Configurar o ChatGPT privado e restringir o acesso a outros aplicativos AI geradores

Contents

Introdução

Este documento descreve como configurar um ChatGPT privado e restringir o acesso a outros aplicativos AI gerativos.

Overview

O panorama da inteligência artificial está evoluindo rapidamente, e um dos principais avanços foi o desenvolvimento da IA Gerativa. Entre estes, o ChatGPT tem tido um impacto significativo.
À medida que as organizações buscam integrar essas ferramentas poderosas em seus fluxos de trabalho, a necessidade de controlar o acesso a aplicativos de IA geradora se tornou cada vez mais evidente. Para empresas que desenvolveram suas próprias instâncias de ChatGPT privadas, garantir que essa é a única ferramenta de IA acessível para sua equipe, ao mesmo tempo em que restringe outras aplicações de IA geradora, é uma medida de segurança crítica.

Felizmente, há uma maneira simples de fazer isso usando o painel Umbrella. Este artigo o orienta através das etapas que você precisa seguir para permitir que sua organização se beneficie de seu ChatGPT privado, mantendo controles rígidos sobre o uso de outros aplicativos de IA.

Passo 1: Crie uma regra da Web para permitir seu bate-papo privadoGPT

Primeiro, você precisa fazer login no painel do Umbrella. Uma vez lá, você pode criar uma regra DNS ou uma regra da Web.
Essa regra deve ter a ação "Permitir" e uma "Lista de destinos" com a URL específica do seu ChatGPT privado.
Esta etapa garante que os usuários dentro da sua organização possam acessar seu ChatGPT privado sem quaisquer restrições.

Passo 2: Bloquear todos os outros aplicativos de IA gerados

Imediatamente após a criação da regra 'Permitir', você deve criar uma segunda regra.
Essa regra deve ter a ação "Bloquear" e deve incluir uma "Lista de aplicativos" que inclua a categoria IA geradora.
Ao fazer isso, você é capaz de impedir o acesso a uma ampla gama de aplicações de IA geradora populares, incluindo a versão pública do ChatGPT.

Política DNS

Para garantir que essas regras sejam efetivamente aplicadas ao usar a política DNS e não a política Web.
É essencial ativar o proxy inteligente e a descriptografia SSL para uma experiência perfeita. Além disso, a instalação do certificado raiz do Cisco Umbrella é necessária para o funcionamento adequado da descriptografia SSL.

Para obter orientação abrangente sobre como configurar a política DNS, você pode consultar a documentação oficial aqui.
Além disso, para otimizar a eficácia das políticas de DNS, consulte as melhores práticas aqui.

Política da Web

Para obter mais detalhes sobre como gerenciar políticas da Web e adaptá-las para atender aos requisitos da sua empresa, vá até aqui.

Implementar essas medidas permite que sua organização aproveite ao máximo sua ChatGPT privada, ao mesmo tempo em que reduz o risco de vazamento de dados ou distrações que podem vir com o uso de outros aplicativos de IA geradora. O equilíbrio certo entre segurança e acessibilidade é fundamental para aproveitar o potencial da IA geradora e, ao mesmo tempo, garantir que os dados e recursos da sua empresa estejam bem protegidos.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.