January 6, 2026

The Privacy Trap

Why Your Employees Are Leaking IP to Public LLMs

"Presented by"

Gittielabs, LLC

PRIVACY RISK

Executive Summary

Your team may be sharing sensitive info with AI tools without realizing it.

Key Points

IP LEAKAGE

Employees unintentionally share sensitive data with unauthorized AI tools, exposing organizations to privacy risks.

SHADOW AI

Unsanctioned AI tool usage creates significant vulnerabilities, increasing legal and regulatory risks for businesses.

COST-EFFECTIVE SOLUTION

Light Wrappers provide a practical security approach for mid-sized organizations, balancing productivity and compliance needs.

SHADOW AI RISKS

Shadow AI Explained

Addressing Unsanctioned Tool Usage

The rise of "Shadow AI" indicates that employees are increasingly using unsanctioned AI tools, often unknowingly putting sensitive corporate data at risk. This trend highlights the urgent need for oversight and governance.

As companies strive for enhanced productivity, employees inadvertently compromise security protocols by leveraging public AI tools. The lack of formal guidelines exacerbates the issue, making it critical to address this challenge.

How the Leak Happens

Vectors of Data Leakage in Public Chatbots

Public chatbots function like **publishing platforms** rather than ephemeral conversations. Employees unknowingly contribute sensitive information, creating three main vectors of leakage: training absorption, where user inputs become model data; server retention, which exposes data to external legal battles; prompt injection, enabling malicious actors to extract past conversations.

These leakage vectors highlight the **urgent need** for organizations to implement protective measures. Without oversight, employees will continue to use unsanctioned AI tools, risking proprietary information. Understanding these mechanisms is essential for developing effective security strategies to safeguard sensitive data and maintain compliance with regulations.

Legal Compliance Risks

Understanding Regulatory Frameworks and Challenges

The rise of Shadow AI poses significant compliance risks, particularly in regulated sectors. Organizations must navigate the complex landscape of data privacy laws, where unauthorized use of public AI tools may lead to severe penalties and reputational damage for non-compliance.

GDPR, CCPA, and HIPAA impose strict requirements for handling personal and sensitive data. Shadow AI complicates these responsibilities, as conventional data deletion practices are ineffective with AI tools that retain user inputs, increasing the potential for legal liabilities and audit trails gaps.

The Solution

Light Wrappers as Secure AI Gateways

Light Wrappers act as essential **gateways** between employees and public AI services, ensuring secure access without needing extensive private infrastructure. By utilizing these AI Gateways, organizations can provide controlled access to AI tools efficiently while safeguarding sensitive information.

Employees can engage with AI through a branded portal that ensures **anonymity** and compliance. With mechanisms in place for data protection, Light Wrappers allow organizations to harness AI's productivity gains without the risks associated with "Shadow AI," creating a balanced approach to modern challenges.

TECHNICAL OVERVIEW

Secure Middleware Proxy

Understanding the Technical Architecture for Light Wrappers

The Technical Architecture Overview illustrates how Light Wrappers function as **secure middleware proxies**. This architecture ensures that employee requests for AI tools are intercepted, sanitized, and logged, allowing organizations to maintain control over their data while leveraging public AI models effectively.

By implementing a five-step data flow process, organizations can safeguard sensitive information. This process includes local interception, PII scrubbing, and encrypted communication with commercial APIs, ensuring compliance and security while accessing advanced AI capabilities through a simple and efficient mechanism.

Security Controls

Protecting Data with Customizable Filters

Security and compliance controls are essential for organizations utilizing AI technologies. Implementing **customizable filters** helps prevent unauthorized data exposure while allowing employees to access the tools they need. This balance ensures sensitive information is protected against potential leaks.

By leveraging advanced **Data Loss Prevention (DLP)** techniques, organizations can effectively manage proprietary data structures. Furthermore, integrating robust **identity and access management** systems enhances security, providing role-based access control that aligns with regulatory requirements and protects critical data against unauthorized access.

Deployment Strategy

Set and Forget Implementation Options

The deployment strategy is designed as a **'set and forget'** solution that simplifies the implementation process for organizations with limited DevOps resources. It provides two deployment options: cloud and on-premise, allowing for flexibility based on the organization's infrastructure capabilities.

Option A involves deploying the solution on a private cloud using Docker or Kubernetes, ensuring that data remains within controlled infrastructure. Option B allows for installation on internal servers with strict data sovereignty, catering to sensitive government and regulatory requirements.

Comparison

Evaluating Light Wrappers Against Direct ChatGPT Usage

Data Privacy	User Management	Visibility	Cost Control
Low	Individual	None	Expensable
High	Centralized	Full Logs	Centralized
Medium	Individual	None	Expensable
High	Centralized	Full Logs	Centralized
Implementation	None	Docker	Low

Contact Us

www.gittielabs.com

thegittiecrew@gittie.co

GITTIELABS