Democratize GenAI through Private AI

Enable Privacy, Security & Compliance for Government Deployment of AI

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

Private AI is a non-proprietary architectural approach that works in any environment, from on-premises to hybrid cloud to the edge. It aims to balance the operational gains from AI with the practical privacy and compliance needs of an organization, by bringing AI models adjacent to data.

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

Concerns with Government Deployment of GenAI

Many government agencies have expressed concerns about deploying GenAI. 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:** Government agencies can achieve cost savings with Private AI environments compared to public cloud AI services. With open-source models and managing their own AI infrastructure, agencies gain the benefit of a predictable cost model versus public AI token-based billing.
- **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, especially when providing direct government services that could lead to public disclosure of personal information.

Controlling and Securing GenAI Models Through Private AI

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

Deploying private AI allows governments to deliver on key use cases with complete control and security over their data.
Use cases include:

- Securing data, AI models, and model training
- Improving contact center resolution experience
- Increasing IT operations automation
- Accelerating information generation and retrieval
- Managing logistics and supply chains

Three Core Tenants of Private AI:

- **Bring AI Models to the Data:** Compute capacity and trained AI models are brought to the data and 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:** Governments 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.
- **Efficiency through Resource Sharing:** Government agencies can achieve operational efficiencies by virtualizing and intelligently sharing GPUs, networks, memory, and compute capacity, driving automated provisioning and load balancing.
- **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: vmware.com/privateAI

vmware® by Broadcom

Item No: 38534-vmw-privateai-solutionoverview-usletter 12/24