GC CYBERSECURITY
PROTECT YOUR DATA

USE CASE:

Protecting against Gen-AI data leaks

Background

According to the 2024 report - Securing Generative AI by IBM's Institute for Business Value in collaboration with AWS*, only 24% of AI projects are being secured today. 82% of respondents say "*secure and trustworthy AI is essential to the success of their business*", but nearly 70% say innovation takes precedence over security.

The IBM/AWS report continues with additional salient facts that "Organizations are turning to third-party products and partners for over 90% of their gen AI security requirements" because "a new approach is needed to address the changing threat landscape posed by today's LLMs." When it comes to accidental or malicious data leaks from insiders, Gen-AI is among today's top data security use cases.

Types of Gen-AI Data Threats

Among the many Gen-AI data threats, several stand out for which every organization or enterprise needs protection.

- **Membership and Property leakage**
- **Model Features leakage**
- **Privacy leakage**
- **Privacy Compliance**
- **LLM data theft or data poisoning**

*https://www.ibm.com/think/insights/generative-ai-security-recommendations

OVERVIEW

Challenge

- Gen-AI model data and feature leaks caused by insiders.
- "Only 24% of AI projects are being secured today" (IBM & AWS).
- In-house products and services do not protect data from accidental or malicious theft.

Solution

GC Cybersecurity's Deep-AI Platform:

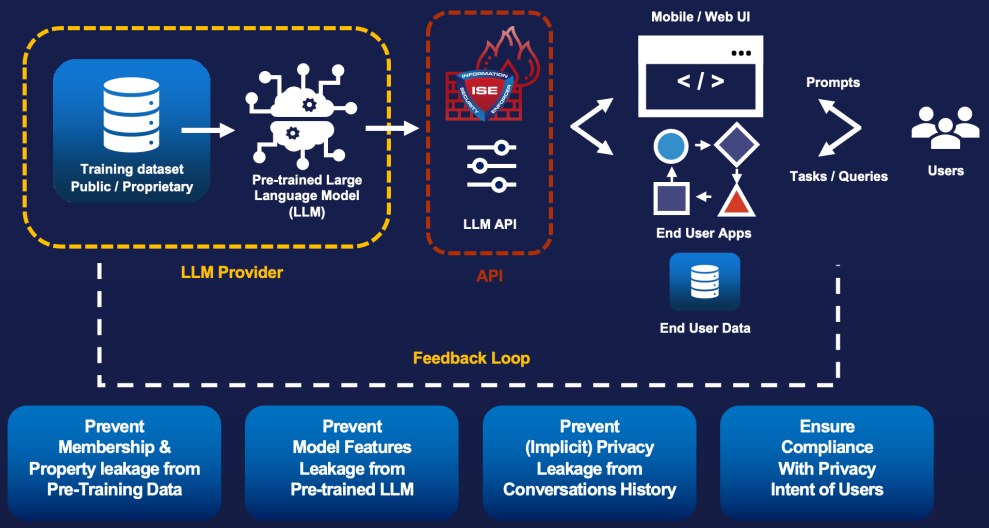
- Auto identifies and classifies sensitive data in transit.
- Auto synthesizes policies and auto enforces data access controls.
- Turn-key classification, leak and exfiltration prevention
- CASB and C4i CyberSOC
- Monitors and alerts abnormal behavior on critical systems

Benefits

Lowest TCO, Minimize Cap Ex and Op Ex:

- Automated security operations
- No end-user training
- Minimal human oversight
- Flexible deployment modes
- Highly scalable
- Extensible to other major data protection use cases.

GC Cybersecurity Offers Advanced Data Protection in the age of AI



Data Protection Solution:

Advanced Data Security Capabilities

- Real-time, auto-Classification of sensitive data, information and content
- Automated Policy Synthesis and Enforcement
- Identity & Role-Based Advanced Data Protection
- Cloud Access Security Broker - CASB
- Advanced Workflow Monitoring and Policy Enforcement
- Adaptive Architectural Enterprise Deployments
- Centralized Data Protection Command and Control

Detect Gen-AI and LLM insider Leakage

- Detect sensitive data leakage into LLMs.
- Prevent membership & property leakage from training data.
- Prevent model features leakage from pre-trained LLM.
- Prevent implicit privacy data from leaking from conversational histories.
- Ensure compliance with privacy intent of users.

GC CYBERSECURITY

Headquartered in Silicon Valley, GC Cybersecurity by Ghangorcloud, Inc is a leading provider of next-generation advanced data protection and data security solutions.

Ghangorcloud, Inc. 2001, Gateway Place
Ste: 710 West Tower San Jose, CA-95110 USA
Main: (408) 713-3303
Technical Support: (408) 713-3303 x105
US Sales: (408) 713-3303 x108