Best Practices to Prevent Data Loss to GenAI

Protect sensitive data while using GenAI

Data loss prevention (DLP) is far from a new idea. A wide variety of DLP tools are available that focus on what type of data is being protected and where policy is enforced. Some familiar categories include Data in motion (network DLP); Cloud DLP (typically CASB-integrated); Database DLP (sometimes a component of Data Discovery and Classification offerings); Data at Rest DLP (Storage DLP), Email DLP; Cloud-native/API-based DLP; Data in Use, or endpoint DLP, Unified/integrated DLP (sometimes known as Enterprise DLP Suites), and finally, Browser or Web DLP.

Given the breadth of tools available, it is tempting to assume that every aspect of data protection would be covered, but, in fact, the opposite may be true. That's because different DLP tools look at different elements of data at different stages, and this fragmented view can create blind spots, conflicts, and a false sense of security.

72% of respondents agree that they lack visibility into how users interact with sensitive data across endpoints and cloud applications.[1]

As GenAI continues to grow, DLP in the browser has emerged as a major challenge. To begin, we must understand how DLP in the browser fits into safeguarding GenAI use, as well as in the overall enterprise DLP initiatives as a whole.

DLP operating on browser traffic focuses on the user's interaction with data on web pages and the files carried in web traffic. This offers benefits different from traditional tools:

[1] 2025 Data Security Report – Fortinet

- Browser DLP sees actions within the browser tab, like copying or pasting from another app or document, or entering text on browser forms. Network DLP only sees the data leaving the corporate perimeter. Browser DLP can provide granular controls that consider the context of different applications or websites. Device-level or traffic-level DLP can only apply broad policies to the device or all traffic on a protocol; neither can consider the context of the application.
- Browser DLP directly considers actions where it matters most in the context of GenAI in particular because on non-mobile platforms, users interact with GenAI in a browser.

To mitigate data loss and leakage as users interact with GenAI tools, consider the following best practices.

Establish governance and policy controls

- Create and document a clear enterprise policy outlining approved vs. prohibited GenAI tools, acceptable use, and data handling expectations. Ensure that all users are aware of this policy when you roll it out. In-process notifications are a good way to reinforce user understanding.
- Classify tools by associated risk levels. Ensure that you are considering all AI tools in use, which may require soliciting user feedback or observing traffic. Types of AI could include generative AI tools, including LLM-based GenAI being used for productivity, research, writing assistance, coding, meeting transcription, graphic design, and data analysis. Assign limitations on roles based on role and risk.
- Require employees to acknowledge the GenAI acceptable use policy. While it is appropriate to publish this form, it is also useful to ensure a method whereby users are warned/reminded of policy via alerts as the AI tools are used or data is accessed.
- Match your Shadow AI detection policies to your DLP policies. Advice about controlling Shadow AI use is detailed in Best Practices to Enable the Safe Use of GenAI.

Enable data protection and DLP integration in the browser

Menlo can help with robust DLP tools in the browser, including copy/paste and upload/download controls, watermarking, and data redaction.

Menlo also enables specific data protection and DLP integration. Menlo DLP can examine documents against more than 380 different dictionaries. Menlo also makes it easy to build your own dictionaries to highlight specific language, branding, IP, or terms. These capabilities enable DLP policy enforcement in real time, and, together with Menlo browser context, can automatically identify and block prompt submissions that may attempt to share regulated data, such as financials, IP, or PII.

Another important step is to ensure that users are aware of DLP policies. With Menlo you can go beyond one-time trainings to block DLP policy violations as they are about to occur. You can also configure custom DLP warnings for users and simultaneously notify auditors.

Apply browser DLP policies to all users and all endpoints, including BYOD and unmanaged devices

When considering DLP, it is easy to forget users who need to access internal and SaaS apps and data to do their jobs, but who may be working on unmanaged machines. This can include remote users on their own devices (BYOD), as well as contractors or partners. It is vital to ensure that browser DLP can be applied consistently.

It is easy to solve that challenge with Menlo Secure Application Access, which enables access only to the applications that you have allowed. You can change interaction parameters for those applications, such enabling read-only mode, and can apply all DLP policies as well, regardless of the endpoint device.

Consider browser security

Best practices emphasize the importance of preventing AI tools from directly executing on the endpoint to the greatest degree possible. This provides clean separation between users, endpoints, data, and the AI tool.

The Menlo Secure Cloud Browser builds a hardened digital twin of the user's browser on their endpoint, intermediating the browsing session to automatically enforce guardrails and policies without touching the device.

Ensure visibility

Once you have established DLP policies, you need to ensure that they are working as intended. This can be an issue with many browser-based products, because the browser is a notorious blind spot for legacy visibility tools. Particularly in the case of GenAI, easily observable auditing and logging are essential for ensuring compliance. To make the best use of DLP-related data, you should correlate DLP telemetry with information about GenAI tool use.

Menlo Browsing Forensics can be triggered to perform session recording when DLP policy violations are observed to give you more information about what is going on in real time. The Browsing Forensics Flow feature can show you an at-a-glance session summary, so you can the user actions before and after the triggering event as well, saving time that otherwise would have to be spent going through log entries. Menlo Insights provides an easily configurable regular snapshot of browser-based activities, including details about DLP events and all GenAI tools accessed. Browser activity logs can then be fed into SIEM/SOAR platforms for correlation with DLP and endpoint telemetry.

GenAI can be a major source of data loss, but it doesn't have to be

While these steps could seem difficult, Menlo makes it easy to understand and enforce DLP in the browser as you control Shadow AI and maintain compliance.

Learn more by downloading the Menlo DLP Solution Brief and the Best Practices to Enable the Safe Use of GenAI

Full DLP Reference Table

DLP Category	What It Protects	Where It Operates
Data in motion (Network DLP)	Data moving across the network — email, web uploads, cloud transfers, FTP, IM, etc.	Network perimeter, secure web gateway (SWG), email gateways
Data at rest (Storage DLP)	Data stored on servers, databases, endpoints, cloud repositories, or file shares	On-prem storage, endpoints, or cloud storage (e.g., OneDrive, Box, AWS S3)
Data in use (Endpoint DLP)	Data currently being accessed, edited, or copied by users or applications	Endpoint agents on laptops, desktops, VDI, and virtual apps
Cloud DLP (CASB-integrated DLP)	Data stored or shared in SaaS and IaaS environments	Cloud applications (e.g., Google Workspace, Salesforce, Slack, ChatGPT)
Email DLP	Data transmitted via email (internal or external)	Secure Email Gateway or MTA integration
Browser/Web DLP	Data being downloaded from internal and SaaS apps, or leaving via browsers or browser-based GenAI tools	Browser runtime, isolation layer, or SWG proxy
Database DLP (or Data Discovery & Classification)	Structured data stored in databases	Database layer, data warehouses
Cloud-Native/API-Based DLP	Cloud data flowing via APIs	Cloud security platform, CASB, or cloud API integrations
Unified/Integrated DLP (Enterprise DLP Suites)	Data in motion, at rest, and in use	Network, endpoint, cloud

About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Secure Cloud Browser. Menlo delivers on the promise of cloud-based security — enabling zero trust access that is simple to deploy. The Menlo Secure Cloud Browser prevents attacks and makes cyber defenses invisible to end users while they work online, reducing the operational burden on security teams.

Menlo protects your users and secures access to applications, providing a complete enterprise browser solution. With Menlo, you can deploy browser security policies in a single click, secure SaaS and private application access, and protect enterprise data down to the last mile. Secure your digital transformation with trusted and proven cyber defenses, on any browser.

Work without worry and move business forward with Menlo Security.

Learn more: https://www.menlosecurity.com
Contact us: ask@menlosecurity.com