security quotient®

How to mitigate third-party ChatGPT plugin security risks?

1

Implement secure web gateway policies

Implement policies on secure web gateways to identify and monitor the use of third-party ChatGPT plugins, ensuring only authorized plugins are used.

2

Enforce DLP policies

Enforce Data Loss Prevention policies (DLP) to monitor and control data submitted to these plugins, preventing unintentional or malicious sharing of sensitive information.

3

Implement behavioral monitoring

Set up behavioral monitoring to track data access and usage, identify unusual patterns, and promptly respond to unauthorized activities.

4

Educate the workforce

Educate employees on potential risks related to third-party ChatGPT plugins and the best practices to ensure secure use.

Change human cyber security behavior with

security® quotient.

Singapore | India | Malaysia