



portal26

ENTERPRISE GENAI ADOPTION PLATFORM



Customer Case Study

Portal26 for secure and responsible GenAI adoption



**DISCOVERING AND
TRACKING MALICIOUS
INTENT IN GENAI USE**

Customer Background

Portal26's customer is an industry leading B2B and B2C company with thousands of employees and millions of customers. Most of their business transactions include financial and personal data. They also invest heavily in internal departments like engineering, product design and marketing and see Generative AI as a way to improve overall organizational productivity and competitiveness.

Business Problem

A critical concern for leadership is the proper usage of GenAI tools, and reducing the risk associated with malicious insiders. Employees with access to private data can exfiltrate this data via prompts to external GenAI tools. With GenAI being a brand new technology lacking mature security controls such malicious activity could remain undiscovered and eventually come back to harm the company.

Stakeholders



CISO



Chief Risk Officer



Chief Internal Auditor



General Counsel

Desired State

The company would like to eliminate the potential for intentional, malicious use of its GenAI program as well as ensure its employees are using GenAI as a productivity and workflow enhancer. In the event of malicious use of GenAI, the company would like to have an auditable historical record of all GenAI activity including prompt content and attachments. This data should be available for forensic investigation, regulatory reporting, and detailed audit. The company would also like to scan all GenAI activity for risky behavior and provide metrics to the leadership team. Finally, the company would like to educate employees on avoiding risky behavior and following acceptable use guidelines.

Required Capabilities

- Real-time, in-depth visibility into who is using GenAI, what tools are being used and what data and attachments are leaving the organization via prompts
- Understanding of prompt intent and real-time notifications of potential mis-use related to prompt inputs
- DLP integration for policy enforcement
- Detailed forensics capability for specific incidents
- Audit and compliance reporting

Portal26 Solution

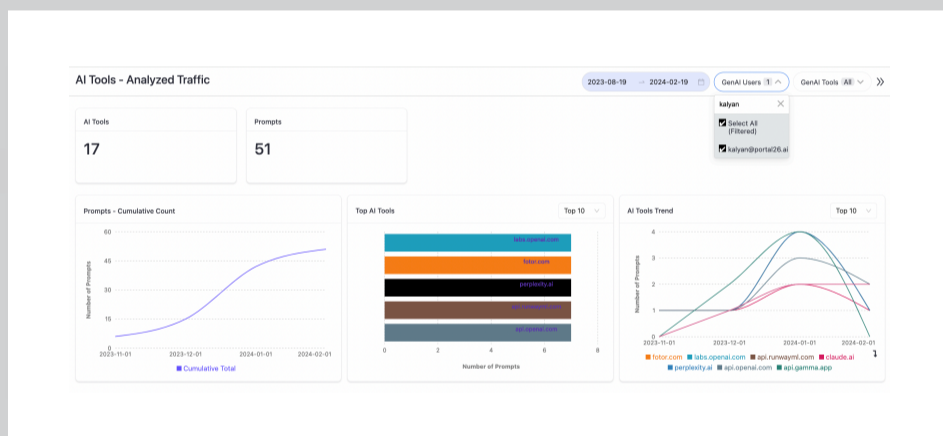
The company deployed the Portal26 GenAI Adoption Platform in a half-day with full DLP integration providing them with 24/7 real time monitoring and reporting of all GenAI usage throughout the organization, sanctioned or not. Portal26 automatically scans all GenAI usage for risky behavior and enables the company to identify and correct malicious activity.

1/2 Day Deployment

10,000+ Monitored Employees

1 Malicious Insider Identified

4 Investigations In first month



Results

Within days of deploying the Portal26 GenAI Adoption Platform, the company had visibility into GenAI usage by tools, departments, locations, and users throughout the enterprise. The company was able to monitor prompt usage for malicious activity as well as use AI to understand user intent. With this data available in real-time, and the opportunity to mitigate risks, the company was able to move forward with GenAI adoption with confidence and trust.

To learn more about the Portal26 GenAI Adoption Platform
Find us at portal26.ai Email us at info@portal26.ai