeking an alternative that takes full advantage of GenAI while controlling and securing data, access, and intellectual property. That alternative is Private AI.

*SOURCE: "The State of AI in the Department of Defense", Deputy Secretary of Defense Kathleen H. Hicks, November 2, 2023.

Deploying Private AI allows agencies to deliver on key outcomes, with complete control and security:

- Secure Data, AI Models, and Model Training
- Improve Contact Center Resolution Experience
- Increase IT Operations Automation
- Accelerate Information Generation and Retrieval
- Manage logistics and supply chains

Three Core Tenants of Private AI:

- **Highly Distributed:** Compute capacity and trained AI models reside adjacent to where data is created, processed, and/or consumed. Organizations keep control of their data and AI models, maximizing security and privacy.
- **Data Privacy and Control:** An organization's data remains private to the organization and is not used to train, tune, or augment any public models without the organization's consent. The organization maintains full control of its data plus the capability and training data of the AI models.
- **Access Control and Auditability:** Access controls are in place to govern who can access and change AI models, associated training data, and applications. This allows organizations to showcase GenAI implementations in accordance with policies and regulations.

Private AI infrastructure delivers key capabilities to government agencies:

- **Secure:** Agencies can reap the benefits of GenAI while maintaining privacy, security, and compliance requirements that are already in place.
- **Flexible:** Open ecosystem that allows governments to stand up an AI model very quickly, with their choice of hardware, AI models, or applications.
- **Future Proofed:** One investment in AI infrastructure through an open ecosystem that allows organizations to work at the speed of software.
- **Accurate and Reliable AI Models:** Through Retrieval-Augmented Generation (RAG), AI Models fetch facts from external sources, enhancing the accuracy and reliability of the models.

Broadcom is a leader in enabling AI and can guide government agencies on the imperative of deploying Private AI to ensure control, privacy, and security of data, AI models, and the training of those models.

To Learn More About Private AI, Go to:

https://www.vmware.com/artificial-intelligence/private-ai-foundation-nvidia.html

BROADCOM
connecting everything®

For product information, visit our website at: www.broadcom.com

1239_brcm_privateaiforgovernment_onepager_05102024 May 29, 2024