Get the Benefits of Generative AI Tools Without Risk of Data Loss

Safely enable use of ChatGPT, Bard and other Generative AI tools while protecting against exfiltration of sensitive data

ChatGPT, Bard and other Generative AI tools are sweeping the business world. And for good reason: They make quick work of tasks like summarizing complex material, creating drafts and writing code.

But use of these tools is far from risk-free. ChatGPT records and stores transcripts of every conversation. Data entered in the app may be incorporated into its dataset and used to enhance the language models or for research purposes — and may potentially be exposed to other users in future responses. Significantly, it is also accessible to human trainers.

If you have ever asked in a generative AI chat, "How do you know this?" it's not hard to imagine how competitors or other parties could discover confidential data that your users have copied into the app. They might also discover confidential data that you've entered in other apps. For instance, if your enterprise user enters sensitive data in Google Translate, might that information be used to train the company's AI models and perhaps exposed in a Bard response?

Creators of these tools are well aware of the risks, as well as data privacy issues. They're all laid out in the privacy notices — the ones that your users most likely agree to without troubling to read. For instance, the ChatGPT privacy policy states that if personal data will be entered, customer consent is required. If the data is classified as private by GDPR, your users must ask OpenAI to execute a"Data Processing Addendum." Failing to do so may result in non-compliance with data privacy regulations, risk of penalties and legal exposure.

ericom security
by cradlepoint

Ericom Security Generative AI Isolation Highlights

- Enable full use of valuable generative AI productivity tools
- Restrict which users can access generative AI platforms
- Protect confidential data, PII and other sensitive information from exposure
- Issue warnings and reminders regarding proper use
- Enforce granular controls on uploads, downloads and clipboarding functions
- Clientless, scalable cloud-delivered service
- Easy to deploy, install and manage
- Rapid user onboarding
- User-friendly centralized policy control

The Solution: Ericom Generative AI Isolation

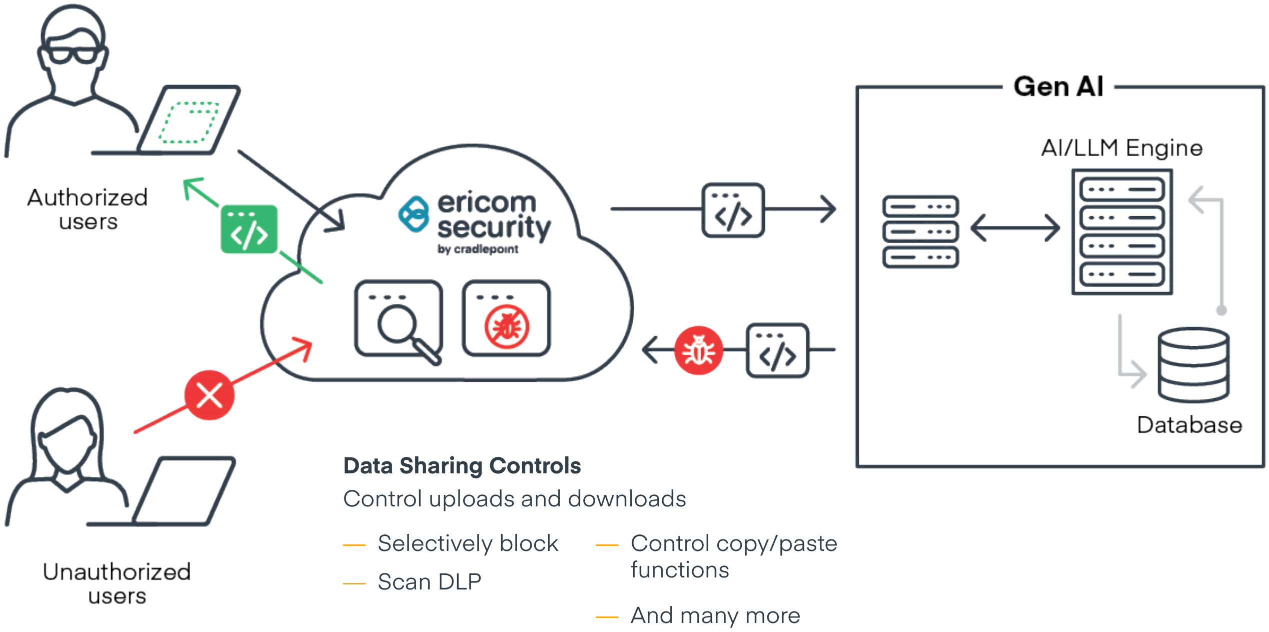
Ericom Generative AI Isolation is a clientless solution that empowers your organization to leverage the productivity and efficiency benefits of generative AI platforms while protecting sensitive data from being exposed. Instead of blocking these valuable sites at significant opportunity cost, Ericom Generative AI Isolation allows authorized users to reap the benefits of generative AI while ensuring a robust security posture.

Guided by easy-to-set policies, Ericom Generative AI Isolation executes interactions of authorized users with generative AI sites like ChatGPT in a virtual browser that is isolated in the Ericom Cloud Platform. From the user perspective, they enter content on the generative AI site in a completely standard way. But behind the scenes, data loss protection and access policy controls are applied in the cloud to block confidential data, PII or other sensitive information from being submitted to the generative AI site and potentially exposed.

Similarly, any malicious content that may have been introduced into the AI platform and from there, provided in response to a prompt, will remain in the isolated container, and not reach the user device or network.

While the solution can be fully transparent to users, IT admins can opt to issue suitable use instructions when authorized users enter a generative AI site or download content generated by the app. Warnings may also be issued to users who have attempted to upload sensitive data, or to remind users to verify that AI-generated content is accurate.

Ericom Security Generative AI Isolation Prevents Data Loss When Using Gen AI



Data Sharing Controls
Control uploads and downloads

- Selectively block
- Scan DLP
- Control copy/paste functions
- And many more

Clientless Security Controls

Security controls enforce least privilege access to generative AI platforms and restrict activities to prevent exposure of PII and sensitive or proprietary data. Ericom Generative AI Isolation controls and functionality include

- Blocking or restricting data uploads to platform
- Scanning data OK'd for upload with DLP to prevent data exfiltration
- Checking documents for malware and if needed, sanitizing prior to download
- Disabling or restricting cut and paste from protected resources or local device (clip-boarding) based on DLP inspection
- Issuing warnings and reminders regarding proper use
- No application data is cached in unmanaged device browsers

Discover how Ericom Generative AI Isolation can empower your organization to safely leverage the benefits of generative AI tools while protecting your sensitive data.

Contact us today for a personalized demonstration or to learn more about our scalable cloud-delivered service at ericom.com/contact-us.