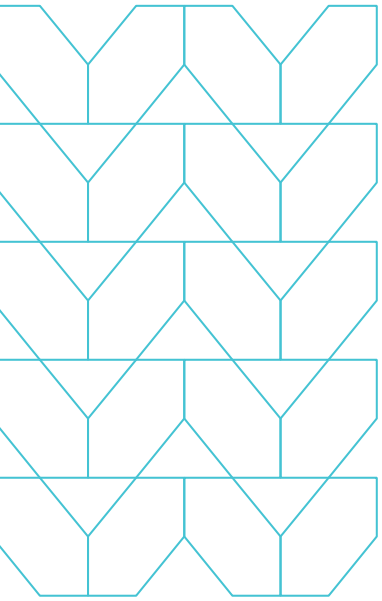
MENLO SECURITY

Use generative AI safely and reduce the risk of data loss

Menlo Security delivers a layered approach to the secure use of generative AI, providing data protection from first access to the last mile.

Solution Brief

The Opportunities and Risks of Generative AI



Generative Artificial Intelligence (GenAI), platforms such as ChatGPT and Bard, are transforming the way people work - improving content, helping with inspiration and brainstorming, automating mundane tasks and so much more. This creates many opportunities for organizations to increase productivity and improve the quality of work. The use of these platforms, however, also introduce significant cybersecurity concerns, raising questions about the privacy and security of personal or organizational data.

As employees utilize generative AI to increase productivity, they may be deliberately or accidentally leaking proprietary data or other intellectual property (IP).

When users interact with GenAI tools, those underlying systems retain content, putting that content at risk, exposed by traditional breaches, through malicious prompt engineering, or even used to train the underlying machine learning model. In addition, enterprises lose all control over how such data is stored, processed, and protected. Much of the content in these queries are exposed to the GenAI tool builder, where they can be reviewed by human trainers to examine and improve the AI model.

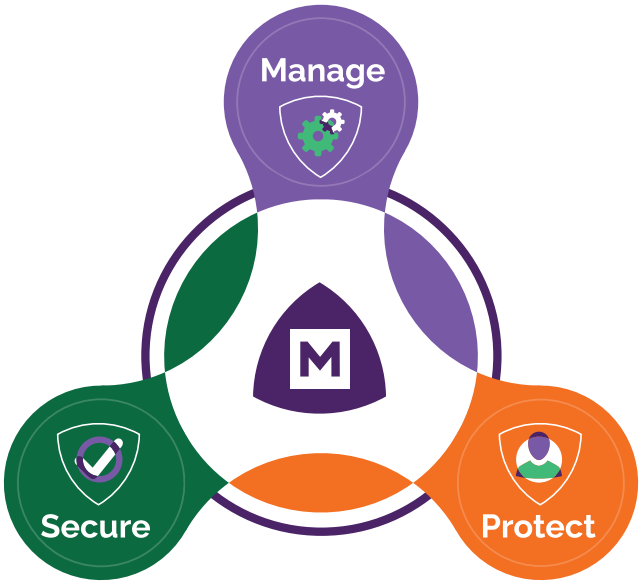
This conundrum creates a problem for enterprises. They cannot just block ChatGPT and other generative AI platforms. These tools offer legitimate value and can enhance productivity dramatically. Not using them inhibits agility and risks a competitive disadvantage. But as they become ubiquitous in today's business environment, the risk they present must be addressed.

Employees are knowingly or unknowingly inputting sensitive data into generative AI platforms. 55% of entries into generative AI sites included personally identifiable information.[1]

[1] Source: https://resources.menlosecurity.com/reports/the-continued-impact-of-generative-AI-on-security-posture

Menlo Security brings security to GenAI

Menlo Security provides comprehensive browser security to any local browser, controlling the data input into ChatGPT and other generative AI tools. Menlo Security protects organizations against data loss risk while preserving choice.



- Menlo Last-Mile Data Protection
- Copy & Paste Controls
- Menlo Browsing Forensics

Menlo Security Last-Mile Data Protection provides reliable inspection of web file uploads and user input for every browsing session. This protection stops employees from uploading sensitive files, inputting trade secrets and other sensitive information into generative AI tools. Copy & Paste Control and character limits can be layered in as additional security to stop large amounts of data leakage. This protects sensitive data from being exposed to an external site where it can be misused, while still allowing users to copy results from sites.

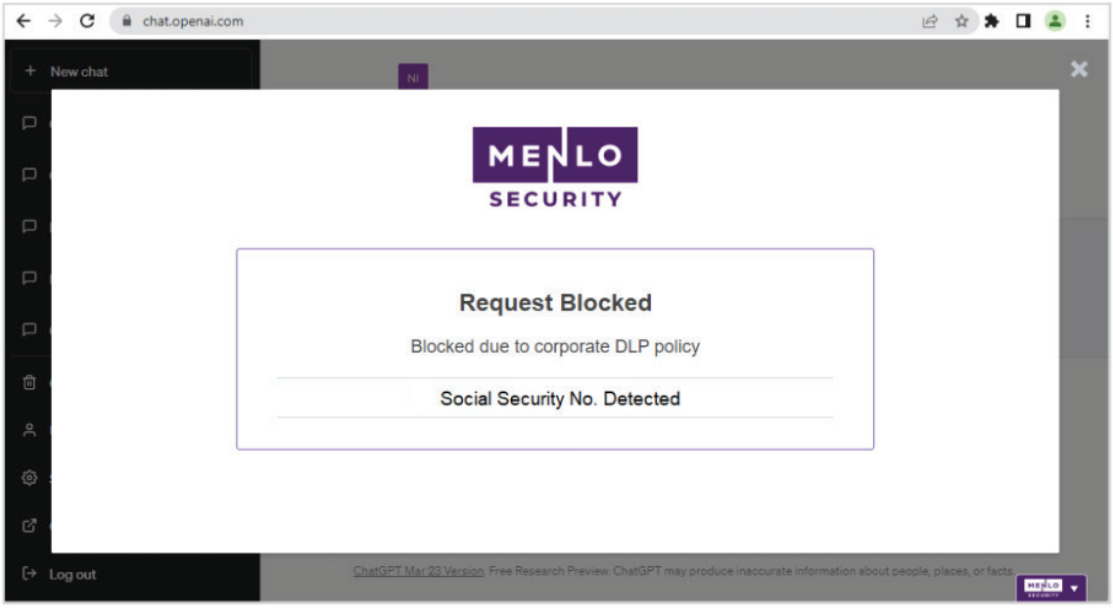
Menlo Browsing Forensics enables SOCs, Human Capital or Audit / Compliance Teams to “playback” actions - such as mouse clicks and data entry - as they occurred within a web session to understand the intent and impact of end user actions.

Menlo Security Last-Mile Data Protection

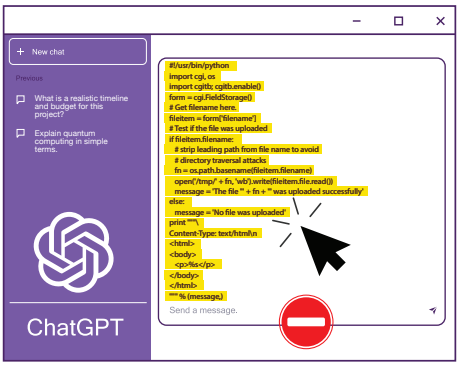
Combined with the Menlo Secure Cloud Browser and cloud proxy technologies, Menlo Security Data Protection brings advances that extend traditional data loss prevention (DLP) to the last mile, such as granular Copy & Paste controls. The combination of data protection and traditional DLP functionality helps organizations monitor every device in their ecosystem with completely reliable data inspection.

Menlo Security Data Protection works by first identifying specific data types that are sensitive, for example, by file type, regular expressions, or set data-type libraries.

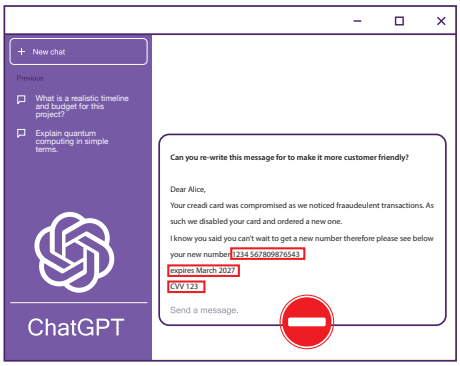
The data from inspection can either be contained in a file (such as an Excel spreadsheet) or a browser web form with user input. Additionally, DLP policies are enforced globally and consistently for every browser session. Menlo Security has visibility and control over traffic and reliably observes all data egress. Menlo Security Data Protection observes and prevents data leaks that arise through user input from browser activity.



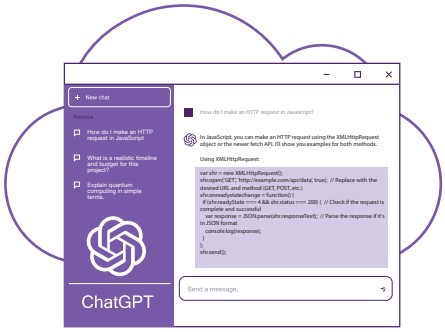
Prevent unauthorized data transfer with copy & paste controls, coupled with character limit policies



Detect and block deliberate or accidental exposure of sensitive data to AI



End-user policy violations are stored in a secure cloud repository for easy resolution and post event analysis



Forensic retention of screenshots and session metadata stored in cloud.

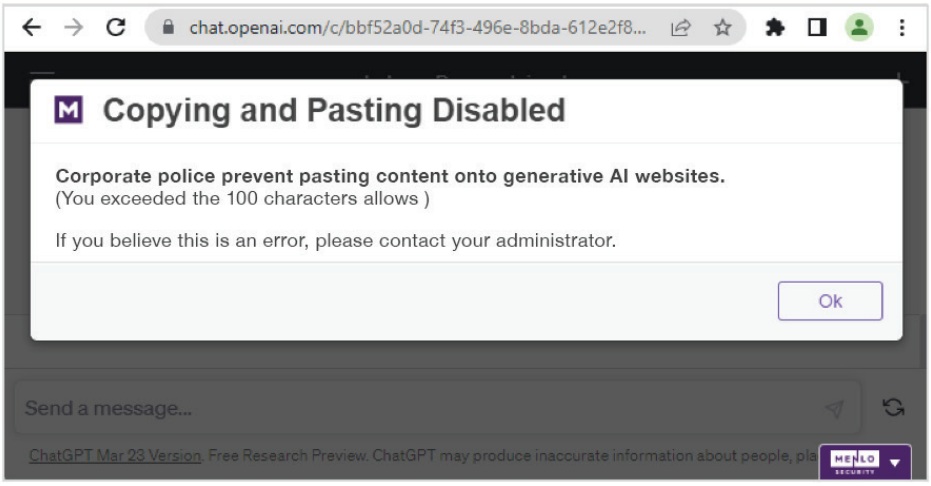
Copy and Paste Controls

Menlo Last-Mile Data Protection

Menlo Browsing Forensics

Copy & Paste Control

Menlo Security protects against careless use, where a user might leak large amounts of data. GenAI browsing sessions are isolated within the Secure Cloud Browser, and the isolated session is controlled, for example, Menlo can prevent sensitive information, such as Personal Identifiable Information (PII) or other confidential data, from being copied from the user's device and pasted into the isolated browsing session.



To the user, ChatGPT looks and feels like it's running locally, but the Secure Cloud Browser works in the background to prevent data leaks or unauthorized use. Additionally policy controls, such as character-count limits on paste operations can help prevent large amounts of data leakage. These policies can be created to protect employees without negatively impacting their productivity.

Menlo Browsing Forensics

Menlo Security enables organizations to apply security policies that trigger automated security controls, such as event logging or initiating a browser recording – to aid in resolution and post event analysis.

Menlo Browsing Forensics enables organizations to view user interactions with generative AI sites, such as submitting sensitive data and copy & paste attempts. Security and IT teams can investigate common user behaviors and analyze the information inputs and the responses received.

Menlos Security logs provide details on user interactions with these and other sites. Menlo Insights enables customers to easily query and mine for specific interactions, such as uploads to generative AI category sites. These queries can be saved as reports and emailed to predefined users, such as analysts or administrators, to monitor user interactions with generative AI sites.

Benefits

Strike the perfect balance between data-driven productivity gains and exposure risk

Utilize best-in-class enterprise browser security without impacting end user performance

Easily maintain a historical record of end-user actions and the use of generative AI within your organization

Securing your sensitive data while you accelerate your innovation

Data loss prevention has re-emerged as a top priority for security teams. Users adopting GenAI tools in their day-to-day work largely circumvent legacy DLP deployments. These DLP scanners lack visibility into these new behaviors, especially in hybrid work environments. Enterprise security teams require visibility into and control over corporate data beyond the perimeter. Menlo Security Last-Mile Data Protection identifies and prevents sensitive data from leaving your company, reducing the risk of costly and embarrassing data loss incidents. Menlo Security has pioneered an approach that controls how information enters and exits the browser, and your network, and your systems.

To learn more about securing the ways people work, visit menlosecurity.com or email us at ask@menlosecurity.com.

MENLO SECURITY

To find out more, contact us:

menlosecurity.com

(650) 695-0695

ask@menlosecurity.com

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.