WebKeeper DLP

ChatGPT DLP Solution

SOMANSA

Conversation with ChatGPT

Utilization of ChatGPT for the purpose of improving work efficiency may pose a risk of **Confidential Data Leakage**

|		
Production yield, official price, etc. ⚠ **Sensitive quoting information can be leaked**	development projects, litigation status ⚠ **Confidential data & trade secret can be disclosed**	Customer·employee data, etc. ⚠ **Personal data can be exposed**
The use of ChatGPT for translating quotation contents into English may pose a risk of data leakage	Converting meeting recording files into text may lead to content leakage	Transferring data to the ChatGPT server for the purpose of classifying customer data may pose a risk of leakage

Key Technical Features

PlayBack Conversation Storage

· Saves all ChatGPT conversations
· Records the actual conversation screens
· Utilizes saved conversations as post-incidents audit materials if a data leakage occurs.

Detection and Prevention of Personal Data Leakage

Detects and **blocks** the inclusion of personal data such as social security numbers and driver's license numbers in ChatGPT conversations, and **stores** logs of such actions.
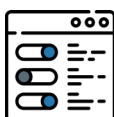
Department·Time−based Selective Control Policy

· Restricts the use of ChatGPT for employees of finance department, where the risk of data leakage is high.

· Allows limited use of ChatGPT for employees of development department, where the usage rate of ChatGPT is high. (ex. code review)

Big Data Search of Audit Logs

Detects keywords in confidential data, such as production yield, budget, and trade secrets within 3 minutes from one billion records of data accumulated over one year.

Preservation of Original ChatGPT Conversations

Records personal·confidential data leakage while using ChatGPT
Stores and secures audit logs of the use of ChatGPT

Employee PC

Somansa Bank
CREDIT CARD REQUEST FORM

Note :

Name	Last Name	Sammuel
	First Name	Barry
Address		3003 N. First St., Suite 301 San Jose, CA 95134
Date of Birth		05-10-2003
Mobile No.		408-701-1302

Extract only the text from the image file please.

The extracted text from the image is as follows.
• Somansa Bank
• CREDIT CARD REQUEST FORM
• Note :
• Name :
• Last Name : Sammuel
• First Name : Barry

When the employee uploads images in ChatGPT4, WebKeeper DLP stores the original image and conversation logs

Your company can comply with **local data privacy laws and industry regulatory compliance** relate to ChatGPT.

Admin Page

Messenger Information   Close

☰ Body Content   〈ᐱ〉〈ᐯ〉

sambarry@somansa.com   2023-12-27 15:29:57

Extract only the text from the image file please.

ChatGPT   2023-

The extract text from the image is as foll

• Somansa Bank
• CREDIT CARD REQUEST FORM
• Note :
• Name :
• Last Name : Sammuel
• First Name : Barry
• Address : 3003 N. First St., Suite
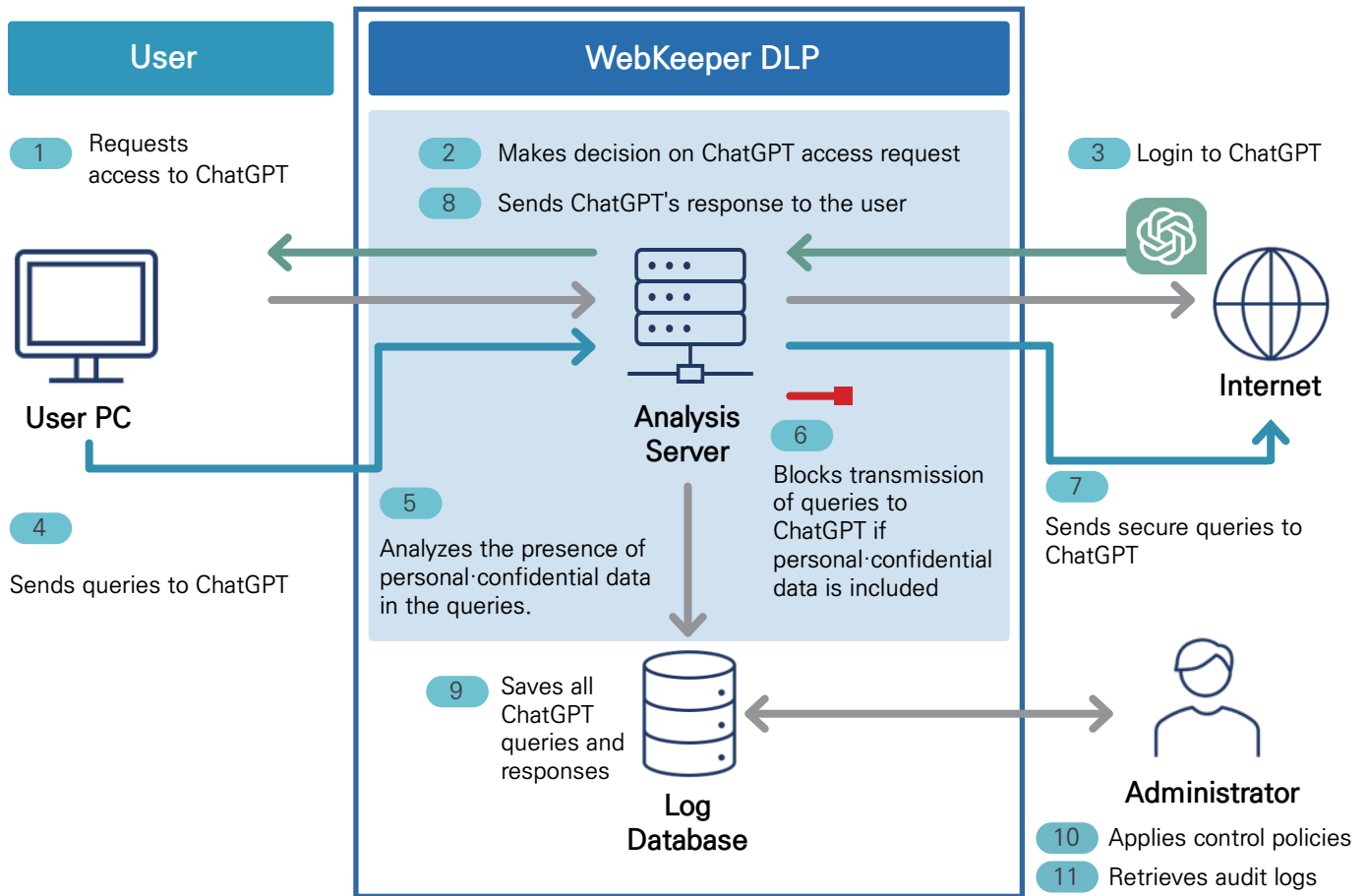 95134
• Mobile No. : 408-701-****

The information above is based solely on the text extracted from the image.

WebKeeper DLP saves the original packet and reproduces it in the form of a messenger.

☰ Pattern/File/Text Information   Expand All   Collapse All   Execute Analysis

Content	Quntity of Pattern	File Size(KB)	Analysis Result
Body Content	0		Before Analysis
Somansa Bank_Sammuel Barry_Card Request Form.jpg	-	963.13	Before Analysis 🖫
Total	0	963.13	

The administrator or data handler can **check the original image.**

Product Configuration

User

WebKeeper DLP

1 Requests access to ChatGPT

2 Makes decision on ChatGPT access request

8 Sends ChatGPT's response to the user

3 Login to ChatGPT

User PC

Analysis Server

Internet

4 Sends queries to ChatGPT

5 Analyzes the presence of personal·confidential data in the queries.

6 Blocks transmission of queries to ChatGPT if personal·confidential data is included

7 Sends secure queries to ChatGPT

9 Saves all ChatGPT queries and responses

Log Database

Administrator

10 Applies control policies

11 Retrieves audit logs

Comparison Tables

Technology Features		WebKeeper DLP	Symantec	McAfee
Audit Log	Saves both queries and responses	○	△	△
	Provides combined view of queries and answers in the form of chat.	○	X	X
Block Alert	Blocks personal data including Social Security Numbers, Credit Card Numbers, Passport Numbers, etc.	○	△	△
	Blocks leakage of confidential data based on keywords (Ex : production yield, budget, etc.)	○	X	X
	Selective blocking by department and time	○	○	○
	Blocks access to ChatGPT (including bypassing)	○	○	○
Retrieval	Big Data Search (keywords, data patterns, and repetition frequency of data)	○	X	X
	Retrieves data based on user, time, and action(allow·block)	○	○	○