ChatGPT Risk Module

Generative AI has transformed the world and can have a powerful effect on how people live and work. However, the risks associated with AI make managing its use challenging for organizations. The iboss ChatGPT Risk Module allows the controlled use of ChatGPT with security and monitoring in place to enable users to leverage the power of ChatGPT while reducing and eliminating the associated risks.

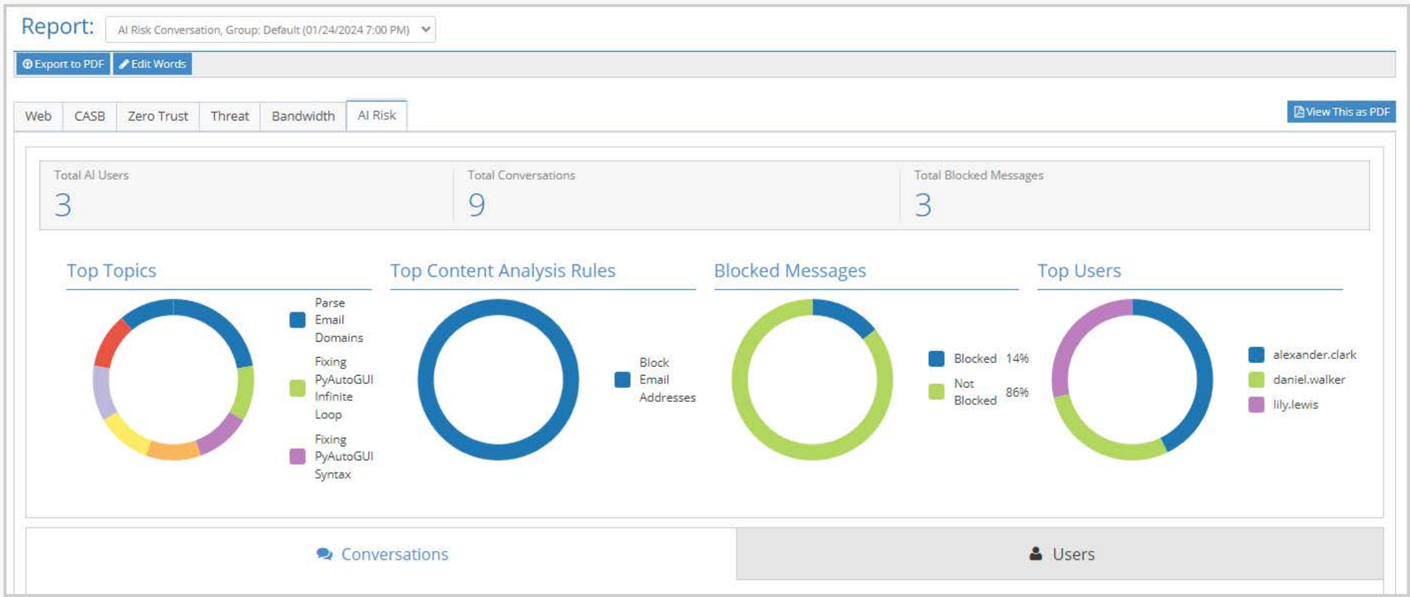
Generative AI has transformed the world and can have a powerful effect on how people live and work. However, the risks associated with AI make managing its use challenging for organizations. There is a high risk of data and intellectual property loss if users present questions to AI that contain sensitive information. This sensitive information is gathered by AI to produce valuable responses but is also used to train the AI models making the information available to unauthorized third-parties. However, blocking the use of AI entirely can put an organization at a disadvantage as other organizations leverage its power to solve problems and support the workforce. The iboss ChatGPT Module allows the controlled use of ChatGPT with security and monitoring in place to enable users to leverage the power of ChatGPT while reducing and eliminating the associated risks.

The iboss Zero Trust SSE provides full security and visibility into all transactions between users and services. This allows the iboss platform to go deep into content to inspect, secure and capture relevant contextual information from those connections. The iboss ChatGPT Module continuously inspects all conversations between users and ChatGPT and logs both questions prompts and AI responses so that all conversations can be reviewed and monitored. In addition, the ChatGPT Module runs deep Data Loss Prevention against the user prompts to ensure sensitive intellectual property is never sent to ChatGPT. If source code or other sensitive information is detected, the request is prevented and the situation is logged so that security administrators can respond to the threat. This allows users to benefit from ChatGPT's power in a productive and low risk manner.

BENEFITS

- **Logs all conversations between users and ChatGPT so that they can be reviewed by security teams to ensure compliance.**
- **Inspects all conversations between users and Chat GPT to reduce risk of data loss.**
- **Automatically detects risk of data loss and prevents question prompts from reaching ChatGPT if detected.**
- **Ensures users can leverage ChatGPT to increase productivity while reducing risk.**
- **Prevent unapproved users from accessing ChatGPT altogether.**
- **Alerts administrators of risky conversations to provide coaching to ChatGPT enabled users.**

ChatGPT Risk Module



Report: AI Risk Conversation, Group: Default (01/24/2024 7:00 PM)

Total AI Users 3

Total Conversations 9

Total Blocked Messages 3

Ordering Information SKU:

ChatGPT Risk Add-On

Required Package: Zero Trust Core or Higher

HOW IT WORKS

- iboss Windows Cloud Connectors are installed onto devices which connects them to the iboss Zero Trust SSE for access, security, and logging.
- The iboss ChatGPT Risk Module capability is enabled and applied to users that have access to Chat GPT.
- The ChatGPT Module continuously monitors conversations between users and ChatGPT in real-time.
- If sensitive or non-compliant request prompts are made to ChatGPT, the ChatGPT Module will prevent the prompt from reaching ChatGPT.
- The ChatGPT Module will log the incident with details related to the risky prompt. Security responders can respond to risky incidents with complete context.
- All conversations are logged regardless of the presence of risky content so that security teams can review conversations.
- Users that should not have access to ChatGPT can be completely restricted from accessing ChatGPT altogether.
- The organization benefits from the power of ChatGPT in a productive and low risk manner allowing it to compete in the AI Era