



# Generative AI Assessment

Usage and Data Security Findings

May 2025



# Summary



## Time Period

May 1 - May 31, 2025



## Scope

2,000 enterprise users across customer success, claims agents marketing, legal, IT, and sales.



## Requirements

Understand Shadow AI risk and enforce controls



# Overview

## AI App Usage

254 GenAI Apps in use across the enterprise, with 1,150 active users (65% of company)

01

## Unapproved App Use

42% of GenAI users rely exclusively on unapproved tools, bypassing company policy (to use ChatGPT Enterprise/MS Copilot)

02

## High Risk App Use

Employees are actively using high-risk apps that train on customer data and/or operate in high-risk jurisdictions

03

## Sensitive data exposure

Insurance claims data, customer data, and private equity agreements were submitted to GenAI tools-with the majority outside of corporate accounts

04

## Risky users

A small group of persistent users generated 68% of all alerts in April 2025

05

## Department use

Majority of sensitive data exposure originated from marketing and engineering teams.

06



# AI Use Snapshot



Widespread AI Use, But Sensitive Data Exposed to Unapproved Tools



254

GenAI Apps in Use

—  
Newly-discovered GenAI or GenAI-enabled tools



1,150

Active GenAI Users

—  
65% of employees are using at least one GenAI tool



# Unauthorized AI Application Use



251

Users are relying solely on critical/high-risk tools like DeepSeek, Grok, Claude Free Edition



35%

Of GenAI traffic is going to unapproved tools-nearly 75% of that is to ChatGPT Free or Plus



23%

Using personal GenAI accounts instead of corporate-assigned accounts



134

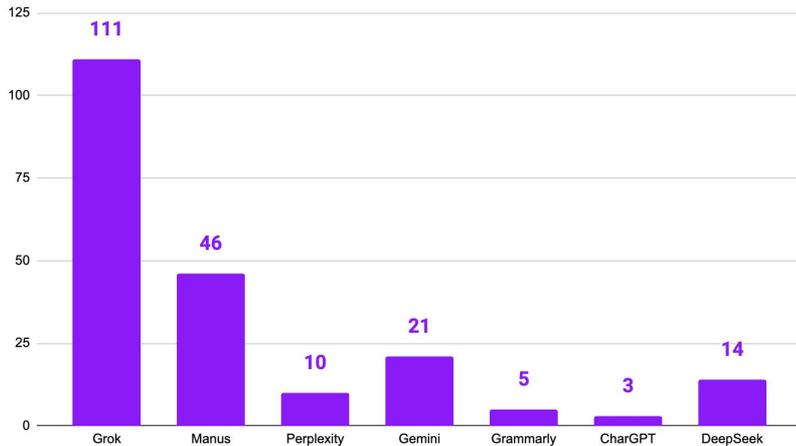
Unapproved GenAI apps detected-21 train on user data, 4 are China-based



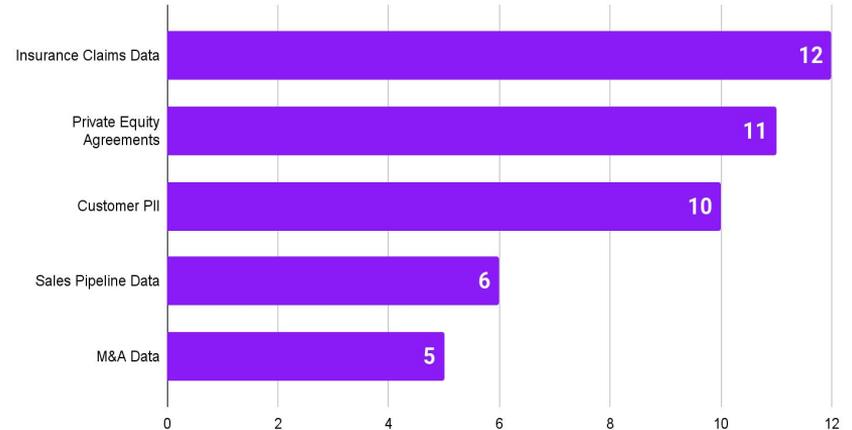


# Sensitive Data Exposure

## Sensitive Data Exposure by Apps



## Top 5 Sensitive Data Types





# Risky Users



68%

68% of all sensitive data alerts came from just 23 users



19

19 users submitted sensitive content to DeepSeek



70%

Of the high-risk users came from Marketing and Engineering





# Recommendations

1



## Enable Harmonic interventions

for free app use, personal account use, and Chinese-HQ sites.

2



## Provide proactive awareness training

to the small, high-risk group of users to improve AI literacy and reduce exposures.

3



## Enable banner warnings

to redirect users to enterprise ChatGPT tool.