Generative AI

How generative AI is impacting security posture

Generative AI (GenAI) platforms like ChatGPT and Bard are transforming work processes by improving content quality, aiding inspiration, automating tasks, and more. While offering significant productivity benefits, their use raises cybersecurity concerns regarding data privacy and security.

Employees leveraging GenAI may inadvertently expose proprietary data or intellectual property, as these platforms retain content from user interactions. 89% of employees would bypass cybersecurity guidance to meet a business objective. This poses risks such as data breaches, prompt manipulation, or unauthorized training of machine learning models. Enterprises lose control over how their data is stored, processed, and protected.

Balancing security and innovation is crucial. Blocking GenAI tools is not feasible due to their value and productivity enhancements. However, their widespread adoption necessitates addressing associated risks.

As organizations grapple with the implications of GenAI, developing a comprehensive policy is important. While the technology is here to stay and will continue to evolve, security and IT teams must prioritize implementing adaptable technology and policies to safeguard against emerging threats.

Menlo Security advantage

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

The Menlo Secure Cloud Browser offers various controls to mitigate the risk of data loss when using ChatGPT or similar tools. Copy and paste controls within ChatGPT, along with a forensic record of all user inputs, help prevent careless data leaks. Users are informed that inputs are monitored, encouraging thoughtful usage.

Additionally, data protection rules can be applied to input, scanning for keywords, project code names, or other sensitive information. Over 300 data protection dictionaries are utilized, with customizable options available. Browsing Forensics provides a comprehensive history of web sessions, allowing quick resolution of any issues.

Combined with HEAT Shield, Posture Manager, and Secure Application Access, these controls offer unmatched protection. They can be deployed in many ways, including providing the same browser security on both managed and unmanaged endpoints. Menlo's approach minimizes intrusion into end-user environments, operating client-free or with an extension, and offering deployment options by the network security team.

Capabilities

Last-Mile Data Protection

With the combination of Menlo Secure Cloud Browser and cloud proxy technologies, Menlo Security Data Protection enhances traditional data loss prevention (DLP) capabilities, extending them to the last mile. This includes granular Copy & Paste controls and reliable data inspection across all devices in the ecosystem.

Data inspection can occur within files or browser web forms, ensuring comprehensive coverage. DLP policies are enforced consistently across all browser sessions, providing global protection against data leaks. Menlo Security maintains visibility and control over traffic, effectively monitoring and preventing data egress resulting from browser activity.

Copy & Paste Control

Menlo Security works in the background to prevent data leaks during GenAI browsing sessions by isolating them within the Secure Cloud Browser. Controls are in place to block the transfer of sensitive information like Personal Identifiable Information (PII) into these sessions. Additional policy controls, such as character-count limits on paste operations, enhance data protection without hindering productivity.

Menlo Browsing Forensics

Menlo Security allows organizations to enforce security policies that trigger automated controls like event logging or browser recording to aid in resolution and post-event analysis. With Menlo Browsing Forensics, organizations can view user interactions with GenAI 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.

Menlo logs provide comprehensive details on user interactions with these sites, and Menlo Insights facilitates easy querying and mining for specific interactions, such as uploads to GenAI category sites. Reports generated from these queries can be emailed to predefined users, such as analysts or administrators, for monitoring user interactions with GenAI sites.

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.