



WebKeeper AI DLP

NEW

Prevent Personal, Confidential, and Sensitive Data Leakage Through Generative AI

WebKeeper AI DLP protects your organization from data leakage through generative AI services using LLM-powered semantic detection. It accurately identifies and controls personal, confidential, and sensitive information shared with AI applications, preventing both accidental disclosures and unauthorized insider transmissions while maintaining a complete audit trail of every interaction. Trusted by leading public sector organizations—including the National Tax Service and the Korea Heritage Service—WebKeeper AI DLP has been successfully deployed and proven in production environments. Optimized for Korea's N2SF National Network Security Framework and the first solution of its kind implemented in the country's financial sector, it has become the benchmark for securing enterprise use of generative AI.

1 Developed Ahead of the Market by Somansa, No.1 in Network DLP market share for 30 years

- **39.7% of employee interactions with generative AI contain sensitive corporate data**
Generative AI lifts business productivity, but it also opens corporate security risk.
- **Gain complete visibility enterprise AI usage**
Monitor and control access to generative AI services, maintain audit logs, and accurately identify personal and confidential information leaving your organization using detection technology refined through three decades of Network DLP expertise.

2 Covers every blind spot left by pattern and keyword based AI DLP

	Conventional Pattern-Based DLP	NEW AI DLP with LLM Analysis Engine
Detection Method	- Relies on patterns and keywords - Cannot interpret complex phrasing or conversational context	- An LLM analysis model reads meaning and understands the full context of the prompt - Far higher accuracy on unstructured addresses, API keys, sensitive data, prompt injection and harmful prompts
Image Analysis	Struggles to analyze images such as maps, blueprints and technical drawings	- Classifies drawings, images and scanned files by their content and structure - Extracts the text inside an image and classifies it in context for greater accuracy
Intent Analysis	- Cannot distinguish between an intentional data leakage and legitimate use - Cannot identify prompts written for illegal or criminal purposes	- Reads the flow of the conversation to pinpoint deliberate leakage attempts - Identifies and distinguishes illegal, criminal and threatening intent

Major Customers



and many more

Key Advantages



Conversation Logging and Replay in a Familiar Chat Interface

Every AI interaction is captured and replayed exactly as it occurred in an intuitive messenger-style interface. During investigations and audits, security teams can quickly understand user intent and determine whether sensitive data exposure was accidental or deliberate.



Selective Control Over Generative AI Access

Predefined AI service categories allow organizations to approve only authorized generative AI applications while automatically blocking all others, minimizing unauthorized AI usage.



LLM- and Vector-Based Detection for Prompts, Images, and Documents

Unlike traditional keyword-based approaches, WebKeeper AI DLP analyzes context and intent. Whatever is detected is sorted into confidential, personal and sensitive data, prompt injection attempts, or harmful content.

Functions



Prevent Data Leakage Through Generative AI with Complete Audit Visibility

- Detects and blocks personal, confidential, and sensitive information within prompts and uploaded files in real time. Blocked content is automatically masked to prevent further exposure.
- Stores original files and complete user activity logs to support compliance, investigations, and forensic audits.
- Reconstructs prompts and AI responses in a familiar messenger-style conversation view, allowing auditors and non-technical users to review interactions with ease.
- Enforces policy-based controls for keywords, repeated usage, file uploads, file size limits, and other organizational security policies.



Real-Time LLM-Powered Detection of Sensitive Data

- A multi-layered analysis system combining regular expressions, keyword dictionaries, embedding vectors and LLM analysis.
- Continuously monitors prompts and uploads for personal, confidential, and sensitive information, as well as prompt injection attacks, in real time.
- Analyzes document structure, language, context, and user intent while identifying semantic similarities across text, images, and documents to instantly detect, classify, block, and log security events.



Automatic document categorization

- Automatically classifies documents using SOMANSA's proprietary AI classification engine, supporting 20 major categories and more than 100 detailed subcategories.
- Automatically assigns confidentiality levels and risk classifications, enabling consistent, fine-grained data governance and security policy enforcement across the organization.

WebKeeper AI DLP controls almost every commercial generative AI service, and its coverage keeps on growing.

