Ericom Introduces Isolation-Based Security Solution to Address Generative AI Data Loss and Malware Risks

Adoption of Artificial Intelligence Applications Creates New Cybersecurity Threats

NEW YORK, NY, US, September 25, 2023 /EINPresswire.com/ -- Ericom Software, a leading provider of Zero Trust cloud cybersecurity solutions, today announced the launch of Ericom Generative Artificial Intelligence (AI) Isolation. With a focus on allowing organizations to implement user controls to protect against data exposure, malware threats, and compliance challenges, Ericom Generative AI Isolation empowers businesses to leverage the benefits of generative AI websites while maintaining a secure environment that protects sensitive data and intellectual property.

> Generative AI websites provide unparalleled productivity enhancements, but organizations must be proactive in addressing the associated risks."
>
> *Gerry Grealish*

With the emergence of ChatGPT late last year, generative AI tools have quickly become one of the most compelling productivity technologies due to their ability to offer businesses, and their staff members, increased efficiency and reduced costs. However, along with these advantages come significant risks. Any data input to generative prompts on AI application websites, including source code, proprietary or sensitive information, and Personally Identifiable Information (PII), becomes part of the public domain. This data could be incorporated into an AI tool's dataset and used to enhance the content exposed in future responses, potentially leading to data leaks.

Large Language Models (LLMs) used in generative AI are trained on internet data, making them susceptible to integrating harmful content such as zero-day exploits, weaponized responses, and copyrighted material. Generative AI responses that go unchecked may lead to misinformation and legal issues. Enterprises face potential legal and compliance challenges when sensitive data, such as intellectual property or customers' financial information, is inadvertently exposed through the website interfaces of generative AI tools.

"Generative AI websites provide unparalleled productivity enhancements, but organizations must be proactive in addressing the associated risks," said Gerry Grealish, Vice President of Marketing, Ericom Cybersecurity Unit of Cradlepoint. "Our Generative AI Isolation solution empowers businesses to attain the perfect balance, harnessing the potential of generative AI while safeguarding against data loss, malware threats, and legal and compliance challenges."

Key features of Ericom's clientless Generative AI Isolation include:

•Data Protection: Data loss prevention policies are enforced to block confidential data, PII, or other sensitive information from being submitted to Generative AI websites, ensuring only permitted non-sensitive content is processed.

•Access Controls: Easy-to-set policies manage interactions between authorized users and Generative AI websites, enabling users to leverage Generative AI while adhering to their organization's data security guidelines.

•Secure Access and Downloads: Generative AI interactions are executed within a virtual cloud-based browser isolated from the organization's environment, which minimizes the risk of malware infecting their endpoints and network. The solution provides an extra layer of security, utilizing content disarm and reconstruction (CDR) to clean documents or chats that users download to their devices.

•Protected Clipboard: Copy/paste functions can be completely disabled or partially constrained to limit (a) how internal content is input into Generative AI prompts or (b) how responses can be copied into an organization's documents.

•Data Loss Prevention (DLP): DLP scans uploaded files and manually typed text in Generative AI prompt fields, to ensure no PII is exposed, or file uploads can be completely blocked if an organization elects to do so.

Watch this video for more information about Ericom Generative AI Isolation.

Read the solution sheet for additional information.

About Ericom Software

Ericom Software, the cybersecurity unit of Cradlepoint, part of Ericsson (Nasdaq: ERIC), is a leading provider of cloud-delivered, Zero Trust cybersecurity solutions that protect today's digitally distributed organizations from advanced security threats. Ericom's Web Application Isolation platform is a comprehensive, simple, and cost-effective Security Service Edge (SSE) solution deployed on a high availability global cloud infrastructure. Learn more at www.ericom.com.

Mike Benedetto
Ericom Software
+1 908-616-8355
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
