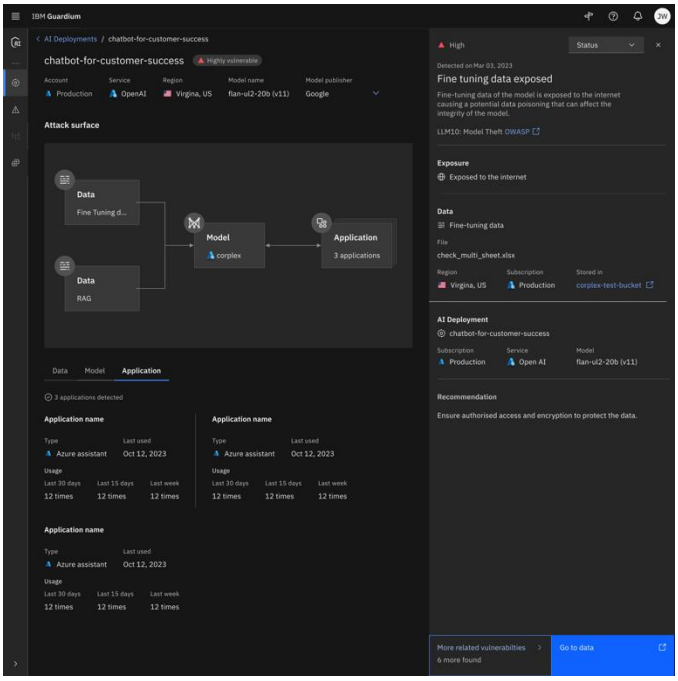
Secure your AI deployment



Manage security risk of sensitive AI data and AI models

According to a study[1], 81% of executives say secure and trustworthy AI is essential to the success of their business, yet only 24% of current generative AI projects are being secured. This leaves a staggering gap in securing known generative AI projects, and when shadow AI is added to the mix, the gap is amplified. As your organization races to implement generative AI projects, the security risks need to be better managed.

IBM® Guardium® has been securing data for decades and we are now bringing our data security capabilities to securing AI as well. Introducing IBM® Guardium® AI Security, which allows you to manage security risk of sensitive AI data and AI models.

With IBM Guardium AI Security, you can:

- Discover shadow AI with automated and continuous scanning of AI deployments
- Detect security vulnerabilities and misconfigurations to protect AI deployments
- Map to assessment frameworks and manage compliance

Securing your AI deployments needs to be a methodological approach. First, you need to discover shadow AI in your organization. With Guardium AI Security you get a comprehensive inventory – known and unknown — of all generative AI deployments across the entire organization.

Second, as you implement generative AI projects, you need to secure the model, secure the data, and secure the usage of the AI deployment. Guardium AI Security helps you identify and manage vulnerabilities and misconfigurations within the AI deployment – in the model, its underlying data and the applications accessing it. Each vulnerability is assigned a criticality score so you can prioritize your next steps.

Third, you need to comply with data security and AI regulations. Guardium AI Security helps you manage security risk and address compliance issues related to AI models and AI data. Vulnerabilities are mapped to assessment frameworks, like OWASP Top 10 for LLM, to enable you to easily learn more about the risk identified and controls to mitigate.

Additionally, with the out-of-the-box integration with IBM® watsonx.governance™, manage risk and compliance on a single dashboard.

Visit ibm.com/products/guardium-ai-security to learn more.

1. Securing Generative AI , May 2024