

Secure Foundation Models on AWS with Privacera AI Governance

Challenges

GENERATIVE AI RISKS ARE CONCRETE

Foundational models (FM) pose a significant risk to enterprises—namely the unintended exposure of sensitive information embedded in the training data. The data used for fine-tuning and embedding themselves can contain sensitive or regulated data that is subject to strict compliance policies. While organizations have invested in data governance and security tools and techniques to protect traditional platforms, FMs and generative AI present a unique set of challenges.




Privacera AI Governance

SECURELY INNOVATE WITH GENERATIVE AI

Privacera AI Governance (PAIG) provides the ability to responsibly govern sensitive or regulated data within foundational models. PAIG does this by seamlessly integrating with Amazon Bedrock supported open-source and proprietary FMs and workflows. PAIG provides a comprehensive suite of capabilities to address privacy, security, and compliance concerns associated with the use of FMs.

BENEFITS

PAIG secures the entire lifecycle of building and deploying generative AI models and apps, from discovery of sensitive data to protecting and continuously monitoring model usage.

-  **Prevent Sensitive Data Leakage**
 PAIG provides the ability to define governance and security policies in natural language and easily enforce these policies across any application and model.
-  **Detects and Filters Risk and Abuse**
 PAIG detects potential abuse of generative AI models by filtering input questions and flagging responses that are toxic or could potentially violate internal policies.
-  **Observability and Traceability**
 PAIG monitors and analyzes user actions. It provides visibility across different applications and models. PAIG also proactively identifies potential security risks. Privacera audits can be used to track which user created what outputs.



Privacera AI Governance on AWS

PAIG provides the ability to responsibly govern sensitive or regulated data within FMs supported by Amazon SageMaker or Amazon Bedrock. PAIG does this by seamlessly integrating with Amazon Bedrock and Amazon SageMaker JumpStart supported open-source and proprietary FMs and workflows. PAIG provides a comprehensive suite of capabilities to address privacy, security, and compliance concerns associated with the use of FMs on AWS.

FEATURES



Secure Model Inputs and Outputs

PAIG protects data exposure using context-aware data protection, inspecting user-prompted queries and masking or redacting sensitive data before it enters the model.



Secure Embedding and Training Data

PAIG continuously scans training data for sensitive data before it is ingested into FMs and tags this data. Sensitive training data can be masked or blocked from being utilized in models, reducing PII exposure and model bias.



Comprehensive Compliance Monitoring

PAIG provides comprehensive dashboards and audit logs of what sensitive data is leveraged in each model, how it is protected, and who is accessing it.

LEARN MORE ABOUT PAIG:

Video:

PAIG Overview

Blog:

Securing and Governing AI
with Privacera

Whitepaper:

Use GenAI to Safely
Disrupt

Fortune 500 enterprises trust Privacera for their universal data security, access control, and governance. Discover how to streamline data security governance with Privacera.

Take a unified approach to data access, privacy, and security with Privacera.

[REQUEST A DEMO](#) [CONTACT US](#)



Privacera, based in Fremont, CA, was founded in 2016 by the creators of Apache Ranger™ and Apache Atlas. Delivering trusted and timely access to data consumers, Privacera provides data privacy, security, and governance through its SaaS-based unified [data security platform](#). Privacera's latest innovation, Privacera AI Governance (PAIG), is the industry's first AI data security governance solution. Privacera serves Fortune 500 clients across finance, insurance, life sciences, retail, media, consumer, and government entities. The company achieved AWS Data and Analytics Competency Status, and partners with and supports leading data sources, including AWS, Snowflake, Databricks, Azure and Google. Privacera is recognized as a leader in the 2023 GigaOm Radar for Data Governance; was named a 2022 CISO Choice Awards Finalist; and received the 2022 Digital Innovator Award. The company is also named a "Sample Vendor" for data security platforms in the Gartner® Hype Cycle™ for Data Security, 2023. Learn more at [Privacera.com](#).

