DATA SHEET

Privacera AI Governance (PAIG)

Responsibly Optimize Your GenAI

Generative AI (GenAI) and Large Language Models (LLMs) have captured imaginations.

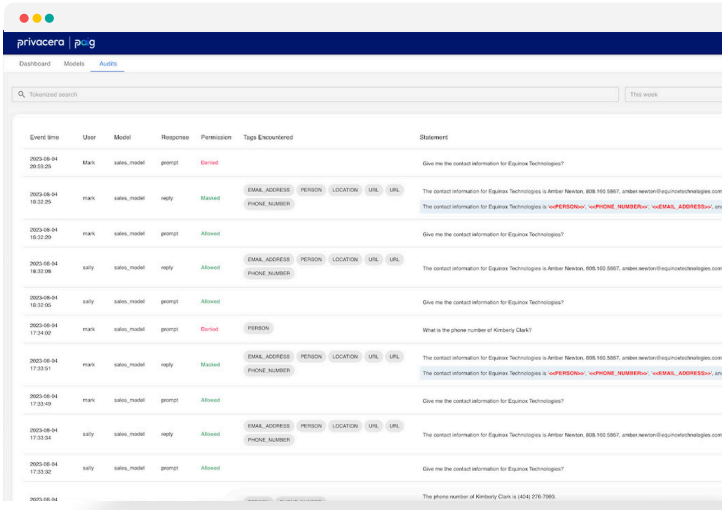
While the promises are significant, the risks are concrete, including sensitive and unauthorized data exposure, IP leakage, and regulatory compliance failures. Privacera AI Governance (PAIG) builds on Privacera's Unified Data Security Platform to secure the entire lifecycle of building and deploying GenAI models and apps. Data earmarked for training AI Models should be secured and used in accordance with your privacy and security entitlements, and the user inputs and model outputs of the GenAI application itself should comply with similar security and privacy controls to ensure accidental leakage of sensitive data. All user activities with GenAI apps and models should continuously be audited to ensure easy reporting and compliance monitoring.

KEY BENEFITS

- Securely Innovate
- Protect PII
- Prevent IP Leakage
- Track & Audit

Secure Model Inputs and Outputs

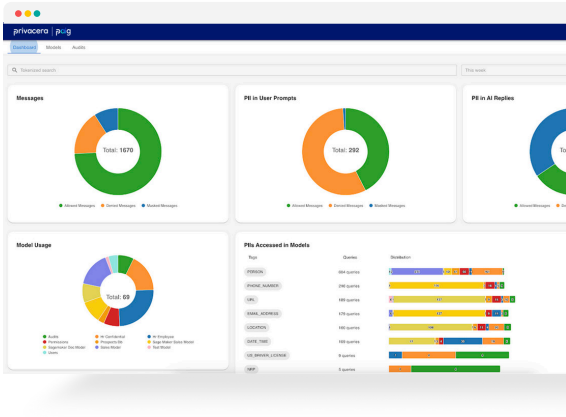
PAIG protects data exposure using context-aware data protection, inspecting user-prompted queries and masking or redacting data requests containing improper or sensitive data. Additionally, Attribute-Based Access Control (ABAC) ot Tag-Based Access Controls (TBAC) can be applied to mask sensitive data model output, ensuring users can only see data they are authorized to see. User prompts into the application and model are also inspected. Unauthorized questions that could expose sensitive data or are deemed toxic can be denied. Not only does this capability add an additional layer of security, but it also eliminates the massively expensive and wasteful LLM compute costs associated with processing unauthorized requests.



Comprehensive Compliance Monitoring

PAIG provides comprehensive dashboards and audit logs of all application and model activity, detailing what sensitive data is leveraged in each model, how it is protected, and who is accessing it. PAIG audit logs show:

- Who is accessing what models
- What sensitive data they are accessing
- When they accessed the model
- Flagged, inappropriate conversations
- What protections were applied



Additionally, PAIG provides a security and compliance dashboard that provides a view of your entire model landscape, including an overview of approved requests, denied requests, and requests that require masking to be applied. The dashboard also provides an overview of all sensitive data across models. PAIG's audit log and dashboard simplifies model monitoring and compliance.

Support for Open Standards

PAIG leverages the open standards and approaches already used in the Privacera Data Security Platform. In addition, PAIG is designed to embed easily into existing Generative AI application libraries and frameworks to make it frictionless to add to an existing Generative AI application. PAIG supports seamless integration into Open AI, Bedrock, Sagemaker, Langchain, and key prompt and query execution systems.

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.

privacera