

DATA SHEET

Privacera AI Governance (PAIG)

Securely Innovative with Generative AI

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, from discovery of sensitive data to protecting and continuously monitoring model usage.

KEY BENEFITS











Track & Audit

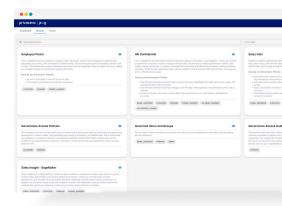
KEY CAPABILITIES

Secure Embedding and Training Data

PAIG continuously scans training data for sensitive data before it is ingested into foundational LLMs, and PAIG automatically tags this data. Additionally, sensitive training data can be masked or blocked from being utilized in models, reducing PII exposure and model bias. PAIG also uses rules, machine learning (ML) and context to scan and tag model embeddings to identify sensitive content. This is accomplished as they are created or while they are within the vector database. Additionally, PAIG provides a model catalog that displays:

- · Sensitive data the model contains
- · Security and governance policies applied to the model
- Model description
- Critical information to understand the model and how to use it

PAIG's RESTful software development kit (SDK) enables customers to connect to their choice of common LLM Libraries, such as SageMaker, langchain, llama, transformers, and OpenAI.



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. Additionally, Attribute-Based Access Control (ABAC) can be applied to mask sensitive data model output, ensuring users can only see data they are authorized to see. User prompts to the model are also inspected. Unauthorized questions that could expose sensitive data are 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.

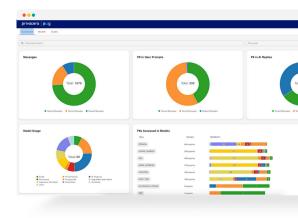
Comprehensive Compliance Monitoring

PAIG provides comprehensive dashboards and audit logs of 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
- Flagged, inappropriate conversations
- What sensitive data they are accessing
 - What
- When they accessed the model
- 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.

shboord M	lodela A	udh _								
										Dis wet
Event Sime	Usor	Macal	Response	Pemission	Tags Encountered					Statement
205-05-04 2055-05	Max	1041,7004	pongt	Dened						Give me the context Monwhon for Equines Section(spice)*
2025-08-04 16:02:25	nax	stes, radel	нау	Mathed	INVAL ACCHESS PHONE_MARKER	PERION	LOCATION	-	URL	The control information for Expense Technologies is Antice Technol. SEE 100 SEET, and an excited incursion for Expense Technologies is the CERCERCO. In PROCE INSUREMOV, INS
2005-08-04 18.52-29	mati	sales, rankel	panyi	Alment						dive ne tre castat Monaton for Equinar Sectiongeo?
N05-00-34 18.32.38	sely	sales_model	ngiy	Alment	DMA_ROORESS PHONE_MANDER	201004	LOCATION	(94)	101	The control information for Expansion Technologies is Antion Merslam, EDE JMC JMET, and an annihold expanded settingent score,
2003-09-04 18-52-86	sely	seles, redai	porte	Abust						Give me the contract information for Eguinear Sectionalogue?
2005-08-04 17:34:82	max	sales_readed	porqu	Derived	PERSON					What is the phase surface of Kinderly Clark?
2025-00-04 1732-01	mati	sales_readed	werky	Masked	DMA_RCENESS PHONE_MUNICIP	PENDA	LOCATION	-	uni.	The control information for Equines Technologies is finited Review, 866-865, 404-80, and en availability-industry-based pro- The control information for Equines Technologies is UNERPORE , UNERPORE
2005-00-54 17 50-49	max	sales, nodal	pong	Advent						Gave mail the constant information for Engineer Technologies?
2012-09-04 17:00:34	uty	1041.7004	мау	Abust	IMAL ACCHESS PHONE NUMBER	757001	LOCATION	-	UPL.	The control information for Eguines Taxtmologies is limited Newton, 806-100-1001, under wanted Seguinovier/Indepension
2025-08-94	nity	stes, node	pongt	Abead						Give me the context information for Equinox Sectioning/ex1



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

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 <u>data security</u> <u>platform</u>. 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 <u>Privacera.com</u>.