BUILDING TRUST AND ENSURING COMPLIANCE TO TACKLE SECURITY CHALLENGES IN THE AGE OF AI

We are fully in the era of artificial intelligence (AI), and as businesses unlock unprecedented opportunities for growth and efficiency, AI agents (also known as agentic AI) are providing assistance for in-context insights, incident response, change risk prediction, and vulnerability management in IT service and operations (ServiceOps). AI technologies such as large language models (LLMs) require large and diverse datasets to train on, make predictions, and derive insights—which can pose significant challenges for data security and compliance.

Many AI models operate as "black boxes," and it can be difficult for users to understand how their data is processed, stored, and compliant with policies. AI technologies may also include multiple components and data sources, which can lead to questions regarding data residency. Without the proper data governance, transparency, and security, customer data, intellectual property, or other sensitive corporate information may be fed into LLM models, risking unintended data leakage.

Questions about AI models that CIOs and CISOs should be asking

Chief information officers (CIOs) and chief information security officers (CISOs) are tasked with maximizing the benefits of generative AI (GenAI) and agentic AI while keeping applications, usage, and data secure. Staying abreast of the latest developments and approaches to data security and compliance is crucial for harnessing the benefits of AI and limiting risk. To select the right AI platform—one that includes AI agents—you must consider the specific needs of your organization,

as well as:

1. **How are access controls implemented?** Look for solutions that honor role-based access controls and ensure sensitive information is only accessible to authorized users. Controls should include varying levels of permissions, strict adherence to least-privilege policies, and extensive safeguards against unauthorized access and data breaches.
2. **How is data encrypted?** Look for solutions that encrypt data transmitted over the internet and use allow lists to restrict any unauthorized IP addresses or IP address ranges from accessing your AI applications.
3. **What are the data residency considerations?** Ensure data remains stored within contracted regions in accordance with existing agreements and applicable commercial or federal regulations. This alignment with regional and sector-specific compliance requirements simplifies regulatory adherence for customers.
4. **How are AI models trained?** Know which type of data is used to train AI models for specific use cases and ensure that it adheres to data privacy and compliance policies.
5. **Do I retain ownership of my data?** Make sure you retain full ownership of your data. Know your LLM provider's data logging and retention policies and configuration options.
6. **Do the AI models expose my data to third-party AI vendors?** Ensure that your chosen LLM provider meets your organization's data compliance requirements.
7. **How are AI models audited?** Contact your chosen LLM or AI infrastructure provider for a data compliance assessment.

How BMC Helix satisfies top security concerns

BMC Helix customers retain full ownership of their data, ensuring that all tickets, incidents, observability data, knowledge articles, configuration data, and files remain within their BMC Helix or third-party applications—with roles and permissions governing GenAI responses. For example, an IT support agent cannot access HR support tickets and a support agent and an administrator will receive different answers to the same question based on their access credentials.

This open-first approach allows organizations to use the security and compliance mechanisms they already have in place, eliminating concerns about data copying, retention, or misuse by the LLM and fostering trust and clarity in AI operations.

Additionally, BMC Helix customers can configure whether internal knowledge articles can be used for their GenAI responses. The content in the customer's third-party applications is indexed using an admin profile, which is available to end users interacting with BMC HelixGPT, BMC's proprietary GPT model.

Other benefits include:

- **Strong encryption for data in transit over the internet and for data at rest**. Data in BMC Helix AI applications remain within the customer's contracted regions. Organizations need to directly contact their chosen LLM provider for their data residency policy outside of BMC Helix.
- **BMC HelixGPT does not copy or store customer data in AI models**. The data is used only for training purposes and adheres to strict data privacy and compliance regulations under BMC Helix's policies. Furthermore, the data is isolated and logically segregated from other customer access or use.
- **A stateless AI model**. For service management use cases, BMC HelixGPT uses a stateless AI

model to process each ITSM, employee navigation, service collaboration, or other request independently. For IT operations management with AIOps use cases, BMC HelixGPT is trained using the customer's incident data, resolution worklog, and more to assist the AI with categorizing incidents, identifying root causes, summarizing impacts, and assessing risks intelligently.

It's important to bear in mind that while we ensure our own data security measures with our solutions, BMC HelixGPT integration with third-party LLM providers means those providers will use customer data for processing, so the customer will need to verify each provider's data processing and retention practices and commercial and federal compliance requirements.

The bottom line

As AI continues to transform IT work, the importance of building trust and ensuring compliance is crucial. By responsibly managing data and prioritizing transparency and security, organizations can maximize the benefits of AI and overcome some of its associated security and compliance challenges to create a future where AI enhances work and multiplies human productivity.

Contact BMC if you would like to discuss this further.