MENLO SECURITY

www.menlosecurity.com

Best Practices to Enable the Safe Use of GenAI

Controlling Shadow AI

Shadow AI, in which enterprise users turn to their personal instance(s) of GenAI tools, has become one of the most pressing problems faced by enterprises today. Research overwhelmingly shows that most users do not have malicious intent – rather, they seek the productivity gains that GenAI has provided in other facets of their lives. While users' intent may be laudable, the results of these actions can cause significant issues, as security and IT teams have no way to get information about what users are sharing with these tools. Worse, most free tiers of popular GenAI tools may share prompts and responses to train their LLM or retain the data for testing.

Shadow AI is increasing too: *69% of cybersecurity leaders report suspecting or having evidence that employees are using prohibited public GenAI tools, while 79% report that employees' use of authorized public GenAI tools doesn't align with their approved policies.*

Protect your data from loss or leakage

The first step toward countering the negative effects of Shadow AI is to develop a comprehensive plan to protect your data; after all, data loss or leakage is a major reason that Shadow AI is dangerous. By ensuring that data is consistently protected, you greatly lower your enterprise risk profile. For advice on how to provide consistent DLP in GenAI use cases, see Best Practices to Prevent Data Loss

Select which GenAI tools you want to allow

A complete ban on the use of GenAI tools may still be necessary in highly regulated environments, but it is difficult to make such a ban completely effective, as determined users can often find a workaround. For that reason, Menlo suggests that you protect confidential, proprietary, or sensitive data, and select a tool or set of tools that can be monitored.

Give users what they need

Categories of GenAI tools most frequently seen in the enterprise include:

- Text generation/conversation AI (built on LLM)
  - Multimodal – some tools in this category can process text, audio, and some video
- Code assistance/development

HINT – By far, the most common tools exposed in Shadow AI use cases are text/conversation tools. It is strongly suggested that enterprises license one of the better-known tools and make sure that users are aware of it.

Next, consider purchasing Enterprise or Pro licenses for these tools. Not only will this action ensure that prompts and responses remain in the company, but enterprise versions of these tools also empower admins to monitor their overall use.

Finally, try to make the tools offered more appealing than those users might have on their own. For example, Enterprise, Pro, or Business tiers of GenAI tools typically offer the latest models and more functionality than is available in free tools. Because GenAI tools “learn” about a user over time, they become increasingly convenient. For this reason, the more compelling you can make the sanctioned tool, the more likely users are to work with it. By offering the latest tool, users have a reason to move from a tool that they have gotten to know (and that has gotten to know them) to the one approved by the enterprise.

Create clear policies and governance, as well as incentives

Once you have selected the right tool for your organization, notify users that you want them to use this tool, and communicate the consequences of noncompliance. To encourage the use of the approved tool, your communications can include its advantages over free-tier tools, as mentioned above, or bring out any other unique features that users might want to leverage. The objective is to make it easier and more appealing to use the approved tool than to bypass control. It is also imperative to create user training and support to ensure low-friction adoption. While such training is fairly straightforward for general tools that correct grammar or offer summaries, more specialized tools, such as those used by programmers and developers, might require more detailed instructions.

While published policies are vital, they are most effective when combined with other notifications that can be applied inline, as users are working. Menlo offers a variety of ways to provide this information inline. One approach Menlo offers is a customizable block-and-redirect screen that notifies users of the sanctioned tools and provides links to them in real time. Another useful element is the availability of customizable coaching pages, which can be invoked when the user goes to the sanctioned tool. This helps to reinforce the overall policy.

Ban the use of non-sanctioned GenAI tools as you monitor use and enforce policy

Once you have clarified which AI tools are sanctioned, you need to find a way to ban those that are not. To prohibit the use of non-sanctioned tools, it is essential that you have visibility into which tools are really in use. This requires visibility into browsing sessions to help you determine which policies are working successfully and which have not been embraced by users. Not only will this visibility help you to modify policies as needed, including by user or group, locations, or specific app, but it is an essential part of monitoring tools as their use continues. For example, should an AI tool become susceptible to adversarial vulnerabilities, you will be able to immediately assess any possible exposure, or update the tool that users are directed to.

Menlo provides this visibility in a variety of ways. To see user actions in detail, sessions can be recorded using Menlo Browsing Forensics, which can be triggered by traffic category, user/group, or DLP violations. For a more general, enterprise-wide view, Menlo Insights enables you to quickly run custom reports to pinpoint what is really going on as users browse.

Provide segmentation

It is important to ensure that there is a degree of separation between users and data in order to ensure least-privileged access and protect data. This is particularly important in the case of BYOD users or those working on devices that you don't manage. To protect data in these use cases, access to data from internal and SaaS apps should be both visible and monitored, while the data itself must be protected.

The Menlo architecture provides separation between the user and the internet and the internal network. Secure Application Access from Menlo makes it easy to extend this separation to everyone, including remote users, contractors, or partners. Users on BYOD or unmanaged devices can be restricted to only the applications essential for the performance of their jobs. Inline DLP rules can be applied to assets that are accessed by these users, and visibility provided by Browsing Forensics and Insights reports make it easy to ensure that policies are working as desired.

Use of AI will not go away

Ignoring the use of Shadow AI comes with real consequences that are only going to grow as tools become more broadly adopted. This dangerous "blind spot" can lead to data loss, compliance failures, inconsistency, and brand or reputational damage. According to the 2025 Gartner Cybersecurity Innovations in AI Risk Management and Use Survey, 66 percent of respondents believe that significant or comprehensive changes are required to manage cybersecurity risks associated with public generative AI tools in their organization.

Curtailing Shadow AI can seem like an insurmountable challenge, but it doesn't have to be. With Menlo, it is easy to quickly implement a cohesive program to observe, control, enforce, and monitor the use of AI tools in the browser — where the majority of these tools are accessed by individuals. Menlo enables enterprises to harness the energy of users that seek to improve productivity, without losing control.

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. © 2025 Menlo Security, All Rights Reserved.

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