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







privacera



Track & Audit

KEY CAPABILITIES

Enforce and Maintain Privacy Controls on Vector Databases and Enrichments

PAIG enables fine-grained data access and privacy controls for all vector databases and embeddings, transforming your GenAI application security, privacy, and compliance from brick to a titanium firewall for your GenAI applications. PAIG accomplishes this for you via the following mechanisms:

OVERVIEW	PERMISSIONS		
Sales VectorDB			
User/Group Access-Lim	aited Retrieval		
Enabled			
RAG Contextual	Data Filtering		
	Data Filtering Tag Value	Granted Access	Derved Access
RAG Contextual Teg (CCPA_CONSENT)	-	Granted Access	
Тад	Tag Value		
Teg CCPA_CONSENT	Tap Value (YES)	the Marketing	Denied Access
Tag CCPA_CONSENT BUSINESS_GROUP	Tag Vake YES MARKETING	La mark	Denied Access
Tag CCPA_CONSENT BUSINESS_GROUP BUSINESS_GROUP	Tag Value YES MARKETING SALES	(1) Marketing (1) mark (1) softy	Denied Access

- All access and policies applicable on the source systems is retained and replicated into the vector database. To do this, PAIG applies user/group permissions where vector databases (VectorDBs) contain sensitive information only users with clearance can access.
- Additionally, fine-grained authorization can be implemented to comply with regulatory requirements. PAIG enables enforcement of policies based upon realtime content scanning.
- During retrieval, PAIG filters results, returning only data chunks the user or group has permissions and entitlements to access. This ensures users receive only appropriate information, but also limits the amount of data processed and returned. To work, administrators create user and group-level policies for VectorDB collections. As data chunks are imported, they are tagged with appropriate classifications. PAIG then manages the tags accessible for individual users, either directly or through group memberships. This determines which data chunks should be accessible when querying through a GenAI application.
- Fine-grained metadata filtering takes this a step further by adding a layer of specificity based on the values within each tag. This enables policies based on metadata values. It also allows for nuanced access control that can be tailored to organizational needs and compliance requirements.

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.

steast N	lodeb A	kdfa	_						_	
Telastices) por										This upp
Event line :	User	Macer	Regona	Persisten	Taps Encourtered					Stanword
762-08-04 865235	Max	1941.7004	ponst	Elened						Gue me the conset Monufor for Zophon Technologies?
305-06-04 16:02.25	Hax	Mes.com	Hery.	Machine	EMAL ADDRESS PHONE MUNITIP	717501	LOCATION	(98)	UPL	The sontal information for Equinas Section2004 is Antice Newton, SDE NO SEC, and an association procession and an The sontal information for Equines Technologies is SecTESEOLaw, SecTESEO, MARKETSW, SECTION ACCESSED, and R3
2005-05-04 10.52.29	max	sales, rasht	partyl	Almed						dive the central information for Kauliner Sectionary
2005-00-34 18-32-38	sely	salari, madal	NEW	About	EMAL ICCRESS FICKE MANDA	101005	LOCATION	98	101	The contral information for Express Technologies is feeline Rendon, ISB 302 MICL andre sector/linguin-celocheologies core, an
2002-09-04 18-22-85	140	sec.com	140202	Alcent						Give me the central Information for Equinors Technologies?
2025-00-04 17:54:82	nes	sales, realid	posst	Derived	PRARON					What is the process surgers of Kindery Clark?
2005-00-04 1732-01	mati	sales, realist	NUTY	Dariest	PMAL ADDRESS PHONE MARDIN	101004	LOCATION	-	101	The control information for Exposes Technologies is first Western, KMI MED MED, and an available for general information for Exposes Technologies is out EXPOSED on the control information for Exposes Technologies is out EXPOSED on the control information for Exposes Technologies is out EXPOSED on the control information for Exposes Technologies is out EXPOSED on the control information for Exposes Technologies is out EXPOSED on the control information for Exposes Technologies and the control information for Exposes Technologies is out EXPOSED on the control information for Exposes Technologies is out EXPOSED on the control information for Exposes Technologies and the control information for Exposes Technologies
2005-00-04 (7.52-09	net.	sales,robil	possi	Altered						Gue na the natival advectation for Enjance Technologies?
2012-08-04 (7.05-54	uty	1001.7006	HOY	Abant	TMAK, ADDRESS PHONE, MUNIER	11.1101	LOCATION	(15)	(R)	The control information for Elphanes Technologies is larger Newson, 608.160.0652, amber revision Disputice/amberdagies.com, e
2025-02-04	any.	10111-7401	ponst	A10+62						Give the two consists information for Equinox Technologies?



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>.