Fortanix

Armet AI

Unlock trusted insights from your data with a secure, turnkey GenAI solution

Concerns with GenAI Adoption

Enterprises of all types are eager to take advantage of generative AI technology. They look to turn their data from a passive resource into an active engine of growth and competitive advantage. Yet, many organizations don’t see off-the-shelf Gen AI solutions as a viable option because they fear adverse outcomes. Worries about security failures like data breaches and exposure of PII data, as well as AI trustworthiness concerns due to malicious tampering or limited data sets have pushed teams to explore building their own Gen AI Retrieval-Augmented Generation (RAG) solutions. However, these do-it-yourself solutions can be complex, costly, and resource- intensive.

Solution

Quickly customize and deploy a Gen AI RAG pipeline that prioritizes data and model security to minimize AI risk, ensure trusted responses, and drive compliance with regulations. Use readily available connectors to easily pipe in internal data sources and provide context to LLMs for trusted answers. Integrated guardrails prevent exposure of sensitive data to Gen AI and thwart malicious prompt injections.

Unlike other solutions that offer a piecemeal approach, Armet AI is a turnkey solution that allows AI teams to run their AI pipeline components on Confidential Computing for a holistic solution built on the world’s most secure technology. Knowledge workers now can access instant, relevant answers from their internal data and reap the benefits of AI in a safe and responsible way.

Key Benefits

Mitigate AI Risk

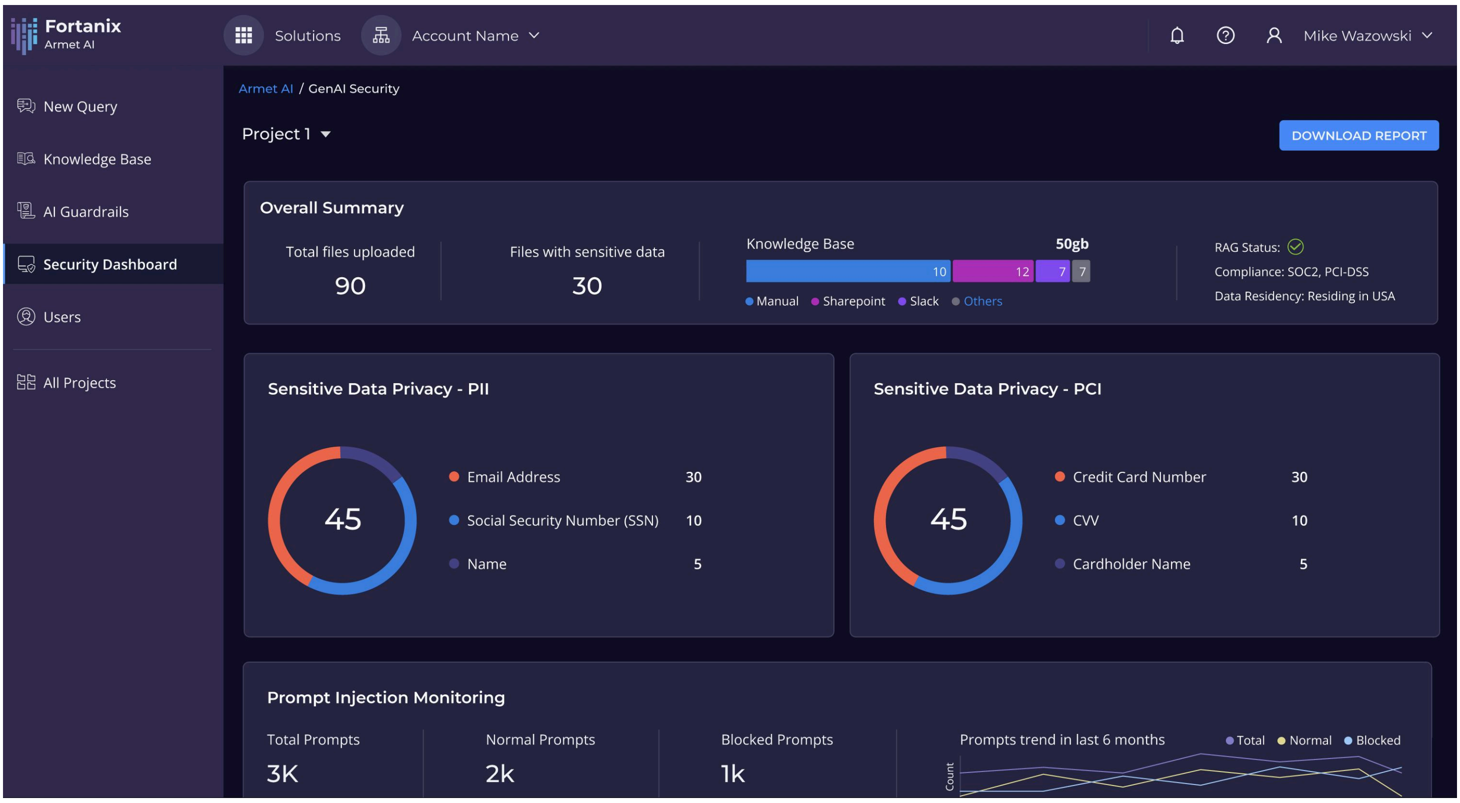
Ensure data and AI pipeline security

Get Trusted Responses

Prevent malicious Gen AI misuse and train LLMs with own compliant and private data

Drive Speed and Agility

Turnkey deployment that can be tailored to your needs



Overall Summary

Total files uploaded 90

Files with sensitive data 30

Knowledge Base 50gb: 10 12 7 7

● Manual ● Sharepoint ● Slack ● Others

RAG Status: ✓

Compliance: SOC2, PCI-DSS

Data Residency: Residing in USA

Sensitive Data Privacy - PII: 45

Email Address	30
Social Security Number (SSN)	10
Name	5

Sensitive Data Privacy - PCI: 45

Credit Card Number	30
CVV	10
Cardholder Name	5

Prompt Injection Monitoring

Total Prompts 3K

Normal Prompts 2k

Blocked Prompts 1k

Prompts trend in last 6 months ● Total ● Normal ● Blocked

Key Features

Data and AI security platform built on Confidential Computing provides end-to-end Confidential AI pipeline security to protect data and Large Language Models.

AI role-based access control drives data and AI governance and regulatory compliance by maintaining complete control with fine-grained access policies that define who can train, use, and see what data

AI Guardrails ensure data and model security. It shields sensitive data by anonymizing it and filters harmful inputs and outputs for secure GenAI operations.

Rest APIs and pre-built connectors bring data from any source to a collaborative hub for data insights and seamless knowledge sharing

Chat interface enables knowledge workers to have secure and private conversations with their internal documents.

Gen AI Security dashboard enhances your AI governance and helps you stay ahead of risks with real-time monitoring and actionable insights.

About Fortanix

Fortanix is a global leader in data security. We prioritize data exposure management, as traditional perimeter-defense measures leave your data vulnerable to malicious threats in hybrid multi-cloud environments. Our unified data security platform makes it simple to discover, assess, and remediate data exposure risks, whether it's to enable a Zero Trust enterprise or to prepare for the post-quantum computing era. We empower enterprises worldwide to maintain the privacy and compliance of their most sensitive and regulated data, wherever it may be.

For more information, visit www.fortanix.com.